



Documentación de ONTAP 9

ONTAP 9

NetApp
April 24, 2024

This PDF was generated from <https://docs.netapp.com/es-es/ontap/index.html> on April 24, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

| | |
|---|-----|
| Documentación de ONTAP 9 | 1 |
| Notas de la versión | 2 |
| Aspectos destacados de la versión de ONTAP 9 | 2 |
| Compatibilidad con la versión ONTAP 9 | 7 |
| Novedades en ONTAP 9.14.1 | 8 |
| Novedades en ONTAP 9.13.1 | 13 |
| Novedades en ONTAP 9.12.1 | 18 |
| Novedades en ONTAP 9.11.1 | 24 |
| Novedades en ONTAP 9.10.1 | 29 |
| Novedades en ONTAP 9.9.1 | 34 |
| Integración de System Manager con BlueXP | 40 |
| Descubra sus clústeres directamente desde BlueXP | 40 |
| Más información sobre BlueXP | 41 |
| Introducción y conceptos | 42 |
| Conceptos de ONTAP | 42 |
| Configure, actualice y revierta el software y el firmware de ONTAP | 93 |
| Configure ONTAP | 93 |
| Actualice ONTAP | 110 |
| Firmware y actualizaciones del sistema | 251 |
| Revierte ONTAP | 258 |
| Administración de clústeres | 291 |
| Gestión de clústeres con System Manager | 291 |
| Gestión de licencias | 307 |
| Gestión de clústeres con la CLI | 317 |
| Gestión de discos y niveles (agregados) | 434 |
| Gestión de niveles FabricPool | 530 |
| Movilidad de datos de SVM | 586 |
| Gestión de parejas de HA | 597 |
| Gestión de API de REST con System Manager | 622 |
| Administración de volúmenes | 626 |
| Gestión de volúmenes y LUN con System Manager | 626 |
| Gestión de almacenamiento lógico con CLI | 650 |
| Aprovisiona almacenamiento NAS para sistemas de archivos de gran tamaño con volúmenes FlexGroup | 794 |
| Gestión de volúmenes de FlexGroup con interfaz de línea de comandos | 796 |
| Gestión de volúmenes de FlexCache | 885 |
| Gestión de redes | 905 |
| Manos a la obra | 905 |
| Componentes de red | 909 |
| Flujo de trabajo de conmutación al nodo de respaldo de ruta NAS (ONTAP 9,8 y versiones posteriores) | 914 |
| Flujo de trabajo de conmutación al nodo de respaldo de ruta NAS (ONTAP 9,7 y versiones anteriores) | 923 |
| Puertos de red | 938 |
| Espacios IP | 963 |
| Dominios de retransmisión | 970 |

| | |
|--|------|
| Grupos y políticas de conmutación por error | 992 |
| Subredes (solo administradores de clúster) | 996 |
| Cree SVM | 1004 |
| Interfaces lógicas (LIF) | 1011 |
| Equilibre las cargas de red | 1042 |
| Resolución del nombre de host | 1051 |
| Proteja su red | 1054 |
| Marcado de QoS (solo para administradores de clústeres) | 1069 |
| Gestionar SNMP (solo administradores de clústeres) | 1071 |
| Gestione el enrutamiento en una SVM | 1082 |
| Ver información de red | 1087 |
| Gestión del almacenamiento nas | 1121 |
| Gestione protocolos NAS con System Manager | 1121 |
| Configure NFS con la CLI | 1141 |
| Gestione NFS con la interfaz de línea de comandos | 1210 |
| Gestión de enlaces NFS | 1331 |
| Gestione NFS a través de RDMA | 1341 |
| Configure SMB con la interfaz de línea de comandos | 1347 |
| Gestione SMB con la interfaz de línea de comandos | 1390 |
| Proporcione acceso del cliente S3 a los datos NAS | 1749 |
| Configuración de SMB para Microsoft Hyper-V y SQL Server | 1759 |
| Gestión del almacenamiento san | 1822 |
| Conceptos de SAN | 1822 |
| Administración de SAN | 1846 |
| Protección de DATOS SAN | 1923 |
| Referencia para la configuración DE SAN | 1944 |
| Gestión del almacenamiento de objetos S3 | 1989 |
| Conozca el soporte de S3 en ONTAP 9 | 1989 |
| Planificación | 1992 |
| Configurar | 1997 |
| Proteja los bloques con SnapMirror de S3 | 2047 |
| Auditar eventos S3 | 2082 |
| Autenticación y control de acceso | 2092 |
| Información general sobre el control de acceso y autenticación | 2092 |
| Gestione la autenticación de administrador y RBAC | 2092 |
| Autenticación y autorización mediante OAuth 2,0 | 2176 |
| Configurar la autenticación SAML | 2198 |
| Gestionar servicios web | 2205 |
| Compruebe la identidad de los servidores remotos mediante certificados | 2216 |
| Autentique mutuamente el clúster y un servidor KMIP | 2219 |
| Seguridad y cifrado de datos | 2223 |
| Información general sobre la gestión de seguridad con System Manager | 2223 |
| Protéjase contra el ransomware | 2223 |
| Protéjase contra virus | 2249 |
| Auditar eventos NAS en SVM | 2290 |

| | |
|---|------|
| Utilice FPolicy para supervisar y gestionar archivos en SVM | 2340 |
| Verifique el acceso mediante el seguimiento de seguridad | 2402 |
| Gestione el cifrado con System Manager | 2415 |
| Gestione el cifrado con la interfaz de línea de comandos | 2416 |
| Protección de datos y recuperación ante desastres | 2511 |
| Protección de datos con System Manager | 2511 |
| Relaciones entre iguales de clústeres y SVM con la CLI | 2525 |
| Gestione copias Snapshot locales | 2552 |
| Replicación de volúmenes de SnapMirror | 2565 |
| Gestione la replicación de volúmenes de SnapMirror | 2586 |
| Gestione la replicación de SVM de SnapMirror | 2628 |
| Gestionar la replicación de volúmenes raíz de SnapMirror | 2661 |
| Detalles técnicos de SnapMirror | 2666 |
| Archivado y cumplimiento de normativas con tecnología SnapLock | 2676 |
| Grupos de consistencia | 2722 |
| Continuidad del negocio de SnapMirror | 2760 |
| Servicio mediador para la continuidad empresarial de MetroCluster y SnapMirror | 2795 |
| Gestione sitios de MetroCluster con System Manager | 2850 |
| Protección de datos mediante backup en cinta | 2861 |
| Configuración de NDMP | 2960 |
| Replicación entre software de NetApp Element y ONTAP | 2976 |
| Supervisión de eventos, rendimiento y estado | 2997 |
| Supervise el rendimiento del clúster con System Manager | 2997 |
| Supervise y gestione el rendimiento de los clústeres mediante la CLI | 3008 |
| Supervise el rendimiento del clúster con Unified Manager | 3046 |
| Supervise el rendimiento del clúster con Cloud Insights | 3046 |
| Registro de auditoría | 3047 |
| AutoSupport | 3053 |
| Supervisión del estado | 3082 |
| Análisis del sistema de archivos | 3096 |
| Configuración de EMS | 3111 |
| Referencia de comandos de la ONTAP | 3128 |
| Referencias de comandos para versiones compatibles de ONTAP | 3128 |
| Referencias de comandos para versiones de soporte limitadas de ONTAP (solo PDF) | 3128 |
| Herramienta de comparación de CLI | 3128 |
| Avisos legales | 3129 |
| Derechos de autor | 3129 |
| Marcas comerciales | 3129 |
| Estadounidenses | 3129 |
| Política de privacidad | 3129 |
| Código abierto | 3129 |

Documentación de ONTAP 9

Notas de la versión

Aspectos destacados de la versión de ONTAP 9

Cada versión del software de gestión de datos ONTAP 9 ofrece funciones nuevas y mejoradas que mejoran las capacidades, la capacidad de gestión, el rendimiento y la seguridad que ofrece ONTAP.

Además de estas características destacadas, puede encontrar una cobertura completa por versión de todas las funciones nuevas y mejoradas que se introdujeron en versiones recientes de ONTAP.

Para obtener más detalles sobre la compatibilidad con plataformas de hardware y switches, los problemas conocidos y las limitaciones en todas las versiones de ONTAP 9 o para las funciones introducidas en versiones anteriores a ONTAP 9.9.1, consulte ["Notas de la versión de ONTAP 9"](#). Debe iniciar sesión con su cuenta de NetApp o crear una cuenta para acceder a las Notas de la versión.

Para actualizar a la última versión de ONTAP, consulte [Actualice a la última versión de ONTAP](#) y.. [¿Cuándo debo actualizar ONTAP?](#)

Aspectos destacados de ONTAP 9.14.1

ONTAP 9.14.1 ofrece características nuevas y mejoradas en las áreas de FabricPool, protección contra ransomware, OAuth y más. Para obtener una lista completa de las nuevas funciones y mejoras, consulte [Novedades de ONTAP 9.14.1](#).

- [Reducción de la reserva de WAFL](#)

ONTAP 9.14.1 introduce un aumento inmediato del cinco por ciento en espacio utilizable en sistemas FAS y Cloud Volumes ONTAP al reducir la reserva de WAFL en agregados con 30 TB o más.

- [Mejoras de FabricPool](#)

FabricPool ofrece un aumento de [rendimiento de lectura](#) y permite la escritura directa en el cloud, lo que reduce el riesgo de quedarse sin espacio y reduce los costes de almacenamiento al trasladar los datos inactivos a un nivel de almacenamiento más barato.

- ["Soporte para OAuth 2,0"](#)

ONTAP admite el marco OAuth 2,0, que se puede configurar mediante System Manager. Con OAuth 2,0, puede proporcionar acceso seguro a ONTAP para marcos de automatización sin crear ni exponer ID de usuario y contraseñas a scripts y runbooks de texto sin formato.

- ["Mejoras de protección autónoma frente a ransomware \(ARP\)"](#)

ARP le otorga más control sobre la seguridad de eventos, lo que le permite ajustar las condiciones que crean alertas y reducir la posibilidad de falsos positivos.

- [Ensayo de recuperación ante desastres de SnapMirror en System Manager](#)

System Manager proporciona un flujo de trabajo sencillo para probar fácilmente la recuperación ante desastres en una ubicación remota y limpiar tras la prueba. Esta función permite realizar pruebas más sencillas y frecuentes, así como aumentar la confianza en los objetivos de tiempo de recuperación.

- [Soporte de bloqueo de objetos S3](#)

ONTAP S3 admite el comando de API object-lock, lo que le permite proteger los datos escritos en ONTAP con S3 tras su eliminación

Utilizando comandos estándar de la API S3 y para garantizar que los datos importantes estén protegidos durante el tiempo adecuado.

- [Clúster y.. volumen](#) etiquetado

Añada etiquetas de metadatos a volúmenes y clústeres, que siguen los datos mientras se mueven de las instalaciones al cloud y viceversa.

Aspectos destacados de ONTAP 9.13.1

ONTAP 9.13.1 ofrece funciones nuevas y mejoradas en las áreas de protección frente al ransomware, grupos de coherencia, calidad de servicio, gestión de capacidad de inquilinos y más. Para obtener una lista completa de las nuevas funciones y mejoras, consulte [Novedades de ONTAP 9.13.1](#).

- Mejoras de la protección autónoma frente a ransomware (ARP):

- [Habilitación automática](#)

Con ONTAP 9.13.1, ARP pasa automáticamente del modo de entrenamiento al modo de producción después de tener suficientes datos de aprendizaje, lo que elimina la necesidad de un administrador para habilitarlo después del período de 30 días.

- [Compatibilidad con verificación multiadministradora](#)

Los comandos ARP disable son compatibles con la verificación multiadministrador, lo que garantiza que ningún administrador pueda deshabilitar ARP para exponer los datos a posibles ataques de ransomware.

- [Soporte de FlexGroup](#)

ARP admite FlexGroups a partir de ONTAP 9.13.1. ARP puede supervisar y proteger FlexGroups que abarcan varios volúmenes y nodos en el clúster, lo que permite proteger incluso los conjuntos de datos de mayor tamaño con ARP.

- [Supervisión del rendimiento y la capacidad para grupos de consistencia en System Manager](#)

La supervisión del rendimiento y la capacidad ofrece detalles para cada grupo de consistencia, lo que permite identificar y informar rápidamente problemas potenciales en el nivel de las aplicaciones, en lugar de solo en el nivel de objeto de datos.

- [Gestión de la capacidad del inquilino](#)

Los clientes multi-tenant y los proveedores de servicios pueden establecer un límite de capacidad en cada SVM, lo que permite que los inquilinos realicen el aprovisionamiento de autoservicio sin el riesgo de que un usuario consuma en exceso la capacidad del clúster.

- [Calidad de servicio techos y pisos](#)

ONTAP 9.13.1 le permite agrupar objetos como volúmenes, LUN o archivos en grupos y asignar un techo de calidad de servicio (IOPS máxima) o un piso (IOPS mínimo), lo que mejora las expectativas de rendimiento de las aplicaciones.

Aspectos destacados de ONTAP 9.12.1

ONTAP 9.12.1 ofrece funciones nuevas y mejoradas en las áreas de la seguridad reforzada, la retención, el rendimiento, etc. Para obtener una lista completa de las nuevas funciones y mejoras, consulte [Novedades de ONTAP 9.12.1](#).

- [Copias Snapshot a prueba de manipulaciones](#)

Con la tecnología SnapLock, las copias Snapshot se pueden proteger contra la eliminación en el origen o el destino.

Conserve más puntos de recuperación al proteger las copias Snapshot en el almacenamiento principal y secundario contra la eliminación por parte de atacantes de ransomware o administradores malintencionados.

- [Mejoras de protección autónoma contra ransomware \(ARP\)](#)

Active inmediatamente la protección autónoma e inteligente frente a ransomware en el almacenamiento secundario, basada en el modelo de filtrado ya completado para el almacenamiento principal.

Tras una conmutación por error, identifique instantáneamente posibles ataques de ransomware en el almacenamiento secundario. Se toma inmediatamente una instantánea de los datos que empiezan a verse afectados y se notifica a los administradores, lo que ayuda a detener un ataque y a mejorar la recuperación.

- [FPolicy](#)

Activación con un solo clic de ONTAP FPolicy para permitir el bloqueo automático de archivos maliciosos conocidos. La activación simplificada ayuda a protegerse contra ataques de ransomware típicos que usan extensiones de archivos conocidas comunes.

- [Refuerzo de la seguridad: Registro de retención a prueba de manipulaciones](#)

Registro de retención a prueba de manipulaciones en ONTAP que garantiza que las cuentas de administrador comprometidas no puedan ocultar acciones maliciosas. El administrador y el historial de usuario no se pueden modificar ni eliminar sin el conocimiento del sistema.

Registre y audite todas las acciones de administración independientemente del origen, garantizando que se capturen todas las acciones que afectan a los datos. Se genera una alerta cada vez que se manipulan los logs de auditoría del sistema para notificar a los administradores el cambio.

- [Refuerzo de la seguridad: Autenticación multifactor ampliada](#)

La autenticación multifactor (MFA) para CLI (SSH) admite dispositivos de token de hardware físico Yubikey, lo que garantiza que un atacante no pueda acceder al sistema ONTAP con credenciales robadas o un sistema cliente comprometido. Cisco DUO es compatible con la MFA con System Manager.

- [Dualidad de objetos de archivos \(acceso de varios protocolos\)](#)

La dualidad de objetos de archivos permite el acceso de lectura y escritura del protocolo S3 nativo a la misma fuente de datos que ya tiene acceso a protocolo NAS. Puede acceder simultáneamente al almacenamiento como archivos o como objetos desde la misma fuente de datos, lo que elimina la necesidad de utilizar copias duplicadas de datos para usarlas con diferentes protocolos (S3 o NAS), como los análisis que usan datos de objetos.

- [Reequilibrado de FlexGroup](#)

Si los componentes de FlexGroup se desequilibran, FlexGroup puede reequilibrarse y gestionarse de forma no disruptiva desde el CLI, API de REST y System Manager. Para un rendimiento óptimo, los miembros constituyentes dentro de una FlexGroup deben tener su capacidad utilizada distribuida uniformemente.

- [Mejoras de la capacidad de almacenamiento](#)

La reserva de espacio de WAFL se ha reducido significativamente y proporciona hasta 400 TiB más de capacidad utilizable por agregado.

Aspectos destacados de ONTAP 9.11.1

ONTAP 9.11.1 ofrece funciones nuevas y mejoradas en las áreas de seguridad, retención, rendimiento, etc. Para obtener una lista completa de las nuevas funciones y mejoras, consulte [Novedades de ONTAP 9.11.1](#).

- [Verificación de varios administradores](#)

La verificación multiadministradora (MAV) es un enfoque de verificación nativo pionero en el sector, que requiere varias aprobaciones en tareas administrativas confidenciales, como la eliminación de una copia Snapshot o un volumen. Las aprobaciones requeridas en una implementación de MAV evitan ataques maliciosos y cambios accidentales en los datos.

- [Mejoras en la protección autónoma frente a ransomware](#)

La protección autónoma contra ransomware (ARP) utiliza el aprendizaje automático para detectar las amenazas de ransomware con una mayor granularidad, lo que le permite identificar amenazas rápidamente y acelerar la recuperación en caso de una brecha.

- [Cumplimiento de normativas SnapLock para volúmenes FlexGroup](#)

Protege conjuntos de datos de varios petabytes para cargas de trabajo como la automatización de diseño electrónico o los medios y el entretenimiento al proteger los datos con el bloqueo de ARCHIVOS WORM para que no se puedan modificar ni eliminar.

- [Eliminación asíncrona del directorio](#)

Con ONTAP 9.11.1, la eliminación de archivos se produce en segundo plano del sistema ONTAP, lo que permite eliminar fácilmente directorios grandes y eliminar los impactos en el rendimiento y la latencia de las operaciones de I/O del host

- [Mejoras de S3](#)

Simplificar y expandir las funcionalidades de gestión de datos de objetos de S3 con ONTAP con extremos de API y versiones de objetos adicionales a nivel del bucket, lo que permite almacenar varias versiones de un objeto en el mismo bucket.

- [Mejoras de System Manager](#)

System Manager admite funcionalidades avanzadas para optimizar los recursos de almacenamiento y mejorar la gestión de auditorías. Estas actualizaciones incluyen capacidad mejorada para gestionar y configurar agregados de almacenamiento, visibilidad mejorada en los análisis del sistema y visualización de hardware para sistemas FAS.

Aspectos destacados de ONTAP 9.10.1

ONTAP 9.10.1 ofrece funciones nuevas y mejoradas en las áreas de refuerzo en la seguridad, análisis de rendimiento, compatibilidad con el protocolo NVMe y opciones de backup de almacenamiento de objetos. Para obtener una lista completa de las nuevas funciones y mejoras, consulte [Novedades de ONTAP 9.10.1](#).

- [Protección autónoma de ransomware](#)

Autonomous Ransomware Protection crea automáticamente una copia de SnapVault de tu volumen y alerta a los administradores cuando se detecta una actividad anormal. Esto te permite detectar rápidamente ataques por ransomware y recuperarte más rápidamente.

- Mejoras de System Manager

System Manager descarga automáticamente actualizaciones de firmware para discos, bandejas y procesadores de servicio, además de ofrecer nuevas integraciones con el asesor digital de NetApp Active IQ, BlueXP y la gestión de certificados. Estas mejoras simplifican la administración y mantienen la continuidad del negocio.

- [Mejoras de análisis de sistema de archivos](#)

File System Analytics proporciona telemetría adicional para identificar los principales archivos, directorios y usuarios de su recurso compartido de archivos, lo que le permite identificar problemas de rendimiento de las cargas de trabajo para mejorar la planificación de recursos y la implementación de QoS.

- [Compatibilidad de NVMe sobre TCP \(NVMe/TCP\) para sistemas AFF](#)

Consiga un alto rendimiento y reduzca el TCO para su SAN empresarial y las cargas de trabajo modernas en el sistema AFF cuando utilice NVMe/TCP en su red Ethernet actual.

- [Compatibilidad de NVMe over Fibre Channel \(NVMe/FC\) para los sistemas NetApp FAS](#)

Use el protocolo NVMe/FC en sus cabinas híbridas para permitir la migración uniforme a NVMe.

- [Backup nativo de cloud híbrido para el almacenamiento de objetos](#)

Proteja sus datos de ONTAP S3 con los objetivos de almacenamiento de objetos que elija. Utilice la replicación de SnapMirror para realizar backups en un almacenamiento en las instalaciones con StorageGRID, en el cloud con Amazon S3 o en otro bloque de ONTAP S3 en los sistemas NetApp AFF y FAS.

- [Bloqueo de archivos global con FlexCache](#)

Garantice la consistencia de los archivos en las ubicaciones de la caché durante las actualizaciones de los archivos de origen con el bloqueo de archivos global mediante FlexCache. Esta mejora habilita los bloqueos exclusivos de lectura de archivos en una relación de origen a caché para cargas de trabajo que requieren bloqueos mejorados.

Aspectos destacados de ONTAP 9.9.1

ONTAP 9.9.1 ofrece funciones nuevas y mejoradas en las áreas de eficiencia de almacenamiento, autenticación multifactor, recuperación ante desastres y mucho más. Para obtener una lista completa de las nuevas funciones y mejoras, consulte [Novedades de ONTAP 9.9.1](#).

- Seguridad mejorada para gestión del acceso remoto de interfaz de línea de comandos

La compatibilidad con el hash de contraseña de SHA512 y SSH A512 protege las credenciales de la cuenta de administrador de actores maliciosos que intentan obtener acceso al sistema.

- ["Mejoras de IP de MetroCluster: Compatibilidad con clústeres de 8 nodos"](#)

El nuevo límite es el doble de grande que el anterior, ya que ofrece compatibilidad con configuraciones de MetroCluster y permite la disponibilidad continua de los datos.

- [Mejoras en SnapMirror Business Continuity](#)

Ofrece más opciones de replicación para backup y recuperación ante desastres para contenedores de datos de gran tamaño para cargas de trabajo NAS.

- [Rendimiento SAN mejorado](#)

Ofrece hasta cuatro veces más rendimiento SAN para aplicaciones de LUN únicas, como almacenes de datos VMware, para que pueda lograr un alto rendimiento en su entorno SAN.

- [Nueva opción de almacenamiento de objetos para el cloud híbrido](#)

Permite el uso de StorageGRID como destino para NetApp Cloud Backup Service para simplificar y automatizar el backup de sus datos de ONTAP en las instalaciones.

Siguientes pasos

- [Actualice a la última versión de ONTAP](#)
- [¿Cuándo debo actualizar ONTAP?](#)

Compatibilidad con la versión ONTAP 9

A partir del lanzamiento de ONTAP 9,8, NetApp ofrece lanzamientos de ONTAP dos veces al año. Si bien los planes pueden modificarse, el objetivo es ofrecer nuevos lanzamientos de ONTAP en el segundo y cuarto trimestre de cada año. Utilice esta información para planificar el período de tiempo de su actualización para aprovechar la última versión de ONTAP.

| Versión | Fecha de lanzamiento |
|---------|----------------------|
| 9.14.1 | A enero de 2024 |
| 9.13.1 | Junio de 2023 |
| 9.12.1 | Febrero de 2023 |
| 9.11.1 | Julio de 2022 |
| 9.10.1 | A enero de 2022 |
| 9.9.1 | Junio de 2021 |

Niveles de soporte

El nivel de soporte disponible para una versión específica de ONTAP varía en función de cuándo se lanzó el software.

| Nivel de soporte | Soporte completo | | | Soporte limitado | | Soporte de autoservicio | | |
|---|------------------|----|----|------------------|----|-------------------------|----|----|
| Año | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Acceso a la documentación en línea | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí |
| Soporte técnico | Sí | Sí | Sí | Sí | Sí | | | |
| Análisis de las causas subyacentes | Sí | Sí | Sí | Sí | Sí | | | |
| Descargas de software de | Sí | Sí | Sí | Sí | Sí | | | |
| Actualizaciones de servicio (versiones de parches [P-releases]) | Sí | Sí | Sí | | | | | |
| Alertas sobre vulnerabilidades | Sí | Sí | Sí | | | | | |

Para actualizar a la última versión de ONTAP, consulte [Actualice a la última versión de ONTAP](#) y.. [¿Cuándo debo actualizar ONTAP?](#)

Novedades en ONTAP 9.14.1

Obtenga más información sobre las nuevas funcionalidades disponibles en ONTAP 9.14.1.

Para obtener información detallada sobre versiones anteriores de ONTAP 9, compatibilidad con plataformas de hardware y switches, problemas conocidos y limitaciones, consulte ["Notas de la versión de ONTAP 9"](#). Debe iniciar sesión con su cuenta de NetApp o crear una cuenta de NetApp para acceder a las notas de la versión *ONTAP 9*.

Para actualizar a la última versión de ONTAP, consulte [Prepárese para actualizar ONTAP](#).

Protección de datos

| Actualizar | Descripción |
|---|---|
| NVE admitido en los volúmenes raíz de SVM | Los volúmenes raíz de SVM pueden cifrarse mediante claves únicas con el cifrado de volúmenes de NetApp. |

| Actualizar | Descripción |
|---|---|
| Capacidad para establecer bloqueos de copias de Snapshot en copias de Snapshot de retención a largo plazo y.. Para reiniciar el reloj de cumplimiento | En los clústeres con una licencia de SnapLock, el bloqueo de copia Snapshot a prueba de manipulaciones para copias Snapshot con una retención a largo plazo puede establecerse para las copias Snapshot creadas en volúmenes de destino que no sean de SnapMirror SnapLock y el reloj de cumplimiento se puede inicializar cuando no hay volúmenes de SnapLock presentes. |
| SnapMirror Business Continuity (SM-BC) es compatible con SCSI3 reservas persistentes y clustering de conmutación al nodo de respaldo de Windows | SCSI3 reservas persistentes y Window Failover Clustering para SM-BC admite múltiples nodos que acceden a un dispositivo mientras que al mismo tiempo bloquean el acceso a otros nodos, lo que garantiza que la agrupación en clústeres para diferentes entornos de aplicación se mantenga consistente y estable. |
| Copie copias Snapshot granulares de volúmenes con grupos de consistencia | Se pueden utilizar grupos de coherencia para replicar snapshots de SnapMirror asíncronas y snapshots granulares de volúmenes en los grupos de coherencia de destino para una capa adicional de recuperación ante desastres. |
| Soporte de protección de datos asíncrona para grupos de consistencia dentro de una relación de recuperación de desastres de SVM | Las SVM configuradas para la recuperación ante desastres de SVM pueden replicar la información del grupo de consistencia al sitio secundario si la SVM contiene un grupo de consistencia. |
| "Compatibilidad asíncrona de SnapMirror para destinos de despliegue de 20" | El número de destinos de dispersión asíncrona de SnapMirror admitidos en sistemas A700 y superiores aumenta de 16 a 20 cuando se utiliza ONTAP 9.14.1. |
| Compatibilidad con CLI para grupos de consistencia | Gestione los grupos de consistencia mediante la interfaz de línea de comandos de ONTAP. |

Protocolos de acceso a archivos

| Actualizar | Descripción |
|----------------------------------|--|
| Troncalización de sesión NFSv4,1 | El trunking de sesión permite varias rutas a un almacén de datos exportado. De este modo, se simplifica la gestión y mejora el rendimiento a medida que las cargas de trabajo se escalan verticalmente. Resulta especialmente adecuado en entornos con cargas de trabajo VMware. |

MetroCluster

| Actualizar | Descripción |
|--|---|
| Compatibilidad con almacenamiento de objetos S3 en agregados reflejados y no reflejados | Habilite un servidor de almacenamiento de objetos S3 en una SVM en un agregado reflejado o no reflejado en configuraciones de MetroCluster IP y FC. |
| Compatibilidad para aprovisionar un bloque de S3 en agregados reflejados y no reflejados de un clúster de MetroCluster | Puede crear un bucket en un agregado reflejado o no reflejado en las configuraciones de MetroCluster. |

Para obtener más información sobre las mejoras de la configuración de la plataforma y los switches para configuraciones de MetroCluster, consulte ["Notas de la versión de ONTAP 9"](#).

Almacenamiento de objetos S3

| Actualizar | Descripción |
|---|---|
| Se habilitó el redimensionamiento automático en los volúmenes S3 FlexGroup para eliminar la asignación de capacidad excesiva cuando se crean buckets en ellos | Cuando se crean buckets en los volúmenes de FlexGroup nuevos o existentes o se eliminan, el tamaño de los volúmenes se cambia a un tamaño mínimo requerido. El tamaño mínimo requerido es el tamaño total de todos los bloques de S3 KB de un volumen FlexGroup. |
| Compatibilidad con almacenamiento de objetos S3 en agregados reflejados y no reflejados | Puede habilitar un servidor de almacenamiento de objetos S3 en una SVM en un agregado reflejado o no reflejado en configuraciones de MetroCluster IP y FC. |
| Bloqueo de objetos basado en roles de usuarios y período de retención de bloqueo | Los objetos de los cubos S3 se pueden bloquear para que no se sobrescriban o eliminen. La capacidad de bloquear objetos se basa en usuarios o tiempo específicos. |
| Configurar el acceso para grupos de usuarios LDAP para que soporten servicios de directorio externos y agregar un período de validez para claves de acceso y secretas | Los administradores de ONTAP pueden configurar el acceso para grupos de usuarios de LDAP o de Active Directory al almacenamiento de objetos de ONTAP S3 con la capacidad de habilitar la autenticación en el modo de vinculación rápida LDAP. Los usuarios de grupos de dominios locales o grupos LDAP pueden generar sus propias claves de acceso y secretas para clientes S3. Puede definir un período de validez para las claves de acceso y las claves secretas de S3 usuarios. ONTAP ofrece compatibilidad con variables como <code>\$aws:username</code> para las políticas de bloque y de grupo. |

SAN

| Actualizar | Descripción |
|--|--|
| Detección de host automatizada de NVMe/TCP | La detección de host de controladoras que utilizan el protocolo NVMe/TCP se automatiza de manera predeterminada. |
| Informes y solución de problemas del host de NVMe/FC | De forma predeterminada, ONTAP admite la capacidad de los hosts NVMe/FC de identificar las máquinas virtuales mediante un identificador único y para que los hosts NVMe/FC supervisen la utilización de los recursos de la máquina virtual. Esto mejora la generación de informes y la solución de problemas del host. |
| Priorización de host de NVMe | Puede configurar su subsistema NVMe para priorizar la asignación de recursos para hosts específicos. Al host al que se asigna una prioridad alta se asignan números de colas de I/O más grandes y profundidades de colas más grandes. |

Seguridad

| Actualizar | Descripción |
|---|---|
| Soporte para autenticación multifactor Cisco DUO para usuarios SSH | Los usuarios de SSH pueden autenticarse utilizando Cisco DUO como segundo factor de autenticación durante el inicio de sesión. |
| "Mejoras en la compatibilidad con OAuth 2,0" | ONTAP 9.14.1 amplía la autenticación principal basada en tokens y el soporte OAuth 2,0 proporcionado inicialmente con ONTAP 9.14.0. La autorización puede configurarse mediante Active Directory o LDAP con asignación de grupos a roles. Los tokens de acceso restringidos por remitente también son compatibles y seguros basados en TLS mutuos (MTLS). Además de Auth0 y Keycloak, Microsoft Windows Active Directory Federation Service (ADFS) es compatible como proveedor de identidad (IdP). |
| "Marco de Autorización de OAuth 2,0" | Se añade el marco de autorización abierta (OAuth 2,0) y proporciona autenticación basada en tokens para los clientes de la API DE REST DE ONTAP. Esto permite una gestión y una administración más seguras de los clústeres de ONTAP mediante flujos de trabajo de automatización impulsados por scripts de la API de REST o Ansible. Las funciones estándar de OAuth 2,0 son compatibles, incluyendo emisor, audiencia, validación local, introspección remota, reclamación de usuario remoto y soporte de proxy. La autorización del cliente se puede configurar mediante ámbitos de OAuth 2,0 independientes o mediante la asignación de los usuarios locales de ONTAP. Los proveedores de identidad (IdP) compatibles incluyen Auth0 y Keycloak que utilizan varios servidores simultáneos. |
| Alertas ajustables para protección autónoma frente a ransomware | Configure Autonomous Ransomware Protection para recibir notificaciones cada vez que se detecte una nueva extensión de archivo o cuando se tome una instantánea ARP, recibiendo una advertencia anterior sobre posibles eventos de ransomware. |
| FPolicy es compatible con almacenes persistentes para reducir la latencia | FPolicy le permite configurar un almacén persistente para capturar eventos de acceso a archivos para políticas asíncronas no obligatorias en la SVM. Los almacenes persistentes pueden ayudar a desacoplar el procesamiento de I/O del cliente del procesamiento de notificaciones de FPolicy para reducir la latencia del cliente. No se admiten configuraciones obligatorias síncronas y asíncronas. |
| FPolicy es compatible con FlexCache Volumes en SMB | FPolicy es compatible con los volúmenes FlexCache con NFS o SMB. Anteriormente, FPolicy no era compatible con FlexCache Volumes con SMB. |

Eficiencia del almacenamiento

| Actualizar | Descripción |
|---|--|
| Rastreo de escaneo en File System Analytics | Realice un seguimiento del análisis de inicialización de File System Analytics con información en tiempo real sobre el progreso y la limitación. |
| Aumente el espacio útil agregado en plataformas FAS | Para las plataformas FAS, la reserva WAFL para agregados de más de 30TB TB se reduce del 10 % al 5 %, lo que aumenta el espacio útil del agregado. |

| Actualizar | Descripción |
|--|--|
| Cambio en los informes de espacio físico utilizado en volúmenes TSSE | <p>En los volúmenes con eficiencia del almacenamiento sensible a la temperatura (TSSE) habilitada, la métrica de la interfaz de línea de comandos de ONTAP para informar de la cantidad de espacio utilizado en el volumen incluye el ahorro de espacio obtenido como resultado del TSSE. Esta métrica se refleja en los comandos <code>volume show -physical-used</code> y <code>volume show-space -physical used</code>.</p> <p>Para FabricPool, el valor de <code>-physical-used</code> es una combinación del nivel de capacidad y el nivel de rendimiento.</p> <p>Para obtener comandos específicos, consulte LINK:https://docs.netapp.com/us-en/ontap-cli-9141/volume-show.html[volume show^] y <code>volume show space#</code>.</p> |

Mejoras de administración de recursos de almacenamiento

| Actualizar | Descripción |
|---|---|
| Reequilibrado proactivo de FlexGroup | Los volúmenes FlexGroup ofrecen compatibilidad para mover automáticamente archivos en crecimiento de un directorio a un componente remoto para reducir los cuellos de botella de I/O del componente local. |
| Etiquetado de copias de Snapshot en FlexGroup Volumes | Puede añadir, modificar y eliminar etiquetas y etiquetas (comentarios) en para ayudar a identificar las copias de Snapshot y para evitar la eliminación accidental de copias de Snapshot en volúmenes de FlexGroup. |
| Escribir directamente en el cloud con FabricPool | FabricPool añade la capacidad de escribir datos en un volumen en FabricPool, por lo que van directamente al cloud sin esperar a que llegue el análisis de organización en niveles. |
| Lectura anticipada agresiva con FabricPool | FabricPool ofrece lectura anticipada agresiva de archivos, como transmisiones de películas en volúmenes de FabricPool, para garantizar que no se descarten tramas. |

Mejoras de gestión de SVM

| Actualizar | Descripción |
|---|--|
| Compatibilidad de movilidad de datos de SVM para migrar SVM que contengan cuotas y qtrees de usuarios y grupos | La movilidad de datos de SVM añade compatibilidad para migrar SVM que contienen cuotas y qtrees de usuarios y grupos. |
| Da soporte para un máximo de 400 volúmenes por SVM, un máximo de 12 parejas de alta disponibilidad, y pNFS con NFS 4,1 usando movilidad de datos de SVM | El número máximo de volúmenes admitidos por SVM con movilidad de datos SVM aumenta hasta 400 y el número de pares de alta disponibilidad compatibles aumenta hasta 12. |

System Manager

| Actualizar | Descripción |
|---|---|
| Compatibilidad con recuperación tras fallos en pruebas de SnapMirror | Puede usar System Manager para realizar ensayos de conmutación al nodo de respaldo de prueba de SnapMirror sin interrumpir las relaciones de SnapMirror existentes. |
| Gestión de puertos en un dominio de retransmisión | Puede usar System Manager para editar o eliminar puertos que se hayan asignado a un dominio de retransmisión. |
| Habilitación de conmutación automática no planificada asistida por mediador (MAUSO) | Puede usar System Manager para habilitar o deshabilitar MAUSO (conmutación automática de sitios no planificada asistida por mediadores) al realizar una conmutación de sitios y conmutación de estado de MetroCluster IP. |
| Clúster y.. volumen etiquetado | Puede usar System Manager para utilizar etiquetas para categorizar clústeres y volúmenes de distintas formas, por ejemplo, por objetivo, propietario o entorno. Esto es útil cuando hay muchos objetos del mismo tipo. Los usuarios pueden identificar rápidamente un objeto específico en función de las etiquetas que se le han asignado. |
| Soporte mejorado para la supervisión del grupo de consistencia | System Manager muestra datos históricos sobre el uso del grupo de consistencia. |
| Autenticación NVMe en banda | Puede usar System Manager para configurar la autenticación segura, unidireccional y bidireccional entre un host NVMe y una controladora a través de los protocolos NVMe/TCP y NVMe/FC usando el protocolo de autenticación DH-HMAC-CHAP. |
| Soporte para la gestión del ciclo de vida de bloques de S3 TB ampliada a System Manager | Puede usar System Manager para definir reglas para eliminar objetos concretos de un bloque y, mediante estas reglas, caducar esos objetos de bloque. |

Novedades en ONTAP 9.13.1

Obtenga más información sobre las nuevas funcionalidades disponibles en ONTAP 9.13.1.

Para obtener información detallada sobre versiones anteriores de ONTAP 9, compatibilidad con plataformas de hardware y switches, problemas conocidos y limitaciones, consulte ["Notas de la versión de ONTAP 9"](#). Debe iniciar sesión con su cuenta de NetApp o crear una cuenta de NetApp para acceder a las notas de la versión ONTAP 9.

Para actualizar ONTAP, consulte [Prepárese para actualizar ONTAP](#).

Protección de datos

| Actualizar | Descripción |
|--|---|
| "Verificación de varios administradores" | El administrador del clúster puede habilitar de manera explícita la verificación multiadministrador en un clúster para que requiera la aprobación del quórum antes de ejecutar algunas operaciones de SnapLock. |

| Actualizar | Descripción |
|---|--|
| "Compatibilidad mejorada para gestionar grupos de coherencia, incluido el movimiento de volúmenes y la geometría" | Es posible mover volúmenes entre grupos de coherencia, modificar la geometría de grupos de coherencia jerárquicos y obtener información de capacidad para convertirlos en grupos de coherencia. System Manager admite la creación de un grupo de coherencia con volúmenes NAS o espacios de nombres NVME nuevos. |
| "Restauración de NDMP con SnapMirror síncrono" | La restauración NDMP se admite con SnapMirror síncrono. |
| Mejoras de continuidad del negocio con SnapMirror (SM-BC) | <ul style="list-style-type: none"> • "Añada volúmenes sin interrupciones a un grupo de coherencia con una relación de SM-BC activa." • "Utilice la restauración NDMP con SM-BC". |
| xref:./release-notes/" Compatibilidad de SnapMirror asíncrono con un único grupo de consistencia " | Los grupos de coherencia son compatibles con configuraciones de SnapMirror asíncrono, lo que permite el almacenamiento de backups de SnapMirror para grupos de coherencia individuales. |

Protocolos de acceso a archivos

| Actualizar | Descripción |
|---|--|
| "Soporte NFSv4.x storepool" | Algunos clientes consumen demasiados recursos de la agrupación de almacenamiento NFSv4.x, lo que provoca el bloqueo de otros clientes de NFSv4.x debido a la falta de disponibilidad de los recursos de la agrupación de almacenamiento NFSv4.x. Puede tener la opción de habilitar la denegación y el bloqueo de clientes que consumen mucho recurso de pool de almacenamiento NFSv4.x en sus entornos. |

MetroCluster

| Actualizar | Descripción |
|---|---|
| "Transición de FC de MetroCluster a IP de MetroCluster mediante un switch compartido para el almacenamiento conectado a Ethernet y MetroCluster IP" | Puede realizar la transición de forma no disruptiva de una configuración MetroCluster FC a una configuración de IP de MetroCluster (ONTAP 9,8 y versiones posteriores) mediante un switch compartido. |
| "Transiciones no disruptivas de una configuración FC de MetroCluster de ocho nodos a una configuración IP de MetroCluster" | Puede realizar la transición de cargas de trabajo y datos de forma no disruptiva de una configuración FC de MetroCluster de ocho nodos existente a una nueva configuración de IP de MetroCluster. |
| "Actualizaciones de la configuración IP de MetroCluster de cuatro nodos mediante conmutación de sitios y conmutación de estado" | Actualice controladoras en una configuración IP de MetroCluster de cuatro nodos mediante la conmutación de sitios y la conmutación con <code>system controller replace</code> comandos. |

| Actualizar | Descripción |
|---|--|
| "La conmutación automática no planificada asistida por mediador (MAUSO) se activa para un cierre medioambiental" | Si un sitio se cierra correctamente debido a un cierre ambiental, se activa MAUSO. |
| "Se admiten configuraciones IP de MetroCluster de ocho nodos" | Es posible actualizar las controladoras y el almacenamiento en una configuración IP de MetroCluster de ocho nodos. Para ello, se debe expandir la configuración para convertirse en una configuración temporal de doce nodos y, a continuación, quitar los grupos anteriores de recuperación ante desastres. |
| "Conversión de la configuración de IP de MetroCluster a una configuración de switch de MetroCluster de almacenamiento compartido" | Es posible convertir una configuración IP de MetroCluster en una configuración de switch de MetroCluster de almacenamiento compartido. |

Para obtener más información sobre las mejoras de la configuración de la plataforma y los switches para configuraciones de MetroCluster, consulte ["Notas de la versión de ONTAP 9"](#).

Redes

| Actualizar | Descripción |
|---|--|
| Compatibilidad de hardware ampliada para la interconexión de clústeres RDMA | ONTAP admite sistemas AFF A900, ASA A900 y FAS9500 para RDMA de interconexión de clústeres con una NIC en clúster de X91153A, lo que ayuda a reducir la latencia, reducir los tiempos de conmutación al nodo de respaldo y acelerar la comunicación entre los nodos. |
| Límites de LIF para datos aumentados | ONTAP proporciona una mayor flexibilidad aumentando los límites de escalado de LIF de datos para parejas y clústeres de alta disponibilidad. |
| Compatibilidad con IPv6 durante la configuración de clústeres en las plataformas A800 y FAS8700 | En las plataformas A800 y FAS8700, se puede usar la interfaz de línea de comandos de ONTAP para crear y configurar clústeres nuevos en entornos de red solo IPv6. |

Almacenamiento de objetos S3

| Actualizar | Descripción |
|--|---|
| Gestión del ciclo de vida de los bloques de S3 | Las acciones de caducidad de objetos S3 definen cuándo caducan los objetos de un depósito. Esta funcionalidad le permite gestionar versiones de objetos para que pueda cumplir los requisitos de retención y gestionar de forma eficaz el almacenamiento de objetos S3. |

SAN

| Actualizar | Descripción |
|---|---|
| Compatibilidad con NVMe/FC en hosts AIX | ONTAP admite el protocolo NVMe/FC en hosts AIX. Consulte "Herramienta de interoperabilidad de NetApp" para configuraciones admitidas. |

Seguridad

| Función | Descripción |
|---|--|
| Protección autónoma de ransomware | <ul style="list-style-type: none"> • Funcionalidad de verificación multiadministrador con protección autónoma frente a ransomware • Transición automática del aprendizaje al modo activo • Soporte de FlexGroup, Incluidos los análisis e informes para volúmenes y operaciones de FlexGroup que expanden un volumen de FlexGroup, conversiones de FlexVol a FlexGroup y reequilibrio de FlexGroup. |
| Autenticación de clave pública SSH con Active Directory | Puede utilizar una clave pública SSH como método de autenticación principal con un usuario de Active Directory (AD) o puede utilizar una clave pública SSH como método de autenticación secundario después de un usuario de AD. |
| Certificados X,509 con claves públicas SSH | ONTAP permite asociar un certificado X,509 a la clave pública SSH para una cuenta, lo que le proporciona la seguridad añadida de las comprobaciones de caducidad y revocación de certificados al iniciar sesión SSH. |
| Notificación de error de acceso a archivos FPolicy | FPolicy admite notificaciones sobre eventos de acceso denegado. Se generan notificaciones para la operación de archivo fallidas debido a la falta de permiso, que incluye: Fallo debido a permisos NTFS, fallo debido a bits de modo Unix y fallo debido a ACL NFSv4. |
| Autenticación multifactor con TOTP (contraseñas puntuales basadas en el tiempo) | Configure cuentas de usuario locales con autenticación multifactor mediante una contraseña de un solo uso basada en el tiempo (TOTP). El TOTP siempre se utiliza como segundo método de autenticación. Puede usar una clave pública SSH o una contraseña de usuario como método de autenticación principal. |

Eficiencia del almacenamiento

| Actualizar | Descripción |
|--|--|
| Cambio en la generación de informes de ratio de reducción de datos primarios en System Manager | <p>El ratio de reducción de datos primarios que se muestra en System Manager ya no incluye el ahorro de espacio de la copia de Snapshot en el cálculo. Solo ilustra la relación entre el espacio lógico usado y el espacio físico usado. En las versiones anteriores de ONTAP, la ratio de reducción de datos primarios incluía importantes ventajas para la reducción del espacio de las copias Snapshot.</p> <p>Como resultado, al actualizar a ONTAP 9.13.1, observará que se registra una relación primaria significativamente más baja. Las tasas de reducción de datos aún son visibles con las copias de Snapshot en la vista de detalles Capacidad.</p> |
| Eficiencia del almacenamiento sensible a la temperatura | La eficiencia del almacenamiento sensible a la temperatura agrega paquetes secuenciales de bloques físicos contiguos para mejorar la eficiencia del almacenamiento. Los volúmenes que tienen habilitada la eficiencia del almacenamiento sensible a la temperatura tendrán habilitada automáticamente el empaquetado secuencial cuando los sistemas se actualicen a ONTAP 9.13.1. |

| Actualizar | Descripción |
|---|---|
| Cumplimiento del espacio lógico | El cumplimiento del espacio lógico se admite en los destinos de SnapMirror. |
| Compatibilidad con los límites de capacidad de la máquina virtual de almacenamiento | Puede establecer límites de capacidad en una máquina virtual de almacenamiento (SVM) y habilitar alertas cuando la SVM se acerca a un umbral de porcentaje. |

Mejoras de administración de recursos de almacenamiento

| Actualizar | Descripción |
|--|---|
| Aumente el número máximo de inodos | ONTAP continuará agregando inodos automáticamente (a una velocidad de 1 inodo por 32 KB de espacio del volumen) incluso si el volumen crece por encima de 680 GB. ONTAP seguirá añadiendo inodos hasta que alcance el máximo de 2.147.483.632. |
| Compatibilidad para especificar un tipo de SnapLock durante la creación de FlexClone | Al crear FlexClone de un volumen de lectura/escritura, puede especificar uno de los tres tipos de SnapLock, ya sea cumplimiento de normativas, empresarial o no de SnapLock. |
| Active File System Analytics de forma predeterminada | Establezca el análisis del sistema de archivos para que se active de forma predeterminada en nuevos volúmenes. |
| Relaciones de abanico de recuperación ante desastres de SVM con volúmenes de FlexGroup | Se elimina la restricción de fanout de la recuperación de desastres de SVM con volúmenes FlexGroup. La Recuperación de desastres de SVM con FlexGroup incluye soporte para relaciones de distribución de SnapMirror en ocho sitios. |
| Operación de reequilibrio de FlexGroup único | Puede programar una sola operación de reequilibrio de FlexGroup para que comience en una fecha y hora futura que especifique. |
| Rendimiento de lectura de FabricPool | FabricPool proporciona un rendimiento de lectura secuencial mejorado para cargas de trabajo únicas y de varios flujos para datos que residen en el cloud y rendimiento en la organización en niveles. Esta mejora puede enviar una tasa más alta de Gets y Puts al almacén de objetos back-end. Si tiene almacenes de objetos en las instalaciones, debe considerar el margen adicional de rendimiento en el servicio de almacén de objetos y determinar si es posible que deba acelerar los puestos de FabricPool. |
| Plantillas de políticas de calidad de servicio adaptativas | Las plantillas de políticas de calidad de servicio adaptativas le permiten establecer pisos de rendimiento en el nivel de la SVM. |

Mejoras de gestión de SVM

| Actualizar | Descripción |
|---|--|
| Movilidad de datos de SVM | Aumenta la compatibilidad para migrar SVM que contienen hasta 200 volúmenes. |
| Compatibilidad para volver a crear directorios de SVM | El nuevo comando de la CLI <code>debug vserver refresh-vserver-dir -node node_name</code> vuelve a crear los directorios y archivos que faltan. Para obtener más información y sintaxis de comandos, consulte " La referencia de comandos de la ONTAP ". |

System Manager

A partir de ONTAP 9.12.1, System Manager se integra con BlueXP. Más información acerca de [Integración de System Manager con BlueXP](#).

| Actualizar | Descripción |
|---|---|
| Cambio en los informes de ratio de reducción de datos primarios | El ratio de reducción de datos primarios que se muestra en System Manager ya no incluye el ahorro de espacio de la copia de Snapshot en el cálculo. Solo ilustra la relación entre el espacio lógico usado y el espacio físico usado. En las versiones anteriores de ONTAP, la ratio de reducción de datos primarios incluía importantes ventajas para la reducción del espacio de las copias Snapshot. Como resultado, al actualizar a ONTAP 9.13.1, observará que se registra una relación primaria significativamente más baja. Aún es posible ver las tasas de reducción de datos con las copias de Snapshot en la vista de detalles de capacidad. |
| Bloqueo de copias snapshot a prueba de manipulaciones | Puede usar System Manager para bloquear una copia Snapshot en un volumen que no sea de SnapLock, a fin de brindar protección contra ataques de ransomware. |
| Compatibilidad con gestores de claves externos | Puede usar System Manager para gestionar administradores de claves externos a fin de almacenar y gestionar las claves de autenticación y cifrado. |
| Solución de problemas de hardware | Los usuarios de System Manager pueden ver descripciones visuales de otras plataformas de hardware en la página «Hardware», incluidas las plataformas ASA y las plataformas AFF C-Series. La compatibilidad con las plataformas AFF C-Series también se incluye en las últimas versiones de parches de ONTAP 9.12.1, ONTAP 9.11.1 y ONTAP 9.10.1. Las visualizaciones identifican problemas o inquietudes con las plataformas, proporcionando un método rápido para que los usuarios puedan solucionar problemas de hardware. |

Novedades en ONTAP 9.12.1

Obtenga más información sobre las nuevas funcionalidades disponibles en ONTAP 9.12.1.

Para obtener información detallada sobre versiones anteriores de ONTAP 9, compatibilidad con plataformas de hardware y switches, problemas conocidos y limitaciones, consulte ["Notas de la versión de ONTAP 9"](#). Debe iniciar sesión con su cuenta de NetApp o crear una cuenta de NetApp para acceder a las notas de la versión *ONTAP 9*.

Para actualizar ONTAP, consulte [Prepárese para actualizar ONTAP](#).

Protección de datos

| Actualizar | Descripción |
|---|---|
| Compatibilidad con volúmenes de FlexVol más grandes con SnapMirror síncrono | El tamaño máximo del volumen FlexVol admitido en las configuraciones síncronas de SnapMirror aumentó de 100 TB a 300 TB. Los clústeres de origen y de destino deben ejecutar <i>ONTAP 9.12.1P2 o posteriores</i> . |
| Compatibilidad con tamaños de archivos y LUN más grandes en SnapMirror síncrono | El tamaño máximo de archivos y LUN admitido en las configuraciones síncronas de SnapMirror ha aumentado de 16 TB a 128 TB. Los clústeres de origen y de destino deben ejecutar <i>ONTAP 9.12.1 P2</i> o versiones posteriores. |
| Soporte mejorado para grupos de consistencia | <ul style="list-style-type: none"> • Puede añadir y quitar volúmenes de un grupo de consistencia, clonar un grupo de consistencia (incluso de una copia Snapshot). • Los grupos de consistencia admiten el etiquetado de aplicaciones para optimizar los procesos de protección y gestión de datos. • La API de REST DE ONTAP admite configurar grupos de coherencia con volúmenes NFS/SMB o espacios de nombres NVMe. |
| OPERACIONES NO DISRUPTIVAS síncronas de SnapMirror | SnapMirror Synchronous admite operaciones no disruptivas (NDO) de toma de control y retorno al nodo primario de alta disponibilidad, movimiento de volúmenes y otras operaciones relacionadas con el mantenimiento. Esta función solo está disponible en las plataformas AFF/ASA. |
| Mediator 1,5 de ONTAP es compatible con la continuidad del negocio de SnapMirror | ONTAP Mediator 1,5 está disponible para supervisar las relaciones de continuidad del negocio de SnapMirror (SM-BC). |
| Mejoras en la continuidad de SnapMirror Business (SM-BC) | SM-BC admite la restauración parcial de LUN desde Snapshots. Además, SM-BC amplía la calidad de servicio a los volúmenes que no están en la relación de SM-BC. |
| Indicador de reconstrucción de almacenes de datos para SnapMirror asíncrono | SnapMirror asíncrono proporciona un indicador que muestra el tiempo que tarda una recompilación del almacén de datos después de un ensayo de recuperación ante desastres, mostrando el porcentaje completado. |
| Opción de SnapLock para establecer el tiempo de retención absoluto mínimo no especificado | SnapLock incluye una opción para establecer un tiempo de retención mínimo cuando el tiempo de retención absoluto se define como “no especificado”. |
| Copias Snapshot a prueba de manipulaciones | Puede bloquear una copia Snapshot en un volumen que no sea de SnapLock para protegerse contra ataques de ransomware. Bloquear las copias snapshot ayuda a garantizar que no se eliminan por accidente o de forma malintencionada. |

Protocolos de acceso a archivos

| Actualizar | Descripción |
|--|--|
| Desactive los tipos de cifrado débiles para la comunicación Kerberos | Una nueva opción de seguridad SMB le permite deshabilitar RC4 y DES en favor de los tipos de cifrado Advanced Encryption Standard (AES) para la comunicación basada en Kerberos con el KDC de Active Directory (AD). |

| Actualizar | Descripción |
|--|---|
| Acceso de clientes S3 a datos NAS | Los clientes S3 pueden acceder a los mismos datos NAS que los clientes NFS y SMB sin necesidad de reformatar, lo cual facilita el servicio de aplicaciones S3 que requieren datos de objetos. |
| Atributos NFS extendidos | Los servidores NFS habilitados para NFSv4,2 pueden almacenar y recuperar atributos extendidos NFS (xattrs) de clientes compatibles con xattr. |
| NFSv4,2 archivos dispersos y soporte de reserva de espacio | El cliente NFSv4,2 puede reservar espacio para un archivo disperso. El espacio también puede desasignarse y desreservarse de un archivo. |

MetroCluster

| Actualizar | Descripción |
|--|--|
| ONTAP Mediator 1,5 se admite en una configuración IP de MetroCluster | ONTAP Mediator 1,5 está disponible para supervisar las configuraciones IP de MetroCluster. |
| La compatibilidad con IPsec para el protocolo de host front-end (como NFS e iSCSI) está disponible en configuraciones FAS de MetroCluster IP y MetroCluster. | La compatibilidad con IPsec para el protocolo de host front-end (como NFS e iSCSI) está disponible en configuraciones FAS de MetroCluster IP y MetroCluster. |
| "Función de cambio forzado automático de MetroCluster en una configuración de IP de MetroCluster" | Se puede habilitar la función de conmutación automática forzada de MetroCluster en una configuración de IP de MetroCluster. Esta característica es una extensión de la función de cambio no planificado asistido por Mediator (MAUSO). |
| "S3 en una SVM en un agregado no reflejado en una configuración de IP de MetroCluster" | Se puede habilitar la función de conmutación automática forzada de MetroCluster en una configuración de IP de MetroCluster. Esta característica es una extensión de la función de cambio no planificado asistido por Mediator (MAUSO). |

Para obtener más información sobre las mejoras de la configuración de la plataforma y los switches para configuraciones de MetroCluster, consulte ["Notas de la versión de ONTAP 9"](#).

Redes

| Actualizar | Descripción |
|-------------------------------|---|
| Servicios LIF | Puede utilizar el <code>management-log-forwarding</code> Servicio para controlar qué LIF se utilizan para reenviar registros de auditoría a un servicio syslog remoto |

Almacenamiento de objetos S3

| Actualizar | Descripción |
|---|--|
| Compatibilidad ampliada para acciones de S3 | <p>Se admiten las siguientes acciones de API de Amazon S3:</p> <ul style="list-style-type: none"> • CopyObject • UploadPartCopy • BucketPolicy (OBTENER, PONER, ELIMINAR) |

SAN

| Actualizar | Descripción |
|---|---|
| Tamaño máximo de LUN aumentado para las plataformas AFF y FAS | A partir de ONTAP 9.12.1P2, el tamaño máximo de LUN admitido en las plataformas AFF y FAS aumentó de 16 TB a 128 TB. |
| "Límites de NVMe aumentados" | <p>El protocolo NVMe admite lo siguiente:</p> <ul style="list-style-type: none"> • 8K subsistemas en un único equipo virtual de almacenamiento y un único clúster • Clústeres de 12 nodos NVMe/FC admiten 256 controladoras por puerto y NVMe/TCP admite 2K controladoras por nodo. |
| Compatibilidad con NVMe/TCP para una autenticación segura | La autenticación segura, unidireccional y bidireccional entre un host NVMe y una controladora es compatible con NVMe/TCP mediante el protocolo de autenticación DHHMAC-CHAP. |
| Soporte de IP de MetroCluster para NVMe | El protocolo NVMe/FC se admite en configuraciones IP MetroCluster de 4 nodos. |

Seguridad

En octubre de 2022, NetApp implementó cambios para rechazar las transmisiones de mensajes AutoSupport que no son enviadas por HTTPS con TLSv1,2 o SMTP seguro. Para obtener más información, consulte ["SU484: NetApp rechazará los mensajes AutoSupport transmitidos con seguridad de transporte insuficiente"](#).


| Función | Descripción |
|---|--|
| Mejoras de interoperabilidad de la protección autónoma contra ransomware | <p>La protección autónoma frente a ransomware está disponible para estas configuraciones:</p> <ul style="list-style-type: none"> • Volúmenes protegidos con SnapMirror • SVM protegidas con SnapMirror • SVM habilitadas para migración (movilidad de datos de SVM) |
| Compatibilidad de autenticación multifactor (MFA) para SSH con FIDO2 y PIV (ambos usados por Yubikey) | SSH MFA puede utilizar intercambio de claves públicas/privadas asistido por hardware con nombre de usuario y contraseña. Yubikey es un dispositivo de token físico que se conecta al cliente SSH para aumentar la seguridad MFA. |

| Función | Descripción |
|---|--|
| Registro a prueba de manipulaciones | Todos los registros internos de ONTAP están a prueba de manipulaciones de forma predeterminada, lo que garantiza que las cuentas de administrador comprometidas no puedan ocultar acciones maliciosas. |
| Transporte TLS para eventos | Los eventos de EMS se pueden enviar a un servidor de syslog remoto mediante el protocolo TLS, lo que mejora la protección a través del cable para el registro de auditoría externa central. |

Eficiencia del almacenamiento

| Actualizar | Descripción |
|--|--|
| Eficiencia del almacenamiento sensible a la temperatura | La eficiencia del almacenamiento sensible a la temperatura está activada de forma predeterminada en las nuevas plataformas AFF C250, AFF C400 y AFF C800 y volúmenes. TSSE no está habilitado de forma predeterminada en los volúmenes existentes, pero se puede habilitar manualmente mediante la interfaz de línea de comandos de ONTAP. |
| Aumente el espacio utilizable del agregado | Para All Flash FAS (AFF) y las plataformas FAS500f, la reserva WAFL para agregados superiores a 30TB TB se reduce del 10 % al 5 %, lo que aumenta el espacio útil del agregado. |
| Análisis del sistema de archivos: Principales directorios por tamaño | File System Analytics ahora identifica los directorios en un volumen que consumen más espacio. |

Mejoras de administración de recursos de almacenamiento

| Actualizar | Descripción |
|--|---|
| Reequilibrado de FlexGroup | <p>Puede habilitar el reequilibrado automático de volúmenes de FlexGroup no disruptivo para redistribuir archivos entre componentes FlexGroup.</p> <div>  <p>Se recomienda no utilizar el reequilibrio automático de FlexGroup después de una conversión de FlexVol a FlexGroup. En su lugar, puede utilizar la función de movimiento de archivos retroactivo disruptiva disponible en ONTAP 9.10.1 y versiones posteriores, para introducir la <code>volume rebalance file-move</code> comando. Para obtener más información y sintaxis de comandos, consulte "La referencia de comandos de la ONTAP".</p> </div> |
| Compatibilidad de SnapLock para SnapVault para FlexGroup Volumes | Compatibilidad de SnapLock para SnapVault para FlexGroup Volumes |

Mejoras de gestión de SVM

| Actualizar | Descripción |
|--|---|
| Mejoras de movilidad de datos de SVM | Los administradores de clúster pueden reubicar sin interrupciones una SVM de un clúster de origen a un de destino mediante FAS, las plataformas AFF, en agregados híbridos. Se ha añadido soporte tanto para el protocolo SMB disruptivo como para la protección autónoma frente a ransomware. |

System Manager

A partir de ONTAP 9.12.1, System Manager se integra con BlueXP. Con BlueXP, los administradores pueden gestionar la infraestructura de multinube híbrida desde un único plano de control conservando la conocida consola de System Manager. Cuando inician sesión en System Manager, se da a los administradores la opción de acceder a la interfaz de System Manager en BlueXP o acceder a System Manager directamente. Más información acerca de [Integración de System Manager con BlueXP](#).

| Actualizar | Descripción |
|---|--|
| Compatibilidad de System Manager para SnapLock | Las operaciones de SnapLock, incluida la inicialización de Compliance Clock, la creación de volúmenes SnapLock y el mirroring de ARCHIVOS WORM, se admiten en System Manager. |
| Visualización hardware del cableado | Los usuarios de System Manager pueden ver información sobre la conectividad sobre el cableado entre dispositivos de hardware en su clúster para solucionar problemas de conectividad. |
| Soporte para la autenticación multifactor con Cisco DUO cuando se inicia sesión en System Manager | Puede configurar Cisco DUO como proveedor de identidad SAML (IdP), lo que permite a los usuarios autenticarse mediante Cisco DUO cuando inician sesión en System Manager. |
| Mejoras en las redes de System Manager | System Manager ofrece más control sobre la selección de puertos domésticos y de subred durante la creación de la interfaz de red. System Manager también admite la configuración de NFS sobre conexiones RDMA. |
| Temas de visualización del sistema | Los usuarios de System Manager pueden seleccionar un tema claro u oscuro para mostrar la interfaz de System Manager. También pueden elegir por defecto el tema utilizado para su sistema operativo o navegador. Esta capacidad permite a los usuarios especificar un ajuste que sea más cómodo para leer la pantalla. |
| Mejoras en los detalles de la capacidad del nivel local | Los usuarios de System Manager pueden ver los detalles de capacidad de niveles locales específicos para determinar si el espacio está comprometido en exceso, lo que puede indicar que necesitan añadir más capacidad para garantizar que el nivel local no se quede sin espacio. |
| Búsqueda mejorada | System Manager tiene una capacidad de búsqueda mejorada que permite a los usuarios buscar y acceder a información de soporte relevante y contextual, y a un documento de productos de System Manager desde el sitio de soporte de NetApp directamente a través de la interfaz de System Manager. Esto permite a los usuarios adquirir la información necesaria para tomar las medidas adecuadas sin tener que buscar en varias ubicaciones en el sitio de soporte. |

| Actualizar | Descripción |
|--|--|
| Mejoras de aprovisionamiento de volúmenes | Los administradores de almacenamiento pueden elegir una política de copia de Snapshot al crear un volumen mediante System Manager en lugar de usar la política predeterminada. |
| Aumente el tamaño de un volumen | Los administradores de almacenamiento pueden ver el impacto en el espacio de datos y la reserva de copias de Snapshot cuando utilizan System Manager para cambiar el tamaño de un volumen. |
| Del banco de almacenamiento y.. Flash Pool gestión | Los administradores de almacenamiento pueden usar System Manager para añadir discos SSD a un pool de almacenamiento SSD, crear niveles locales de Flash Pool (agregado) mediante unidades de asignación de pools de almacenamiento SSD y crear niveles locales de Flash Pool mediante SSD físicos. |
| Compatibilidad de NFS sobre RDMA en System Manager | System Manager es compatible con las configuraciones de la interfaz de red para NFS over RDMA e identifica los puertos compatibles con RoCE. |

Novedades en ONTAP 9.11.1


Obtenga más información sobre las nuevas funcionalidades disponibles en ONTAP 9.11.1.

Para obtener información detallada sobre versiones anteriores de ONTAP 9, compatibilidad con plataformas de hardware y switches, problemas conocidos y limitaciones, consulte ["Notas de la versión de ONTAP 9"](#). Debe iniciar sesión con su cuenta de NetApp o crear una cuenta de NetApp para acceder a las notas de la versión *ONTAP 9*.

Para actualizar a la última versión de ONTAP, consulte [Prepárese para actualizar ONTAP](#).

Protección de datos

| Actualizar | Descripción |
|---|--|
| Servidores de claves externos del clúster | Se ha añadido compatibilidad con servidores de gestión de claves externos en clúster para socios de NetApp que ofrecen una solución del servidor KMIP en clúster. Esto permite agregar servidores KMIP primarios y secundarios, lo que evita la duplicación de los datos de clave de cifrado. Para obtener información sobre los partners admitidos, consulte "Herramienta de matriz de interoperabilidad" . |

| Actualizar | Descripción |
|---|---|
| Política asíncrona de SnapMirror en System Manager | <p>Puede usar System Manager para añadir políticas de mirroring y almacén precreadas y personalizadas, mostrar políticas heredadas y anular las programaciones de transferencia definidas en una política de protección al proteger volúmenes y máquinas virtuales de almacenamiento. También es posible usar System Manager para editar las relaciones de protección de volúmenes y máquinas virtuales de almacenamiento.</p> <div>  <p>Si su sistema utiliza ONTAP 9.8P12 o una versión posterior de ONTAP 9,8, configure SnapMirror mediante System Manager y planifique actualizar a versiones ONTAP 9.9.1 o ONTAP 9.10.1, utilice ONTAP 9,9.1P13 o posterior y las versiones de parches ONTAP 9.10.1P10 o posterior para la actualización.</p> </div> |
| Restauración de un directorio único de SnapMirror Cloud | <p>Permite que los administradores de clúster en el nivel de privilegio de administrador realicen una única operación de restauración de directorio desde un extremo de cloud. Se debe proporcionar el UUID de extremo de origen para identificar el extremo de copia de seguridad desde el que se va a restaurar. Porque varios backups pueden usar lo mismo <code>cloud_endpoint_name</code> Como destino, se debe proporcionar el UUID asociado con el backup para el comando restore. Puede utilizar el <code>snapmirror show</code> comando para obtener el <code>source_endpoint_uuid</code>.</p> |
| Compatibilidad mejorada para SnapMirror Business Continuity (SM-BC) | <ul style="list-style-type: none"> • SM-BC admite AIX como host • SM-BC admite SnapRestore de archivo único, lo que permite restaurar un LUN individual o un archivo normal en una configuración SM-BC. |
| Resincronización rápida de replicación de datos de SVM | <p>La resincronización rápida de la replicación de datos de SVM ofrece a los administradores de almacenamiento la posibilidad de eludir una recompilación completa de un almacén de datos y recuperarse más rápidamente de un ensayo de recuperación ante desastres.</p> |
| Compatibilidad de replicación de datos de SVM con MetroCluster | <p>El origen SVM-DR es compatible con ambos extremos de una configuración MetroCluster.</p> |
| Creación de copias Snapshot de grupo de consistencia en dos fases | <p>En la API de REST, los grupos de coherencia admiten un procedimiento Snapshot de dos fases, lo que permite realizar una comprobación previa antes de confirmar la Snapshot.</p> |

Protocolos de acceso a archivos

| Actualizar | Descripción |
|---------------------------------------|--|
| Compatibilidad con TLSv1,3 GbE | <p>ONTAP admite TLS 1,3 para los protocolos de gestión HTTPS y API de REST. TLS 1,3 no es compatible con el SP/BMC ni con el cifrado de clúster entre iguales.</p> |
| Compatibilidad con enlace rápido LDAP | <p>Si el servidor LDAP es compatible, puede utilizar la vinculación rápida de LDAP para autenticar usuarios administradores de ONTAP de forma rápida y sencilla.</p> |

MetroCluster

| Actualizar | Descripción |
|---|--|
| Soporte para ONTAP Mediator 1,4 | La versión 1,4 del software ONTAP Mediator se admite en las configuraciones IP de MetroCluster. |
| Soporte del grupo de consistencia | Los grupos de coherencia son compatibles con las configuraciones MetroCluster. |
| "Transición de una configuración FC MetroCluster a una configuración IP MetroCluster de AFF A250 o FAS500f" | Puede realizar la transición de una configuración FC de MetroCluster a una configuración IP de MetroCluster de AFF A250 o FAS500f. |

Para obtener más información sobre las mejoras de la configuración de la plataforma y los switches para configuraciones de MetroCluster, consulte ["Notas de la versión de ONTAP 9"](#).

Redes

| Actualizar | Descripción |
|---|---|
| Protocolo de detección de capa de enlace (LLDP) | La red de clústeres es compatible con LLDP para permitir que ONTAP funcione con switches de clúster que no sean compatibles con el protocolo de detección (CDP) de Cisco. |
| Servicios LIF | Los nuevos servicios LIF del cliente proporcionan un mayor control sobre qué LIF se utilizan para solicitudes AD, DNS, LDAP y NIS de salida. |

Almacenamiento de objetos S3

| Actualizar | Descripción |
|---|--|
| Soporte adicional para acciones de objetos S3 | Las API de ONTAP admiten las siguientes acciones: CreateBucket, DeleteBucket, DeleteObjects. Además, ONTAP S3 admite el control de versiones de objetos y las acciones asociadas con PutBucketVersioning, GetBucketVersioning, ListBucketVersions. |

SAN

| Actualizar | Descripción |
|---|--|
| Recuperación tras fallos de LIF de iSCSI | La nueva función de recuperación tras fallos de LIF iSCSI admite la migración automática y manual de LIF iSCSI en una recuperación tras fallos de partner SFO y en una recuperación tras fallos local. La recuperación tras fallos de LIF iSCSI está disponible en todas las plataformas de cabinas SAN (ASA). |
| Migración no destructiva de LUN a espacio de nombres NVMe y del espacio de nombres NVMe a LUN | Utilice la interfaz de línea de comandos de ONTAP para convertir sin movimiento un EI LUN existente a un espacio de nombres de NVMe o una Espacio de nombres NVMe existente a un LUN . |

Seguridad

| Actualizar | Descripción |
|--|--|
| Mejoras de protección autónoma frente a ransomware (ARP) | El algoritmo de detección ARP se ha mejorado para detectar amenazas de malware adicionales. Además, se usa una nueva clave de licencia para activar Autonomous Ransomware Protection. Para las actualizaciones de sistemas ONTAP desde ONTAP 9.10.1, la clave de licencia anterior todavía proporciona la misma funcionalidad. |
| Verificación de varios administradores | Si se habilita la verificación multiadministrador, ciertas operaciones, como eliminar volúmenes o copias Snapshot, solo se pueden ejecutar después de las aprobaciones de los administradores designados. De este modo, se evita que administradores comprometidos, malintencionados o inexpertos realicen cambios no deseados o eliminen datos. |

Eficiencia del almacenamiento

| Actualizar | Descripción |
|---|---|
| Ver el ahorro en huella física | Cuando la eficiencia de almacenamiento sensible a la temperatura está habilitada en un volumen, puede utilizar el comando <code>volume show-footprint</code> para mostrar el ahorro de la huella física. |
| Compatibilidad de SnapLock con volúmenes de FlexGroup | SnapLock incluye soporte para los datos almacenados en volúmenes de FlexGroup. La compatibilidad con FlexGroup Volumes está disponible con los modos SnapLock Compliance y SnapLock Enterprise. |
| Movilidad de datos de SVM | Aumenta el número de cabinas de AFF que se admiten a tres y añade compatibilidad con las relaciones de SnapMirror cuando el origen y el destino ejecutan ONTAP 9.11.1 o una versión posterior. También se introduce la gestión de claves externa (KMIP) y está disponible para instalaciones en la nube y en las instalaciones. |

Mejoras de administración de recursos de almacenamiento


| Actualizar | Descripción |
|--|---|
| Seguimiento de actividad a nivel de SVM en File System Analytics | El seguimiento de la actividad se agrega a nivel de SVM, haciendo un seguimiento de las IOPS de lectura/escritura y los accesos para proporcionar información instantánea y práctica sobre los datos. |
| Activar actualizaciones de tiempo de acceso a archivos | Cuando está habilitada, la hora de acceso se actualiza en el volumen de origen de FlexCache solo si la antigüedad del tiempo de acceso actual es superior a la duración especificada por el usuario. |
| Eliminación asíncrona del directorio | La eliminación asíncrona está disponible para los clientes NFS y SMB cuando el administrador de almacenamiento les otorga derechos en el volumen. Cuando se habilita la eliminación asíncrona, los clientes Linux pueden utilizar el comando <code>mv</code> y los clientes de Windows pueden usar el comando <code>rename</code> para eliminar un directorio y moverlo a uno oculto <code>.ontaptrashbin directorio</code> . |


| Actualizar | Descripción |
|---|---|
| Compatibilidad de SnapLock con volúmenes de FlexGroup | SnapLock incluye soporte para los datos almacenados en volúmenes de FlexGroup. La compatibilidad con FlexGroup Volumes está disponible con los modos SnapLock Compliance y SnapLock Enterprise. SnapLock no es compatible con las siguientes operaciones en FlexGroup Volumes: SnapLock para SnapVault, retención basada en eventos y conservación legal. |

Mejoras de gestión de SVM

| Actualizar | Descripción |
|---|--|
| Movilidad de datos de SVM | Aumenta el número de cabinas de AFF que se admiten a tres y añade compatibilidad con las relaciones de SnapMirror cuando el origen y el destino ejecutan ONTAP 9.11.1 o una versión posterior. También se introduce la gestión de claves externa (KMIP) y está disponible para instalaciones tanto en las instalaciones cloud como en las instalaciones. |

System Manager

| Actualizar | Descripción |
|---|--|
| Gestione las políticas asíncronas de SnapMirror | <p>Utilice System Manager para agregar políticas de mirroring y almacén precreadas y personalizadas, mostrar políticas heredadas y anular las programaciones de transferencia definidas en una política de protección al proteger volúmenes y máquinas virtuales de almacenamiento. También es posible usar System Manager para editar las relaciones de protección de volúmenes y máquinas virtuales de almacenamiento.</p> <div>  <p>Si utiliza la versión de revisión ONTAP 9.8P12 o posterior de ONTAP 9,8 y configuró SnapMirror mediante System Manager. Además, tiene pensado actualizar a las versiones ONTAP 9.9.1 o ONTAP 9.10.1, debe utilizar ONTAP 9,9.1P13 o posterior y las versiones de parches ONTAP 9.10.1P10 o posterior para la actualización.</p> </div> |
| Visualización de hardware | La función de visualización de hardware de System Manager admite todas las plataformas AFF y FAS actuales. |
| Información de análisis del sistema | En la página Insights, System Manager le ayuda a optimizar su sistema mostrando información adicional sobre capacidad y seguridad y nueva información sobre la configuración de los clústeres y de las máquinas virtuales de almacenamiento. |

| Actualizar | Descripción |
|---|---|
| Mejoras en la facilidad de uso | <ul style="list-style-type: none"> • De forma predeterminada, los volúmenes recién creados no se pueden compartir. En su lugar, los usuarios pueden especificar los permisos de acceso predeterminados, como exportar a través de NFS o compartir a través de SMB/CIFS y especificar el nivel de permiso. • Simplificación de SAN - Al agregar o editar un iGroup, los usuarios de System Manager pueden ver el estado de conexión de los iniciadores en el grupo y asegurarse de que los iniciadores conectados se incluyan en el grupo para que se pueda acceder a los datos de LUN. |
| Operaciones de nivel local (agregado) avanzadas | <p>Los administradores de System Manager pueden especificar la configuración de un nivel local si no desean aceptar la recomendación de System Manager. Además, los administradores pueden editar la configuración de RAID de un nivel local existente.</p> <div>  <p>Si utiliza la versión de revisión ONTAP 9.8P12 o posterior de ONTAP 9,8 y configuró SnapMirror mediante System Manager. Además, tiene pensado actualizar a las versiones ONTAP 9.9.1 o ONTAP 9.10.1, debe utilizar ONTAP 9,9.1P13 o posterior y las versiones de parches ONTAP 9.10.1P10 o posterior para la actualización.</p> </div> |
| Gestionar registros de auditoría | Es posible usar System Manager para ver y gestionar registros de auditoría de ONTAP. |

Novedades en ONTAP 9.10.1

Obtenga más información sobre las nuevas funcionalidades disponibles en ONTAP 9.10.1.

Para obtener información detallada sobre versiones anteriores de ONTAP 9, compatibilidad con plataformas de hardware y switches, problemas conocidos y limitaciones, consulte ["Notas de la versión de ONTAP 9"](#). Debe iniciar sesión con su cuenta de NetApp o crear una cuenta de NetApp para acceder a las notas de la versión *ONTAP 9*.

Para actualizar ONTAP, consulte [Prepárese para actualizar ONTAP](#).

Protección de datos

| Actualizar | Descripción |
|---|--|
| Establezca el período de retención de SnapLock en un máximo de 100 años | En versiones anteriores a ONTAP 9.10.1, el tiempo de retención máximo admitido es 19 de enero de 2071. Comenzando con ONTAP 9.10.1, SnapLock Enterprise y Compliance admiten un tiempo de retención hasta el 26 de octubre de 3058 y un período de retención de hasta 100 años. Las políticas más antiguas se convierten automáticamente al ampliar las fechas de retención. |

| Actualizar | Descripción |
|---|--|
| Capacidad de crear volúmenes de SnapLock y no SnapLock en el mismo agregado | A partir de ONTAP 9.10.1, pueden existir volúmenes SnapLock y no SnapLock en el mismo agregado, por lo que ya no es necesario crear un agregado de SnapLock independiente para volúmenes de SnapLock. |
| Grupos de consistencia | Organice volúmenes y LUN en grupos de coherencia para gestionar políticas de protección de datos y garantizar la fidelidad en orden de escritura de cargas de trabajo que abarcan varios volúmenes de almacenamiento. |
| Archive backups con el cloud público | SnapMirror Cloud admite la organización en niveles de backups de ONTAP en clases de almacenamiento de objetos de cloud público de menor coste en AWS y MS Azure para su retención a largo plazo. |
| Compatibilidad con AES para la comunicación segura del canal Netlogon | Si se conecta a los controladores de dominio de Windows mediante el servicio de autenticación Netlogon, puede usar el estándar de cifrado avanzado (AES) para comunicaciones de canal seguras. |
| Kerberos para la autenticación del túnel de dominio SMB | La autenticación de Kerberos está disponible para las autenticaciones del túnel de dominio para la gestión de ONTAP además de NTLM. Esto permite iniciar sesión más seguros en la interfaz de línea de comandos de ONTAP y la interfaz gráfica de usuario de System Manager mediante las credenciales de Active Directory. |

Protocolos de acceso a archivos

| Actualizar | Descripción |
|------------------------------|--|
| NFS sobre RDMA (solo NVIDIA) | NFS a través de RDMA utiliza adaptadores RDMA, que permiten que los datos se copien directamente entre la memoria del sistema de almacenamiento y la memoria del sistema host, lo que elude las interrupciones y la sobrecarga de la CPU. NFS over RDMA permite utilizar el almacenamiento GPUDirect de NVIDIA para cargas de trabajo aceleradas por GPU en hosts con GPU de NVIDIA compatibles. |

MetroCluster

| Actualizar | Descripción |
|--|---|
| "Configuración de la dirección IP de MetroCluster de capa 3 en configuraciones IP de MetroCluster" | Puede editar la dirección IP, la máscara de red y la pasarela de MetroCluster para los nodos en una configuración de capa 3. |
| "Actualización de controladoras simplificada de nodos en una configuración MetroCluster FC" | Se ha simplificado el procedimiento de actualización para el proceso de actualización mediante la conmutación de sitios y la conmutación de estado. |

Para obtener más información sobre las mejoras de la configuración de la plataforma y los switches para configuraciones de MetroCluster, consulte ["Notas de la versión de ONTAP 9"](#).

Redes

| Actualizar | Descripción |
|---|---|
| Interconexión de clústeres RDMA | Con el sistema de almacenamiento A400 o ASA A400 y una NIC de clúster de X1151A puede acelerar las cargas de trabajo de alto rendimiento en un clúster de varios nodos aprovechando RDMA para el tráfico dentro del clúster |
| Es necesario confirmar antes de establecer el estado del administrador en Inactividad para una LIF en una SVM del sistema | De este modo le protege frente a la retirada accidental de LIF que sean esenciales para un correcto funcionamiento del clúster. Si tiene scripts que invocan este comportamiento en la CLI, debe actualizarlos para que tengan en cuenta el paso de confirmación. |
| Recomendaciones de detección y reparación automáticas para problemas de cableado de red | Cuando se detecta un problema de accesibilidad del puerto, ONTAP System Manager recomienda una operación de reparación para resolver el problema. |
| Certificados de seguridad del protocolo de Internet (IPsec) | Las directivas IPsec admiten claves precompartidas (PSKs) además de certificados para la autenticación. |
| Políticas de servicio de LIF | Las políticas de firewall quedan obsoletas y son reemplazadas por las políticas de servicio de LIF. También se ha agregado una nueva política de servicio LIF de NTP para proporcionar un mayor control sobre qué LIF se utilizan para las solicitudes NTP salientes. |

Almacenamiento de objetos S3

| Actualizar | Descripción |
|--|---|
| Protección de datos de objetos, backup y recuperación ante desastres de S3 | S3 SnapMirror proporciona servicios de protección de datos para el almacenamiento de objetos S3 de ONTAP, incluido el mirroring de buckets en configuraciones S3 de ONTAP y el backup bucket en destinos NetApp y no NetApp. |
| Auditoría de S3 | Puede auditar datos y eventos de gestión en entornos de ONTAP S3. La funcionalidad de auditoría de S3 es similar a las funcionalidades de auditoría NAS existentes, y la auditoría de S3 y NAS puede coexistir en un clúster. |

SAN

| Actualizar | Descripción |
|---|--|
| Espacio de nombres NVMe | Puede usar la CLI de ONTAP para aumentar o reducir el tamaño de un espacio de nombres. Puede usar System Manager para aumentar el tamaño de un espacio de nombres. |
| Compatibilidad con el protocolo NVMe para TCP | El protocolo exprés de memoria no volátil (NVMe) está disponible para entornos SAN a través de una red TCP. |

Seguridad

| Actualizar | Descripción |
|---|---|
| Protección autónoma de ransomware | Mediante el análisis de cargas de trabajo en entornos NAS, la protección autónoma frente a ransomware le advierte de actividad anormal que podría indicar un ataque de ransomware. Autonomous Ransomware Protection también crea backups automáticos de Snapshot cuando se detecta un ataque, además de la protección existente de las copias Snapshot programadas. |
| Gestión de claves de cifrado | Utilice Azure Key Vault y el servicio de gestión de claves de Google Cloud Platform para almacenar, proteger y utilizar claves de ONTAP, simplificando así la gestión de claves y el acceso. |

Eficiencia del almacenamiento

| Actualizar | Descripción |
|---|--|
| Eficiencia del almacenamiento sensible a la temperatura | Puede habilitar la eficiencia del almacenamiento sensible a la temperatura usando el modo «predeterminado» o «eficiente» en los volúmenes de AFF nuevos o existentes. |
| Capacidad de mover SVM entre clústeres sin interrupciones | Puede reubicar SVM entre clústeres de AFF físicos, de un origen a un destino, para equilibrio de carga, mejoras del rendimiento, actualizaciones del equipo y migraciones de centros de datos. |

Mejoras de administración de recursos de almacenamiento

| Actualizar | Descripción |
|---|--|
| Seguimiento de actividad para objetos activos con File System Analytics (FSA) | Para mejorar la evaluación del rendimiento del sistema, FSA puede identificar objetos activos: Archivos, directorios, usuarios y clientes con más tráfico y rendimiento. |
| Bloqueo de lectura de archivo global | Habilite un bloqueo de lectura desde un único punto en todas las cachés y el artículo afectado de origen en la migración. |
| Compatibilidad de NFSv4 con FlexCache | Los volúmenes FlexCache admiten el protocolo NFSv4. |
| Crear clones a partir de volúmenes de FlexGroup existentes | Puede crear un volumen FlexClone con volúmenes de FlexGroup existentes. |
| Convertir un volumen de FlexVol en FlexGroup en un origen de recuperación ante desastres de SVM | Puedes convertir volúmenes de FlexVol en FlexGroup Volumes en un origen de recuperación ante desastres de SVM. |

Mejoras de gestión de SVM

| Actualizar | Descripción |
|---|--|
| Capacidad de mover SVM entre clústeres de forma no disruptiva | Puede reubicar SVM entre clústeres de AFF físicos, de un origen a un destino, para equilibrio de carga, mejoras del rendimiento, actualizaciones del equipo y migraciones de centros de datos. |

System Manager

| Actualizar | Descripción |
|--|--|
| Habilitar el registro de telemetría de rendimiento en los registros de System Manager | Los administradores pueden habilitar el registro de telemetría si experimentan problemas de rendimiento con System Manager y, después, ponerse en contacto con el servicio de soporte para analizar el problema. |
| Archivos de licencia de NetApp | Todas las claves de licencia se entregan como Archivos de licencia de NetApp en lugar de claves de licencia individuales de 28 caracteres, lo que permite obtener licencias de varias funciones usando un archivo. |
| Actualice el firmware automáticamente | Los administradores de System Manager pueden configurar ONTAP para que actualice automáticamente el firmware. |
| Revisa las recomendaciones de mitigación de riesgos y reconoce los riesgos reportados por Active IQ | Los usuarios de System Manager pueden ver los riesgos informados por Active IQ y revisar recomendaciones sobre la mitigación de riesgos. A partir de 9.10.1, los usuarios también pueden reconocer los riesgos. |
| Configure la recepción de administradores de las notificaciones de eventos de EMS | Los administradores de System Manager pueden configurar cómo se envían las notificaciones de eventos de Event Management System (EMS) de modo que se notifiquen de los problemas del sistema que requieren su atención. |
| Gestionar certificados | Los administradores de System Manager pueden gestionar entidades de certificación de confianza, certificados de cliente/servidor y autoridades de certificación locales (integradas). |
| Use System Manager para ver el uso histórico de la capacidad y predecir las necesidades futuras de capacidad | La integración entre Active IQ y System Manager permite a los administradores ver datos acerca de las tendencias históricas de capacidad de uso para clústeres. |
| Use System Manager para crear backups de datos en StorageGRID mediante Cloud Backup Service | Como administrador de Cloud Backup Service, puede realizar backups en StorageGRID si tiene Cloud Manager puesto en marcha en las instalaciones. También puede archivar objetos con Cloud Backup Service con AWS o Azure. |

| Actualizar | Descripción |
|--------------------------------|--|
| Mejoras en la facilidad de uso | <p>A partir de ONTAP 9.10.1, puede:</p> <ul style="list-style-type: none"> • Asigne políticas de calidad de servicio a las LUN en lugar del volumen principal (VMware, Linux, Windows) • Editar el grupo de políticas de calidad de servicio de la LUN • Mover una LUN • Desconectar una LUN • Realice una actualización gradual de la imagen ONTAP • Cree un conjunto de puertos y vincúlelo a un igroup • Recomendaciones de detección y reparación automáticas para problemas de cableado de red • Habilitar o deshabilitar el acceso de los clientes al directorio de copia Snapshot • Calcule el espacio que se puede reclamar antes de eliminar las copias snapshot • Acceso continuo a cambios de campo disponibles en recursos compartidos de SMB • Ve a las mediciones de capacidad utilizando unidades de visualización más precisas • Gestione usuarios y grupos específicos de host para Windows y Linux • Administrar la configuración de AutoSupport • Cambie el tamaño de los volúmenes como una acción independiente |

Novedades en ONTAP 9.9.1

Descubra las nuevas funcionalidades disponibles en ONTAP 9.9.1.

Para obtener información detallada sobre versiones anteriores de ONTAP 9, compatibilidad con plataformas de hardware y switches, problemas conocidos y limitaciones, consulte ["Notas de la versión de ONTAP 9"](#). Debe iniciar sesión con su cuenta de NetApp o crear una cuenta de NetApp para acceder a las notas de la versión *ONTAP 9*.

Para actualizar a la última versión de ONTAP, consulte [Prepárese para actualizar ONTAP](#).

Protección de datos

| Actualizar | Descripción |
|--|---|
| "Compatibilidad con la eficiencia del almacenamiento en volúmenes y agregados de SnapLock" | Las funcionalidades de eficiencia del almacenamiento de agregados y volúmenes SnapLock se han ampliado para incluir compactación de datos, deduplicación entre volúmenes, compresión adaptable y TSSE (Temperature Sensitive Storage Efficiency), permitiendo mayores ahorros de espacio para DATOS WORM. |

| Actualizar | Descripción |
|--|---|
| "Soporte para configurar diferentes políticas de Snapshot en el origen y el destino de la recuperación ante desastres de la máquina virtual de almacenamiento" | Las configuraciones de Recuperación de desastres de Storage Virtual Machine pueden utilizar la política de reflejo-almacén para configurar distintas políticas de Snapshot en el origen y el destino, y las políticas del origen no sobrescriben las del destino. |
| "Compatibilidad de System Manager con SnapMirror Cloud" | SnapMirror Cloud ahora es compatible con System Manager. |
| SVM habilitadas para auditoría | El número máximo de SVM habilitadas para la auditoría que se admiten en un clúster se ha aumentado de 50 a 400. |
| SnapMirror síncrono | El número máximo de extremos síncronos de SnapMirror admitidos por par de alta disponibilidad ha aumentado de 80 a 160. |
| Topología de SnapMirror de FlexGroup | Los volúmenes FlexGroup admiten dos o más relaciones de abanico; por ejemplo, A→B, A→C. Al igual que FlexVol Volumes, el ventilador FlexGroup admite un máximo de 8 rutas de distribución y está en cascada hasta dos niveles; por ejemplo, Un circuito→B→C. |

Protocolos de acceso a archivos

| Actualizar | Descripción |
|---|--|
| "Mejoras en la búsqueda de referencias LDAP" | La búsqueda de referencias LDAP se admite con la firma y el sellado LDAP, las conexiones TLS cifradas y las comunicaciones a través del puerto LDAPS 636. |
| "Compatibilidad con LDAPS en cualquier puerto" | LDAPS se puede configurar en cualquier puerto; el puerto 636 sigue siendo el predeterminado. |
| "Las versiones NFSv4.x están habilitadas de forma predeterminada" | NFSv4,0, NFSv4,1 y NFSv4,2 están habilitados de forma predeterminada. |
| "Soporte NFSv4,2 etiquetado" | El control de acceso obligatorio (MAC) con la etiqueta NFS se admite cuando NFSv4,2 está habilitado. Con esta funcionalidad, los servidores NFS de ONTAP tienen en cuenta MAC, almacenan y recuperan <code>sec_label</code> atributos enviados por los clientes. |

MetroCluster

| Actualizar | Descripción |
|---|---|
| "Compatibilidad con IP para enlace compartido en la capa 3" | Las configuraciones de IP de MetroCluster se pueden implementar con conexiones back-end enrutadas por IP (capa 3). |
| "Compatibilidad con clústeres de 8 nodos" | Los clústeres permanentes de 8 nodos se admiten en configuraciones de IP y conectadas a la estructura. Además, las plataformas de AFF ASA admiten configuraciones IP de MCC de 8 nodos. |

Para obtener más información sobre las mejoras de la configuración de la plataforma y los switches para configuraciones de MetroCluster, consulte ["Notas de la versión de ONTAP 9"](#).

Redes

| Actualizar | Descripción |
|-------------------------------------|--|
| "Resiliencia del clúster" | <ul style="list-style-type: none">• Supervisión y prevención de puertos para clústeres de dos nodos sin switch (antes solo disponible en configuraciones con switch)• Conmutación automática de respaldo de nodo cuando un nodo no puede proporcionar datos a través de su red de clúster• Nuevas herramientas para mostrar qué rutas de clúster están experimentando pérdida de paquetes |
| "Extensión LIF de IP virtual (VIP)" | <ul style="list-style-type: none">• El número de sistema autónomo (ASN) para el protocolo de puerta de enlace de borde (BGP) admite un entero no negativo de 4 bytes.• El discriminador de salidas múltiples (MED) permite seleccionar rutas avanzadas con soporte para la priorización de rutas. MED es un atributo opcional en el mensaje de actualización de BGP.• VIP BGP proporciona automatización de rutas predeterminada mediante la agrupación por pares BGP para simplificar la configuración. |

Almacenamiento de objetos S3

| Actualizar | Descripción |
|---------------------------------------|--|
| "Soporte de metadatos y etiquetas S3" | El servidor de ONTAP S3 proporciona funcionalidades de automatización mejoradas para S3 clientes y aplicaciones compatibles con metadatos de objetos definidos por el usuario y etiquetado de objetos. |

SAN

| Actualizar | Descripción |
|--|---|
| Importación LUN externa (FLI) | La aplicación SAN LUN Migrate del sitio de soporte de NetApp se puede usar para calificar una cabina externa que no aparezca en la matriz de interoperabilidad de FLI. |
| Acceso de ruta remota a NVMe-oF | Si se pierde el acceso directo a la ruta de recuperación tras fallos, la I/O remota permite al sistema recuperarse de una ruta remota y continuar con el acceso a los datos. |
| Compatibilidad con clústeres de 12 nodos en ASAS | Los clústeres de 12 nodos son compatibles con las configuraciones de AFF ASA. Los clústeres de ASA pueden incluir una combinación de distintos tipos de sistemas de ASA. |
| Protocolo NVMe-oF en ASAS | La compatibilidad con el protocolo NVMe-oF también está disponible en un sistema AFF ASA. |
| | <ul style="list-style-type: none">• Puede crear un igroup compuesto por iGroups existentes.• Se puede añadir una descripción a un igroup o iniciadores de host que funciona como alias para el iniciador del igroup o del host.• Puede asignar iGroups a dos o más LUN simultáneamente. |

| Actualizar | Descripción |
|---|--|
| Mejora del rendimiento de una única LUN | El rendimiento de una única LUN para AFF ha mejorado de forma significativa, lo cual lo hace ideal para simplificar las puestas en marcha en entornos virtuales. Por ejemplo, A800 puede proporcionar hasta un 400 % más de IOPS de lectura aleatoria. |

Seguridad

| Actualizar | Descripción |
|---|--|
| Soporte para la autenticación multifactor con Cisco DUO cuando se inicia sesión en System Manager | A partir de ONTAP 9.9.1P3, puede configurar Cisco DUO como proveedor de identidad (IdP) SAML, lo que permite a los usuarios autenticarse mediante Cisco DUO cuando inician sesión en System Manager. |

Eficiencia del almacenamiento

| Actualizar | Descripción |
|---|---|
| "Establezca el número máximo de archivos para el volumen" | Automatice los máximos de archivos con el parámetro <code>volume -files-set -maximum</code> , eliminando la necesidad de controlar los límites de los archivos. |

Mejoras de administración de recursos de almacenamiento

| Actualizar | Descripción |
|---|--|
| Mejoras de gestión de análisis del sistema de archivos (FSA) en System Manager | FSA proporciona funciones adicionales de System Manager para realizar búsquedas y filtros, y para tomar medidas según las recomendaciones de FSA. |
| Soporte para caché de consulta negativa | Almacena en la caché un error de archivo no encontrado en el volumen FlexCache para reducir el tráfico de red provocado por las llamadas al origen. |
| Recuperación ante desastres con FlexCache | Proporciona migración de clientes sin interrupciones de una caché a otra. |
| Compatibilidad de SnapMirror en cascada y distribución ramificada para volúmenes FlexGroup | Ofrece compatibilidad con relaciones de dispersión de SnapMirror y SnapMirror para volúmenes de FlexGroup. |
| Compatibilidad de recuperación ante desastres de SVM para volúmenes de FlexGroup | La compatibilidad con la recuperación ante desastres de SVM para volúmenes de FlexGroup proporciona redundancia mediante SnapMirror para replicar y sincronizar la configuración y los datos de una SVM. |
| Compatibilidad de generación de informes sobre espacio lógico y aplicación de políticas para volúmenes de FlexGroup | Puede mostrar y limitar la cantidad de espacio lógico que consumen los usuarios de volúmenes de FlexGroup. |
| Soporte de acceso SMB en qtrees | El acceso SMB es compatible con qtrees en volúmenes FlexVol y FlexGroup con SMB habilitado. |

System Manager

| Actualizar | Descripción |
|---|--|
| System Manager muestra los riesgos que informa Active IQ | Utilice System Manager para enlazar con NetApp Active IQ. Este documento informa de oportunidades para reducir el riesgo y mejorar el rendimiento y la eficiencia de su entorno de almacenamiento. |
| Asigne manualmente los niveles locales | Los usuarios de System Manager pueden asignar un nivel local manualmente cuando se crean o se añaden volúmenes y LUN. |
| Eliminación rápida de directorios | Los directorios se pueden eliminar en System Manager con una funcionalidad de eliminación rápida de directorios de baja latencia. |
| Genere libros de estrategia de Ansible | Los usuarios de System Manager pueden generar libros de estrategia de Ansible desde la interfaz de usuario para unos pocos flujos de trabajo seleccionados y pueden usarlos en una herramienta de automatización para añadir o editar repetidamente volúmenes o LUN. |
| Visualización de hardware | Presentada por primera vez en ONTAP 9,8, la función de visualización de hardware ahora es compatible con todas las plataformas AFF. |
| Integración con Active IQ | Los usuarios de System Manager pueden ver casos de soporte asociados con el clúster y la descarga. También pueden copiar los detalles del clúster necesarios para enviar nuevos casos de soporte en la página de soporte de NetApp. Los usuarios de System Manager pueden recibir alertas de Active IQ para informarles cuando haya nuevas actualizaciones de firmware disponibles. A continuación, podrán descargar la imagen de firmware y cargarla mediante System Manager. |
| Integración con Cloud Manager | Los usuarios de System Manager pueden configurar una protección para hacer backups de los datos en extremos de cloud público mediante Cloud Backup Service. |
| Mejoras en el flujo de trabajo de aprovisionamiento de protección de datos | Los usuarios de System Manager pueden asignar manualmente un destino de SnapMirror y un nombre de igroup al configurar la protección de datos. |
| Gestión de puertos de red mejorada | La página de interfaces de red tiene capacidades mejoradas para mostrar y gestionar interfaces en sus puertos domésticos. |
| Mejoras de administración del sistema | <ul style="list-style-type: none"> • Compatibilidad con iGroups anidados • Asigne varias LUN a un igroup en una única tarea y puede utilizar un alias WWPN para filtrar durante el proceso. • Durante la creación de NVMe-oF, ya no es necesario seleccionar puertos idénticos en ambas controladoras. • Deshabilite los puertos FC con un botón de alternar para cada puerto. |
| Visualización mejorada en System Manager de información sobre las copias Snapshot | <ul style="list-style-type: none"> • Los usuarios de System Manager pueden ver el tamaño de las copias de Snapshot y la etiqueta de SnapMirror. • Las reservas de copias snapshot se establecen en cero si están deshabilitadas las copias snapshot. |

| Actualizar | Descripción |
|--|--|
| <p>Pantalla mejorada en System Manager acerca de información de capacidad y ubicación para los niveles de almacenamiento</p> | <ul style="list-style-type: none"> • Una nueva columna Tiers identifica los niveles locales (agregados) en los que reside cada volumen. • System Manager muestra la capacidad física utilizada junto con la capacidad utilizada lógica en el nivel de clúster y el nivel local (agregado). • Los nuevos campos de visualización de capacidad permiten supervisar la capacidad, realizar un seguimiento de los volúmenes que se acercan a la capacidad o que están infrautilizados. |
| <p>Muestre en System Manager de alertas de emergencia de EMS y otros errores y advertencias</p> | <p>La cantidad de alertas de EMS recibidas en 24 horas, así como otros errores y advertencias, se muestran en la tarjeta de estado de System Manager.</p> |

Integración de System Manager con BlueXP

A partir de ONTAP 9.12.1, System Manager está totalmente integrado con BlueXP. Con BlueXP, puede gestionar su infraestructura multicloud híbrida desde un único plano de control sin perder la consola conocida de System Manager.

BlueXP permite crear y administrar almacenamiento en nube (por ejemplo, Cloud Volumes ONTAP), utilizar los servicios de datos de NetApp (por ejemplo, Backup en nube) y controlar muchos dispositivos de almacenamiento local y perimetral.

Para usar System Manager en BlueXP, lleve a cabo los siguientes pasos:

Pasos

1. Abra un explorador web e introduzca la dirección IP de la interfaz de red de gestión del clúster.

Si el clúster tiene conectividad con BlueXP, aparecerá una solicitud de inicio de sesión.

2. Haga clic en **continuar con BlueXP** para seguir el enlace a BlueXP.



Si la configuración de tu sistema ha bloqueado redes externas, no podrás acceder a BlueXP. Para acceder a System Manager mediante BlueXP, debe asegurarse de que su sistema pueda acceder a la dirección «`cloudmanager.cloud.netapp.com`». De lo contrario, en el símbolo del sistema de, puede elegir usar la versión de System Manager instalada en el sistema ONTAP.

3. En la página de inicio de sesión de BlueXP, seleccione **Iniciar sesión con sus credenciales del sitio de soporte de NetApp** e introduzca sus credenciales.

Si ya ha utilizado BlueXP y tiene un inicio de sesión utilizando un correo electrónico y una contraseña, deberá continuar utilizando esa opción de inicio de sesión en su lugar.

["Más información sobre el inicio de sesión en BlueXP"](#).

4. Si se le solicita, introduzca un nombre para la nueva cuenta de BlueXP.

En la mayoría de los casos, BlueXP crea automáticamente una cuenta basada en los datos de su clúster.

5. Introduzca las credenciales de administrador del clúster para el clúster.

Resultado

System Manager muestra y ahora puede gestionar el clúster desde BlueXP.

Descubra sus clústeres directamente desde BlueXP

BlueXP ofrece dos formas de detectar y gestionar sus clústeres:

- Detección directa para la gestión mediante System Manager

Esta es la misma opción de descubrimiento descrita en la sección anterior con la que sigue la redirección.

- Detección a través de un conector

El conector es un software instalado en su entorno que le permite acceder a funciones de gestión a través de System Manager y también a servicios en nube de BlueXP que proporcionan funciones como replicación de datos, backup y recuperación, clasificación de datos, organización en niveles de datos y mucho más.

Vaya a la ["Documentación de BlueXP"](#) para obtener más información sobre estas opciones de detección y administración.

Más información sobre BlueXP

- ["Introducción a BlueXP"](#)
- ["Gestione sus sistemas AFF y FAS de NetApp a través de BlueXP"](#)

Introducción y conceptos

Conceptos de ONTAP

Descripción general de conceptos

Los siguientes conceptos informan al software para la gestión de datos ONTAP, incluidos el almacenamiento en clúster, la alta disponibilidad, la virtualización, la protección de datos Eficiencia del almacenamiento, seguridad y FabricPool. Debe comprender toda la gama de funciones y ventajas de ONTAP antes de configurar la solución de almacenamiento.

Para obtener información adicional, consulte lo siguiente:

- ["Administración de clústeres y SVM"](#)
- ["Pares de alta disponibilidad"](#)
- ["Gestión de redes y LIF"](#)
- ["Gestión de discos y agregados"](#)
- ["FlexVol Volumes, tecnología FlexClone y funciones de eficiencia del almacenamiento"](#)
- ["Aprovisionamiento de hosts SAN"](#)
- Acceso a archivos NAS
 - ["Gestión de NFS"](#)
 - ["Gestión de SMB"](#)
- ["Recuperación ante desastres y archivado"](#)

Plataformas ONTAP

El software de gestión de datos ONTAP ofrece almacenamiento unificado para aplicaciones que leen y escriben datos en protocolos de acceso a bloques o archivos, en configuraciones de almacenamiento que abarcan desde flash de alta velocidad hasta medios giratorios con un precio más bajo, hasta almacenamiento de objetos basado en cloud.

Las implementaciones de ONTAP se ejecutan en plataformas FAS diseñadas con la tecnología de NetApp, A-Series y C-Series de AFF y ASA para cabinas all-SAN, así como en hardware de consumo (ONTAP Select) y en clouds privados, públicos o híbridos (Cloud Volumes ONTAP). Una implementación especializada ofrece la mejor infraestructura convergente de su clase (FlexPod Datacenter).

Estas implementaciones combinadas forman el marco básico del _Data Fabric de NetApp, con un enfoque común definido por software para la gestión de datos y la replicación rápida y eficiente entre plataformas.

Almacenamiento en clúster

La iteración actual de ONTAP se desarrolló originalmente para la arquitectura de almacenamiento Scale Out *cluster* de NetApp. Es la arquitectura que se suele encontrar

en las implementaciones de centros de datos de ONTAP. Dado que esta implementación ejerce la mayoría de las funcionalidades de ONTAP, es un buen lugar para empezar a comprender los conceptos que informan la tecnología ONTAP.

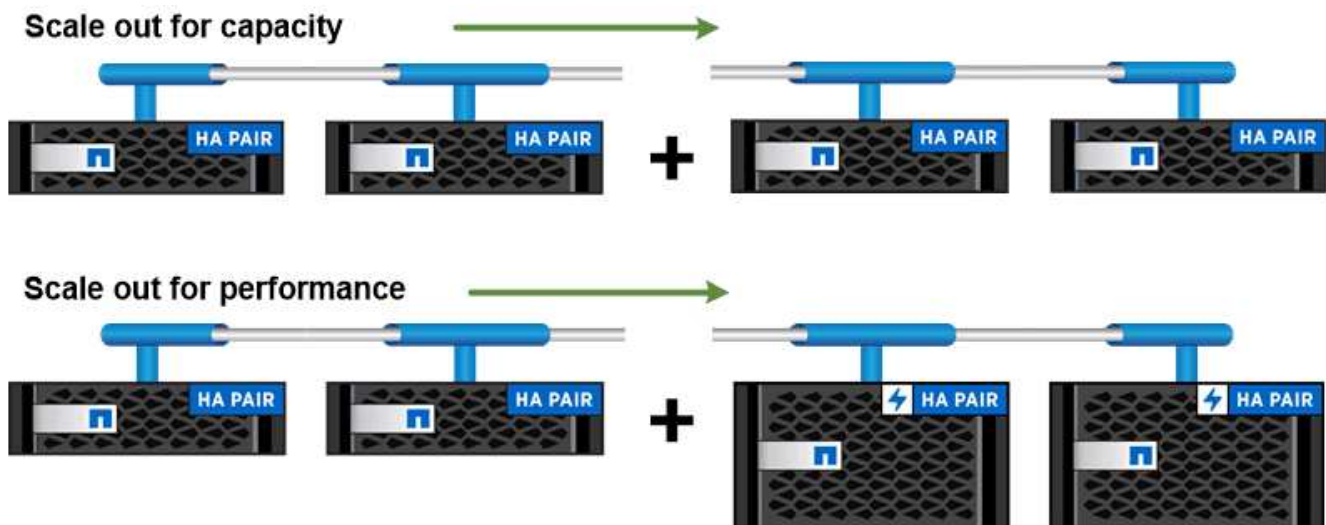
Las arquitecturas de centros de datos suelen poner en marcha controladoras FAS o AFF dedicadas que ejecutan el software para la gestión de datos de ONTAP. Cada controladora, su almacenamiento, su conectividad de red y la instancia de ONTAP que se ejecuta en la controladora se denominan *nodo*.

Los nodos están emparejados para alta disponibilidad (ha). La combinación de estos pares (hasta 12 nodos para SAN y un máximo de 24 nodos para NAS) abarca el clúster. Los nodos se comunican entre sí a través de una interconexión de clúster dedicada y privada.

Según el modelo de controladora, el almacenamiento de nodos consta de discos flash, unidades de capacidad o ambos. Los puertos de red de la controladora proporcionan acceso a los datos. Los recursos de conectividad de red y del almacenamiento físico se virtualizan; solo los administradores de clústeres pueden ver, no los clientes NAS ni los hosts SAN.

Los nodos de una pareja de alta disponibilidad deben usar el mismo modelo de cabina de almacenamiento. De lo contrario, puede utilizar cualquier combinación de controladoras compatible. Puede escalar horizontalmente para obtener capacidad añadiendo nodos con modelos de cabina de almacenamiento o para el rendimiento añadiendo nodos con cabinas de almacenamiento de gama superior.

Por supuesto, puede escalar verticalmente de la misma forma que en los sistemas tradicionales, y actualizar los discos o las controladoras según sea necesario. La infraestructura de almacenamiento virtualizado de ONTAP facilita el movimiento de datos de forma no disruptiva, por lo que puede escalar vertical u horizontalmente sin tiempos de inactividad.



You can scale out for capacity by adding nodes with like controller models, or for performance by adding nodes with higher-end storage arrays, all while clients and hosts continue to access data.

Pares de alta disponibilidad

Los nodos de clúster están configurados en pares de *alta disponibilidad (ha)* para tolerancia a fallos y operaciones no disruptivas. Si un nodo falla o si necesita desconectar un nodo para realizar un mantenimiento rutinario, su partner puede *sustituir* su almacenamiento y continuar sirviendo datos. El partner *devuelve* el almacenamiento

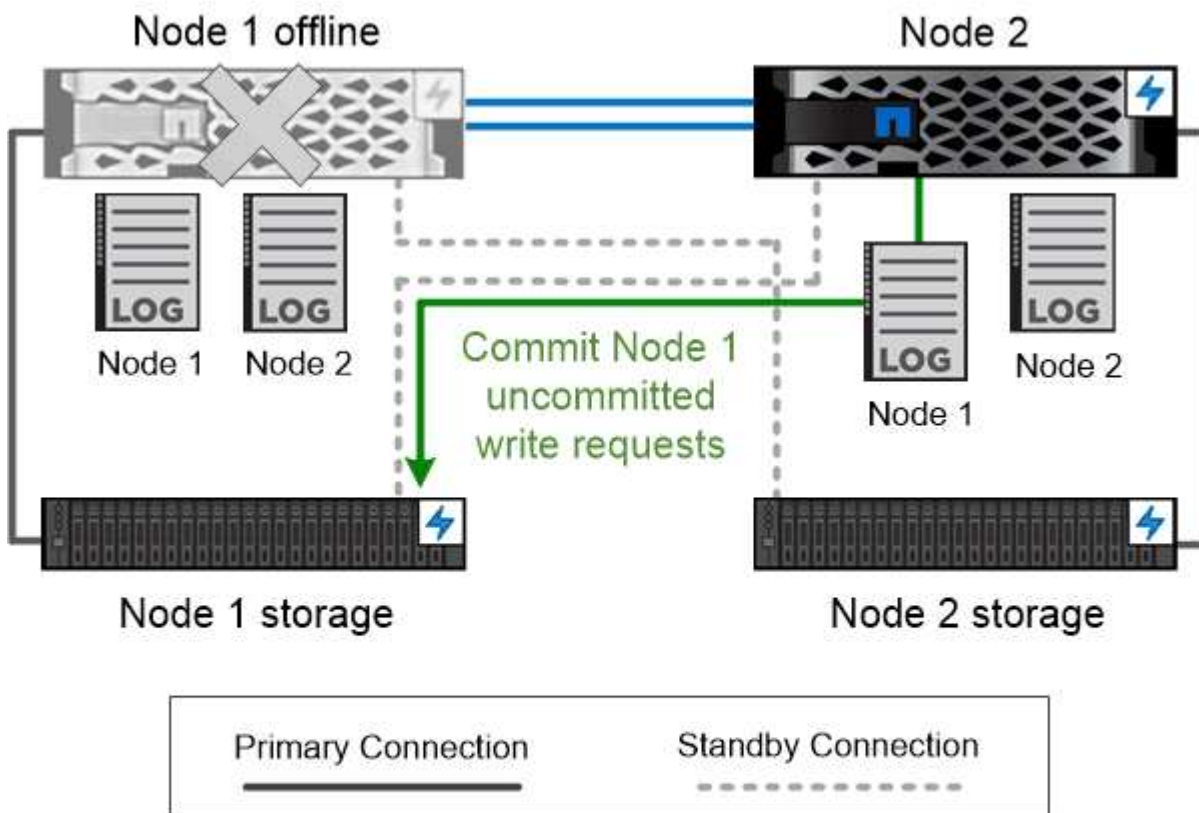
cuando el nodo vuelve a estar online.

Los pares de ALTA DISPONIBILIDAD siempre constan de modelos de controladora similares. Las controladoras suelen residir en el mismo chasis con suministros de alimentación redundantes.

Los pares de alta disponibilidad son nodos con tolerancia a fallos que pueden comunicarse entre sí de distintas formas para permitir que cada nodo compruebe continuamente si el compañero está funcionando y refleje los datos del registro de la memoria no volátil del otro. Cuando se realiza una solicitud de escritura en un nodo, este se registra en NVRAM en ambos nodos antes de volver a enviar una respuesta al cliente o al host. En caso de conmutación por error, el partner que aún continúa activo confirma las solicitudes de escritura del nodo que ha fallado al disco y garantiza la coherencia de los datos.

Las conexiones a los medios de almacenamiento de la otra controladora permiten que cada nodo acceda al almacenamiento del otro en caso de que se produzca una toma de control. Los mecanismos de conmutación al nodo de respaldo de ruta de red garantizan que los clientes y los hosts sigan comunicarse con el nodo superviviente.

Para garantizar la disponibilidad, debe mantener la utilización de capacidad de rendimiento en cualquiera de los nodos en un 50 % para acomodar la carga de trabajo adicional en el caso de conmutación por error. Por la misma razón, puede que desee configurar no más del 50% del número máximo de interfaces de red virtual NAS para un nodo.



On failover, the surviving partner commits the failed node's uncommitted write requests to disk, ensuring data consistency.

toma de control y devolución en implementaciones virtualizadas de ONTAP

El almacenamiento no se comparte entre los nodos de implementaciones virtualizadas de ONTAP «sin elementos» como Cloud Volumes ONTAP para AWS o ONTAP Select. Cuando un nodo deja de funcionar, su partner sigue sirviendo datos desde una copia duplicada de los datos del nodo. No toma el control del almacenamiento del nodo, solo su función de suministro de datos.

Asesor digital AutoSupport y Active IQ

ONTAP ofrece supervisión y generación de informes del sistema basados en inteligencia artificial a través de un portal web y una aplicación para móviles. El componente AutoSupport de ONTAP envía telemetría analizada por el Asesor digital de Active IQ.

Active IQ le permite optimizar su infraestructura de datos en el cloud híbrido global mediante la entrega de análisis predictivos aplicables y soporte proactivo a través de un portal basado en cloud y una aplicación para dispositivos móviles. En Active IQ, todos los clientes de NetApp con un contrato activo de SupportEdge disponen de información y recomendaciones basadas en los datos (las funciones varían según el producto y el nivel de soporte).

Estas son algunas cosas que puede hacer con Active IQ:

- Planificación de actualizaciones. Active IQ identifica los problemas en su entorno que se pueden resolver actualizando a una versión más reciente de ONTAP y el componente Upgrade Advisor le ayuda a planificar una actualización correcta.
- Ver el bienestar del sistema. Su consola de Active IQ informa de cualquier problema con el bienestar y le ayuda a corregir estos problemas. Supervise la capacidad del sistema para asegurarse de que nunca se queda sin espacio de almacenamiento.
- Gestión del rendimiento. Active IQ muestra el rendimiento del sistema durante un período más largo de lo que se puede ver en System Manager. Identifique problemas de configuración y del sistema que afectan a su rendimiento.
- Optimice la eficiencia. Consulte los criterios de medición de la eficiencia del almacenamiento e identifique formas de almacenar más datos en menos espacio.
- Ver el inventario y la configuración. Active IQ muestra información completa sobre la configuración de inventario y software y hardware. Consulte cuándo caducan los contratos de servicio para asegurarse de que permanece cubierto.

Información relacionada

["Documentación de NetApp: Asesor digital de Active IQ"](#)

["Inicie Active IQ"](#)

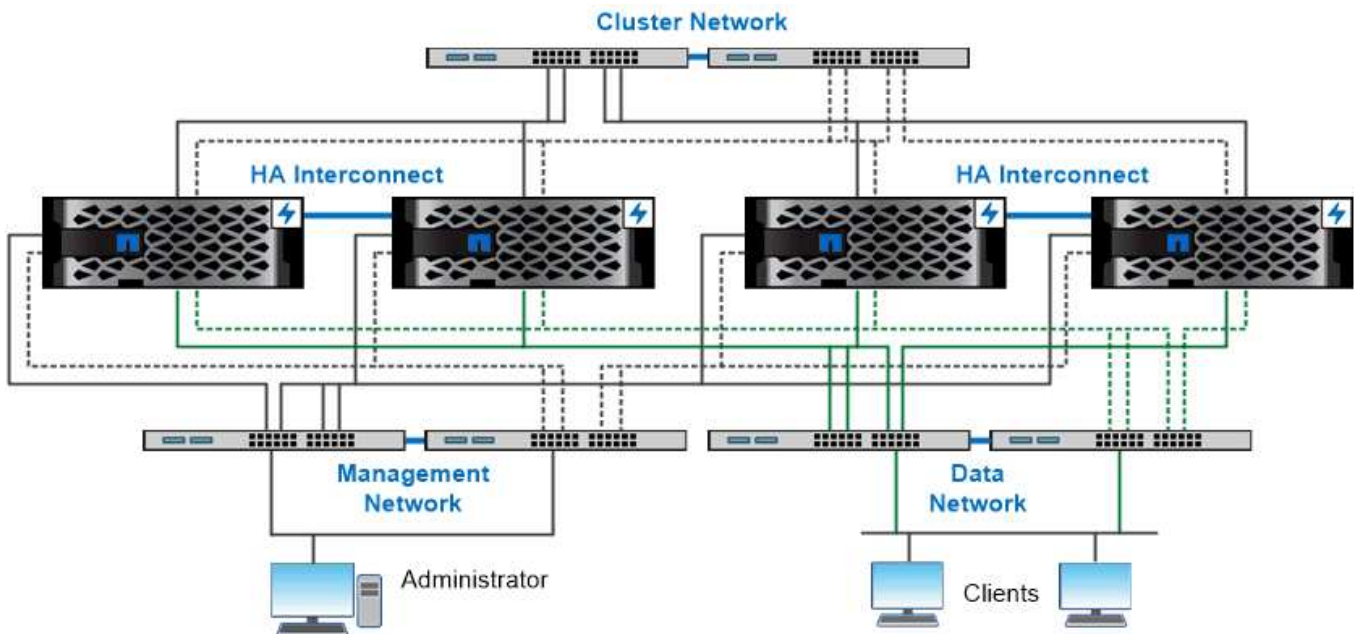
["Servicios de SupportEdge"](#)

Arquitectura de red

Información general de la arquitectura de red

La arquitectura de red para la implementación de un centro de datos ONTAP generalmente consiste en una interconexión de clúster, una red de gestión para la

administración de clústeres y una red de datos. Las NIC (tarjetas de interfaz de red) proporcionan puertos físicos para conexiones Ethernet. Los HBA (adaptadores de bus de host) proporcionan puertos físicos para conexiones FC.



The network architecture for an ONTAP datacenter implementation typically consists of a cluster interconnect, a management network for cluster administration, and a data network.

Puertos lógicos

Además de los puertos físicos proporcionados en cada nodo, puede utilizar *logical ports* para gestionar el tráfico de red. Los puertos lógicos son grupos de interfaces o VLAN.

Grupos de interfaces

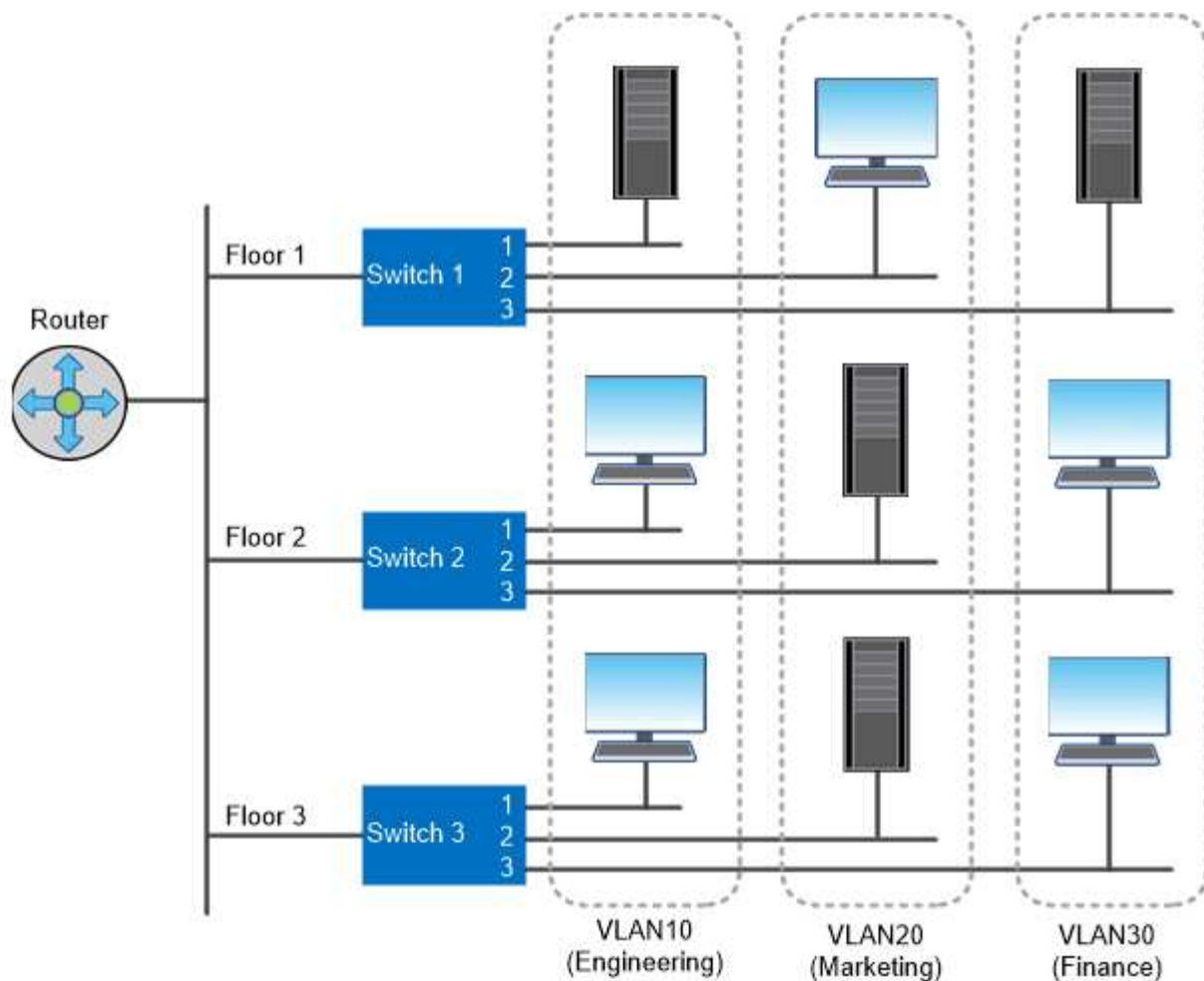
Grupos de interfaces combine varios puertos físicos en un único «puerto troncal» lógico. Puede que desee crear un grupo de interfaces compuesto por puertos de NIC en diferentes ranuras PCI para garantizar que no se produzca un fallo en una ranura, lo que reduce el tráfico empresarial esencial.

Un grupo de interfaces puede ser de modo único, multimodo o multimodo dinámico. Cada modo ofrece distintos niveles de tolerancia a fallos. Se puede usar cualquier tipo de grupo de interfaces multimodo para equilibrar la carga de tráfico de red.

VLAN

VLAN separa el tráfico de un puerto de red (que podría ser un grupo de interfaces) en segmentos lógicos definidos por puerto de switch, en lugar de por límites físicos. Las *estaciones finales* pertenecientes a una VLAN están relacionadas por función o aplicación.

Puede agrupar las estaciones finales por departamento, como Ingeniería y Marketing, o por proyecto, como release1 y release2. Debido a que la proximidad física de las estaciones finales es irrelevante en una VLAN, las estaciones finales pueden ser geográficamente remotas.



You can use VLANs to segregate traffic by department.

Compatibilidad con tecnologías de red estándares del sector

ONTAP admite las principales tecnologías de red estándar del sector. Entre las tecnologías clave se incluyen espacios IP, equilibrio de carga DNS y capturas SNMP.

Los dominios de retransmisión, los grupos de conmutación al nodo de respaldo y las subredes se describen en [Recuperación tras fallos de ruta NAS](#).

Espacios IP

Puede usar un *IPspace* para crear un espacio de dirección IP diferente para cada servidor de datos virtual en un clúster. Esto permite a los clientes en dominios de red separados administrativamente acceder a los datos del clúster mientras utilizan direcciones IP superpuestas del mismo rango de subredes de direcciones IP.

Un proveedor de servicios, por ejemplo, podría configurar distintos espacios IP para clientes que utilizan las mismas direcciones IP para acceder a un clúster.

Balanceo de carga de DNS

Puede utilizar *DNS load balancing* para distribuir el tráfico de la red de usuarios a través de los puertos disponibles. Un servidor DNS selecciona de forma dinámica una interfaz de red para el tráfico en función del

número de clientes montados en la interfaz.

Capturas SNMP

Puede utilizar *SNMP Traps* para comprobar periódicamente si hay fallos o umbrales operativos. Las capturas SNMP capturan la información de supervisión del sistema que se envía de forma asíncrona desde un agente SNMP a un administrador SNMP.

Cumplimiento de normativas FIPS

ONTAP cumple con los estándares de procesamiento de información federal (FIPS) 140-2 para todas las conexiones SSL. Puede activar y desactivar el modo FIPS de SSL, establecer protocolos SSL a nivel global y desactivar todos los cifrados débiles, como RC4.

Información general de RDMA

La oferta de acceso directo a memoria remota (RDMA) de ONTAP admite cargas de trabajo sensibles a la latencia y de ancho de banda elevado. RDMA permite que los datos se copien directamente entre la memoria del sistema de almacenamiento y la memoria del sistema host, evitando así las interrupciones y gastos generales de la CPU.

NFS sobre RDMA

A partir de ONTAP 9.10.1, es posible configurar ["NFS sobre RDMA"](#) Permitir el uso de NVIDIA GPUDirect Storage para cargas de trabajo aceleradas por GPU en hosts con GPU de NVIDIA compatibles.

Interconexión de clústeres RDMA

La interconexión de clústeres RDMA reduce la latencia, reduce los tiempos de conmutación al nodo de respaldo y acelera la comunicación entre los nodos de un clúster.

A partir de ONTAP 9.10.1, la tecnología RDMA de interconexión de clústeres es compatible con algunos sistemas de hardware cuando se utilizan con NIC de clúster de X1151A. A partir de ONTAP 9.13.1, las NIC de X91153A también admiten RDMA de interconexión de clústeres. Consulte la tabla para saber qué sistemas son compatibles con las distintas versiones de ONTAP.

| Sistemas | Versiones de ONTAP compatibles |
|---|--------------------------------------|
| <ul style="list-style-type: none">• A400• ASA A400 | ONTAP 9.10.1 y posteriores |
| <ul style="list-style-type: none">• AFF A900• ASA A900• FAS9500 | ONTAP 9.13.1 y versiones posteriores |

Dada la configuración del sistema de almacenamiento adecuada, no es necesaria ninguna configuración adicional para utilizar RDMA Interconnect.

Protocolos de cliente

ONTAP es compatible con los principales protocolos de cliente estándares del sector:

NFS, SMB, FC, FCoE, iSCSI, NVMe/FC y S3.

NFS

NFS es el protocolo tradicional de acceso a archivos para sistemas UNIX y LINUX. Los clientes pueden acceder a los archivos de los volúmenes de ONTAP utilizando los siguientes protocolos.

- NFSv3
- NFSv4
- NFSv4,2
- NFSv4,1
- PNFs

Puede controlar el acceso a archivos mediante permisos de estilo UNIX, permisos de estilo NTFS o una combinación de ambos.

Los clientes pueden acceder a los mismos archivos utilizando los protocolos NFS y SMB.

SMB

SMB es el protocolo tradicional de acceso a archivos para sistemas Windows. Los clientes pueden acceder a los archivos de los volúmenes ONTAP mediante los protocolos SMB 2.0, SMB 2.1, SMB 3.0 y SMB 3.1.1. Al igual que con NFS, se admite una combinación de estilos de permisos.

SMB 1.0 está disponible, pero deshabilitado de manera predeterminada en ONTAP 9.3 y versiones posteriores.

FC

Fibre Channel es el protocolo de bloques en red original. En lugar de archivos, un protocolo de bloque presenta todo un disco virtual a un cliente. El protocolo FC tradicional utiliza una red FC dedicada con switches FC especializados y requiere que el equipo cliente tenga interfaces de red FC.

Un LUN representa el disco virtual y uno o más LUN se almacenan en un volumen ONTAP. Se puede acceder al mismo LUN a través de los protocolos FC, FCoE e iSCSI, pero varios clientes solo pueden acceder a la misma LUN si forman parte de un clúster que evita las colisiones de escritura.

FCoE

FCoE es básicamente el mismo protocolo que FC, pero utiliza una red Ethernet para centros de datos en lugar del transporte tradicional de FC. El cliente sigue requiriendo una interfaz de red específica de FCoE.

iSCSI

iSCSI es un protocolo de bloques que puede ejecutarse en redes Ethernet estándar. La mayoría de los sistemas operativos de clientes ofrecen un iniciador de software que funciona sobre un puerto Ethernet estándar. iSCSI es una buena opción cuando se necesita un protocolo de bloque para una aplicación en particular, pero no tiene redes de FC dedicadas disponibles.

NVMe/FC

El protocolo de bloques más reciente, NVMe/FC, está específicamente diseñado para funcionar con almacenamiento basado en flash. Ofrece sesiones escalables, una reducción significativa de la latencia y un

aumento del paralelismo, lo que lo hace adecuado para aplicaciones de baja latencia y alto rendimiento, como bases de datos en memoria y análisis.

A diferencia de FC e iSCSI, NVMe no utiliza LUN. En cambio, usa espacios de nombres, que se almacenan en un volumen ONTAP. Se puede acceder a los espacios de nombres NVMe solo mediante el protocolo NVMe.

S3

A partir de ONTAP 9.8, puede habilitar un servidor de ONTAP simple Storage Service (S3) en un clúster de ONTAP, lo que permite servir datos en el almacenamiento de objetos con bloques S3.

ONTAP es compatible con dos casos prácticos en las instalaciones para dar servicio al almacenamiento de objetos S3:

- Organización en niveles FabricPool para un bloque en el clúster local (nivel a un bloque local) o clúster remoto (nivel de cloud).
- Acceso de aplicación de cliente S3 a un bloque del clúster local o de un clúster remoto.



ONTAP S3 es adecuado si se desean funcionalidades de S3 en los clústeres existentes sin necesidad de hardware ni gestión adicionales. Para implementaciones de más de 300 TB, el software StorageGRID de NetApp sigue siendo la solución insignia de NetApp para el almacenamiento de objetos. Descubra "[StorageGRID](#)".

Discos y agregados

=
:allow-uri-read:

Niveles locales (agregados) y grupos RAID

Las modernas tecnologías RAID protegen frente a fallos de disco, al reconstruir los datos de un disco en el que han fallado. El sistema compara la información de índice de un "disco de paridad" con los datos de los discos en buen estado restantes para reconstruir los datos que faltan, todo ello sin tiempo de inactividad ni un coste de rendimiento significativo.

Un nivel local (agregado) consta de uno o varios grupos *RAID*. El *RAID type* del nivel local determina el número de discos de paridad del grupo RAID y el número de errores de disco simultáneos contra los que protege la configuración de RAID.

El tipo de RAID predeterminado, RAID-DP (RAID-doble paridad), requiere dos discos de paridad por grupo RAID y protege contra la pérdida de datos en caso de que fallen dos discos al mismo tiempo. Para RAID-DP, el tamaño de grupo RAID recomendado es de entre 12 y 20 HDD y entre 20 y 28 SSD.

Puede distribuir el coste de sobrecarga de los discos de paridad al crear grupos RAID en el extremo más alto de la recomendación de configuración. Este es especialmente el caso de las unidades de estado sólido, que son mucho más fiables que las unidades de capacidad. En el caso de los niveles locales que utilizan HDD, debe equilibrar la necesidad de maximizar el almacenamiento en disco con factores compensatorios como el tiempo de recompilación más largo necesario para los grupos RAID de mayor tamaño.

Niveles locales (agregados) reflejados y sin mirroring

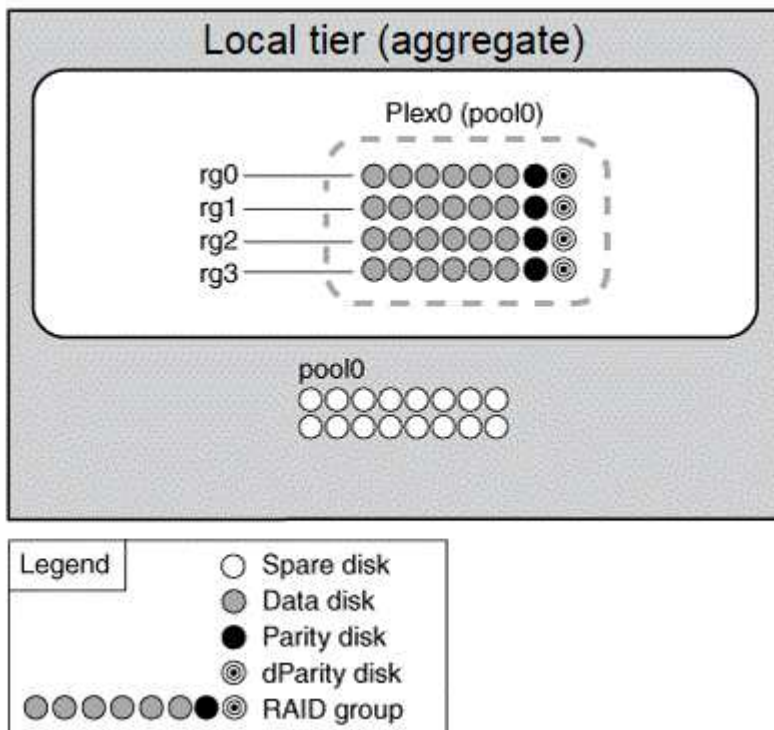
ONTAP tiene una función opcional denominada *SyncMirror* que puede utilizar para reflejar de forma síncrona datos del nivel local (agregado) en copias o *plexes*, almacenados en diferentes grupos RAID. Los complejos se aseguran de la pérdida de datos si fallan más discos de los que protege el tipo RAID, o si hay una pérdida de conectividad con los discos de grupo RAID.

Cuando se crea un nivel local con System Manager o mediante la CLI, es posible especificar que el nivel local se encuentre reflejado o no reflejado.

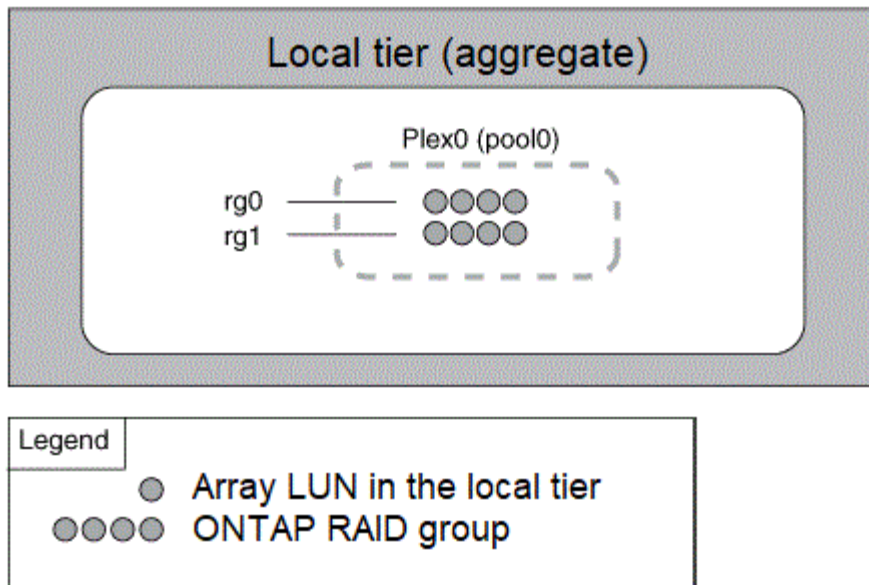
Cómo funcionan los niveles locales (agregados) sin reflejar

Si no se especifica que los niveles locales se reflejan, estos se crean como niveles locales no reflejados (agregados). Los niveles locales no reflejados tienen solo un *plex* (una copia de sus datos), que contiene todos los grupos RAID que pertenecen a ese nivel local.

El siguiente diagrama muestra un nivel local sin duplicación compuesto por discos, con su único complejo. El nivel local tiene cuatro grupos RAID: Rg0, rg1, rg2 y rg3. Cada grupo RAID tiene seis discos de datos, un disco de paridad y un disco dparity (doble paridad). Todos los discos utilizados por el nivel local provienen del mismo pool, "pool0".



El siguiente diagrama muestra un nivel local sin reflejar con los LUN de cabina, con su único complejo. Tiene dos grupos RAID, rg0 y rg1. Todos los LUN de cabina utilizados por el nivel local proceden del mismo pool "pool0".



Cómo funcionan los niveles locales (agregados) reflejados

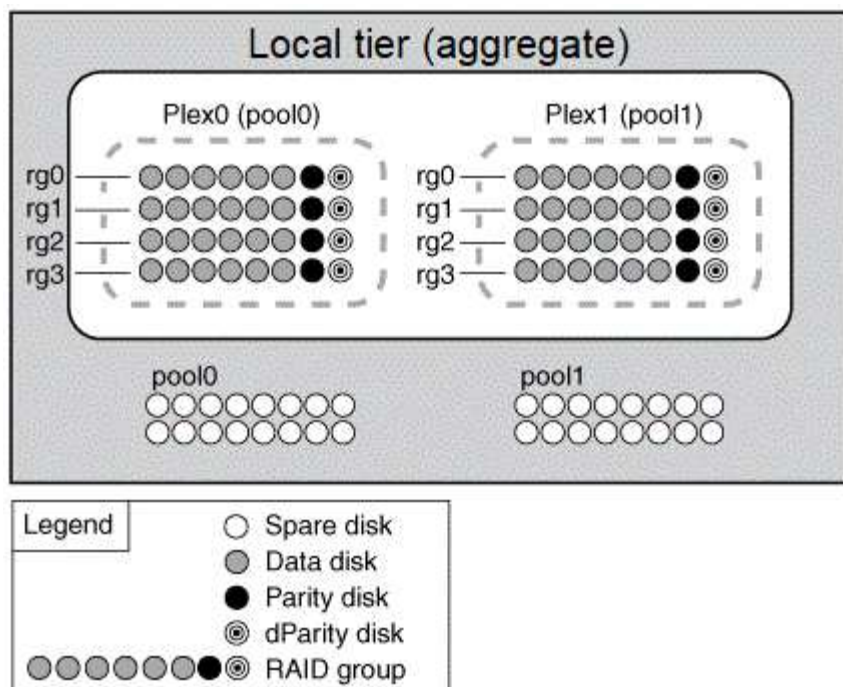
Los agregados reflejados tienen dos *plexes* (copias de sus datos), que utilizan la funcionalidad SyncMirror para duplicar los datos y proporcionar redundancia.

Al crear un nivel local, puede especificar que sea un nivel local reflejado. Además, puede agregar un segundo complejo a un nivel local no reflejado existente para hacerlo un nivel reflejado. Mediante la funcionalidad SyncMirror, ONTAP copia los datos del plex original (plex0) en el complejo nuevo (plex1). Los complejos están separados físicamente (cada complejo tiene sus propios grupos RAID y su propio pool), y los complejos se actualizan simultáneamente.

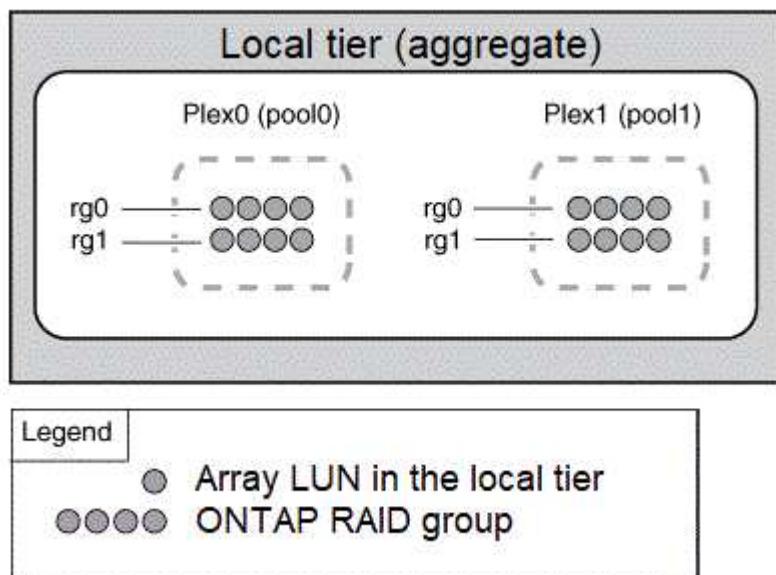
Esta configuración proporciona una protección añadida contra la pérdida de datos si fallan más discos, la cual protege el nivel de RAID del agregado o si se produce una pérdida de conectividad, ya que el plex no afectado sigue sirviendo datos mientras se soluciona la causa del fallo. Una vez solucionado el complejo que tenía un problema, los dos complejos se resincronizaron y restablecen la relación de reflejo.

Los discos y las LUN de matriz del sistema se dividen en dos grupos: "pool0" y "pool1". Plex0 obtiene su almacenamiento de pool0 y plex1 obtiene su almacenamiento de pool1.

En el siguiente diagrama, se muestra un nivel local compuesto por discos con la funcionalidad de SyncMirror habilitada e implementada. Se ha creado un segundo complejo para el nivel local "plex1". Los datos en plex1 son una copia de los datos en plex0 y los grupos RAID son también idénticos. Los 32 discos de repuesto se asignan a la piscina 0 o a la pool1 usando 16 discos para cada pool.



En el siguiente diagrama, se muestra un nivel local compuesto por LUN de cabina con la funcionalidad SyncMirror habilitada e implementada. Se ha creado un segundo complejo para el nivel local "plex1". Plex1 es una copia de plex0 y los grupos RAID son también idénticos.



Se recomienda mantener al menos un 20% de espacio libre para agregados reflejados para lograr un rendimiento y una disponibilidad de almacenamiento óptimos. Aunque la recomendación es del 10% para agregados no duplicados, el sistema de archivos puede utilizar el 10% adicional del espacio para absorber cambios incrementales. Los cambios incrementales aumentan el aprovechamiento del espacio para agregados reflejados gracias a la arquitectura basada en Snapshot de copia en escritura de ONTAP. Si no se siguen estas mejores prácticas, puede tener un impacto negativo en el rendimiento.

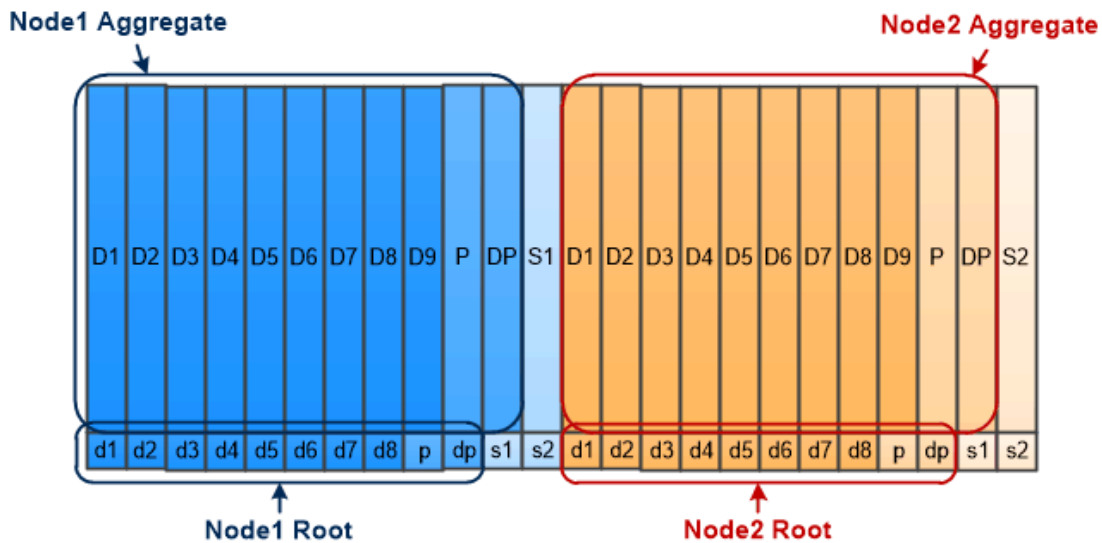
Partición de datos raíz

Cada nodo debe tener un agregado raíz para los archivos de configuración del sistema de almacenamiento. El agregado raíz tiene el tipo de RAID del agregado de datos.

System Manager no admite la partición de datos raíz ni datos raíz.

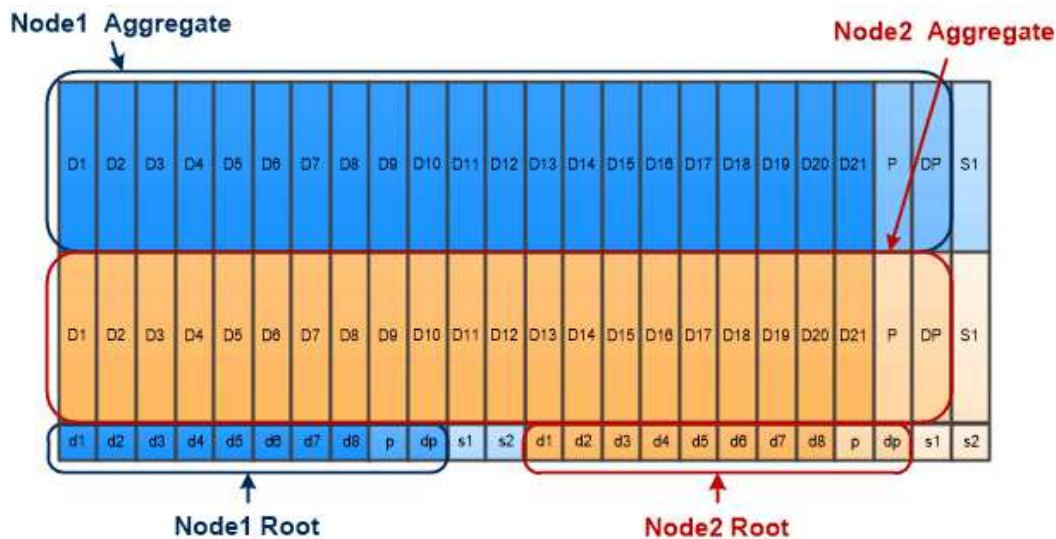
Un agregado raíz de tipo RAID-DP suele consistir en un disco de datos y dos discos de paridad. Esto supone un "impuesto de paridad" significativo a pagar por los archivos del sistema de almacenamiento, cuando el sistema ya reserva dos discos como discos de paridad para cada grupo RAID del agregado.

Partición raíz-datos reduce el impuesto de paridad al distribuir el agregado raíz en las particiones de disco, reservando una partición pequeña en cada disco como partición raíz y una partición grande para los datos.



Root-data partitioning creates one small partition on each disk as the root partition and one large partition on each disk for data.

Como se indica en la ilustración, cuantos más discos se utilicen para almacenar el agregado raíz, más pequeña será la partición raíz. Este es también el caso de una forma de partición de datos raíz llamada *root-data-partitioning*, que crea una partición pequeña como la partición raíz y dos particiones más grandes y de igual tamaño para los datos.



Root-data-data partitioning creates one small partition as the root partition and two larger, equally sized partitions for data.

Ambos tipos de particiones de datos raíz forman parte de la función ONTAP *Advanced Drive Partitioning (ADP)*. Ambos están configurados de fábrica: Creación de particiones de datos raíz para sistemas FAS2xxx, FAS9000, FAS8200, FAS80xx y AFF de gama básica, creación de particiones de datos raíz solo para sistemas AFF.

Más información acerca de ["Creación avanzada de particiones de unidades"](#).

Unidades con particiones y utilizadas para el agregado raíz

Las unidades que se particionan para el uso en el agregado raíz dependen de la configuración del sistema.

Saber cuántas unidades se usan para el agregado raíz ayuda a determinar la cantidad de capacidad de las unidades se reserva para la partición raíz y cuánto se encuentra disponible para usar en un agregado de datos.

La funcionalidad de creación de particiones de datos raíz es compatible con plataformas de gama básica, plataformas All Flash FAS y plataformas FAS solo con unidades SSD conectadas.

Para las plataformas de gama básica, solo se crean particiones de las unidades internas.

Para las plataformas All Flash FAS y las plataformas FAS con solo SSD conectados, todas las unidades conectadas a la controladora cuando se inicializa el sistema se crean en particiones, hasta un límite de 24 por nodo. Las unidades que se añaden después de la configuración del sistema no particionan.

Volúmenes, qtrees, archivos y LUN

ONTAP ofrece datos a los clientes y hosts a partir de contenedores lógicos denominados volúmenes *FlexVol*. dado que estos volúmenes solo se asocian de forma flexible con su agregado que lo contiene, ofrecen una mayor flexibilidad a la hora de gestionar datos que los volúmenes tradicionales.

Puede asignar varios volúmenes de FlexVol a un agregado, cada uno dedicado a una diferente aplicación o servicio. Puede ampliar y contraer un volumen de FlexVol, mover un volumen de FlexVol y realizar copias eficientes de un volumen de FlexVol. Puede usar *Qtrees* para dividir un volumen FlexVol en unidades más

gestionables, y *Quotas* para limitar el uso de recursos por volumen.

Los volúmenes contienen sistemas de archivos en un entorno NAS y LUN en un entorno SAN. Un LUN (número de unidad lógica) es un identificador de un dispositivo llamado *unidad lógica* que se dirige mediante un protocolo SAN.

Los LUN son la unidad básica de almacenamiento en una configuración SAN. El host de Windows ve los LUN en el sistema de almacenamiento como discos virtuales. Puede mover LUN de forma no disruptiva a diferentes volúmenes según sea necesario.

Además de los volúmenes de datos, es necesario conocer algunos volúmenes especiales:

- Un *node root volume* (normalmente "vol0") contiene información y registros de configuración del nodo.
- Un volumen raíz *SVM* actúa como punto de entrada del espacio de nombres que proporciona la SVM y contiene información del directorio de espacios de nombres.
- *System Volumes* contiene metadatos especiales, como registros de auditoría de servicio.

No se pueden usar estos volúmenes para almacenar datos.



Volumes contain files in a NAS environment and LUNs in a SAN environment.

volúmenes de FlexGroup

En algunas empresas, un espacio de nombres único puede requerir petabytes de almacenamiento, lo que supera con creces la capacidad de 100 TB de un volumen FlexVol.

Un *FlexGroup volume* admite hasta 400 mil millones de archivos con 200 volúmenes constituyentes que trabajan conjuntamente para equilibrar dinámicamente la carga y la asignación de espacio de forma uniforme entre todos los miembros.

Gracias a los volúmenes de FlexGroup, no se incurre en gastos generales de mantenimiento o gestión. Simplemente puede crear el volumen FlexGroup y compartirlo con sus clientes NAS. ONTAP se encarga del resto.

Virtualización del almacenamiento

Información general sobre virtualización del almacenamiento

Utilice *máquinas virtuales de almacenamiento (SVM)* para proporcionar datos a los clientes y hosts. Al igual que un equipo virtual que se ejecuta en un hipervisor, un SVM es una entidad lógica que abstrae los recursos físicos. Los datos a los que se accede a través de la SVM no están vinculados a una ubicación en el almacenamiento. El acceso de red a la SVM no está vinculado a un puerto físico.



Antes, las SVM se denominaban «vservers». La interfaz de línea de comandos de ONTAP sigue utilizando el término «Vserver».

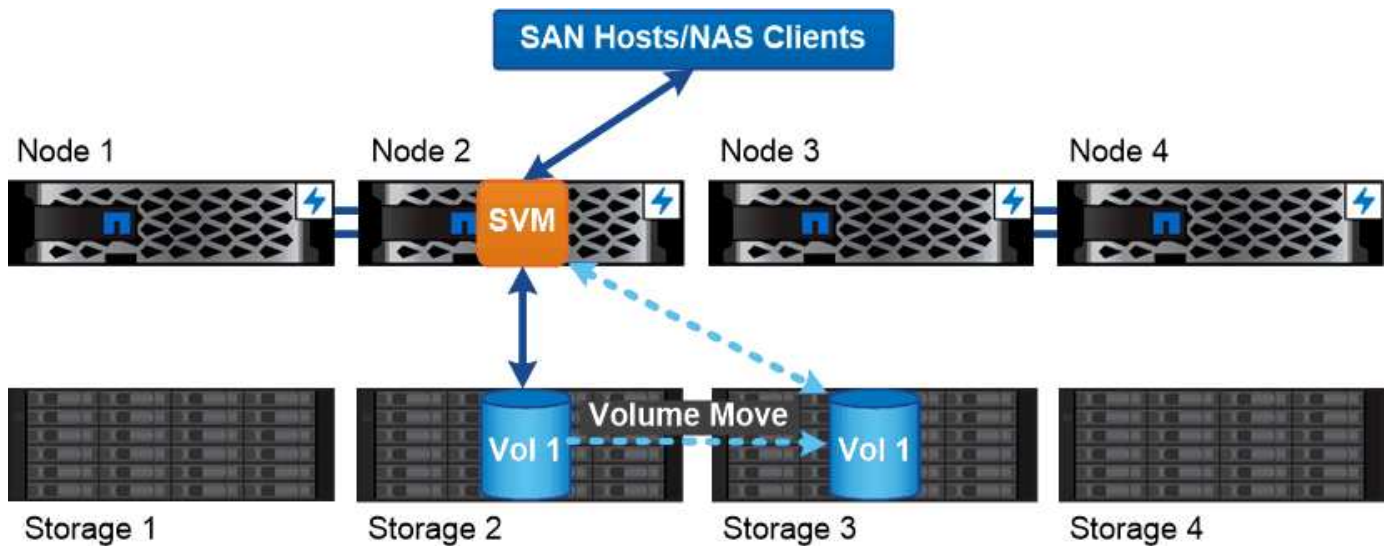
Una SVM proporciona datos a clientes y hosts de uno o más volúmenes a través de una o varias interfaces *lógicas (LIF)* de red. Se pueden asignar volúmenes a cualquier agregado de datos en el clúster. Los LIF pueden alojarse en cualquier puerto físico o lógico. Pueden moverse tanto los volúmenes como los LIF sin interrumpir el servicio de datos, tanto si realiza actualizaciones de hardware, agrega nodos, equilibra el rendimiento o optimiza la capacidad entre agregados.

La misma SVM puede tener un LIF para tráfico NAS y un LIF para tráfico SAN. Los clientes y hosts solo necesitan la dirección de la LIF (dirección IP para NFS, SMB o iSCSI; WWPN para FC) para acceder a la SVM. Las LIF mantienen sus direcciones a medida que se mueven. Los puertos pueden alojar varias LIF. Cada SVM tiene su propia seguridad, administración y espacio de nombres.

Además de las SVM de datos, ONTAP pone en marcha SVM especiales para la administración:

- Cuando se configura el clúster, se crea una SVM_de_admin.
- Se crea una *node SVM* cuando un nodo se une a un clúster nuevo o existente.
- Se crea automáticamente una *SVM del sistema* para las comunicaciones a nivel de clúster en un espacio IP.

No puede utilizar estas SVM para servir datos. También hay LIF especiales para el tráfico dentro de los clústeres y entre ellos, y para la gestión de clústeres y nodos.



Data accessed through an SVM is not bound to a physical storage location. You can move a volume without disrupting data service.

Por qué ONTAP es como middleware

Los objetos lógicos que utiliza ONTAP para las tareas de administración del almacenamiento se encargan de los objetivos habituales de un paquete de middleware bien diseñado: Proteger al administrador de detalles de implementación de bajo nivel y aislar la configuración de los cambios en las características físicas, como nodos y puertos. La idea básica es que el administrador debe poder mover volúmenes y LIF con facilidad, lo que supone reconfigurar unos pocos campos en vez de toda la infraestructura de almacenamiento.

Casos de uso de SVM

Los proveedores de servicios utilizan SVM en acuerdos de multi-tenancy seguro para aislar los datos de cada cliente, proporcionar a cada cliente su propia autenticación y administración y simplificar el pago por uso. Puede asignar varios LIF a la misma SVM para satisfacer diferentes necesidades del cliente, y puede usar QoS para proteger frente a cargas de trabajo de inquilinos «bullying» de las cargas de trabajo de otros clientes.

Los administradores utilizan SVM para finalidades similares en la empresa. Podría querer segregar datos de diferentes departamentos o mantener los volúmenes de almacenamiento a los que acceden los hosts en una SVM y los volúmenes compartidos de usuario en otra. Algunos administradores colocan LUN de iSCSI/FC y almacenes de datos de NFS en una SVM y recursos compartidos de SMB en otra.



Service providers use SVMs in multitenant environments to isolate tenant data and simplify chargeback.

Administración de clústeres y SVM

Un administrador de *cluster* accede a la SVM de administrador del clúster. La SVM de administrador y un administrador de clúster con el nombre reservado `admin` se crean automáticamente cuando se configura el clúster.

Un administrador de clúster con los valores predeterminados `admin` el rol puede administrar todo el clúster y sus recursos. El administrador de clúster puede crear administradores de clúster adicionales con diferentes roles según sea necesario.

Un administrador de SVM accede a una SVM de datos. El administrador de clúster crea SVM de datos y administradores de SVM según sea necesario.

A los administradores de SVM se les asigna el `vsadmin` función predeterminada. El administrador de clúster puede asignar diferentes roles a los administradores de SVM según sea necesario.

Control de acceso basado en funciones (RBAC)

El *role* asignado a un administrador determina los comandos a los que tiene acceso el administrador. La función se asigna al crear la cuenta para el administrador. Puede asignar un rol diferente o definir roles personalizados según sea necesario.

Espacios de nombres y puntos de unión

Un NAS *Namespace* es una agrupación lógica de volúmenes Unidos en *Junction points* para crear una única jerarquía de sistemas de archivos. Un cliente con permisos suficientes puede acceder a los archivos del espacio de nombres sin especificar la ubicación de los archivos en el almacenamiento. Los volúmenes que se han Unido pueden residir en cualquier parte del clúster.

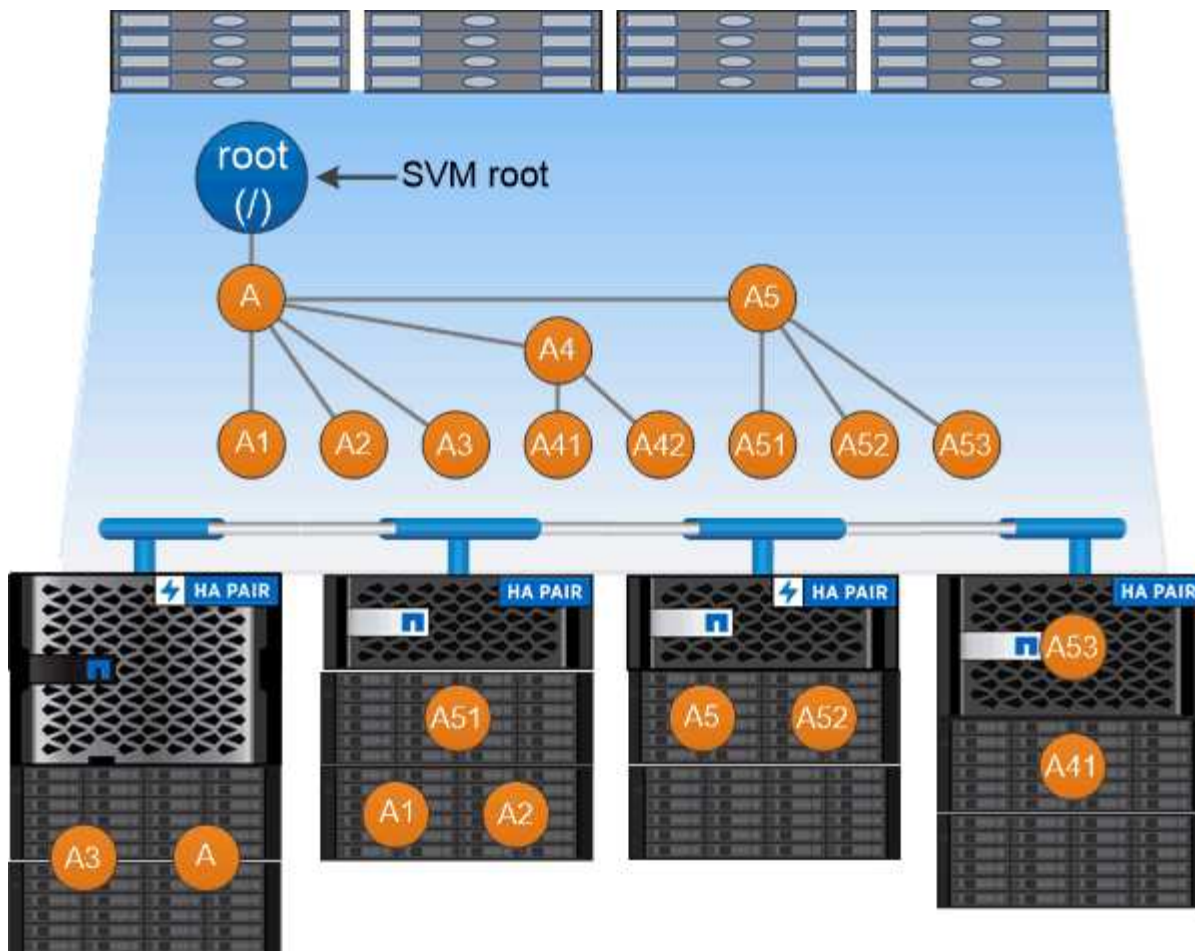
En lugar de montar cada volumen que contenga un archivo de interés, los clientes NAS montan un NFS *export* o acceden a un SMB *share*. La exportación o el recurso compartido representan todo el espacio de nombres o una ubicación intermedia dentro del espacio de nombres. El cliente solo accede a los volúmenes montados por debajo de su punto de acceso.

Es posible añadir volúmenes al espacio de nombres según sea necesario. Puede crear puntos de unión directamente debajo de una unión de volumen principal o en un directorio dentro de un volumen. Puede ser una ruta a una unión de volumen para un volumen denominado «'vol3'» `/vol1/vol2/vol3`, o `/vol1/dir2/vol3`, o incluso `/dir1/dir2/vol3`. La ruta se llama la *ruta de unión*.

Cada SVM tiene un espacio de nombres único. El volumen raíz de la SVM es el punto de entrada de la jerarquía del espacio de nombres.



Para garantizar que los datos sigan estando disponibles en caso de que se produzca una interrupción o conmutación al nodo de respaldo, debe crear una copia *mirror* de uso compartido de la carga para el volumen raíz de la SVM.



A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.

Ejemplo

En el siguiente ejemplo se crea un volumen denominado «'home4'» ubicado en la SVM vs1 que tiene una ruta de unión /eng/home:

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

Recuperación tras fallos de ruta

Información general sobre conmutación por error de rutas

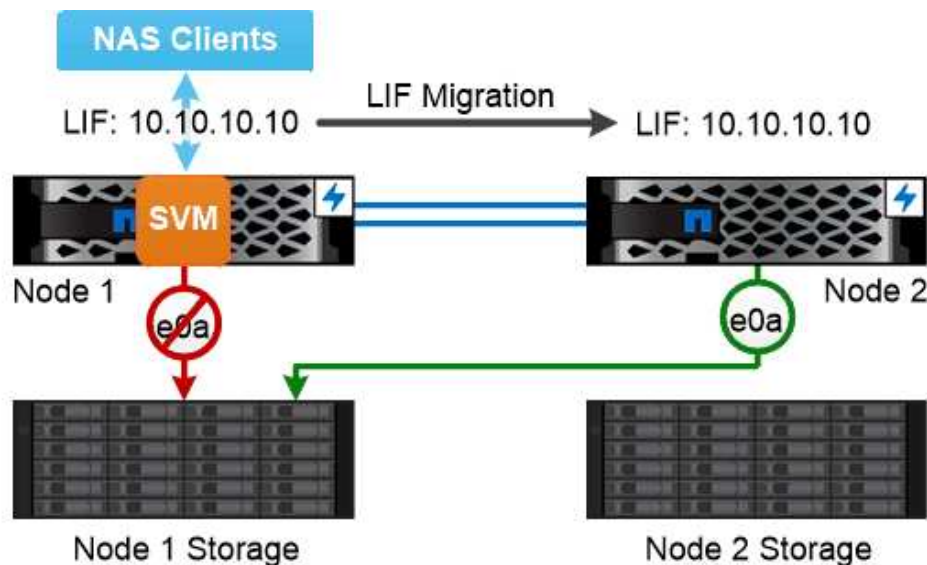
Existen diferencias importantes en la forma en que ONTAP gestiona la conmutación por error de rutas en las topologías NAS y SAN. Un LIF NAS migra automáticamente a un puerto de red diferente tras un error de enlace. Un LIF SAN no migra (a menos que lo mueva manualmente después del fallo). En su lugar, la tecnología multivía en el host desvía el tráfico a un LIF diferente, en la misma SVM, pero accediendo a un puerto de red diferente.

Recuperación tras fallos de ruta NAS

Un LIF NAS migra automáticamente a un puerto de red superviviente tras un error de enlace en su puerto actual. El puerto al que migra la LIF debe ser miembro del *grupo de conmutación por error* de la LIF. La política de *grupo de recuperación tras fallos* reduce los objetivos de conmutación por error de una LIF de datos a los puertos del nodo al que pertenecen los datos y su partner de alta disponibilidad.

Para mayor comodidad administrativa, ONTAP crea un grupo de conmutación por error para cada dominio de difusión de la arquitectura de red. Los puertos de grupo de dominios de difusión que pertenecen a la misma red de capa 2. Si utiliza VLAN, por ejemplo, para segregar el tráfico por departamento (ingeniería, marketing, finanzas, etc.), cada VLAN define un dominio de retransmisión independiente. El grupo de conmutación por error asociado al dominio de retransmisión se actualiza automáticamente cada vez que agrega o quita un puerto de dominio de retransmisión.

Casi siempre es una buena idea usar un dominio de difusión para definir un grupo de conmutación por error para garantizar que el grupo de conmutación por error permanezca actualizado. Sin embargo, en ocasiones es posible que desee definir un grupo de conmutación por error que no esté asociado a un dominio de difusión. Por ejemplo, puede que desee que las LIF solo conmuten al nodo de respaldo en puertos de un subconjunto de los puertos definidos en el dominio de retransmisión.



A NAS LIF automatically migrates to a surviving network port after a link failure on its current port.

subredes

A *subnet* reserva un bloque de direcciones IP en un dominio de difusión. Estas direcciones pertenecen a la misma red de capa 3 y se asignan a puertos en el dominio de retransmisión cuando se crea una LIF. Por lo general, es más fácil y menos propenso a errores a especificar un nombre de subred al definir una dirección de LIF que especificar una dirección IP y una máscara de red.

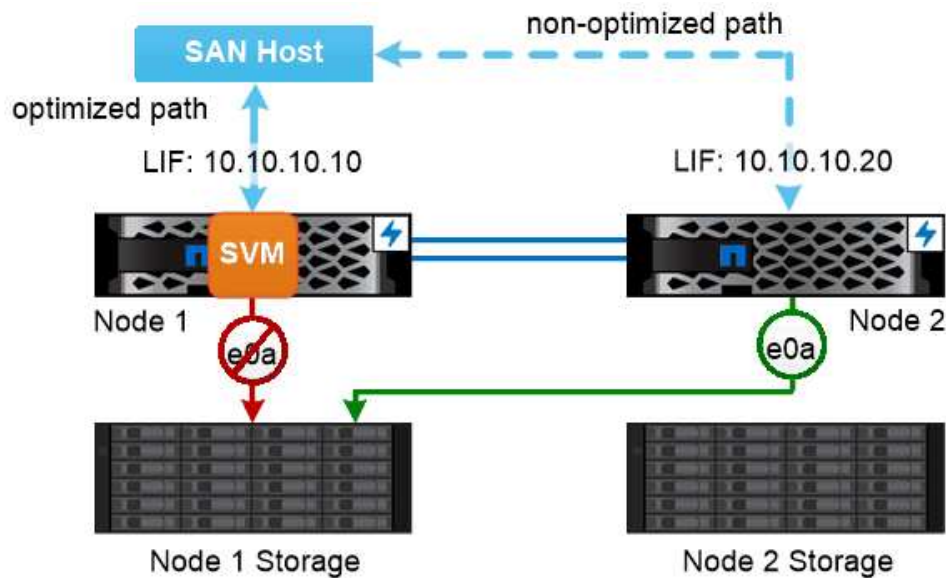
Recuperación tras fallos de rutas SAN

Un host SAN utiliza ALUA (acceso asimétrico de unidad lógica) y MPIO (I/o multivía) para redirigir el tráfico a un LIF superviviente tras un error de enlace. Las rutas predefinidas determinan las posibles rutas a la LUN servida por la SVM.

En un entorno SAN, los hosts se consideran *initiators* of Requests de LUN *Targets*. MPIO permite varias rutas desde iniciadores a destinos. ALUA identifica las rutas más directas, denominadas *_rutas optimizadas*.

Normalmente, configura varias rutas optimizadas a los LIF en el nodo propietario de la LUN y varias rutas no optimizadas a los LIF en su partner de alta disponibilidad. Si un puerto falla en el nodo propietario, el host enruta el tráfico a los puertos supervivientes. Si todos los puertos fallan, el host enruta el tráfico a través de las rutas no optimizadas.

La asignación de LUN selectiva (SLM) de ONTAP limita el número de rutas del host a una LUN de forma predeterminada. Solo se puede acceder a una LUN creada recientemente a través de las rutas al nodo que posee la LUN o su compañero de alta disponibilidad. También puede limitar el acceso a una LUN mediante la configuración de LIF en un *Port set* para el iniciador.



A SAN host uses multipathing technology to reroute traffic to a surviving LIF after a link failure.

mover volúmenes en entornos SAN

De forma predeterminada, ONTAP *selectivo de asignación de LUN (SLM)* limita el número de rutas a un LUN desde un host SAN. Solo es posible acceder a una LUN creada a través de las rutas al nodo propietario de la LUN o de su compañero de alta disponibilidad, el *reporting Nodes* de la LUN.

Esto significa que cuando mueve un volumen a un nodo en otro par de alta disponibilidad, debe añadir nodos de generación de informes para el par de alta disponibilidad de destino a la asignación de LUN. A continuación, puede especificar las nuevas rutas en la configuración de MPIO. Una vez completado el movimiento de volúmenes, es posible eliminar los nodos de generación de informes para la pareja de alta disponibilidad de origen de la asignación.

Balanceo de carga

La latencia comienza a afectar al rendimiento de las cargas de trabajo cuando la cantidad de trabajo en un nodo supera los recursos disponibles. Puede gestionar un nodo sobrecargado aumentando los recursos disponibles (actualizar discos o CPU) o reduciendo la carga (moviendo volúmenes o LUN a nodos diferentes según sea necesario).

También puede utilizar ONTAP *calidad de servicio (QoS)* para garantizar que las cargas de trabajo críticas no degraden el rendimiento de las cargas de trabajo más importantes:

- Puede definir un rendimiento de calidad de servicio *ploter* en una carga de trabajo de la competencia para limitar el impacto sobre los recursos del sistema (QoS máx.).
- Puede establecer un rendimiento de calidad de servicio *floor* para una carga de trabajo crítica y asegurarse de que cumple con los objetivos de rendimiento mínimos sin importar la demanda de otras cargas de trabajo de la competencia (QoS mín.).
- Puede establecer un techo y un piso de calidad de servicio para la misma carga de trabajo.

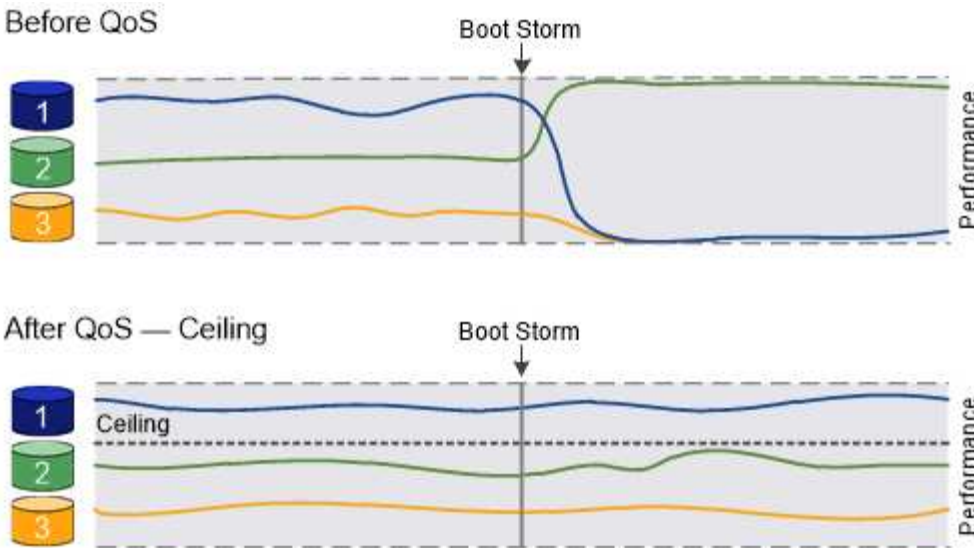
Techos de rendimiento

Un límite máximo de rendimiento limita el rendimiento de una carga de trabajo a un número máximo de IOPS o MB/s. En la siguiente figura, el máximo rendimiento de la carga de trabajo 2 garantiza que no «matones» en las cargas de trabajo 1 y 3.

Un *policy group* define el techo de rendimiento de una o más cargas de trabajo. Una carga de trabajo representa las operaciones de I/O para un objeto de almacenamiento: un volumen, un archivo o una LUN, o todos los volúmenes, archivos o LUN de una SVM. Puede especificar el techo al crear el grupo de políticas, o bien se puede esperar hasta después de supervisar las cargas de trabajo para especificarlo.



El rendimiento en las cargas de trabajo puede superar el límite máximo especificado hasta en un 10 %, especialmente si una carga de trabajo experimenta cambios rápidos en el rendimiento. El techo podría ser superado en hasta un 50% para manejar las ráfagas.



The throughput ceiling for workload 2 ensures that it does not “bully” workloads 1 and 3.

Pisos de rendimiento

Un piso de rendimiento garantiza que el rendimiento de una carga de trabajo no esté por debajo del número mínimo de IOPS. En la siguiente figura, los pisos de rendimiento de la carga de trabajo 1 y la carga de trabajo 3 garantizan que cumplen los objetivos de rendimiento mínimos, sin importar la demanda por carga de trabajo 2.



Tal y como sugieren los ejemplos, un límite máximo de rendimiento limita el rendimiento directamente. Un entorno de rendimiento limita el rendimiento de forma indirecta, al dar prioridad a las cargas de trabajo para las que se ha establecido un piso.

Una carga de trabajo representa las operaciones de I/O para un volumen, LUN o, comenzando por ONTAP 9.3, archivo. Un grupo de políticas que define un piso de rendimiento no se puede aplicar a una SVM. Puede especificar la planta al crear el grupo de políticas, o bien esperar hasta que supervise las cargas de trabajo para especificarlas.



El rendimiento de una carga de trabajo puede caer por debajo de la superficie especificada si no hay suficiente capacidad de rendimiento (margen adicional) en el nodo o el agregado, o durante operaciones críticas como `volume move trigger-cutover`. Incluso cuando hay suficiente capacidad disponible y no se realizan operaciones críticas, el rendimiento de una carga de trabajo puede estar por debajo del nivel especificado hasta en un 5 %.



The throughput floors for workload 1 and workload 3 ensure that they meet minimum throughput targets, regardless of demand by workload 2.

Calidad de servicio adaptativa

Por lo general, el valor del grupo de políticas que asigna a un objeto de almacenamiento es fijo. Es necesario cambiar el valor de forma manual cuando cambia el tamaño del objeto de almacenamiento. Por ejemplo, un aumento de la cantidad de espacio utilizado en un volumen requiere, por lo general, un aumento correspondiente en el techo de rendimiento especificado para el volumen.

Adaptive QoS escala automáticamente el valor del grupo de políticas al tamaño de la carga de trabajo, y mantiene la ratio de IOPS en TB|GB a medida que cambia el tamaño de la carga de trabajo. Esto es una ventaja importante si gestiona cientos o miles de cargas de trabajo en una puesta en marcha grande.

Normalmente, la calidad de servicio adaptativa se puede utilizar para ajustar los techos de rendimiento, pero también para gestionar el uso de pisos de rendimiento (cuando aumenta el tamaño de la carga de trabajo). El tamaño de la carga de trabajo se expresa como el espacio asignado para el objeto de almacenamiento o el espacio utilizado por el objeto de almacenamiento.



El espacio usado está disponible para pisos de rendimiento en ONTAP 9.5 y versiones posteriores. No se admite para pisos de rendimiento en ONTAP 9.4 y versiones anteriores.

+

A partir de ONTAP 9.13.1, puede utilizar la calidad de servicio adaptativa para establecer pisos y techos de rendimiento en el nivel de la SVM.

- Una política de *espacio* mantiene la ratio de IOPS/TB|GB según el tamaño nominal del objeto de almacenamiento. Si la relación es de 100 IOPS/GB, un volumen de 150 GB tendrá un techo de rendimiento de 15,000 IOPS mientras el volumen siga siendo de ese tamaño. Si el tamaño del volumen cambia a 300 GB, la calidad de servicio adaptativa ajusta el techo de rendimiento a 30,000 IOPS.
- Una política de *space* utilizada (predeterminada) mantiene la relación IOPS/TB|GB según la cantidad de datos reales almacenados antes de las eficiencias de almacenamiento. Si la relación es de 100 IOPS/GB, un volumen de 150 GB que tiene 100 GB de datos almacenados tendría un límite máximo de rendimiento de 10,000 IOPS. A medida que cambia la cantidad de espacio usado, la calidad de servicio adaptativa ajusta el techo de rendimiento en función de la ratio.

Replicación

Copias Snapshot

Tradicionalmente, las tecnologías de replicación de ONTAP aumentaban las necesidades de recuperación ante desastres y archivado de datos. Con la llegada de los servicios cloud, la replicación de ONTAP se ha adaptado a la transferencia de datos entre los extremos del Data Fabric de NetApp. La base de todos estos usos es la tecnología Snapshot de ONTAP.

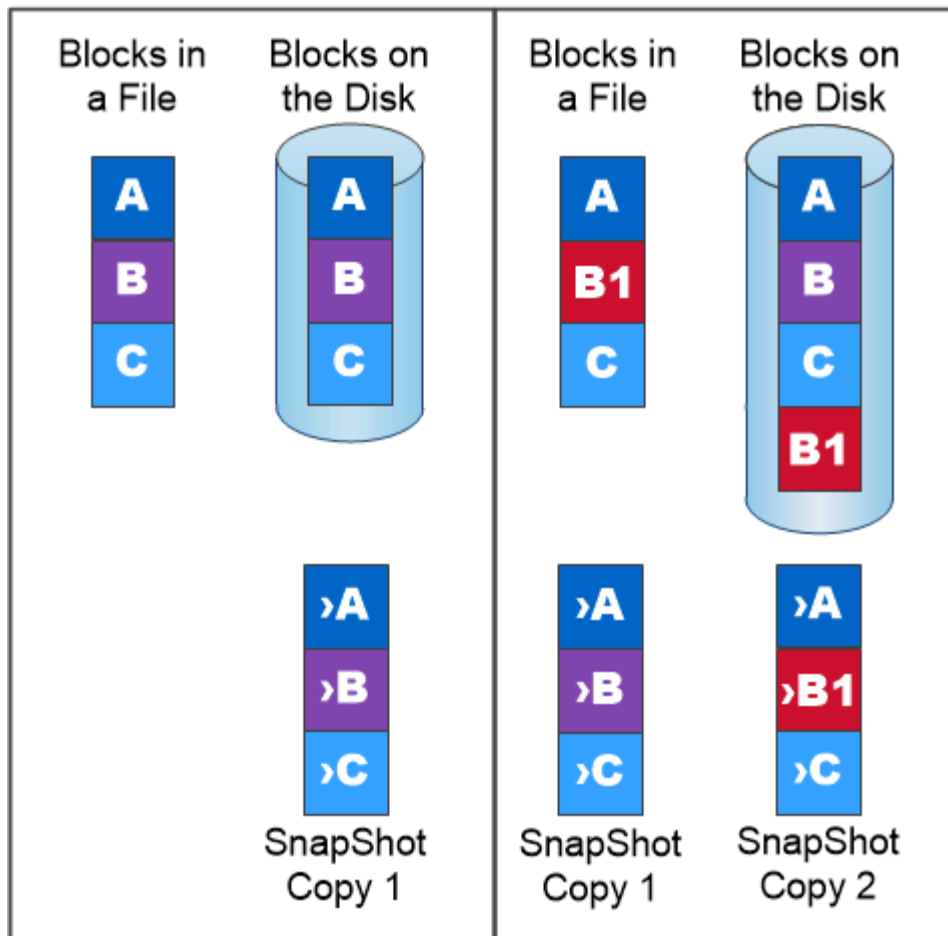
Una *Snapshot copy* es una imagen puntual de solo lectura de un volumen. Una vez creada la copia snapshot, el sistema de archivos activo y la copia snapshot apuntan a los mismos bloques de disco; por lo tanto, la copia snapshot no utiliza espacio en disco extra. Con el tiempo, la imagen consume un espacio de almacenamiento mínimo y apenas tiene una sobrecarga de rendimiento, ya que solo registra los cambios en los archivos desde que se realizó la última copia Snapshot.

Las copias Snapshot deben su eficiencia a la tecnología de virtualización del almacenamiento central de ONTAP, su *Write Anywhere File Layout (WAFL)*. como una base de datos, WAFL utiliza metadatos para dirigir los bloques de datos reales en el disco. Sin embargo, a diferencia de una base de datos, WAFL no sobrescribe los bloques existentes. Escribe los datos actualizados en un bloque nuevo y cambia los metadatos.

Las copias Snapshot son eficientes porque, en lugar de copiar bloques de datos, ONTAP hace referencia a los metadatos cuando se crea una copia Snapshot. De este modo, se elimina el «tiempo de búsqueda» que suponen otros sistemas para localizar los bloques que se van a copiar y el coste de realizar la propia copia.

Puede utilizar una copia Snapshot para recuperar archivos o LUN individuales, o bien para restaurar el contenido completo de un volumen. ONTAP compara la información de punteros de la copia Snapshot con los datos del disco para reconstruir el objeto faltante o dañado, sin tiempo de inactividad ni un coste de rendimiento significativo.

Una *Snapshot policy* define el modo en que el sistema crea copias Snapshot de los volúmenes. La política especifica cuándo se deben crear las copias Snapshot, cuántas copias se deben conservar, cómo se debe asignar un nombre a ellas y cómo etiquetarlas para la replicación. Por ejemplo, un sistema podría crear una copia snapshot todos los días a las 12:10, conservar las dos copias más recientes, nombrarlas «día» (anexadas con fecha de hora) y etiquetarlas «día» para la replicación.



A Snapshot copy records only changes to the active file system since the last Snapshot copy.

Recuperación ante desastres y transferencia de datos con SnapMirror

SnapMirror es la tecnología de recuperación ante desastres diseñada para la conmutación al nodo de respaldo del almacenamiento principal al secundario en un sitio geográficamente remoto. Como su nombre indica, SnapMirror crea una réplica, o *mirror*, de sus datos de trabajo en el almacenamiento secundario desde el cual puede continuar proporcionando datos en caso de catástrofe en el sitio principal.

Los datos se reflejan en el nivel de volumen. La relación entre el volumen de origen del almacenamiento primario y el volumen de destino del almacenamiento secundario se denomina «relación de protección de datos». Los clústeres en los que residen los volúmenes y las SVM que sirven datos de los volúmenes deben tener una relación entre iguales. Una relación entre iguales permite que los clústeres y las SVM se intercambien datos con seguridad.



También puede crear una relación de protección de datos entre las SVM. En este tipo de relación, se replica toda la configuración de la SVM, desde las exportaciones de NFS y los recursos compartidos de SMB hasta RBAC, así como los datos en los volúmenes que posee la SVM.

A partir de ONTAP 9.10.1, se pueden crear relaciones de protección de datos entre bloques de S3 mediante

SnapMirror S3. Los bloques de destino pueden estar en sistemas ONTAP locales o remotos, o en sistemas que no sean ONTAP, como StorageGRID y AWS.

La primera vez que se invoca SnapMirror, se realiza una transferencia *baseline* del volumen de origen al volumen de destino. La transferencia inicial suele consistir en los siguientes pasos:

- Haga una copia Snapshot del volumen de origen.
- Transfiera la copia Snapshot y todos los bloques de datos que hace referencia al volumen de destino.
- Transferir las copias snapshot restantes y menos recientes del volumen de origen al volumen de destino para su uso en caso de que el espejo «activo» esté dañado.

Una vez finalizada la transferencia completa, SnapMirror solo transfiere las nuevas copias Snapshot al duplicado. Las actualizaciones son asíncronas, según la programación configurada. La retención refleja la política de Snapshot en el origen. Se puede activar el volumen de destino con una interrupción mínima en caso de desastre en el sitio primario y reactivar el volumen de origen cuando el servicio se restaure.

Dado que SnapMirror solo transfiere copias Snapshot una vez que se haya creado la configuración básica, la replicación es rápida y no disruptiva. Como se indica en el caso de uso de conmutación por error, las controladoras del sistema secundario deben ser equivalentes o casi equivalentes a las controladoras del sistema primario para servir datos de forma eficiente desde el almacenamiento reflejado.



A SnapMirror data protection relationship mirrors the Snapshot copies available on the source volume.

uso de SnapMirror para la transferencia de datos

También se puede usar SnapMirror para replicar datos entre extremos en el Data Fabric de NetApp. Puede elegir entre una replicación que desee o una replicación recurrente al crear la política de SnapMirror.

Backups de cloud de SnapMirror en almacenamiento de objetos

SnapMirror Cloud es una tecnología de backup y recuperación diseñada para los usuarios de ONTAP que desean realizar la transición de sus flujos de trabajo de protección de datos al cloud. Las organizaciones que abandonen las arquitecturas de

backup a cinta heredadas pueden utilizar almacenamiento de objetos como repositorio alternativo para su retención y archivado de datos a largo plazo. SnapMirror Cloud proporciona replicación de almacenamiento de ONTAP a objetos como parte de una estrategia de backup incremental permanente.

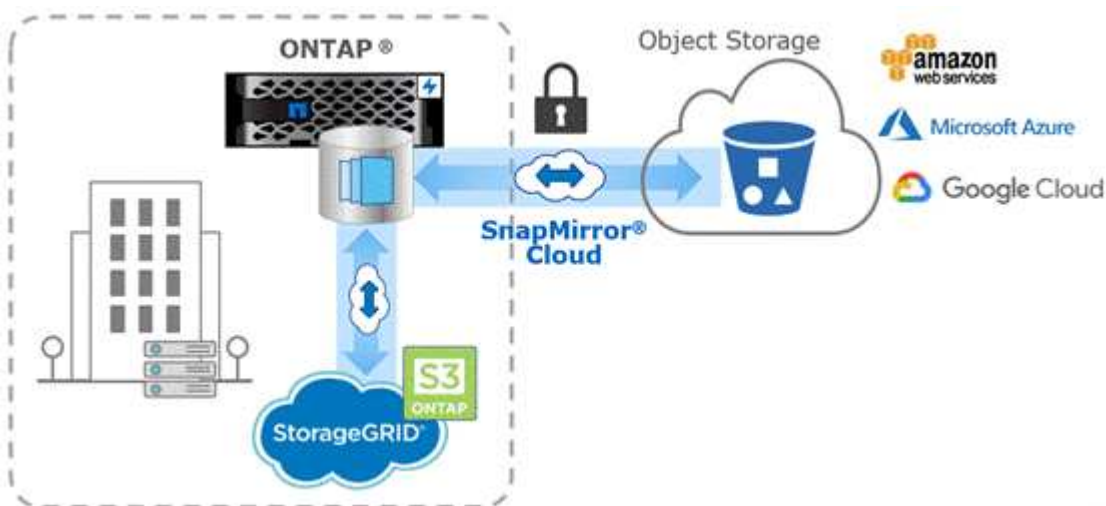
SnapMirror Cloud se introdujo en ONTAP 9.8 como extensión de la familia de tecnologías de replicación de SnapMirror. Aunque SnapMirror se usa frecuentemente para realizar backups de ONTAP a ONTAP, SnapMirror Cloud usa el mismo motor de replicación para transferir copias Snapshot para ONTAP a backups de almacenamiento de objetos compatibles con S3.

SnapMirror Cloud, destinado a casos de uso de backup, es compatible con flujos de trabajo de retención a largo plazo y de archivos. Al igual que sucede con SnapMirror, el backup inicial de SnapMirror Cloud realiza una transferencia básica de un volumen. Para posteriores backups, SnapMirror Cloud genera una copia Snapshot del volumen de origen y transfiere la copia Snapshot con solo los bloques de datos modificados a un destino de almacenamiento de objetos.

Las relaciones de SnapMirror Cloud pueden configurarse entre sistemas ONTAP y seleccionar objetivos de almacenamiento de objetos en las instalaciones y en el cloud público, como Amazon S3, Google Cloud Storage y Microsoft Azure Blob Storage. Otros destinos de almacenamiento de objetos on-premises incluyen StorageGRID y ONTAP S3.

La replicación en cloud de SnapMirror es una función con licencia de ONTAP y requiere una aplicación aprobada para orquestar los flujos de trabajo de protección de datos. Existen varias opciones de orquestación para gestionar los backups de SnapMirror Cloud:

- Varios partners de backup de terceros que ofrecen compatibilidad con la replicación del cloud de SnapMirror. Los proveedores participantes están disponibles en la ["Blog de NetApp"](#).
- Backup y recuperación de BlueXP para una solución nativa de NetApp para entornos de ONTAP
- API para desarrollar software personalizado para los flujos de trabajo de protección de datos o para aprovechar herramientas de automatización



Archivado SnapVault

La licencia de SnapMirror se usa para admitir tanto las relaciones de SnapVault para backup como las relaciones de SnapMirror para la recuperación ante desastres. A partir de ONTAP 9.3, las licencias de SnapVault quedan obsoletas y se pueden usar las

licencias de SnapMirror para configurar relaciones de almacén, mirroring y reflejo y almacén. La replicación de SnapMirror se utiliza para la replicación de ONTAP-to-ONTAP de copias Snapshot, ya que admite casos prácticos de backup y recuperación ante desastres.

SnapVault es la tecnología de archivado, diseñada para la replicación de copias snapshot disco a disco para el cumplimiento de normativas y otros fines relacionados con la gobernanza. A diferencia de la relación de SnapMirror, en la que el destino normalmente solo contiene las copias Snapshot que actualmente se encuentran en el volumen de origen, un destino de SnapVault normalmente conserva las copias Snapshot puntuales creadas durante un período mucho más largo.

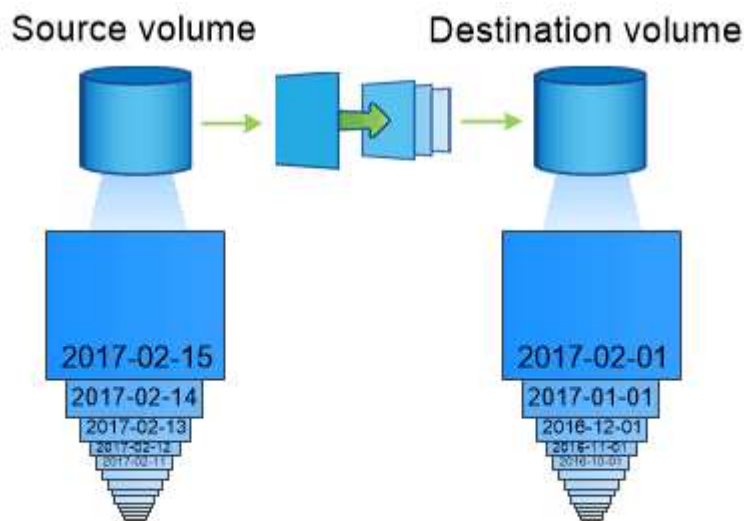
Es posible que desee conservar copias Snapshot mensuales de sus datos en un plazo de 20 años, por ejemplo, para cumplir con las normativas de contabilidad gubernamental de su empresa. Como no hay necesidad de servir datos desde un almacenamiento de almacén, puede utilizar discos más lentos y menos costosos en el sistema de destino.

Al igual que sucede con SnapMirror, SnapVault realiza una transferencia de referencia la primera vez que se invoca. Realiza una copia Snapshot del volumen de origen y, a continuación, transfiere la copia y los bloques de datos que hace referencia al volumen de destino. A diferencia de SnapMirror, SnapVault no incluye copias Snapshot anteriores en la configuración básica.

Las actualizaciones son asíncronas, según la programación configurada. Las reglas que defina en la política para la relación identifican qué nuevas copias Snapshot deben incluir en las actualizaciones y cuántas copias deben retener. Las etiquetas definidas en la política ("mensual", por ejemplo) deben coincidir con una o más etiquetas definidas en la política de Snapshot en la fuente. De lo contrario, la replicación falla.



SnapMirror y SnapVault comparten la misma infraestructura de comandos. Especifique el método que desea utilizar al crear una directiva. Ambos métodos requieren clústeres con una relación entre iguales y SVM.



A SnapVault data protection relationship typically retains point-in-time Snapshot copies created over a longer period than the Snapshot copies on the source volume.

Backup en el cloud y compatibilidad con backups tradicionales

Además de las relaciones de protección de datos de SnapMirror y SnapVault, que eran de disco a disco sólo para ONTAP 9,7 y versiones anteriores, ahora hay varias soluciones de backup que ofrecen una alternativa más económica para la retención de datos a largo plazo.

Numerosas aplicaciones de protección de datos de terceros ofrecen backup tradicional para datos gestionados con ONTAP. Veeam, Veritas y CommVault, entre otros, ofrecen backup integrado para sistemas ONTAP.

A partir de ONTAP 9.8, SnapMirror Cloud proporciona la replicación asíncrona de copias Snapshot de instancias de ONTAP a extremos de almacenamiento de objetos. La replicación cloud de SnapMirror requiere una aplicación con licencia para coordinar y gestionar los flujos de trabajo de protección de datos. Las relaciones de SnapMirror Cloud son compatibles con los sistemas de ONTAP para seleccionar objetivos de almacenamiento de objetos en las instalaciones y en el cloud público, incluidos AWS S3, Google Cloud Storage Platform o Microsoft Azure Blob Storage, lo que proporciona una eficiencia mejorada con el software de backup de proveedores. Póngase en contacto con su representante de NetApp para obtener una lista de aplicaciones certificadas y proveedores de almacenamiento de objetos compatibles.

Si está interesado en la protección de datos nativos del cloud, puede utilizar BlueXP para configurar las relaciones de SnapMirror o SnapVault entre volúmenes de las instalaciones y instancias de Cloud Volumes ONTAP en el cloud público.

BlueXP también ofrece copias de seguridad de instancias de Cloud Volumes ONTAP utilizando un modelo de software como servicio (SaaS). Los usuarios pueden realizar backups de sus instancias de Cloud Volumes ONTAP en un almacenamiento de objetos en cloud público compatible con S3 y S3 utilizando Cloud Backup que se encuentra en Cloud Central de NetApp.

["Recursos de documentación de Cloud Volumes ONTAP y BlueXP"](#)

["Cloud Central de NetApp"](#)

Disponibilidad continua de MetroCluster

Las configuraciones de MetroCluster protegen los datos mediante la implementación de dos clústeres duplicados y físicamente independientes. Cada clúster replica de forma síncrona los datos y la configuración de SVM del otro. En caso de desastre en un sitio, un administrador puede activar la SVM duplicada y comenzar a servir datos desde el sitio superviviente.

- *Las configuraciones MetroCluster* de conexión a la estructura admiten clústeres de todo el área metropolitana.
- *Stretch MetroCluster* las configuraciones admiten clústeres de todo el campus.

Los clústeres deben tener una relación entre iguales en cualquiera de los casos.

MetroCluster utiliza una función de ONTAP denominada *SyncMirror* para reflejar de forma síncrona datos de agregados para cada clúster en copias o *plexes*, en el almacenamiento del otro clúster. Si se produce una conmutación, el plex remoto del clúster superviviente se conecta y la SVM secundaria comienza a servir datos.



When a MetroCluster switchover occurs, the remote plex on the surviving cluster comes online and the secondary SVM begins serving data.

Usando SyncMirror en implementaciones que no sean de MetroCluster

Opcionalmente, puede utilizar SyncMirror en una implementación no perteneciente a MetroCluster para proteger contra la pérdida de datos si fallan más discos que el tipo de RAID protege, o si se produce una pérdida de conectividad con discos de grupo RAID. La función solo está disponible para parejas de alta disponibilidad.

Los datos agregados se reflejan en complejos almacenados en diferentes bandejas de discos. Si una de las bandejas no está disponible, el plex no afectado sigue sirviendo datos mientras se soluciona la causa del fallo.

Tenga en cuenta que un agregado con mirroring SyncMirror requiere el doble de almacenamiento que un agregado no reflejado. Cada complejo requiere tantos discos como el complejo que refleja. Se necesitarían 2,880 GB de espacio en disco, por ejemplo, para reflejar un agregado de 1,440 GB, 1,440 GB para cada plex.

Con SyncMirror, le recomendamos que mantenga al menos un 20 % de espacio libre para agregados reflejados para optimizar el rendimiento y la disponibilidad del almacenamiento. Aunque la recomendación es del 10% para agregados no duplicados, el sistema de archivos puede utilizar el 10% adicional del espacio para absorber cambios incrementales. Los cambios incrementales aumentan el aprovechamiento del espacio para agregados reflejados gracias a la arquitectura basada en Snapshot de copia en escritura de ONTAP. Si no se siguen estas prácticas recomendadas, puede tener un impacto negativo en el rendimiento de resincronización de SyncMirror, lo que afecta indirectamente a los flujos de trabajo operativos, como NDU en puestas en marcha de cloud no compartidas y conmutación de estado para puestas en marcha de MetroCluster.



SyncMirror también está disponible para implementaciones de virtualización de FlexArray.

Eficiencia del almacenamiento

Información general de la eficiencia del almacenamiento de ONTAP

La eficiencia de almacenamiento mide en qué medida un sistema de almacenamiento utiliza el espacio disponible al optimizar los recursos de almacenamiento, minimizar el espacio desperdiciado y reducir el espacio físico de los datos escritos. Una mayor eficacia de almacenamiento le permite almacenar la cantidad máxima de datos en el menor espacio posible y al menor coste posible. Por ejemplo, el uso de tecnologías de eficiencia del almacenamiento que detectan y eliminan los bloques de datos duplicados y los bloques de datos llenos de ceros reduce la cantidad general de almacenamiento físico que necesita y reduce el coste general.

ONTAP ofrece una amplia gama de tecnologías de eficiencia del almacenamiento que reducen la cantidad de almacenamiento en cloud o hardware físico que consumen sus datos y también producen importantes mejoras en el rendimiento del sistema, como lecturas más rápidas de datos, copias más rápidas de conjuntos de datos y un aprovisionamiento más rápido de máquinas virtuales.

Las tecnologías de eficiencia de almacenamiento de ONTAP incluyen:

- **Thin Provisioning**

[Aprovisionamiento ligero](#) Permite asignar almacenamiento en un volumen o LUN a medida que es necesario, en lugar de reservar con antelación. Esto reduce la cantidad de almacenamiento físico que

necesita al permitirle sobreasignar sus volúmenes o LUN en función del uso potencial sin reservar espacio que no se esté utilizando actualmente.

- **Deduplicación**

Deduplicación reduce la cantidad de almacenamiento físico necesario para un volumen de tres maneras distintas.

- **Deduplicación de bloques cero**

La deduplicación de bloque cero detecta y elimina los bloques de datos llenos con todos los ceros y solo actualiza los metadatos. Se ahorra entonces un 100% del espacio utilizado por bloques cero. La deduplicación de bloque cero está habilitada de forma predeterminada en todos los volúmenes deduplicados.

- **Desduplicación en línea**

La deduplicación inline detecta los bloques de datos duplicados y los reemplaza con referencias a un bloque compartido único antes de escribir los datos en el disco. La deduplicación en línea acelera el aprovisionamiento de las máquinas virtuales entre un 20 % y un 30 %. En función de su versión de ONTAP y de su plataforma, la deduplicación inline está disponible en el nivel del volumen o el agregado. Está activado de forma predeterminada en los sistemas AFF y ASA. Debe habilitar la deduplicación inline manualmente en sistemas FAS.

- **Deduplicación de fondo**

La deduplicación en segundo plano también detecta los bloques de datos duplicados y los sustituye con referencias a un bloque compartido único, pero mejora aún más la eficiencia del almacenamiento, ya que lo hace después de escribir los datos en el disco. Puede configurar la deduplicación en segundo plano para que se ejecute cuando se cumplan determinados criterios en el sistema de almacenamiento. Por ejemplo, puede activar la deduplicación en segundo plano cuando el volumen alcanza un 10% de utilización. También puede activar manualmente la deduplicación en segundo plano o configurarla para que se ejecute en una programación específica. Está activado de forma predeterminada en los sistemas AFF y ASA. Debe habilitar manualmente la deduplicación en segundo plano en sistemas FAS.

Es compatible con la deduplicación en volúmenes y entre volúmenes dentro de un agregado. Las lecturas de datos deduplicados normalmente no conllevan cargos por el rendimiento.

- **Compresión**

Compresión reduce la cantidad de almacenamiento físico necesario para un volumen combinando bloques de datos en grupos de compresión, cada uno de los cuales se almacena como un único bloque. Cuando se recibe una solicitud de lectura o sobrescritura, sólo se lee un pequeño grupo de bloques, no el archivo completo. Este proceso optimiza el rendimiento de lectura y sobrescritura y permite una mayor escalabilidad del tamaño de los archivos que se van a comprimir.

La compresión se puede ejecutar online o postprocesamiento. La compresión en línea proporciona un ahorro de espacio inmediato al comprimir los datos de la memoria antes de escribirse en el disco. La compresión de postprocesamiento escribe en primer lugar los bloques en el disco sin comprimir y a continuación comprime los datos en un momento programado. Debe activar manualmente la compresión.

- **Compacción**

La compactación reduce la cantidad de almacenamiento físico necesario para un volumen, tomando fragmentos de datos almacenados en bloques de 4 KB, pero con un tamaño inferior a 4 KB y

combinándolos en un único bloque. La compactación se produce mientras los datos siguen en la memoria, por lo que nunca se consume espacio innecesario en los discos. Está activado de forma predeterminada en los sistemas AFF y ASA. Debe habilitar la compactación manualmente en sistemas FAS.

- **Volúmenes FlexClone, archivos y LUN**

Tecnología FlexClone Aprovecha los metadatos de las copias Snapshot para crear copias puntuales editables de un volumen, archivo o LUN. Las copias comparten bloques de datos con sus principales, no consumen almacenamiento salvo lo necesario para los metadatos hasta que se escriban cambios en una copia o en su principal. Cuando se escribe un cambio, solo se almacena el delta.

Mientras que las copias de conjuntos de datos tradicionales pueden tardar en crearse en minutos o incluso horas, la tecnología FlexClone permite copiar incluso los conjuntos de datos más grandes casi al instante.

- * Eficiencia de almacenamiento sensible a la temperatura*

ONTAP proporciona "eficiencia del almacenamiento sensible a la temperatura" beneficios al evaluar la frecuencia con la que se accede a los datos de su volumen y asignar esa frecuencia al grado de compresión aplicado a esos datos. En el caso de los datos inactivos a los que se accede con poca frecuencia, se comprimen los bloques de datos más grandes, y en el caso de los datos activos, a los que se accede con frecuencia y se sobrescriben con mayor frecuencia, se comprimen los bloques de datos más pequeños, lo que hace que el proceso sea más eficiente.

La eficiencia del almacenamiento sensible a la temperatura (TSSE) se introduce en ONTAP 9,8 y se activa automáticamente en los volúmenes AFF con Thin Provisioning recientemente creados.

Puede obtener el beneficio de estas tecnologías en sus operaciones diarias con el mínimo esfuerzo. Por ejemplo, suponga que necesita proporcionar a 5.000 usuarios almacenamiento para directorios iniciales y estima que el espacio máximo necesario para cualquier usuario es de 1 GB. Puede reservar un agregado de 5 TB por adelantado para satisfacer la necesidad total de almacenamiento potencial. Sin embargo, también sabe que los requisitos de capacidad del directorio inicial varían considerablemente en cada organización. En lugar de reservar 5 TB de espacio total para su organización, puede crear un agregado de 2 TB. Luego, puede utilizar thin provisioning para asignar nominalmente 1 GB de almacenamiento a cada usuario, pero para asignar el almacenamiento únicamente según sea necesario. Puede supervisar de forma activa el agregado a lo largo del tiempo y aumentar el tamaño físico real según sea necesario.

En otro ejemplo, supongamos que utiliza una infraestructura de puestos de trabajo virtuales (VDI) con una gran cantidad de datos duplicados en sus escritorios virtuales. La deduplicación reduce el uso del almacenamiento eliminando automáticamente los bloques de información duplicados en la infraestructura de puestos de trabajo virtuales y sustituyéndolos por un puntero al bloque original. Otras tecnologías de eficiencia del almacenamiento de ONTAP, como la compresión, también pueden ejecutarse en segundo plano sin su intervención.

La tecnología de creación de particiones de disco de ONTAP también permite una mayor eficiencia del almacenamiento. La tecnología de RAID DP ofrece protección frente a un fallo de dos discos sin sacrificar el rendimiento ni incrementar los gastos generales de mirroring de discos. La creación de particiones SSD avanzada con ONTAP 9 aumenta la capacidad de uso en casi un 20 %.

NetApp proporciona las mismas funciones de eficiencia de almacenamiento que hay disponibles con ONTAP en las instalaciones en el cloud. Cuando migra datos desde el almacenamiento ONTAP on-premises a la nube, se conserva la eficiencia del almacenamiento existente. Por ejemplo, suponga que tiene una base de datos de SQL que contiene datos críticos para el negocio que desea pasar de un sistema local al cloud. Puedes utilizar la replicación de datos en BlueXP para migrar tus datos y, como parte del proceso de migración, puedes habilitar la última política de las instalaciones para las copias de Snapshot en la nube.

Aprovisionamiento ligero

ONTAP ofrece una amplia gama de tecnologías de eficiencia del almacenamiento además de copias Snapshot. Las tecnologías clave incluyen thin provisioning, deduplicación, compresión y volúmenes FlexClone, archivos Y LUN. Al igual que las copias Snapshot, todas se basan en el sistema de archivos Write Anywhere File Layout (WAFL) de ONTAP.

Un volumen o LUN con aprovisionamiento ligero es uno para el cual no se reserva almacenamiento con anterioridad. En su lugar, el almacenamiento se asigna de forma dinámica conforme se necesita. El espacio libre se libera de nuevo al sistema de almacenamiento cuando se eliminan datos en el volumen o LUN.

Imagine que su organización necesita suministrar a 5,000 usuarios almacenamiento para directorios iniciales. Usted estima que los directorios de inicio más grandes consumirá 1 GB de espacio.

En este caso, podría adquirir 5 TB de almacenamiento físico. Por cada volumen que almacena un directorio particular, reservaría suficiente espacio para satisfacer las necesidades de los mayores consumidores.

Como cuestión práctica, sin embargo, usted también sabe que los requisitos de capacidad del directorio del hogar varían mucho en toda su comunidad. Por cada gran usuario de almacenamiento, hay diez que consumen poco espacio o ningún.

El thin provisioning le permite satisfacer las necesidades de los grandes consumidores de almacenamiento sin tener que adquirir almacenamiento que podría no utilizar nunca. Dado que el espacio de almacenamiento no se asigna hasta que se consume, se puede «almacenar en exceso» un agregado de 2 TB asignando inicialmente un tamaño de 1 GB a cada uno de los 5,000 volúmenes que contiene el agregado.

Siempre que sea correcto, mantenga una tasa de 10:1 de luz a usuarios habituales y siempre que asuma un rol activo en la supervisión del espacio libre en el agregado, puede estar seguro de que no fallará la escritura del volumen debido a la falta de espacio.

Deduplicación

Deduplication reduce la cantidad de almacenamiento físico necesario para un volumen (o todos los volúmenes de un agregado AFF) al desechar los bloques duplicados y sustituirlos por referencias a un único bloque compartido. Las lecturas de datos deduplicados normalmente no conllevan cargos por el rendimiento. Las escrituras conllevan una carga mínima, excepto en los nodos sobrecargados.

A medida que se escriben los datos durante su uso normal, WAFL utiliza un proceso por lotes para crear un catálogo de *firmas de bloque*. una vez que se inicia la deduplicación, ONTAP compara las firmas del catálogo para identificar los bloques duplicados. Si existe una coincidencia, se realiza una comparación byte por byte para verificar que los bloques candidatos no han cambiado desde que se creó el catálogo. Solo si la coincidencia de todos los bytes es el bloque duplicado descartado y se ha reclamado el espacio en disco.



Deduplication reduces the amount of physical storage required for a volume by discarding duplicate data blocks.

Compresión

Compression reduce la cantidad de almacenamiento físico necesario para un volumen al combinar bloques de datos en *grupos de compresión*, cada uno de los cuales se almacena como un único bloque. Las lecturas de datos comprimidos son más rápidas que con los métodos de compresión tradicionales porque ONTAP descomprime solo los grupos de compresión que contienen los datos solicitados, en lugar de un archivo o una LUN completos.

Puede realizar compresión en línea o de postprocesamiento, por separado o en combinación:

- *Inline compression* comprime los datos en la memoria antes de escribirlos en el disco, lo que reduce considerablemente la cantidad de I/O de escritura en un volumen, pero potencialmente degradará el rendimiento de escritura. Las operaciones de rendimiento intensivo se aplazan hasta la siguiente operación de compresión de postprocesamiento, si la hubiera.
- *Compresión de postprocesamiento* comprime los datos después de que se escriben en el disco con la misma programación que la deduplicación.

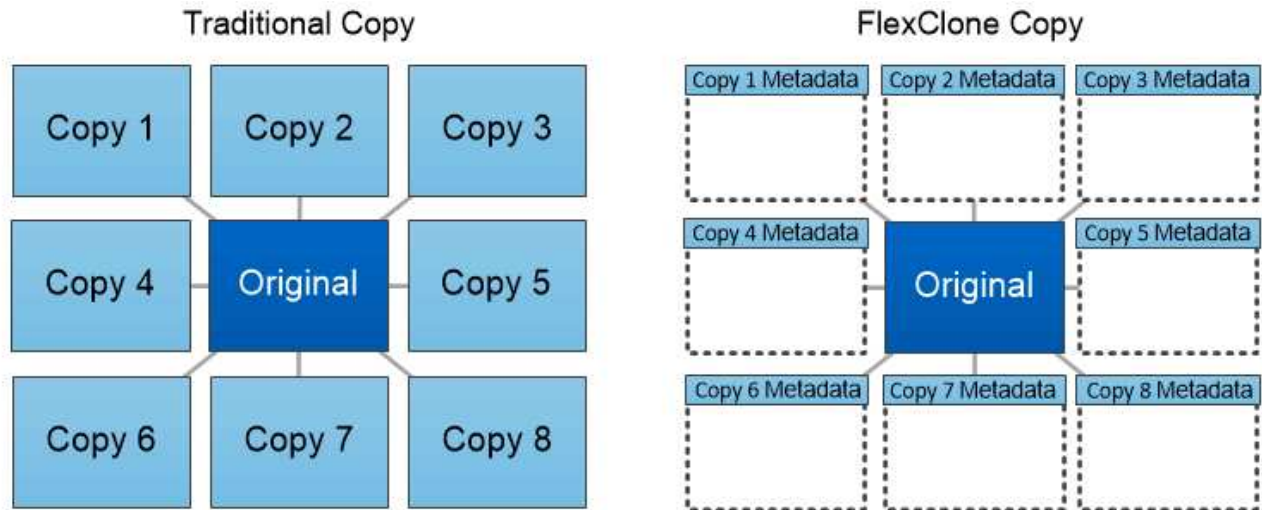
compactación de datos inline los archivos pequeños o E/S acolchados con ceros se almacenan en un bloque de 4 KB, independientemente de si requieren o no 4 KB de almacenamiento físico. *Compactación de datos inline* combina fragmentos de datos que normalmente consumirían varios bloques de 4 KB en un único bloque de 4 KB en el disco. La compactación se realiza mientras los datos siguen en la memoria, por lo que es la mejor opción para controladoras más rápidas.

Volúmenes, archivos y LUN FlexClone

La tecnología *FlexClone* hace referencia a los metadatos de Snapshot para crear copias puntuales y editables de un volumen. Las copias comparten bloques de datos con sus padres, sin consumir almacenamiento, excepto lo que se necesita para los metadatos hasta que se escriben los cambios en la copia. Los archivos FlexClone y las LUN FlexClone utilizan tecnología idéntica, a excepción de que no es necesaria una copia snapshot que realice un backup.

Cuando se pueden crear copias tradicionales en minutos o incluso horas, el software FlexClone le permite copiar incluso los conjuntos de datos más grandes de forma casi instantánea. Esto lo convierte en la opción ideal para las situaciones en las que necesita varias copias de conjuntos de datos idénticos (una puesta en marcha de puestos de trabajo virtuales, por ejemplo) o copias temporales de un conjunto de datos (probar una aplicación contra un conjunto de datos de producción).

Puede clonar un volumen FlexClone existente, clonar un volumen que contenga clones de LUN o clonar datos de mirroring y almacén. Puede *dividir* un volumen FlexClone de su principal, en cuyo caso, la copia tiene asignado su propio almacenamiento.



FlexClone copies share data blocks with their parents, consuming no storage except what is required for metadata.

Mediciones de capacidad en System Manager

La capacidad del sistema se puede medir como espacio físico o como espacio lógico. A partir de ONTAP 9.7, System Manager proporciona mediciones de la capacidad física y lógica.

Las diferencias entre las dos mediciones se explican en las siguientes descripciones:

- **Capacidad física:** El espacio físico se refiere a los bloques físicos de almacenamiento utilizados en el volumen o nivel local. El valor de la capacidad física utilizada suele ser menor que el valor de la capacidad lógica utilizada debido a la reducción de datos de funciones de eficiencia del almacenamiento (como la deduplicación y la compresión).
- **Capacidad lógica:** El espacio lógico se refiere al espacio utilizable (los bloques lógicos) en un volumen o nivel local. El espacio lógico hace referencia a cómo se puede utilizar el espacio teórico, sin tener en cuenta los resultados de la deduplicación o la compresión. El valor del espacio lógico utilizado procede de la cantidad de espacio físico utilizado más el ahorro derivado de las funciones de eficiencia del almacenamiento (como la deduplicación y compresión) que se han configurado. Esta medición suele ser mayor que la capacidad física utilizada porque incluye copias Snapshot, clones y otros componentes, y no refleja la compresión de datos ni otras reducciones del espacio físico. Por lo tanto, la capacidad lógica total podría ser mayor que el espacio provisionado.



En System Manager, las representaciones de capacidad no dan cuenta de las capacidades de niveles de almacenamiento raíz (agregado).

Mediciones de capacidad utilizada

Las mediciones de la capacidad utilizada se muestran de forma diferente según la versión de System Manager que se esté usando, como se explica en la siguiente tabla:

| La versión de System Manager | Término utilizado para capacidad | El tipo de capacidad a la que se hace referencia |
|------------------------------|----------------------------------|---|
| 9.9.1 y posterior | Lógica utilizada | El espacio lógico utilizado si se habilitó la configuración de eficiencia del almacenamiento) |
| 9.7 y 9.8 | Utilizado | El espacio lógico utilizado (si se ha habilitado la configuración de eficiencia del almacenamiento) |
| 9,5 y 9,6 (Vista clásica) | Utilizado | El espacio físico utilizado |

Términos de medición de capacidad

Los siguientes términos se utilizan cuando se describe la capacidad:

- **Capacidad asignada:** La cantidad de espacio que se ha asignado para volúmenes en una VM de almacenamiento.
- **Disponible:** La cantidad de espacio físico disponible para almacenar datos o para aprovisionar volúmenes en una VM de almacenamiento o en un nivel local.
- **Capacidad en volúmenes:** La suma del almacenamiento usado y el almacenamiento disponible de todos los volúmenes en una VM de almacenamiento.
- **Datos del cliente:** La cantidad de espacio utilizado por los datos del cliente (ya sea físico o lógico).
 - A partir de ONTAP 9.13.1, la capacidad utilizada por los datos del cliente se conoce como **Lógica utilizada**, y la capacidad utilizada por las copias snapshot se muestra por separado.
 - En ONTAP 9.12.1 y versiones anteriores, la capacidad utilizada por los datos del cliente añadidos a la capacidad utilizada por las copias snapshot se denomina **Lógica usada**.
- **Comprometido:** La cantidad de capacidad comprometida para un nivel local.
- **Reducción de datos:**
 - A partir de ONTAP 9.13.1, las relaciones de reducción de datos se muestran de la siguiente manera:
 - El valor de reducción de datos que se muestra en el panel **Capacity** es la relación entre el espacio utilizado lógico y el espacio físico utilizado sin tener en cuenta las reducciones significativas que se obtienen al utilizar funciones de eficiencia del almacenamiento, como las copias Snapshot.
 - Al mostrar el panel de detalles, verá tanto la relación que se muestra en el panel de vista general como la relación general de todos los espacios utilizados lógicos en comparación con el espacio utilizado físico. Este valor, conocido como **con las copias Snapshot**, incluye los beneficios derivados del uso de las copias Snapshot y otras funciones de eficiencia del almacenamiento.
 - En ONTAP 9.12.1 y versiones anteriores, las proporciones de reducción de datos se muestran de la siguiente forma:
 - El valor de reducción de datos que se muestra en el panel **Capacidad** es la relación general de

todo el espacio utilizado lógico en comparación con el espacio físico utilizado, e incluye los beneficios derivados del uso de copias Snapshot y otras funciones de eficiencia del almacenamiento.

- Cuando se muestra el panel de detalles, se ve tanto la relación **general** que se muestra en el panel de visión general como la relación del espacio usado lógico utilizado solo por los datos del cliente en comparación con el espacio usado físico utilizado solo por los datos del cliente, denominado **sin copias Snapshot y clones**.

- **Lógica usada:**

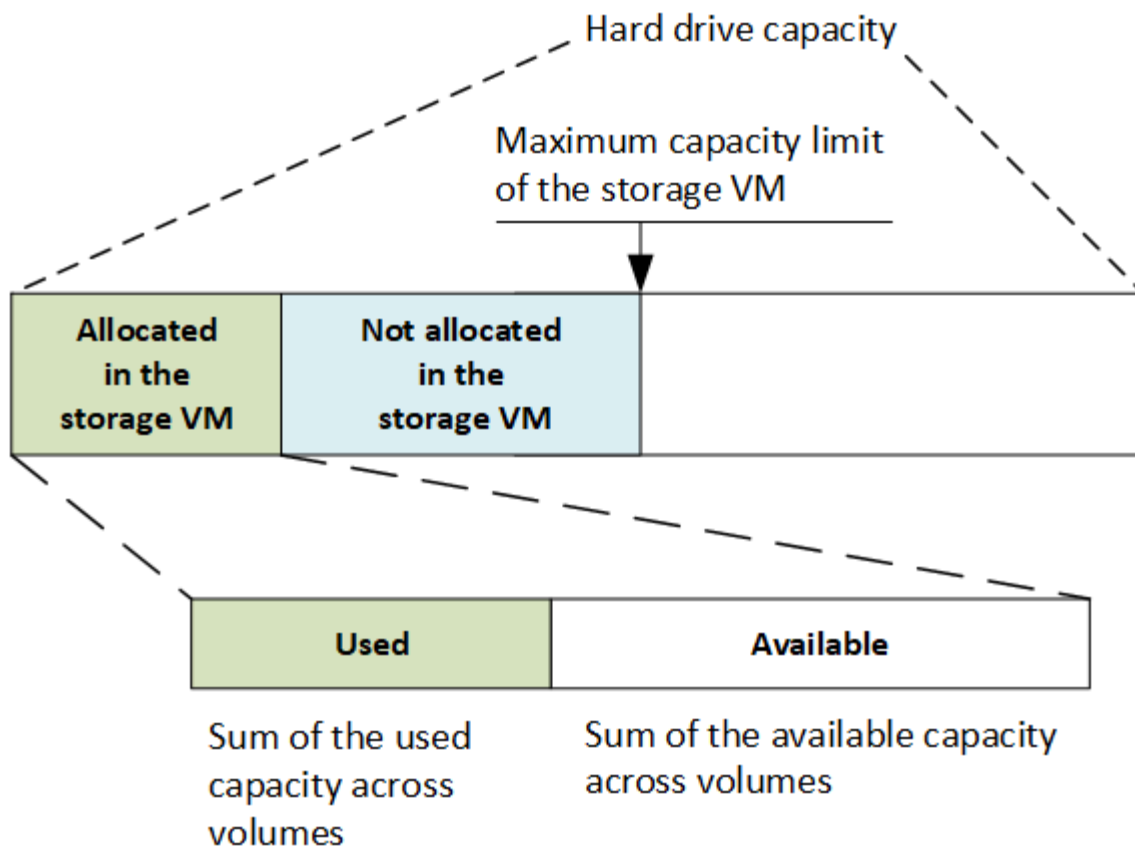
- A partir de ONTAP 9.13.1, la capacidad utilizada por los datos del cliente se conoce como **Lógica utilizada**, y la capacidad utilizada por las copias snapshot se muestra por separado.
- En ONTAP 9.12.1 y versiones anteriores, la capacidad utilizada por los datos del cliente añadidos a la capacidad utilizada por las copias snapshot se conoce como **Lógica usada**.
- *** % Lógico utilizado***: El porcentaje de la capacidad lógica utilizada actual en comparación con el tamaño aprovisionado, excluyendo las reservas Snapshot. Este valor puede ser mayor que el 100%, ya que incluye ahorros de eficiencia en el volumen.
- **Capacidad máxima**: La cantidad máxima de espacio asignado para volúmenes en una VM de almacenamiento.
- **Físico utilizado**: La cantidad de capacidad utilizada en los bloques físicos de un volumen o nivel local.
- **Uso físico %**: El porcentaje de capacidad utilizada en los bloques físicos de un volumen en comparación con el tamaño aprovisionado.
- **Capacidad suministrada**: Un sistema de archivos (volumen) que ha sido asignado desde un sistema Cloud Volumes ONTAP y está listo para almacenar datos de usuario o aplicación.
- **Reservado**: Cantidad de espacio reservado para volúmenes ya aprovisionados en un nivel local.
- **Usado**: La cantidad de espacio que contiene datos.
- **Usado y reservado**: La suma del espacio físico utilizado y reservado.

La capacidad de una máquina virtual de almacenamiento

La capacidad máxima de una máquina virtual de almacenamiento se determina por el espacio total asignado para los volúmenes más el espacio sin asignar restante.

- El espacio asignado para los volúmenes es la suma de la capacidad utilizada y la suma de la capacidad disponible de los volúmenes de FlexVol, FlexGroup Volumes y FlexCache Volumes.
- La capacidad de los volúmenes se incluye en las sumas, incluso cuando están restringidos, sin conexión o en la cola de recuperación después de su eliminación.
- Si los volúmenes se configuran con el crecimiento automático, el valor máximo de tamaño automático del volumen se usa en las sumas. Sin crecimiento automático, la capacidad real del volumen se usa en las sumas.

En el siguiente gráfico se explica cómo la medición de la capacidad entre volúmenes se relaciona con el límite de capacidad máxima.



A partir de ONTAP 9.13.1, los administradores de clúster pueden ["Habilite un límite de capacidad máxima para una máquina virtual de almacenamiento"](#). Sin embargo, no es posible establecer límites de almacenamiento para una máquina virtual de almacenamiento que contiene volúmenes para la protección de datos, en una relación de SnapMirror o en una configuración de MetroCluster. Además, no es posible configurar cuotas para superar la capacidad máxima de un equipo virtual de almacenamiento.

Una vez establecido el límite de capacidad máxima, no se puede cambiar a un tamaño inferior a la capacidad asignada actualmente.

Cuando una máquina virtual de almacenamiento alcanza su límite máximo de capacidad, no se pueden ejecutar ciertas operaciones. System Manager proporciona sugerencias para los siguientes pasos de ["Insights"](#).

Unidades de medida de capacidad

System Manager calcula la capacidad de almacenamiento en función de unidades binarias de 1024 (2^{10}) bytes.

- A partir de ONTAP 9.10.1, las unidades de capacidad de almacenamiento se muestran en System Manager como KiB, MiB, GiB, TiB y PiB.
- En ONTAP 9.10.0 y versiones anteriores, estas unidades se muestran en System Manager como KB, MB, GB, TB y PB.



Las unidades utilizadas en System Manager para el rendimiento siguen siendo KB/s, MB/s, GB/s, TB/s y PB/s en todas las versiones de ONTAP.

| Unidad de capacidad mostrada en System Manager para ONTAP 9.10.0 y versiones anteriores | Unidad de capacidad mostrada en System Manager para ONTAP 9.10.1 y versiones posteriores | Cálculo | Valor en bytes |
|---|--|----------------------------------|-----------------------------|
| KB | KiB | 1024 | 1024 bytes |
| MB | MiB | 1024 * 1024 | 1.048.576 bytes |
| GB | GiB | 1024 * 1024 * 1024 | 1.073.741.824 bytes |
| TB | TiB | 1024 * 1024 * 1024 * 1024 | 1.099.511.627.776 bytes |
| PB | PiB | 1024 * 1024 * 1024 * 1024 * 1024 | 1.125.899.906.842.624 bytes |

Información relacionada

["Supervise la capacidad en System Manager"](#)

["Generación de informes sobre el espacio lógico y cumplimiento para volúmenes"](#)

Descripción general de la eficiencia del almacenamiento en la que la temperatura es importante

ONTAP ofrece ventajas en eficiencia del almacenamiento sensible a la temperatura; para ello, evalúa la frecuencia con la que se accede a los datos del volumen y asigna esa frecuencia al grado de compresión aplicado a esos datos. En el caso de los datos inactivos a los que se accede con poca frecuencia, se comprimen los bloques de datos más grandes, y en el caso de los datos activos, a los que se accede con frecuencia y se sobrescriben con mayor frecuencia, se comprimen los bloques de datos más pequeños, lo que hace que el proceso sea más eficiente.

La eficiencia del almacenamiento sensible a la temperatura (TSSE) se introduce en ONTAP 9,8 y se activa automáticamente en los volúmenes AFF con Thin Provisioning recientemente creados. Se puede habilitar la eficiencia del almacenamiento sensible a la temperatura en volúmenes AFF existentes y en volúmenes de DP que no sean AFF con Thin-Provisioning.

Introducción de los modos «predeterminado» y «eficiente»

A partir de ONTAP 9.10.1, se introducen dos modos de eficiencia de almacenamiento a nivel de volumen solo para sistemas AFF, *default* y *efficient*. Los dos modos proporcionan una opción entre compresión de archivo (predeterminado), que es el modo predeterminado cuando se crean nuevos volúmenes AFF, o la eficiencia del almacenamiento sensible a la temperatura (eficiente), que permite una eficiencia del almacenamiento sensible a la temperatura. Con ONTAP 9.10.1, ["debe definirse explícitamente la eficacia del almacenamiento sensible a la temperatura"](#) para activar la compresión adaptativa automática. Sin embargo, otras funciones de eficiencia del almacenamiento, como la compactación de datos, la programación de deduplicación automática, la deduplicación inline, la deduplicación inline entre volúmenes y la deduplicación en segundo plano entre volúmenes, están habilitadas de forma predeterminada en las plataformas de AFF, tanto en los modos predeterminados como eficientes.

Los dos modos de eficiencia del almacenamiento (predeterminado y eficiente) son compatibles con los agregados habilitados para FabricPool y con todos los tipos de políticas de organización en niveles.

La eficiencia del almacenamiento sensible a la temperatura habilitada en plataformas C-Series

La eficiencia del almacenamiento sensible a la temperatura se activa de forma predeterminada en las plataformas AFF C-Series y cuando se migran volúmenes de una plataforma no TSSE a una plataforma C-Series habilitada para TSSE mediante Volume Move o SnapMirror con las siguientes versiones instaladas en el destino:

- ONTAP 9.12.1P4 y versiones posteriores
- ONTAP 9.13.1 y versiones posteriores

Para obtener más información, consulte ["Comportamiento de la eficiencia del almacenamiento con movimiento de volúmenes y operaciones de SnapMirror"](#).

En el caso de los volúmenes existentes, la eficiencia del almacenamiento sensible a la temperatura no se habilita automáticamente; sin embargo, sí puede ["modifique el modo de eficiencia del almacenamiento"](#) manualmente para cambiar al modo eficiente.



Una vez que cambia el modo de eficiencia del almacenamiento a Eficiencia, no se puede volver a cambiar.

Eficiencia del almacenamiento mejorada con paquetes secuenciales de bloques físicos contiguos

A partir de ONTAP 9.13.1, la eficiencia del almacenamiento sensible a la temperatura añade paquetes secuenciales de bloques físicos contiguos para mejorar aún más la eficiencia del almacenamiento. Los volúmenes con eficiencia del almacenamiento sensible a la temperatura habilitada tienen habilitado automáticamente el empaquetado secuencial al actualizar los sistemas a ONTAP 9.13.1. Una vez activado el empaquetado secuencial, debe hacerlo ["volver a copiar manualmente los datos existentes"](#).

Consideraciones de renovación

Cuando se actualiza a ONTAP 9.10.1 y versiones posteriores, se asigna a los volúmenes existentes un modo de eficiencia del almacenamiento según el tipo de compresión actualmente habilitado en los volúmenes. Durante una actualización, se asigna el modo predeterminado a los volúmenes con compresión habilitada y se asigna el modo eficiente a los volúmenes con eficiencia de almacenamiento sensible a la temperatura habilitada. Si la compresión no está habilitada, el modo de eficiencia del almacenamiento sigue vacío.

Seguridad

Autenticación y autorización de clientes

ONTAP usa métodos estándar para proteger el acceso de clientes y administradores al almacenamiento y para protegerse frente a virus. Existen tecnologías avanzadas para el cifrado de datos en reposo y para el almacenamiento WORM.

ONTAP autentica un equipo de cliente y un usuario al verificar sus identidades con un origen de confianza. ONTAP autoriza a un usuario a acceder a un archivo o directorio comparando las credenciales del usuario con los permisos configurados en el archivo o directorio.

Autenticación

Es posible crear cuentas de usuario locales o remotas:

- Una cuenta local es una en la cual reside la información de la cuenta en el sistema de almacenamiento.
- Una cuenta remota es aquella en la que la información de cuenta se almacena en un controlador de dominio de Active Directory, un servidor LDAP o un servidor NIS.

ONTAP utiliza servicios de nombres locales o externos para buscar información de asignación de nombres, usuarios, grupos, netgroup y nombres. ONTAP admite los siguientes servicios de nombres:

- Usuarios locales
- DNS
- Dominios NIS externos
- Dominios LDAP externos

A *name service switch table* especifica las fuentes que se deben buscar información de la red y el orden en el que buscar (proporcionando la funcionalidad equivalente del archivo `/etc/nsswitch.conf` en sistemas UNIX). Cuando un cliente NAS se conecta a la SVM, ONTAP comprueba los servicios de nombres especificados para obtener la información necesaria.

Kerberos support Kerberos es un protocolo de autenticación de red que proporciona "autenticación de programas" mediante el cifrado de contraseñas de usuario en implementaciones cliente-servidor. ONTAP admite la autenticación Kerberos 5 con comprobación de integridad (krb5i) y la autenticación Kerberos 5 con comprobación de privacidad (krb5p).

Autorización

ONTAP evalúa tres niveles de seguridad para determinar si una entidad está autorizada para realizar una acción solicitada sobre archivos y directorios que residen en una SVM. El acceso se determina mediante los permisos efectivos después de evaluar los niveles de seguridad:

- Seguridad de exportación (NFS) y uso compartido (SMB)

La seguridad de exportación y uso compartido se aplica al acceso de los clientes a una exportación NFS o un recurso compartido de SMB dado. Los usuarios con privilegios administrativos pueden gestionar la seguridad de exportación y nivel de recurso compartido desde clientes SMB y NFS.

- Seguridad de directorio y archivos del protector de acceso a nivel de almacenamiento

La seguridad de protección de acceso a nivel de almacenamiento se aplica al acceso de clientes SMB y NFS a volúmenes de SVM. Sólo se admiten permisos de acceso NTFS. Para que ONTAP realice comprobaciones de seguridad en los usuarios de UNIX con el fin de acceder a los datos de los volúmenes para los que se ha aplicado la protección de acceso a nivel de almacenamiento, el usuario de UNIX debe asignar a un usuario de Windows en la SVM propietaria del volumen.

- Seguridad nativa a nivel de archivo de NTFS, UNIX y NFSv4

Existe una seguridad nativa a nivel de archivo en el archivo o directorio que representa el objeto de almacenamiento. Puede establecer la seguridad a nivel de archivo desde un cliente. Los permisos de archivos son efectivos independientemente de si se utiliza SMB o NFS para acceder a los datos.

Autenticación con SAML

ONTAP admite el lenguaje de marcado de aserción de seguridad (SAML) para la autenticación de usuarios remotos. Se admiten varios proveedores de identidad (IDPs) populares. Para obtener más información sobre

los IDP admitidos e instrucciones para habilitar la autenticación SAML, consulte ["Configurar la autenticación SAML"](#).

OAuth 2,0 con clientes API REST DE ONTAP

La compatibilidad con el marco de autorización abierta (OAuth 2,0) está disponible a partir de ONTAP 9,14. Solo puede usar OAuth 2,0 para tomar decisiones de autorización y control de acceso cuando el cliente usa la API REST para acceder a ONTAP. Sin embargo, puede configurar y habilitar la función con cualquiera de las interfaces de administración de ONTAP, incluidas la interfaz de línea de comandos, System Manager y la API de REST.

Las capacidades estándar de OAuth 2,0 son compatibles junto con varios servidores de autorización populares. Puede mejorar aún más la seguridad de ONTAP mediante el uso de tokens de acceso restringidos por el remitente basados en TLS mutuo. Además, existe una gran variedad de opciones de autorización disponibles, incluidos ámbitos independientes y la integración con los roles REST DE ONTAP y definiciones de usuarios locales. Consulte ["Descripción general de la implementación de ONTAP OAuth 2,0"](#) si quiere más información.

Autenticación de administrador y RBAC

Los administradores utilizan cuentas de inicio de sesión locales o remotas para autenticarse en el clúster y la SVM. El control de acceso basado en roles (RBAC) determina los comandos a los que tiene acceso un administrador.

Autenticación

Puede crear cuentas de administrador de SVM y de clúster local o remoto:

- Una cuenta local es aquella en la que reside la información de la cuenta, la clave pública o el certificado de seguridad en el sistema de almacenamiento.
- Una cuenta remota es aquella en la que la información de cuenta se almacena en un controlador de dominio de Active Directory, un servidor LDAP o un servidor NIS.

Excepto DNS, ONTAP utiliza los mismos servicios de nombre para autenticar cuentas de administrador que utiliza para autenticar clientes.

RBAC

El *role* asignado a un administrador determina los comandos a los que tiene acceso el administrador. La función se asigna al crear la cuenta para el administrador. Puede asignar un rol diferente o definir roles personalizados según sea necesario.

Detección de virus

Puede utilizar la funcionalidad antivirus integrada en el sistema de almacenamiento para proteger los datos frente a amenazas de virus u otro código malintencionado. El análisis de virus de ONTAP, denominado *Vscan*, combina el mejor software antivirus de terceros con funciones de ONTAP que le proporcionan la flexibilidad que necesita para controlar qué archivos se analizan y cuándo.

Los sistemas de almacenamiento descargan las operaciones de análisis en servidores externos que alojan software antivirus de otros proveedores. El *ONTAP Antivirus Connector*, proporcionado por NetApp e instalado en el servidor externo, gestiona las comunicaciones entre el sistema de almacenamiento y el software

antivirus.

- Puede utilizar *análisis en tiempo real* para comprobar si hay virus cuando los clientes abren, leen, renombran o cierran archivos en SMB. La operación de archivo se suspende hasta que el servidor externo informa del estado de análisis del archivo. Si el archivo ya se ha analizado, ONTAP permite la operación de archivo. De lo contrario, solicita un análisis desde el servidor.

El análisis en tiempo real no es compatible con NFS.

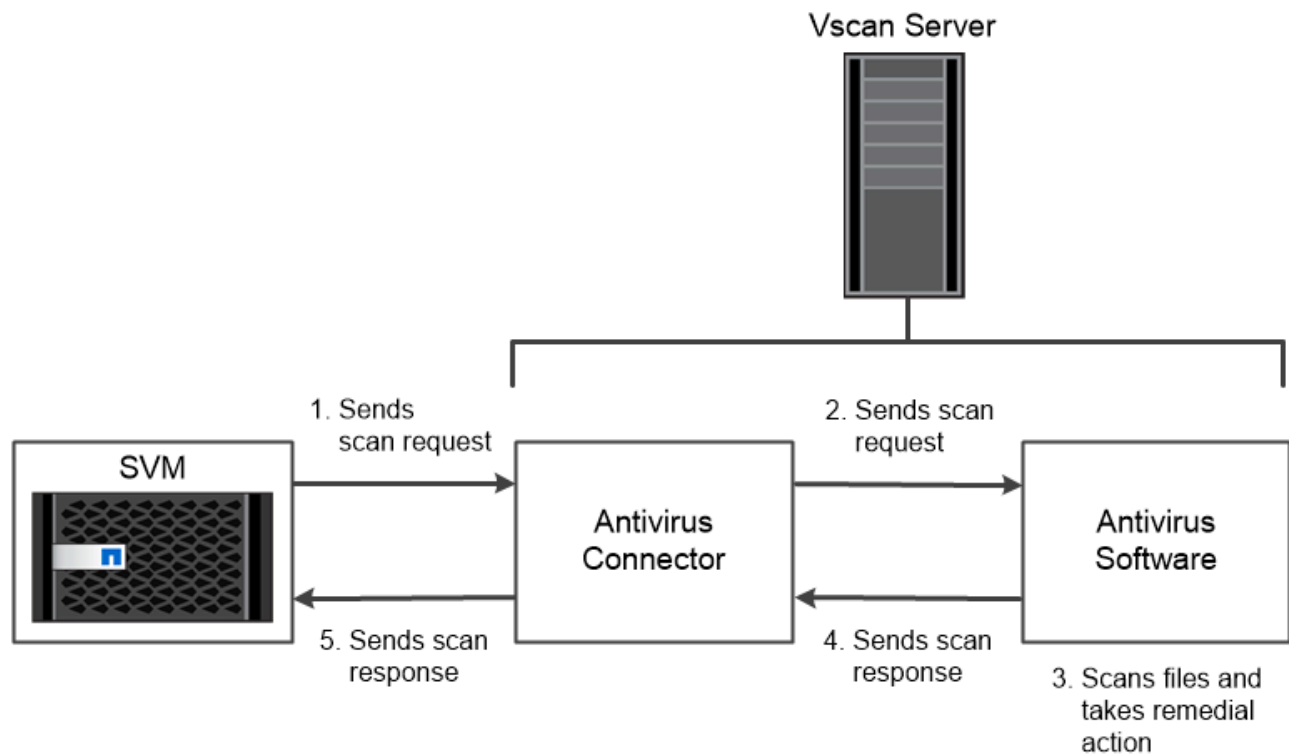
- Puede utilizar *análisis bajo demanda* para comprobar los archivos en busca de virus inmediatamente o en una programación. Por ejemplo, es posible que desee ejecutar análisis sólo en horas de menor actividad. El servidor externo actualiza el estado de análisis de los archivos comprobados, de modo que la latencia de acceso a los archivos de esos archivos (suponiendo que no se hayan modificado) se reduce cuando se accede a ellos a través de SMB a continuación.

Puede utilizar el análisis bajo demanda para cualquier ruta del espacio de nombres de SVM, incluso para los volúmenes que solo se exportan mediante NFS.

Normalmente se habilitan ambos modos de análisis en un SVM. En cualquiera de los dos modos, el software antivirus toma medidas correctivas en los archivos infectados en función de la configuración del software.

detección de virus en recuperación de desastres y configuraciones de MetroCluster

Para la recuperación ante desastres y las configuraciones de MetroCluster, es necesario configurar servidores Vscan independientes para el clúster local y el de asociado.



The storage system offloads virus scanning operations to external servers hosting antivirus software from third-party vendors.

Cifrado

ONTAP ofrece tecnologías de cifrado basadas en software y hardware para garantizar que los datos en reposo no se puedan leer en caso de reasignación, devolución, pérdida o robo del medio de almacenamiento.

ONTAP cumple con los estándares de procesamiento de información federal (FIPS) 140-2 para todas las conexiones SSL. Puede utilizar las siguientes soluciones de cifrado:

- Soluciones de hardware:

- Cifrado en almacenamiento de NetApp (NSE)

NSe es una solución de hardware que utiliza unidades de cifrado automático (SED).

- SED de NVMe

ONTAP proporciona cifrado de disco completo para NVMe SED que no tienen la certificación FIPS 140-2-2.

- Soluciones de software:

- Cifrado de agregados de NetApp (NAE)

NAE es una solución de software que permite el cifrado de cualquier volumen de datos en cualquier tipo de unidad en la que se habilita con claves únicas para cada agregado.

- Cifrado de volúmenes de NetApp (NVE)

NVE es una solución de software que permite el cifrado de cualquier volumen de datos en cualquier tipo de unidad donde se habilita con una clave única para cada volumen.

Use ambas soluciones de cifrado de software (NAE o NVE) y hardware (NSE o NVMe SED) para obtener el doble cifrado en reposo. La eficiencia del almacenamiento no se ve afectada por el cifrado NAE o NVE.

Cifrado del almacenamiento de NetApp

NetApp Storage Encryption (NSE, cifrado del almacenamiento de NetApp) es compatible con SED a medida que se escriben. Los datos no se pueden leer sin una clave de cifrado almacenada en el disco. La clave de cifrado, a su vez, sólo es accesible a un nodo autenticado.

En una solicitud de I/O, un nodo se autentica a sí mismo en una SED mediante una clave de autenticación recuperada de un servidor de gestión de claves externo o el gestor de claves incorporado:

- El servidor de gestión de claves externo es un sistema de terceros en el entorno de almacenamiento que ofrece claves de autenticación a nodos mediante el protocolo de interoperabilidad de gestión de claves (KMIP).
- El gestor de claves incorporado es una herramienta integrada que proporciona claves de autenticación a nodos del mismo sistema de almacenamiento que los datos.

NSe es compatible con unidades de disco duro y SSD de autocifrado. Puede usar el cifrado de volúmenes de NetApp con NSE para cifrar datos por duplicado en unidades NSE.



Si utiliza NSE en un sistema con un módulo Flash Cache, también debe habilitar NVE o NAE. NSE no cifra los datos que residen en el módulo de Flash Cache.

Unidades de autocifrado NVMe

Sin embargo, SED de NVMe no tienen la certificación FIPS 140-2-2, estos discos utilizan el cifrado de disco transparente AES de 256 bits para proteger los datos en reposo.

Las operaciones de cifrado de datos, como la generación de una clave de autenticación, se realizan internamente. La clave de autenticación se genera la primera vez que el sistema de almacenamiento accede al disco. Después de eso, los discos protegen los datos en reposo al requerir la autenticación del sistema de almacenamiento cada vez que se solicitan las operaciones de datos.

Cifrado de agregados de NetApp

El cifrado de agregados de NetApp (NAE) es una tecnología basada en software para cifrar todos los datos en un agregado. Una ventaja de NAE es que se incluyen los volúmenes en la deduplicación a nivel agregado, mientras que se excluyen los volúmenes NVE.

Con la NAE habilitada, los volúmenes del agregado se pueden cifrar con claves de agregado.

A partir de ONTAP 9.7, los agregados y volúmenes recién creados se cifran de forma predeterminada cuando tenga el ["Licencia de NVE"](#) o la gestión de claves externas o incorporadas.

Cifrado de volúmenes de NetApp

El cifrado de volúmenes de NetApp (NVE) es una tecnología basada en software para cifrar datos en reposo un volumen por vez. Una clave de cifrado que solo puede acceder el sistema de almacenamiento garantiza que los datos de volumen no se puedan leer si el dispositivo subyacente está separado del sistema.

Ambos datos, incluidas las copias Snapshot, y los metadatos están cifrados. El acceso a los datos se proporciona mediante una clave XTS-AES-256 exclusiva, una por volumen. Un gestor de claves incorporado protege las claves en el mismo sistema con los datos.

Es posible utilizar el NVE en cualquier tipo de agregado (HDD, SSD, híbrido, LUN de cabina), con cualquier tipo de RAID y en cualquier implementación de ONTAP compatible, incluido ONTAP Select. También puede utilizar NVE con el cifrado de almacenamiento de NetApp (NSE) para cifrar doble los datos en unidades NSE.

Cuándo usar servidores KMIP aunque es menos costoso y, por lo general, más conveniente utilizar el Administrador de claves incorporado, debe configurar servidores KMIP si se cumple alguna de las siguientes condiciones:

- Su solución de gestión de claves de cifrado debe cumplir con el estándar de procesamiento de información federal (FIPS) 140-2 o el estándar KMIP DE OASIS.
- Necesita una solución multiclúster. Los servidores KMIP admiten múltiples clústeres con una gestión centralizada de las claves de cifrado.

Los servidores KMIP admiten múltiples clústeres con una gestión centralizada de las claves de cifrado.

- Su empresa requiere una seguridad añadida para almacenar claves de autenticación en un sistema o en una ubicación distinta de los datos.

Los servidores KMIP almacenan claves de autenticación por separado de los datos.

Información relacionada

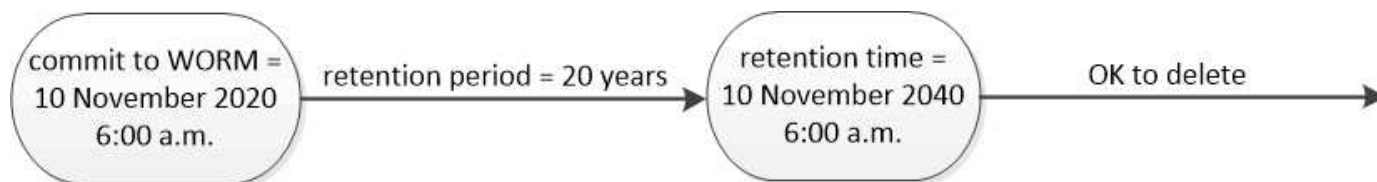
["Preguntas más frecuentes: Cifrado de volúmenes de NetApp y cifrado de agregados de NetApp"](#)

Almacenamiento WORM

SnapLock es una solución de cumplimiento de normativas de alto rendimiento para organizaciones que utilizan almacenamiento *WRITE Once, Read Many (WORM)* para conservar archivos críticos de forma no modificada con fines normativos y de gobernanza.

Una única licencia da derecho a usar *SnapLock* en modo estricto *Compliance*, para satisfacer mandatos externos como la normativa SEC 17a-4 y un modo más flexible *Enterprise*, para cumplir las normativas internas de protección de activos digitales. *SnapLock* utiliza un *ComplianceClock* *prueba de manipulación* para determinar cuándo ha transcurrido el período de retención de un archivo WORM.

Puede utilizar *SnapLock* para *SnapVault* para proteger CON WORM las copias Snapshot en el almacenamiento secundario. Puede usar *SnapMirror* para replicar archivos WORM a otra ubicación geográfica a efectos de recuperación ante desastres y otros fines.



SnapLock uses a tamper-proof ComplianceClock to determine when the retention period for a WORM file has elapsed.

Gestión de datos para aplicaciones

La gestión de datos para aplicaciones permite describir la aplicación que se desea implementar a través de ONTAP en términos de aplicación, en lugar de en términos de almacenamiento. La aplicación puede configurarse y prepararse para servir datos

rápidamente con entradas mínimas mediante System Manager y las API DE REST.

La función de gestión de datos para aplicaciones ofrece una forma de configurar, gestionar y supervisar el almacenamiento en el nivel de aplicaciones individuales. Esta función incorpora las prácticas recomendadas relevantes de ONTAP para aprovisionar de forma óptima aplicaciones, con una colocación equilibrada de objetos de almacenamiento en función de los niveles de servicio de rendimiento deseados y los recursos disponibles del sistema.

La función de gestión de datos compatible con aplicaciones incluye un conjunto de plantillas de aplicación, con cada plantilla compuesta por un conjunto de parámetros que describen de forma colectiva la configuración de una aplicación. Estos parámetros, que a menudo se predefinen con valores predeterminados, definen las características que un administrador de aplicación podría especificar para aprovisionar almacenamiento en un sistema ONTAP, como el tamaño de la base de datos, los niveles de servicio, los elementos de acceso de protocolos como LIF, así como los criterios de protección local y los criterios de protección remota. ONTAP configura entidades de almacenamiento como, por ejemplo, LUN y volúmenes con los tamaños y niveles de servicio adecuados para la aplicación, basándose en los parámetros especificados.

Puede realizar las siguientes tareas para las aplicaciones:

- Cree aplicaciones mediante las plantillas de aplicación
- Gestione el almacenamiento asociado con las aplicaciones
- Modifique o elimine las aplicaciones
- Ver aplicaciones
- Gestione las copias Snapshot de las aplicaciones
- Cree [grupos de consistencia](#) Para ofrecer funcionalidades de protección de datos seleccionando varios LUN en los mismos volúmenes o en diferentes volúmenes

FabricPool

Muchos clientes de NetApp tienen cantidades significativas de datos almacenados a los que rara vez se accede. Nosotros llamamos a eso datos *fríos*. Los clientes también tienen datos a los que se accede con frecuencia, a los que llamamos datos *hot*. Lo ideal es que conserve los datos activos en su almacenamiento más rápido para obtener el mejor rendimiento. Los datos inactivos pueden moverse a un almacenamiento más lento siempre que estén disponibles de forma inmediata si es necesario. Pero ¿cómo sabe qué partes de sus datos están activos y cuáles no?

FabricPool es una función de ONTAP que mueve datos automáticamente entre un nivel local (agregado) de alto rendimiento y un nivel de cloud basado en patrones de acceso. La organización en niveles libera el costoso almacenamiento local para los datos activos al tiempo que mantiene los datos inactivos disponibles en el almacenamiento de objetos de bajo coste en el cloud. FabricPool supervisa constantemente el acceso a los datos y mueve los datos entre niveles para obtener el mejor rendimiento y el máximo ahorro.

FabricPool para organizar los datos inactivos en niveles en el cloud es una de las formas más sencillas de obtener eficiencia del cloud y crear una configuración de cloud híbrido. FabricPool funciona a nivel de bloque de almacenamiento, por lo que funciona tanto con datos de archivos como de LUN.

Pero FabricPool no es solo para la organización en niveles de los datos locales en el cloud. Muchos clientes utilizan FabricPool en Cloud Volumes ONTAP para organizar los datos fríos en niveles desde un almacenamiento en cloud más costoso hasta un almacenamiento de objetos más barato dentro del proveedor de cloud. A partir de ONTAP 9.8, puede capturar análisis en los volúmenes habilitados para FabricPool con

["Análisis del sistema de archivos" o. "eficiencia del almacenamiento sensible a la temperatura"](#).

Las aplicaciones que usan los datos no son conscientes de que los datos se organizan por niveles, por lo que no es necesario realizar ningún cambio en las aplicaciones. La organización en niveles es totalmente automática, por lo que no se requiere una administración continua.

Puede almacenar datos fríos en almacenamiento de objetos de uno de los principales proveedores de cloud. También puede elegir StorageGRID de NetApp para mantener sus datos fríos en su propio cloud privado para obtener el máximo rendimiento y un control total sobre sus datos.

Información relacionada

["Documento de FabricPool System Manager"](#)

["Organización en niveles de BlueXP"](#)

["Lista de reproducción de FabricPool en NetApp TechComm TV"](#)

Configure, actualice y revierta el software y el firmware de ONTAP

Configure ONTAP

Comience a utilizar la configuración del clúster de ONTAP

Puede usar System Manager o la interfaz de línea de comandos (CLI) de ONTAP para configurar clústeres de ONTAP nuevos. Antes de empezar, debe recopilar la información que necesitará para completar la configuración del clúster, como el puerto de la interfaz de gestión del clúster y la dirección IP.

NetApp le recomienda ["Use System Manager para configurar clústeres nuevos"](#). System Manager proporciona un flujo de trabajo sencillo y sencillo para la instalación y la configuración del clúster, incluidas la asignación de una dirección IP de gestión de nodos, la inicialización del clúster, la creación de un nivel local, la configuración de protocolos y el aprovisionamiento del almacenamiento inicial.

Solo es necesario hacerlo ["Use la interfaz de línea de comandos de ONTAP para configurar el clúster"](#) Si ejecuta ONTAP 9,7 o una versión anterior en una configuración de MetroCluster. A partir de ONTAP 9.13.1, en las plataformas A800 y FAS8700 de AFF, también se puede usar la interfaz de línea de comandos de ONTAP para crear y configurar clústeres nuevos en entornos de red solo IPv6. Si necesita usar IPv6 en ONTAP 9.13.0 y versiones anteriores, o en otras plataformas en ONTAP 9.13.1 y versiones posteriores, puede usar System Manager para crear clústeres nuevos con IPv4 y a continuación ["Convertir a IPv6"](#).

Qué necesitará para la configuración del clúster

La configuración del clúster implica recopilar la información necesaria para configurar cada nodo, crear el clúster en el primer nodo y unir los nodos restantes al clúster.

Comience reuniendo toda la información relevante de las hojas de cálculo de la configuración del clúster.

La hoja de cálculo de configuración del clúster le permite registrar los valores que necesita durante el proceso de configuración del clúster. Si se proporciona un valor predeterminado, puede usar dicho valor, o bien puede introducir el que desee.

Valores predeterminados del sistema

Los valores predeterminados del sistema son los valores predeterminados de la red de clúster privada. Se recomienda usar los valores predeterminados. Sin embargo, si estos no cumplen con los requisitos, puede usar la tabla para registrar sus propios valores.



Para los clústeres configurados de manera que usen switches de red, cada switch de clúster debe usar el tamaño de MTU de 9000.

| Tipos de información | Sus valores |
|-----------------------------------|-------------|
| Puertos de red de clúster privada | |
| La máscara de red de clúster | |

| Tipos de información | Sus valores |
|---|-------------|
| <p>Direcciones IP de interfaz de clúster (para cada puerto de red de clúster de cada nodo)</p> <p>Las direcciones IP para cada nodo deben estar en la misma subred.</p> | |

Información del clúster


| Tipos de información | Sus valores |
|--|-------------|
| <p>Nombre del clúster</p> <p>El nombre debe comenzar por una letra y debe tener menos de 44 caracteres. El nombre puede incluir los siguientes caracteres especiales:</p> <p>. - _</p> | |

Claves de licencia de funciones

Puede encontrar las claves de licencia para los pedidos de software iniciales o adicionales en el sitio de soporte de NetApp en **My Support > licencias de software**.

| Tipos de información | Sus valores |
|---------------------------------|-------------|
| Claves de licencia de funciones | |

Máquina virtual de almacenamiento (SVM) de administrador

| Tipos de información | Sus valores |
|--|-------------|
| <p>Contraseña de administrador del clúster</p> <p>La contraseña de la cuenta de administrador que el clúster necesita para brindar acceso de administrador de clúster a la consola o a través de un protocolo seguro.</p> <div>  <p>Por motivos de seguridad, no se recomienda grabar contraseñas en esta hoja de trabajo.</p> </div> <p>Las reglas predeterminadas de las contraseñas son las siguientes:</p> <ul style="list-style-type: none"> • La contraseña debe tener al menos 8 caracteres. • La contraseña debe contener al menos una letra y un número. | |

| Tipos de información | Sus valores |
|---|-------------|
| <p>Puerto de la interfaz de gestión de clústeres</p> <p>El puerto físico que está conectado a la red de datos y que permite que el administrador de clúster gestione el clúster.</p> | |
| <p>Dirección IP de la interfaz de gestión de clústeres</p> <p>Una dirección IPv4 o IPv6 exclusiva para la interfaz de gestión de clústeres. El administrador de clúster utiliza esta dirección para acceder a la SVM de administrador y gestionar el clúster. Generalmente, esta dirección debe estar en la red de datos.</p> <p>Puede pedirle esta dirección IP al administrador responsable de la asignación de direcciones IP en la organización.</p> <p>Ejemplo: 192.0.2.66</p> | |
| <p>Máscara de red de la interfaz de gestión de clústeres (IPv4)</p> <p>La máscara de subred que define el rango de direcciones IPv4 válidas en la red de gestión de clústeres.</p> <p>Ejemplo: 255.255.255.0</p> | |
| <p>Longitud de la máscara de red de la interfaz de gestión de clústeres (IPv6)</p> <p>Si la interfaz de gestión de clústeres utiliza una dirección IPv6, este valor representa la longitud del prefijo que define el rango de direcciones IPv6 válidas en la red de gestión de clústeres.</p> <p>Ejemplo: 64</p> | |
| <p>Puerta de enlace predeterminada de la interfaz de gestión de clústeres</p> <p>La dirección IP del enrutador de la red de gestión de clústeres.</p> | |

| Tipos de información | Sus valores |
|--|--------------------|
| <p>Nombre de dominio DNS</p> <p>El nombre del dominio DNS de la red.</p> <p>El nombre de dominio debe estar compuesto de caracteres alfanuméricos. Para introducir varios nombres de dominio DNS, separe cada uno con una coma o un espacio.</p> | |
| <p>Las direcciones IP del servidor de nombres</p> <p>Las direcciones IP de los servidores de nombres DNS. Separe las direcciones con una coma o un espacio.</p> | |

Información del nodo (para cada nodo del clúster)

| Tipos de información | Sus valores |
|--|--------------------|
| <p>Ubicación física de la controladora (opcional)</p> <p>Una descripción de la ubicación física de la controladora. Use una descripción que identifique la ubicación del nodo en el clúster (por ejemplo, «"Lab 5, fila 7, rack B»).</p> | |
| <p>Puerto de la interfaz de gestión de nodos</p> <p>El puerto físico que está conectado a la red de gestión de nodos y que permite que el administrador de clústeres gestione el nodo.</p> | |
| <p>Dirección IP de la interfaz de gestión de nodos</p> <p>Una dirección IPv4 o IPv6 exclusiva para la interfaz de gestión de nodos en la red de gestión. Si ha definido el puerto de la interfaz de gestión de nodos de manera que sea un puerto de datos, esta dirección IP debe ser una dirección IP exclusiva en la red de datos.</p> <p>Puede pedirle esta dirección IP al administrador responsable de la asignación de direcciones IP en la organización.</p> <p>Ejemplo: 192.0.2.66</p> | |

| Tipos de información | Sus valores |
|---|-------------|
| <p>Máscara de red de la interfaz de gestión de nodos (IPv4)</p> <p>La máscara de subred que define el rango de direcciones IP válidas en la red de gestión de nodos.</p> <p>Si ha definido el puerto de la interfaz de gestión de nodos de manera que sea un puerto de datos, esta máscara de red debe ser la máscara de subred de la red de datos.</p> <p>Ejemplo: 255.255.255.0</p> | |
| <p>Longitud de la máscara de red de la interfaz de gestión de nodos (IPv6)</p> <p>Si la interfaz de gestión de nodos utiliza una dirección IPv6, este valor representa la longitud del prefijo que define el rango de direcciones IPv6 válidas en la red de gestión de nodos.</p> <p>Ejemplo: 64</p> | |
| <p>Puerta de enlace predeterminada de la interfaz de gestión de nodos</p> <p>La dirección IP del enrutador de la red de gestión de nodos.</p> | |

Información del servidor NTP

| Tipos de información | Sus valores |
|--|-------------|
| <p>Direcciones del servidor NTP</p> <p>Las direcciones IP de los servidores de Protocolo de hora de red (NTP) del sitio. Estos servidores se utilizan para sincronizar la hora en todo el clúster.</p> | |

Configure ONTAP en un nuevo clúster con System Manager

System Manager proporciona un flujo de trabajo sencillo y sencillo para configurar un clúster nuevo y el almacenamiento.

En algunos casos, como determinadas puestas en marcha de MetroCluster o los clústeres que requieren direccionamiento de red IPv6, puede que tenga que usar la CLI de ONTAP para configurar un clúster nuevo. Haga clic en ["aquí"](#) Para obtener más detalles sobre estos requisitos, así como los pasos para la configuración del clúster con la CLI de ONTAP.

Antes de empezar

- Debe haber instalado, cableado y encendido el nuevo sistema de almacenamiento de acuerdo con las instrucciones de instalación y configuración de su modelo de plataforma.
Consulte "[Documentación de AFF y FAS](#)".
- Las interfaces de red de clúster se deben configurar en cada nodo del clúster para la comunicación dentro del clúster.
- Debe tener en cuenta los siguientes requisitos de soporte de System Manager:
 - Cuando se configura manualmente la gestión de nodos mediante la CLI, System Manager solo admite IPv4 y no admite IPv6. Sin embargo, si inicia System Manager después de completar la configuración del hardware mediante DHCP con una dirección IP asignada automáticamente y con la detección de Windows, System Manager puede configurar una dirección de gestión IPv6.

En ONTAP 9.6 y versiones anteriores, System Manager no admite puestas en marcha que requieran redes IPv6.

- La compatibilidad con la configuración de MetroCluster está destinada a las configuraciones IP de MetroCluster, con dos nodos en cada sitio.

En ONTAP 9.7 y versiones anteriores, System Manager no admite una nueva configuración de clúster para las configuraciones de MetroCluster.



Asigne una dirección IP de gestión de nodos

Sistema Windows

Debe conectar el equipo con Windows a la misma subred que las controladoras. De este modo se asignará automáticamente una dirección IP de gestión de nodos al sistema.

Paso

1. Desde el sistema Windows, abra la unidad **Network** para descubrir los nodos.
2. Haga doble clic en el nodo para iniciar el asistente de configuración de clúster.

Otros sistemas

Debe configurar la dirección IP de gestión de nodos para uno de los nodos del clúster. Puede usar esta dirección IP de gestión de nodos para iniciar el asistente de configuración del clúster.

Consulte "[Creación del clúster en el primer nodo](#)" Para obtener información sobre la asignación de una dirección IP de gestión de nodos.

Inicialice el clúster

Para inicializar el clúster, debe establecer una contraseña de administrador para el clúster y configurar las redes de gestión de clústeres y nodos. También puede configurar servicios como un servidor DNS para resolver nombres de host y un servidor NTP para sincronizar la hora.

Pasos

1. En un navegador web, introduzca la dirección IP de gestión de nodos que haya configurado: "https://node-management-IP"

System Manager detecta automáticamente los nodos restantes del clúster.

2. Inicialice el sistema de almacenamiento configurando la red de gestión de clústeres y las direcciones IP de gestión de nodos para todos los nodos.

Cree su nivel local

Crear niveles locales a partir de los discos o SSD disponibles en los nodos. System Manager calcula automáticamente la configuración de mejor nivel según su hardware.

Pasos

1. Haga clic en **Panel** y, a continuación, en **preparar almacenamiento**.

Acepte la recomendación de almacenamiento para su nivel local.

Configure los protocolos

Según las licencias habilitadas en el clúster, puede habilitar los protocolos deseados en su clúster. A continuación, debe crear interfaces de red con las que puede acceder al almacenamiento.

Pasos

1. Haga clic en **Panel** y, a continuación, en **Configurar protocolos**.
 - Habilite iSCSI o FC para el acceso SAN.
 - Habilite NFS o SMB para el acceso NAS.
 - Habilite NVMe para el acceso a FC-NVMe.

Aprovisionar almacenamiento

Después de configurar los protocolos, puede aprovisionar almacenamiento. Las opciones que vea dependen de las licencias que se instalen.

Pasos

1. Haga clic en **Panel** y, a continuación, en **aprovisionar almacenamiento**.
 - Para "[Aprovisione el acceso SAN](#)", Haga clic en **Agregar LUN**.
 - Para "[Aprovisione el acceso NAS](#)", Haga clic en **Agregar volúmenes**.
 - Para "[Aprovisione el almacenamiento NVMe](#)", Haga clic en **Agregar espacios de nombres**.

Configure ONTAP en un vídeo de clúster nuevo

Configure ONTAP on a New Cluster

NetApp ONTAP 9 System Manager



© 2020 NetApp, Inc. All rights reserved.

Configure un clúster con la CLI

Cree el clúster en el primer nodo

Utilice el Asistente de configuración de clúster para crear el clúster en el primer nodo. El asistente le permite configurar la red del clústeres que conecta los nodos, crear la máquina virtual de almacenamiento (SVM) de administrador de clústeres, añadir las claves de licencia de funciones y crear la interfaz de gestión de nodos para el primer nodo.

Antes de empezar

- Debe haber instalado, cableado y encendido el nuevo sistema de almacenamiento de acuerdo con las instrucciones de instalación y configuración de su modelo de plataforma. Consulte "[Documentación de AFF y FAS](#)".
- Las interfaces de red de clúster se deben configurar en cada nodo del clúster para la comunicación dentro del clúster.
- Si va a configurar IPv6 en su clúster, IPv6 debe configurarse en la controladora de gestión base (BMC) para poder acceder al sistema mediante SSH.

Pasos

1. Encienda todos los nodos que va a añadir al clúster. Esto es necesario para habilitar la detección para la configuración del clúster.
2. Conéctese a la consola del primer nodo.

El nodo arranca y, a continuación, se inicia el Asistente de configuración de clúster en la consola.

```
Welcome to the cluster setup wizard....
```

3. Reconozca la declaración de AutoSupport.

```
Type yes to confirm and continue {yes}: yes
```



AutoSupport está habilitado de forma predeterminada.

4. Siga las instrucciones que aparecen en pantalla para asignar una dirección IP al nodo.

A partir de ONTAP 9.13.1, puede asignar direcciones IPv6 para las LIF de gestión en las plataformas A800 y FAS8700. Para versiones de ONTAP anteriores a 9.13.1, o para 9.13.1 o versiones posteriores en otras plataformas, debe asignar direcciones IPv4 para las LIF de gestión y, después, convertirlas a IPv6 tras completar la configuración del clúster.

5. Pulse **Intro** para continuar.

```
Do you want to create a new cluster or join an existing cluster?
{create, join}:
```

6. Cree un nuevo clúster: `create`

7. Acepte los valores predeterminados del sistema o introduzca sus propios valores.

8. Una vez completada la configuración, inicie sesión en el clúster y compruebe que el clúster esté activo y que el primer nodo esté en buen estado. Para ello, introduzca el comando de la CLI de ONTAP: `cluster show`

El siguiente ejemplo muestra un clúster en el que el primer nodo (cluster1-01) está en buen estado y puede participar:

```
cluster1::> cluster show
Node                      Health  Eligibility
-----
cluster1-01              true    true
```

Puede acceder al Asistente de configuración de clúster para cambiar cualquiera de los valores introducidos para la SVM de administrador o la SVM de nodo mediante el `cluster setup` comando.

Después de terminar

Si es necesario, ["Convertir de IPv4 a IPv6"](#).

Una los nodos restantes al clúster

Después de crear un nuevo clúster, debe usar el Asistente de configuración de clúster para unir los nodos restantes al clúster de uno en uno. El asistente le permite configurar

la interfaz de gestión de nodos de cada nodo.

Cuando se unen dos nodos en un clúster, se crea un par de alta disponibilidad (ha). Si se une a 4 nodos, se crean dos pares de alta disponibilidad. Para obtener más información sobre alta disponibilidad, consulte ["Obtenga más información sobre ha"](#).

Solo puede unir un nodo a la vez al clúster. Tras comenzar a unir un nodo al clúster, debe completar la operación de unión de ese nodo y el nodo debe formar parte del clúster antes de poder unir el siguiente nodo.

Mejor práctica: Si tiene un sistema FAS2720 con 24 o menos unidades NL-SAS, debe verificar que el valor predeterminado de la configuración de almacenamiento es activo/pasivo para optimizar el rendimiento. Para obtener más información, consulte ["Configuración de una configuración activo-pasivo en nodos mediante la partición de datos raíz"](#)

1. Inicie sesión en el nodo que planea unir en el clúster.

El asistente de configuración de clúster se inicia en la consola.

```
Welcome to the cluster setup wizard....
```

2. Reconozca la declaración de AutoSupport.



AutoSupport está habilitado de forma predeterminada.

```
Type yes to confirm and continue {yes}: yes
```

3. Siga las instrucciones que aparecen en pantalla para asignar una dirección IP al nodo.

A partir de ONTAP 9.13.1, puede asignar direcciones IPv6 para las LIF de gestión en las plataformas A800 y FAS8700. Para versiones de ONTAP anteriores a 9.13.1, o para 9.13.1 o versiones posteriores en otras plataformas, debe asignar direcciones IPv4 para las LIF de gestión y, después, convertirlas a IPv6 tras completar la configuración del clúster.

4. Pulse **Intro** para continuar.

```
Do you want to create a new cluster or join an existing cluster?  
{create, join}:
```

5. Una el nodo al clúster: `join`
6. Siga las instrucciones que aparecen en pantalla para configurar el nodo y unirlo al clúster.
7. Tras completar la configuración, compruebe que el nodo esté en buen estado y que pueda participar en el clúster: `cluster show`

En el siguiente ejemplo se muestra un clúster después de unirle el segundo nodo (cluster1-02):

```
cluster1::> cluster show
Node                Health  Eligibility
-----
cluster1-01         true   true
cluster1-02         true   true
```

Puede acceder al Asistente de configuración de clúster para cambiar cualquiera de los valores introducidos para la SVM de administrador o la SVM de nodo mediante el comando `cluster setup`.

8. Repita esta acción para cada uno de los nodos restantes.

Después de terminar

Si es necesario, ["Convertir de IPv4 a IPv6"](#).

Convierta las LIF de gestión de IPv4 a IPv6

A partir de ONTAP 9.13.1, se pueden asignar direcciones IPv6 a las LIF de administración en plataformas A800 y FAS8700 durante la configuración inicial del clúster. Para versiones de ONTAP anteriores a 9.13.1, o para 9.13.1 o versiones posteriores en otras plataformas, primero debe asignar direcciones IPv4 a las LIF de gestión y, a continuación, convertir en direcciones IPv6 una vez completada la configuración del clúster.

Pasos

1. Habilite IPv6 para el clúster:

```
network options ipv6 modify -enable true
```

2. Establecer privilegio en avanzado:

```
set priv advanced
```

3. Vea la lista de prefijos de RA aprendidos en varias interfaces:

```
network ndp prefix show
```

4. Cree una LIF de gestión IPv6:

Utilice el formato `prefix::id` En el parámetro `address` para construir la dirección IPv6 manualmente.

```
network interface create -vserver <svm_name> -lif <LIF> -home-node  
<home_node> -home-port <home_port> -address <IPv6prefix::id> -netmask  
-length <netmask_length> -failover-policy <policy> -service-policy  
<service_policy> -auto-revert true
```

5. Compruebe que la LIF se ha creado:

```
network interface show
```

6. Compruebe que se pueda acceder a la dirección IP configurada:

```
network ping6
```

7. Marcar el LIF IPv4 como inactivo de forma administrativa:

```
network interface modify -vserver <svm_name> -lif <lif_name> -status  
-admin down
```

8. Elimine la LIF de gestión de IPv4:

```
network interface delete -vserver <svm_name> -lif <lif_name>
```

9. Confirmar que se ha eliminado el LIF de gestión de IPv4:

```
network interface show
```

Compruebe su clúster con Active IQ Config Advisor

Después de haber Unido todos los nodos al nuevo clúster, debe ejecutar Active IQ Config Advisor para validar su configuración y comprobar si hay errores de configuración comunes.

Config Advisor es una aplicación basada en web que instala en su portátil, máquina virtual o servidor, y funciona en plataformas Windows, Linux y Mac.

Config Advisor ejecuta una serie de comandos para validar la instalación y comprobar el estado general de la configuración, incluido el clúster y los switches de almacenamiento.

1. Descargue e instale Active IQ Config Advisor.

["Active IQ Config Advisor"](#)

2. Inicie Active IQ y configure una frase de contraseña cuando se le solicite.
3. Revise su configuración y haga clic en **Guardar**.
4. En la página **objetivos**, haga clic en **validación posterior a la implementación de ONTAP**.
5. Seleccione el modo guiado o experto.

Si elige el modo guiado, los conmutadores conectados se detectan automáticamente.

6. Introduzca las credenciales del clúster.
7. (Opcional) haga clic en **validación de formulario**.
8. Para comenzar a recopilar datos, haga clic en **Guardar y evaluar**.
9. Después de completar la recopilación de datos, en **Monitor de trabajo > acciones**, vea los datos recopilados haciendo clic en el icono **Vista de datos** y vea los resultados haciendo clic en el icono **resultados**.
10. Resuelva los problemas identificados por Config Advisor.

Sincronice la hora del sistema en todo el clúster

La sincronización de la hora asegura que todos los nodos del clúster tengan la misma hora y evita errores de CIFS y Kerberos.

Debe configurarse un servidor de Protocolo de hora de red (NTP) en el sitio. A partir de ONTAP 9.5, puede configurar el servidor NTP con autenticación simétrica.

Para obtener más información, consulte ["Gestionar la hora del clúster \(solo administradores de clúster\)"](#).

Para sincronizar la hora en todo el clúster, debe asociarlo con uno o varios servidores NTP.

1. Compruebe que la hora y la zona horaria del sistema estén configuradas correctamente para cada nodo.

Todos los nodos del clúster deben tener la misma zona horaria.

- a. Use el comando `cluster date show` para mostrar la fecha, la hora y la zona horaria actuales de cada nodo.

```
cluster1::> cluster date show
Node          Date          Time zone
-----
cluster1-01   01/06/2015 09:35:15 America/New_York
cluster1-02   01/06/2015 09:35:15 America/New_York
cluster1-03   01/06/2015 09:35:15 America/New_York
cluster1-04   01/06/2015 09:35:15 America/New_York
4 entries were displayed.
```

- b. Use el comando `cluster date modify` para cambiar la fecha o la zona horaria de todos los nodos.

En este ejemplo se cambia la zona horaria del clúster para que sea GMT:

```
cluster1::> cluster date modify -timezone GMT
```

2. Use el comando `cluster time-service ntp Server create` para asociar el clúster con el servidor NTP.

- Para configurar el servidor NTP sin autenticación simétrica, introduzca el siguiente comando: `cluster time-service ntp server create -server server_name`
- Para configurar el servidor NTP con autenticación simétrica, introduzca el siguiente comando: `cluster time-service ntp server create -server server_ip_address -key-id key_id`



La autenticación simétrica está disponible a partir de ONTAP 9.5. No está disponible en ONTAP 9.4 ni en versiones anteriores.

En este ejemplo se supone que se ha configurado DNS para el clúster. Si no ha configurado DNS, debe especificar la dirección IP del servidor NTP:

```
cluster1::> cluster time-service ntp server create -server  
ntp1.example.com
```

3. Compruebe que el clúster esté asociado con un servidor NTP: `cluster time-service ntp server show`

```
cluster1::> cluster time-service ntp server show  
Server                Version  
-----  
ntp1.example.com      auto
```

Información relacionada

["Administración del sistema"](#)

Comandos para gestionar la autenticación simétrica en servidores NTP

A partir de ONTAP 9.5, se admite la versión 3 del protocolo de tiempo de redes (NTP). NTPv3 incluye autenticación simétrica mediante claves SHA-1 que aumenta la seguridad de la red.

| Para hacer esto... | Se usa este comando... |
|---|--|
| Configure un servidor NTP sin autenticación simétrica | <code>cluster time-service ntp server create -server server_name</code> |
| Configure un servidor NTP con autenticación simétrica | <code>cluster time-service ntp server create -server server_ip_address -key-id key_id</code> |

| Para hacer esto... | Se usa este comando... |
|--|--|
| <p>Habilite la autenticación simétrica para un servidor NTP existente</p> <p>Un servidor NTP existente se puede modificar para habilitar la autenticación mediante la adición del identificador de clave requerido</p> | <pre>cluster time-service ntp server modify -server server_name -key-id key_id</pre> |
| Configure una clave NTP compartida | <pre>cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value</pre> <p>Nota: una ID hace referencia a las claves compartidas. El ID, su tipo y el valor deben ser idénticos tanto en el nodo como en el servidor NTP</p> |
| Configure un servidor NTP con un ID de clave desconocido | <pre>cluster time-service ntp server create -server server_name -key-id key_id</pre> |
| Configure un servidor con un ID de clave no configurado en el servidor NTP. | <pre>cluster time-service ntp server create -server server_name -key-id key_id</pre> <p>Nota: el ID de clave, el tipo y el valor deben ser idénticos al ID de clave, el tipo y el valor configurados en el servidor NTP.</p> |
| Deshabilitar la autenticación simétrica | <pre>cluster time-service ntp server modify -server server_name -authentication disabled</pre> |

Tareas de configuración del sistema adicionales que se deben realizar

Después de configurar un clúster, puede usar System Manager o la interfaz de línea de comandos (CLI) de ONTAP para continuar configurando el clúster.

| Tarea de configuración del sistema | Recurso |
|---|---|
| <p>Configurar redes:</p> <ul style="list-style-type: none"> • Cree dominios de retransmisión • Crear subredes • Cree espacios IP | "Configuración de la red" |
| Configure Service Processor | "Administración del sistema" |
| Distribuir los agregados | "Gestión de discos y agregados" |

| Tarea de configuración del sistema | Recurso |
|--|---|
| Crear y configurar las máquinas virtuales de almacenamiento de datos (SVM) | "Configuración de NFS" "Configuración de SMB" "Administración de SAN" |
| Configure las notificaciones de eventos | "Configuración de EMS" |

Configure el software de cabina SAN All-Flash

Información general de la configuración del software de la cabina SAN all-flash

Las cabinas SAN all-flash (ASAS) de NetApp están disponibles a partir de ONTAP 9.7. ASAS son soluciones all-flash solo SAN creadas sobre las plataformas probadas de AFF de NetApp.

Las plataformas ASA utilizan activo-activo simétrico para la multivía. Todas las rutas son activas/optimizadas de modo que, en caso de conmutación al nodo de respaldo del almacenamiento, el host no necesita esperar a que se produzca la transición ALUA de las rutas de conmutación al nodo de respaldo para reanudar las operaciones de I/O. Esto reduce el tiempo de recuperación tras fallos.

Configure un ASA

Las cabinas SAN All-Flash (ASAS) siguen el mismo procedimiento de configuración que los sistemas no ASA.

System Manager le guía por los procedimientos necesarios para inicializar su clúster, crear un nivel local, configurar protocolos y aprovisionar almacenamiento para su ASA.

[Comience a utilizar la configuración del clúster de ONTAP.](#)

Configuración y utilidades del host ASA

La configuración del host para configurar cabinas All Flash SAN (ASAS) es la misma que la de todos los demás hosts SAN.

Puede descargar la ["Software Host Utilities de NetApp"](#) para los hosts específicos del sitio de soporte.

Formas de identificar un sistema ASA

Puede identificar un sistema ASA mediante System Manager o mediante la interfaz de línea de comandos (CLI) de ONTAP.

- **Desde el panel del Administrador del sistema:** Haz clic en **Clúster > Descripción general** y luego selecciona el nodo del sistema.

La **PERSONALITY** se muestra como **All-Flash SAN Array**.

- **Desde la CLI:** Ingrese el `san config show` comando.

El valor de las «cabinas SAN all-flash» es auténtico para los sistemas ASA.

Información relacionada

- ["Informe técnico 4968: Integridad y disponibilidad de datos de las cabinas All-SAN de NetApp"](#)
- ["Informe técnico de NetApp 4080: Prácticas recomendadas para SAN moderno"](#)

Límites de configuración y compatibilidad de cabinas All Flash SAN

Los límites de configuración y la compatibilidad de las cabinas All Flash SAN (ASA) varían según la versión de ONTAP.

Los detalles más actuales sobre los límites de configuración admitidos están disponibles en ["Hardware Universe de NetApp"](#).

Nodos y protocolos SAN por clúster

La compatibilidad de ASA con los protocolos SAN y los nodos por clúster es la siguiente:

| Iniciando con ONTAP... | Compatibilidad con protocolos | N.o máx. De nodos por clúster |
|------------------------|---|--|
| 9.12.1 | <ul style="list-style-type: none">• NVMe (compatible con configuraciones IP de MetroCluster de 4 nodos y configuraciones IP distintas de MetroCluster)• FC• iSCSI | 12 |
| 9.9.1 | <ul style="list-style-type: none">• NVMe (compatible con configuraciones IP que no sean de MetroCluster)• FC• iSCSI | <ul style="list-style-type: none">• 12 nodos (para configuraciones IP que no sean de MetroCluster)• 8 nodos (para configuraciones IP de MetroCluster) |
| 9,7 | <ul style="list-style-type: none">• FC• iSCSI | 4 |

Compatibilidad con puertos persistentes

A partir de ONTAP 9,8, los puertos persistentes se habilitan de forma predeterminada en las cabinas all-flash SAN (ASAS) que se configuran para usar el protocolo FC. Los puertos persistentes solo están disponibles para FC y requieren pertenencia a una zona identificada por nombre de puerto WWPN.

Los puertos persistentes reducen el impacto de las tomas de control al crear un LIF en la sombra en el puerto físico correspondiente del partner de alta disponibilidad. Cuando se toma el control de un nodo, el LIF de respaldo del nodo del partner asume la identidad del LIF original, incluida la WWPN. Antes de que el estado de la ruta al nodo tomado en defectuoso, la LIF redundante aparece como una ruta activa/optimizada para la pila MPIO del host y se cambia la I/O. De este modo, se reduce el trastorno de I/O porque el host siempre ve el mismo número de rutas al destino, incluso durante las operaciones de conmutación al nodo de respaldo del almacenamiento.

Para los puertos persistentes, las siguientes características de puerto FCP deben ser idénticas en el par de

alta disponibilidad:

- Números de puertos FCP
- Nombres de puerto FCP
- Velocidades de puerto FCP
- División en zonas basada en WWPN de LIF FCP

Si alguna de estas características no es idéntica en la pareja de alta disponibilidad, se genera el siguiente mensaje de EMS:

```
EMS : scsiblade.lif.persistent.ports.fcp.init.error
```

Para obtener más información sobre los puertos persistentes, consulte ["Informe técnico de NetApp 4080: Prácticas recomendadas para SAN moderno"](#).

Actualice ONTAP

Información general de la actualización de ONTAP

Al actualizar el software ONTAP, puede aprovechar las nuevas y mejoradas funciones de ONTAP que le ayudarán a reducir costes, acelerar las cargas de trabajo críticas, mejorar la seguridad y ampliar el alcance de la protección de datos disponible para su organización.

Una importante actualización de ONTAP consiste en pasar de una versión con números ONTAP inferiores a superiores. Un ejemplo sería una actualización de su clúster de ONTAP 9,8 a ONTAP 9.12.1. Una actualización menor (o un parche) consiste en pasar de una versión de ONTAP inferior a una versión de ONTAP superior dentro de la misma versión numerada. Un ejemplo sería una actualización de su clúster de ONTAP 9.12.1P1 a 9.12.1P4.

Para comenzar, debe ["prepare la actualización"](#). Si tienes un contrato activo de SupportEdge para el asesor digital de Active IQ, deberías hacerlo ["Planifique la actualización con el asesor de actualizaciones"](#). El asesor de actualizaciones ofrece inteligencia que le ayuda a minimizar la incertidumbre y el riesgo al evaluar su clúster y crear un plan de actualización específico de su configuración.

Después de prepararse para la actualización, se recomienda realizar las actualizaciones con ["Actualización automatizada y no disruptiva \(ANDU\) de System Manager"](#). ANDU aprovecha la tecnología de conmutación al nodo de respaldo de alta disponibilidad de ONTAP para garantizar que los clústeres siguen sirviendo datos sin interrupciones durante la actualización.



A partir de ONTAP 9.12.1, System Manager está totalmente integrado con BlueXP. Si BlueXP está configurado en tu sistema, puedes actualizarlo a través del entorno de trabajo de BlueXP.

Si necesita ayuda para actualizar su software ONTAP, los servicios profesionales de NetApp ofrecen un ["Servicio de renovación gestionada"](#). Si está interesado en usar este servicio, póngase en contacto con su representante de ventas de NetApp o con ["Envíe el formulario de consulta de ventas de NetApp"](#). El Servicio de Actualización Gestionada, así como otros tipos de soporte de actualización están disponibles para los clientes con ["Servicios de SupportEdge Expert"](#) sin coste adicional.

¿Cuándo debo actualizar ONTAP?

Debe actualizar su software ONTAP en una cadencia regular. La actualización de ONTAP le permite aprovechar las funciones y funcionalidades nuevas y mejoradas, e implementar las correcciones actuales para problemas conocidos.

Importantes renovaciones de ONTAP

Una importante actualización o versión de funciones de ONTAP suele incluir:

- Nuevas funciones de ONTAP
- Cambios clave en la infraestructura, como cambios fundamentales en el funcionamiento de NetApp WAFL o en el funcionamiento de RAID
- Compatibilidad con nuevos sistemas de hardware de ingeniería de NetApp
- Soporte para componentes de hardware de reemplazo, como tarjetas de interfaz de red más recientes o adaptadores de bus del host

Los nuevos lanzamientos de ONTAP tienen derecho a un soporte completo durante 3 años. NetApp recomienda ejecutar la versión más reciente durante 1 año tras la disponibilidad general (GA) y, a continuación, utilizar el tiempo restante dentro del plazo de soporte completo para planificar la transición a una versión de ONTAP más reciente.

Actualizaciones de revisiones de ONTAP

Las actualizaciones de parches proporcionan correcciones oportunas para errores críticos que no pueden esperar a que se publique la siguiente versión principal de la función de ONTAP. Las actualizaciones de parches no críticas se deben aplicar cada 3-6 meses. Las actualizaciones de parches críticos se deben aplicar lo antes posible.

Más información acerca de ["niveles mínimos de parches recomendados"](#) Para versiones ONTAP.

Fechas de lanzamiento de ONTAP

A partir del lanzamiento de ONTAP 9,8, NetApp ofrece lanzamientos de ONTAP dos veces al año. Si bien los planes pueden modificarse, el objetivo es ofrecer nuevos lanzamientos de ONTAP en el segundo y cuarto trimestre de cada año. Utilice esta información para planificar el período de tiempo de su actualización para aprovechar la última versión de ONTAP.

| Versión | Fecha de lanzamiento |
|---------|----------------------|
| 9.14.1 | A enero de 2024 |
| 9.13.1 | Junio de 2023 |
| 9.12.1 | Febrero de 2023 |
| 9.11.1 | Julio de 2022 |
| 9.10.1 | A enero de 2022 |

| Versión | Fecha de lanzamiento |
|---------|----------------------|
| 9.9.1 | Junio de 2021 |

Niveles de soporte de ONTAP

El nivel de soporte disponible para una versión específica de ONTAP varía en función de cuándo se lanzó el software.

| Nivel de soporte | Soporte completo | | | Soporte limitado | | Soporte de autoservicio | | |
|---|------------------|----|----|------------------|----|-------------------------|----|----|
| Año | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Acceso a la documentación en línea | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí |
| Soporte técnico | Sí | Sí | Sí | Sí | Sí | | | |
| Análisis de las causas subyacentes | Sí | Sí | Sí | Sí | Sí | | | |
| Descargas de software de | Sí | Sí | Sí | Sí | Sí | | | |
| Actualizaciones de servicio (versiones de parches [P-releases]) | Sí | Sí | Sí | | | | | |
| Alertas sobre vulnerabilidades | Sí | Sí | Sí | | | | | |

Información relacionada

- Aprenda "[Novedades de las versiones de ONTAP compatibles actualmente](#)".
- Más información acerca de "[Versiones mínimas recomendadas de ONTAP](#)".
- Más información acerca de "[Compatibilidad con la versión del software ONTAP](#)".
- Obtenga más información sobre la "[Modelo de versión de ONTAP](#)".

Ejecute comprobaciones automatizadas previas a la actualización de ONTAP antes de una actualización planificada

No tiene que estar en proceso de actualizar su software ONTAP para ejecutar las comprobaciones previas a la actualización automatizada de ONTAP. La ejecución de las comprobaciones previas a la actualización independientemente del proceso de actualización automatizada de ONTAP le permite ver qué comprobaciones se realizan en su clúster y le ofrece una lista de los errores o advertencias que se deben corregir antes

de empezar la actualización. Por ejemplo, supongamos que espera actualizar el software ONTAP durante un plazo de mantenimiento programado en dos semanas. Mientras espera la fecha programada, puede ejecutar las comprobaciones previas automatizadas de la actualización y realizar las acciones correctivas que sean necesarias antes de su ventana de mantenimiento. Esto reducirá los riesgos de errores de configuración inesperados después de iniciar la actualización.

Si está listo para comenzar la actualización del software ONTAP, no es necesario realizar este procedimiento. Debe seguir el "[proceso de actualización automatizado](#)", que incluye la ejecución de las comprobaciones previas de actualización automatizadas.



Para las configuraciones de MetroCluster, primero debe ejecutar estos pasos en el clúster A y, a continuación, ejecutar los mismos pasos en el clúster B.

Antes de empezar

Usted debe "[Descargue la imagen del software ONTAP de destino](#)".

Para ejecutar las comprobaciones previas de actualización automatizadas de un "[actualización directa de varios saltos](#)", Solo necesita descargar el paquete de software para su versión de destino ONTAP. No será necesario cargar la versión intermedia de ONTAP hasta que comience la actualización. Por ejemplo, si ejecuta comprobaciones automáticas previas a la actualización para una actualización de 9.8 a 9.13.1, deberá descargar el paquete de software de ONTAP 9.13.1. No es necesario descargar el paquete de software para ONTAP 9.12.1.

Ejemplo 1. Pasos

System Manager

1. Valide la imagen de destino de ONTAP:



Si está actualizando una configuración de MetroCluster, debe validar el clúster A y, a continuación, repetir el proceso de validación en el clúster B.

a. Según la versión de ONTAP que esté ejecutando, realice uno de los pasos siguientes:

| Si está ejecutando... | Realice lo siguiente... |
|-----------------------|---|
| ONTAP 9,8 o posterior | Haga clic en Cluster > Overview . |
| ONTAP 9.5, 9.6 y 9.7 | Haga clic en Configuración > clúster > Actualizar . |
| ONTAP 9.4 o anterior | Haga clic en Configuración > actualización de clúster . |

b. En la esquina derecha del panel **Overview**, haga clic en .

c. Haga clic en **actualización de ONTAP**.

d. En la pestaña **Cluster Update**, agregue una nueva imagen o seleccione una imagen disponible.

| Si desea... | Realice lo siguiente... |
|--|---|
| Agregue una nueva imagen de software desde una carpeta local Ya deberías tener "se ha descargado la imagen" al cliente local. | <ul style="list-style-type: none">i. En Imágenes de software disponibles, haga clic en Agregar desde local.ii. Busque la ubicación en la que guardó la imagen de software, seleccione la imagen y, a continuación, haga clic en Abrir. |
| Añada una nueva imagen de software desde un servidor HTTP o FTP | <ul style="list-style-type: none">i. Haga clic en Agregar desde el servidor.ii. En el cuadro de diálogo Agregar una nueva imagen de software, introduzca la URL del servidor HTTP o FTP en el que descargó la imagen del software ONTAP del sitio de soporte de NetApp. Para el FTP anónimo, debe especificar la dirección URL en el ftp://anonymous@ftpserver formato.iii. Haga clic en Agregar. |
| Seleccione una imagen disponible | Elija una de las imágenes mostradas. |

e. Haga clic en **Validar** para ejecutar las comprobaciones de validación previas a la actualización.

Si se encuentran errores o advertencias durante la validación, se muestran junto con una lista de acciones correctivas. Debe resolver todos los errores antes de continuar con la actualización. Se recomienda también resolver las advertencias.

CLI

1. Cargue la imagen de software ONTAP de destino en el repositorio de paquetes del cluster:

```
cluster image package get -url location
```

```
cluster1::> cluster image package get -url  
http://www.example.com/software/9.13.1/image.tgz
```

```
Package download completed.  
Package processing completed.
```

2. Compruebe que el paquete de software esté disponible en el repositorio del paquete de clúster:

```
cluster image package show-repository
```

```
cluster1::> cluster image package show-repository  
Package Version  Package Build Time  
-----  
9.13.1           MM/DD/YYYY 10:32:15
```

3. Ejecute las comprobaciones automatizadas previas a la actualización:

```
cluster image validate -version package_version_number -show  
-validation-details true
```



Si está realizando una "[actualización directa de varios saltos](#)", utilice el paquete target ONTAP para la verificación. No es necesario validar la imagen de actualización intermedia por separado. Por ejemplo, si va a actualizar de 9.8 a 9.13.1, debe usar el paquete 9.13.1 para la verificación. No es necesario validar el paquete 9.12.1 por separado.

```
cluster1::> cluster image validate -version 9.14.1 -show-validation  
-details true
```

It can take several minutes to complete validation...
Validation checks started successfully. Run the "cluster image
show-update-progress" command to check validation status.

4. Compruebe el estado de validación:

```
cluster image show-update-progress
```



Si el **Status** está en curso, espere y ejecute el comando de nuevo hasta que se complete.

```
cluster1::*> cluster image show-update-progress
```

| Update Phase | Status | Duration |
|-------------------|-----------|----------|
| Pre-update checks | completed | 00:10:00 |

Details:

| Pre-update Check | Status | Error-Action |
|--|---------|--------------|
| AMPQ Router and Broker Config Cleanup | OK | N/A |
| Aggregate online status and parity check | OK | N/A |
| Aggregate plex resync status check | OK | N/A |
| Application Provisioning Cleanup | OK | N/A |
| Autoboot Bootargs Status | OK | N/A |
| Backend | OK | N/A |
| ... | | |
| Volume Conversion In Progress Check | OK | N/A |
| Volume move progress status check | OK | N/A |
| Volume online status check | OK | N/A |
| iSCSI target portal groups status check | OK | N/A |
| Overall Status | Warning | Warning |

75 entries were displayed.

Se muestra una lista de comprobaciones previas completas y automatizadas a la actualización, junto con cualquier error o advertencia que deba solucionarse antes de comenzar el proceso de actualización.

Resultado de ejemplo completo de comprobaciones previas de actualización

```
cluster1::*> cluster image validate -version 9.14.1 -show-validation
-details true
```

It can take several minutes to complete validation...

WARNING: There are additional manual upgrade validation checks that must be performed after these automated validation checks have completed successfully.

Refer to the Upgrade Advisor Plan or the "What should I verify before I upgrade with or without Upgrade Advisor" section in the "Upgrade ONTAP" documentation for the remaining manual validation checks that need to be performed before update.

Upgrade ONTAP documentation available at: <https://docs.netapp.com/us-en/ontap/upgrade/index.html>

The list of checks are available at: https://docs.netapp.com/us-en/ontap/upgrade/task_what_to_check_before_upgrade.html

Failing to do so can result in an update failure or an I/O disruption. Please use Interoperability Matrix Tool (IMT <http://mysupport.netapp.com/matrix>) to verify host system supportability configuration information.

Validation checks started successfully. Run the "cluster image show-update-progress" command to check validation status.

```
fas2820-2n-wic-1::*> cluster image show-update-progress
```

| Update Phase | Status | Estimated Duration | Elapsed Duration |
|-------------------|-------------|--------------------|------------------|
| Pre-update checks | in-progress | 00:10:00 | 00:00:42 |

Details:

| Pre-update Check | Status | Error-Action |
|------------------|--------|--------------|
| ----- | ----- | ----- |
| ----- | ----- | ----- |

```
fas2820-2n-wic-1::*> cluster image show-update-progress
```

| Update Phase | Status | Estimated Duration | Elapsed Duration |
|-------------------|-----------|--------------------|------------------|
| Pre-update checks | completed | 00:10:00 | 00:01:03 |

Details:

| Pre-update Check | Status | Error-Action |
|--|---------|---|
| ----- | ----- | ----- |
| AMPQ Router and Broker Config Cleanup | OK | N/A |
| Aggregate online status and parity check | OK | N/A |
| Aggregate plex resync status check | OK | N/A |
| Application Provisioning Cleanup | OK | N/A |
| Autoboot Bootargs Status | OK | N/A |
| Backend Configuration Status | OK | N/A |
| Boot Menu Status | Warning | Warning: bootarg.init.bootmenu is enabled on nodes: fas2820-wic- 1a, fas2820-wic-1b. The boot process of the nodes will be delayed. Action: Set the bootarg.init.bootmenu bootarg to false before proceeding with the upgrade. |
| Broadcast Domain availability and uniqueness for HA pair status | OK | N/A |
| CIFS compatibility status check | OK | N/A |
| CLAM quorum online status check | OK | N/A |
| CPU Utilization Status | OK | N/A |
| Capacity licenses install status check | OK | N/A |
| Check For SP/BMC Connectivity To Nodes | OK | N/A |

| | | |
|---|----|-----|
| Check LDAP fastbind users using unsecure connection. | OK | N/A |
| Check for unsecure kex algorithm configurations. | OK | N/A |
| Check for unsecure mac configurations. | OK | N/A |
| Cloud keymanager connectivity check | OK | N/A |
| Cluster health and eligibility status | OK | N/A |
| Cluster quorum status check | OK | N/A |
| Cluster/management switch check | OK | N/A |
| Compatible New Image Check | OK | N/A |
| Current system version check if it is susceptible to possible outage during NDU | OK | N/A |
| Data ONTAP Version and Previous Upgrade Status | OK | N/A |
| Data aggregates HA policy check | OK | N/A |
| Disk status check for failed, broken or non-compatibility | OK | N/A |
| Duplicate Initiator Check | OK | N/A |
| Encryption key migration status check | OK | N/A |
| External key-manager with legacy KMIP client check | OK | N/A |
| External keymanager key server status check | OK | N/A |
| Fabricpool Object Store Availability | OK | N/A |
| High Availability | OK | N/A |

| | | |
|---------------------|---------|----------------------------------|
| configuration | | |
| status check | | |
| Infinite Volume | OK | N/A |
| availability check | | |
| LIF failover | OK | N/A |
| capability status | | |
| check | | |
| LIF health check | OK | N/A |
| LIF load balancing | OK | N/A |
| status check | | |
| LIFs is on home | OK | N/A |
| node status | | |
| Logically over | OK | N/A |
| allocated DP | | |
| volumes check | | |
| MetroCluster | OK | N/A |
| configuration | | |
| status check for | | |
| compatibility | | |
| Minimum number of | OK | N/A |
| aggregate disks | | |
| check | | |
| NAE Aggregate and | OK | N/A |
| NVE Volume | | |
| Encryption Check | | |
| NDMP sessions check | OK | N/A |
| NFS mounts status | Warning | Warning: This cluster is serving |
| NFS | | |
| check | | clients. If NFS soft mounts are |
| used, | | |
| | | there is a possibility of |
| frequent | | |
| | | NFS timeouts and race conditions |
| that | | |
| | | can lead to data corruption |
| during | | |
| | | the upgrade. |
| | | Action: Use NFS hard mounts, if |
| | | possible. To list Vservers |
| running | | |
| | | NFS, run the following command: |
| | | vserver nfs show |
| Name Service | OK | N/A |
| Configuration DNS | | |
| Check | | |
| Name Service | OK | N/A |

Configuration LDAP

Check

| | | |
|--|---------|--|
| Node to SP/BMC connectivity check | OK | N/A |
| OKM/KMIP enabled systems - Missing keys check | OK | N/A |
| ONTAP API to REST transition warning data last 30 days approaching automation REST | Warning | Warning: NetApp ONTAP API has been used on this cluster for ONTAP storage management within the last 30 days. NetApp ONTAP API is approaching end of availability. Action: Transition your tools from ONTAP API to ONTAP API. For more details, refer to CPC-00410 - End of availability: ONTAPI |
| | | https://mysupport.netapp.com/info/communications/ECMLP2880232.html |
| ONTAP Image Capability Status | OK | N/A |
| OpenSSL 3.0.x upgrade validation check | OK | N/A |
| Openssh 7.2 upgrade validation check | OK | N/A |
| Platform Health Monitor check | OK | N/A |
| Pre-Update Configuration Verification | OK | N/A |
| RDB Replica Health Check | OK | N/A |
| Replicated database schema consistency check | OK | N/A |
| Running Jobs Status | OK | N/A |
| SAN LIF association status check | OK | N/A |

| | | |
|--|----|-----|
| SAN compatibility for manual configurability check | OK | N/A |
| SAN kernel agent status check | OK | N/A |
| Secure Purge operation Check | OK | N/A |
| Shelves and Sensors check | OK | N/A |
| SnapLock Version Check | OK | N/A |
| SnapMirror Synchronous relationship status check | OK | N/A |
| SnapMirror compatibility status check | OK | N/A |
| Supported platform check | OK | N/A |
| Target ONTAP release support for FiberBridge 6500N check | OK | N/A |
| Upgrade Version Compatibility Status | OK | N/A |
| Verify all bgp peer-groups are in the up state | OK | N/A |
| Verify if a cluster management LIF exists | OK | N/A |
| Verify that e0M is home to no LIFs with high speed services. | OK | N/A |
| Volume Conversion In Progress Check | OK | N/A |
| Volume move progress status check | OK | N/A |
| Volume online status check | OK | N/A |
| iSCSI target portal groups status check | OK | N/A |

Overall Status Warning Warning
75 entries were displayed.

Prepárese para una actualización de ONTAP

Prepárese para una actualización del software ONTAP

Prepararse correctamente para una actualización de software de ONTAP le ayuda a identificar y reducir los posibles riesgos o bloqueadores de actualización antes de iniciar el proceso de actualización. Durante la preparación de la actualización, también puede identificar cualquier consideración especial que deba tener en cuenta antes de la actualización. Por ejemplo, si se habilita el modo FIPS SSL en su clúster y las cuentas de administrador utilizan claves públicas SSH para la autenticación, debe verificar que el algoritmo de clave de host sea compatible con la versión de ONTAP de destino.

Debe hacer lo siguiente para prepararse para una actualización:

1. ["Cree un plan de actualización"](#).

Si tiene un contrato activo de SupportEdge para ["Asesor digital de Active IQ"](#), Planifique su actualización con Upgrade Advisor. Si no tiene acceso al asesor digital de Active IQ, cree su propio plan de actualización.

2. ["Elija la versión de ONTAP objetivo"](#).

3. Revise la ["Notas de la versión de ONTAP"](#) para la versión de destino.

La sección "Advertencias de actualización" describe los problemas potenciales que debe tener en cuenta antes de actualizar a la nueva versión. Las secciones "Novedades" y "Problemas y limitaciones conocidos" describen el nuevo comportamiento del sistema después de actualizar a la nueva versión.

4. ["Confirme la compatibilidad de ONTAP para la configuración de hardware"](#).

La plataforma de hardware, los switches de administración de clústeres y los switches IP de MetroCluster deben admitir la versión de destino. Si el clúster está configurado para SAN, la configuración de SAN debe ser totalmente compatible.

5. ["Utilice Active IQ Config Advisor para verificar que no haya errores de configuración comunes."](#)

6. Revise el ONTAP compatible ["rutas de actualización"](#) para determinar si puede realizar una actualización directa o si necesita completar la actualización por etapas.

7. ["Compruebe la configuración de recuperación tras fallos de LIF"](#).

Antes de realizar una actualización, tiene que verificar que las políticas de conmutación por error del clúster y los grupos de conmutación por error están configurados correctamente.

8. ["Compruebe la configuración de enrutamiento de la SVM"](#).

9. ["Verificar consideraciones especiales"](#) para el clúster.

Si existen ciertas configuraciones en el clúster, debe realizar ciertas acciones específicas antes de iniciar una actualización de software de ONTAP.

10. "Reinicie el SP o BMC".

Cree un plan de actualización de ONTAP

Se recomienda crear un plan de actualización. Si tiene una activa ["Servicios de SupportEdge"](#) contrato para ["Asesor digital de Active IQ"](#), Puede utilizar el Asesor de actualizaciones para generar un plan de actualización. De lo contrario, debes crear tu propio plan.

Planifique su actualización con Upgrade Advisor

El servicio Asesor de actualizaciones del Asesor digital de Active IQ proporciona inteligencia que le ayuda a planificar su actualización y minimiza la incertidumbre y el riesgo.

Active IQ identifica problemas en su entorno que se pueden resolver actualizando a una versión más reciente de ONTAP. El servicio de asesor de actualización le ayuda a planificar una actualización correcta y proporciona un informe de problemas que puede que tenga que conocer en la versión de ONTAP a la que está actualizando.

Pasos

1. ["Inicie Active IQ"](#)
2. En Active IQ ["vea cualquier riesgo asociado con su clúster y tome manualmente acciones correctivas"](#).

Los riesgos incluidos en las categorías **SW Config Change**, **HW Config Change** y **HW Replacement** deben resolverse antes de realizar una actualización de ONTAP.

3. Revise la ruta de actualización recomendada y ["genere su plan de actualización"](#).

¿Cuánto tiempo tardará en realizarse una actualización de ONTAP?

Debería planificar al menos 30 minutos para completar los pasos preparatorios para una actualización de ONTAP, 60 minutos para actualizar cada par de alta disponibilidad y al menos 30 minutos para completar los pasos posteriores a la actualización.



Si utiliza el cifrado de NetApp con un servidor de gestión de claves externo y el protocolo de interoperabilidad de gestión de claves (KMIP), debería esperar que la actualización de cada pareja de alta disponibilidad tenga más de una hora.

Estas directrices de duración de la actualización se basan en configuraciones y cargas de trabajo típicas. Puede usar estas directrices para estimar el tiempo que se necesita para realizar una actualización no disruptiva en su entorno. La duración real del proceso de actualización dependerá del entorno individual y del número de nodos.

Elija la versión de ONTAP objetivo para una actualización

Cuando utiliza el asesor de actualizaciones para generar un plan de actualización para su clúster, el plan incluye una versión de ONTAP de destino recomendada para la actualización. La recomendación proporcionada por el asesor de actualización se basa en la configuración actual y en la versión de ONTAP actual.

Si no utiliza el Asesor de actualizaciones para planificar la actualización, debe elegir la versión de ONTAP de destino para la actualización en función de las recomendaciones de NetApp o si tiene que estar en la versión

mínima para satisfacer las necesidades de rendimiento.

- Actualizar a la última versión disponible (recomendado)

NetApp recomienda actualizar el software ONTAP a la versión de revisión más reciente de la última versión numerada de ONTAP. Si no es posible porque los sistemas de almacenamiento del clúster no admiten la última versión numerada, debe actualizar a la última versión numerada que se admite.

- Versión mínima recomendada

Si desea restringir la actualización a la versión mínima recomendada para el clúster, consulte "[Versiones mínimas recomendadas de ONTAP](#)" Para determinar la versión de ONTAP a la que debe actualizar.

Confirme la compatibilidad de ONTAP para la configuración de hardware

Antes de actualizar ONTAP, debe confirmar que la configuración de hardware es compatible con la versión de ONTAP de destino.

Todas las configuraciones

Uso "[Hardware Universe de NetApp](#)" Para confirmar que la plataforma de hardware, el clúster y los switches de administración son compatibles con la versión de ONTAP de destino. El clúster y los switches de administración incluyen los switches de red de clúster (NX-OS), los switches de red de gestión (IOS) y el archivo de configuración de referencia (RCF). Si el clúster y los switches de gestión son compatibles, pero no ejecutan las versiones mínimas de software necesarias para la versión ONTAP de destino, actualice los switches a versiones de software compatibles.

- "[Descargas de NetApp: Switches de clúster de Broadcom](#)"
- "[Descargas de NetApp: Switches Ethernet de Cisco](#)"
- "[Descargas de NetApp: Switches de clúster de NetApp](#)"



Si necesita actualizar los switches, NetApp recomienda primero completar la actualización del software de ONTAP y, a continuación, realizar la actualización del software de los switches.

Configuraciones de MetroCluster

Antes de actualizar ONTAP, si tiene una configuración de MetroCluster, utilice el "[Herramienta de matriz de interoperabilidad de NetApp](#)" Para confirmar que los switches IP de MetroCluster son compatibles con la versión de ONTAP de destino.

Configuraciones SAN

Antes de actualizar ONTAP, si el clúster está configurado para SAN, utilice "[Herramienta de matriz de interoperabilidad de NetApp](#)" Para confirmar que la configuración de SAN es totalmente compatible.

Deben ser compatibles todos los componentes DE SAN, como la versión de software de la ONTAP de destino, el sistema operativo host y las revisiones, el software de utilidades del host requerido, el software multivía y los controladores y el firmware de adaptadores.

Identifique errores de configuración con Active IQ Config Advisor

Antes de actualizar ONTAP, puede utilizar la herramienta Active IQ Config Advisor para

comprobar si hay errores comunes de configuración.

Active IQ Config Advisor es una herramienta de validación de configuración para sistemas NetApp. Puede ponerse en marcha tanto en sitios seguros como en sitios no seguros para la recopilación de datos y el análisis del sistema.



La compatibilidad con Active IQ Config Advisor está limitada y solo está disponible en línea.

Pasos

1. Inicie sesión en la "[Sitio de soporte de NetApp](#)", Y, a continuación, haga clic en **Herramientas > Herramientas**.
2. En **Active IQ Config Advisor**, haga clic en "[Descargue la aplicación](#)".
3. Descargue, instale y ejecute Active IQ Config Advisor.
4. Después de ejecutar Active IQ Config Advisor, revise el resultado de la herramienta y siga las recomendaciones que se proporcionan para resolver cualquier problema detectado por la herramienta.

Rutas de actualización de ONTAP admitidas

La versión de ONTAP que puede actualizar a depende de la plataforma de hardware y de la versión de ONTAP que se ejecuta actualmente en los nodos del clúster.

Para verificar que la plataforma de hardware es compatible con la versión de actualización de destino, consulte "[Hardware Universe de NetApp](#)". Utilice la "[Herramienta de matriz de interoperabilidad de NetApp](#)" para "[confirme la compatibilidad con la configuración](#)".

Para determinar su versión actual de ONTAP:

- En System Manager, haga clic en **clúster > Descripción general**.
- Desde la interfaz de línea de comandos (CLI), utilice `cluster image show` comando. También puede utilizar el `system node image show` comando en el nivel de privilegio avanzado para mostrar los detalles.

Tipos de rutas de actualización

Siempre que sea posible, se recomiendan las actualizaciones automatizadas no disruptivas (ANDU). Dependiendo de sus versiones actuales y de destino, su ruta de actualización será **direct**, **direct multi-hop**, o **multi-stage**.

• Directo

Siempre puede actualizar directamente a la familia de versiones adyacentes de ONTAP mediante una sola imagen de software. En la mayoría de las versiones, también se puede instalar una imagen de software que permite actualizar directamente a versiones que sean dos versiones superiores a la versión en ejecución.

Por ejemplo, puede utilizar la ruta de actualización directa de 9.8 a 9.9.1, o de 9.8 a 9.10.1.

Nota: A partir de ONTAP 9.11.1, las imágenes de software admiten la actualización directa a versiones que son tres o más versiones superiores a la versión en ejecución. Por ejemplo, puede utilizar la ruta de actualización directa de 9,8 a 9.12.1.

Se admiten todas las rutas de actualización *DIRECT* para "[clústeres de versión mixta](#)".

- **Multihop directo**

Para algunas actualizaciones automáticas no disruptivas (ANDU) a versiones no adyacentes, debe instalar la imagen de software en una versión intermedia y en la versión de destino. El proceso de actualización automatizado utiliza la imagen intermedia en segundo plano para completar la actualización a la versión de destino.

Por ejemplo, si el clúster ejecuta 9.3 y desea actualizar a 9.7, deberá cargar los paquetes de instalación de ONTAP para 9.5 y 9.7, a continuación, iniciar ANDU en 9.7. ONTAP actualiza automáticamente el clúster en primer lugar a 9,5 y, posteriormente, a 9,7. Debe esperar varias operaciones de toma de control/devolución y reinicios relacionados durante el proceso.

- **Multi-etapa**

Si no hay disponible una ruta de varios saltos directa o directa para su versión de destino no adyacente, primero debe actualizar a una versión intermedia compatible y, a continuación, actualizar a la versión de destino.

Por ejemplo, si está ejecutando 9.6 y desea actualizar a 9.11.1, debe completar una actualización en varias etapas: Primero de 9.6 a 9.8 y después de 9.8 a 9.11.1. Las actualizaciones desde versiones anteriores pueden requerir tres o más etapas, con varias actualizaciones intermedias.

Nota: antes de comenzar las actualizaciones multietapa, asegúrese de que su versión de destino es compatible con su plataforma de hardware.

Antes de iniciar una actualización importante, se recomienda actualizar primero a la versión de revisión más reciente de la versión de ONTAP que se está ejecutando en el clúster. Esto garantiza que se resuelvan los problemas en la versión actual de ONTAP antes de la actualización.

Por ejemplo, si el sistema está ejecutando ONTAP 9.3P9 y está planeando actualizar a 9.11.1, primero debe actualizar a la versión de revisión 9.3 más reciente, luego siga la ruta de actualización de 9.3 a 9.11.1.

Descubra "[Versiones de ONTAP mínimas recomendadas en el sitio de soporte de NetApp](#)".

Rutas de actualización admitidas

Las siguientes rutas de actualización se admiten para actualizaciones automatizadas y manuales de su software ONTAP. Estas rutas de actualización se aplican a ONTAP y ONTAP Select en las instalaciones. Hay diferentes "[Rutas de actualización admitidas para Cloud Volumes ONTAP](#)".



Para clusters ONTAP de versiones mixtas: Todas las rutas de actualización *direct* y *direct multi-hop* incluyen versiones ONTAP compatibles con clusters de versiones mixtas. Las versiones de ONTAP incluidas en las actualizaciones *multi-stage* no son compatibles con los clústeres de versiones mixtas. Por ejemplo, una actualización de 9,8 a 9.12.1 es una actualización *DIRECT*. Un clúster con nodos que ejecutan 9,8 y 9.12.1 es un clúster de versión mixta que se admite. Una actualización de 9,8 a 9.13.1 es una actualización *multi-stage*. No se admite un clúster con nodos que ejecuten 9,8 y 9.13.1 en una versión mixta de clúster.

Desde ONTAP 9.10.1 y posterior

Las actualizaciones manuales y automatizadas desde ONTAP 9.10.1 y versiones posteriores siguen las mismas rutas de actualización.

| Si su versión actual de ONTAP es... | Y su versión ONTAP de destino es... | Su ruta de actualización automática o manual es... |
|-------------------------------------|-------------------------------------|--|
| 9.13.1 | 9.14.1 | directo |
| 9.12.1 | 9.14.1 | directo |
| | 9.13.1 | directo |
| 9.11.1 | 9.14.1 | directo |
| | 9.13.1 | directo |
| | 9.12.1 | directo |
| 9.10.1 | 9.14.1 | directo |
| | 9.13.1 | directo |
| | 9.12.1 | directo |
| | 9.11.1 | directo |

Desde ONTAP 9.9.1

Las actualizaciones manuales y automatizadas de ONTAP 9.9.1 siguen las mismas rutas de actualización.

| Si su versión actual de ONTAP es... | Y su versión ONTAP de destino es... | Su ruta de actualización automática o manual es... |
|-------------------------------------|-------------------------------------|--|
| 9.9.1 | 9.14.1 | multietapa -9.9.1→9.13.1 -9.13.1→9.14.1 |
| | 9.13.1 | directo |
| | 9.12.1 | directo |
| | 9.11.1 | directo |
| | 9.10.1 | directo |

Desde ONTAP 9,8

Las actualizaciones manuales y automatizadas de ONTAP 9,8 siguen las mismas rutas de actualización.



Si actualiza una configuración de IP de MetroCluster de 9,8 a 9.10.1 o posterior en cualquiera de las plataformas siguientes, debe actualizar a 9.9.1 antes de actualizar a la versión 9.10.1 o una versión posterior.

- FAS2750
- FAS500f
- AFF A220
- AFF A250

Los clústeres de las configuraciones IP de MetroCluster en estas plataformas no se pueden actualizar directamente de la versión 9,8 a la versión 9.10.1 o una versión posterior. Las rutas de actualización directa enumeradas se pueden utilizar para el resto de plataformas.

| Si su versión actual de ONTAP es... | Y su versión ONTAP de destino es... | Su ruta de actualización automatizada o manual es... |
|-------------------------------------|---|--|
| 9,8 | 9.14.1 | multietapa -9,8 → 9.12.1 -9.12.1 → 9.14.1 |
| 9.13.1 | multietapa -9,8 → 9.12.1 -9.12.1 → 9.13.1 | 9.12.1 |
| directo | 9.11.1 | directo |
| 9.10.1 | directo | 9.9.1 |

Desde ONTAP 9,7

Las rutas de actualización de ONTAP 9,7 pueden variar en función de si se realiza una actualización automatizada o manual.

Rutas automatizadas

| Si su versión actual de ONTAP es... | Y su versión ONTAP de destino es... | Su ruta de actualización automatizada es... |
|-------------------------------------|-------------------------------------|---|
| 9,7 | 9.14.1 | multietapa -9,7 → 9,8 -9,8 → 9.12.1 -9.12.1 → 9.14.1 |
| | 9.13.1 | multietapa -9,7 → 9.9.1 -9.9.1 → 9.13.1 |
| | 9.12.1 | multietapa -9,7 → 9,8 -9,8 → 9.12.1 |
| | 9.11.1 | salto múltiple directo (requiere imágenes para 9,8 y 9.11.1) |
| | 9.10.1 | Salto múltiple directo (se necesitan imágenes para la versión 9,8 y 9.10.1P1 o posterior P) |
| | 9.9.1 | directo |
| | 9,8 | directo |

Rutas manuales

| Si su versión actual de ONTAP es... | Y su versión ONTAP de destino es... | La ruta de actualización manual es... |
|-------------------------------------|-------------------------------------|---|
| 9,7 | 9.14.1 | multietapa -9,7 → 9,8 -9,8 → 9.12.1 -9.12.1 → 9.14.1 |
| | 9.13.1 | multietapa -9,7 → 9.9.1 -9.9.1 → 9.13.1 |
| | 9.12.1 | multietapa - 9,7 → 9,8 - 9,8 → 9.12.1 |
| | 9.11.1 | multietapa - 9,7 → 9,8 - 9,8 → 9.11.1 |
| | 9.10.1 | multietapa - 9,7 → 9,8 - 9,8 → 9.10.1 |
| | 9.9.1 | directo |
| | 9,8 | directo |

Desde ONTAP 9,6

Las rutas de actualización de ONTAP 9,6 pueden variar en función de si se realiza una actualización automatizada o manual.

Rutas automatizadas

| Si su versión actual de ONTAP es... | Y su versión ONTAP de destino es... | Su ruta de actualización automatizada es... |
|-------------------------------------|-------------------------------------|---|
| 9,6 | 9.14.1 | multietapa -9,6 → 9,8 -9,8 → 9.12.1 -9.12.1 → 9.14.1 |
| | 9.13.1 | multietapa -9,6 → 9,8 -9,8 → 9.12.1 -9.12.1 → 9.13.1 |
| | 9.12.1 | multietapa - 9,6 → 9,8 -9,8 → 9.12.1 |
| | 9.11.1 | multietapa - 9,6 → 9,8 - 9,8 → 9.11.1 |
| | 9.10.1 | Salto múltiple directo (se necesitan imágenes para la versión 9,8 y 9.10.1P1 o posterior P) |
| | 9.9.1 | multietapa - 9,6 → 9,8 - 9,8 → 9.9.1 |
| | 9,8 | directo |
| | 9,7 | directo |

Rutas manuales

| Si su versión actual de ONTAP es... | Y su versión ONTAP de destino es... | La ruta de actualización manual es... |
|-------------------------------------|-------------------------------------|--|
| 9,6 | 9.14.1 | multietapa - 9,6 → 9,8 - 9,8 → 9.12.1 - 9.12.1 → 9.14.1 |
| | 9.13.1 | multietapa - 9,6 → 9,8 - 9,8 → 9.12.1 - 9.12.1 → 9.13.1 |
| | 9.12.1 | multietapa - 9,6 → 9,8 - 9,8 → 9.12.1 |
| | 9.11.1 | multietapa - 9,6 → 9,8 - 9,8 → 9.11.1 |
| | 9.10.1 | multietapa - 9,6 → 9,8 - 9,8 → 9.10.1 |
| | 9.9.1 | multietapa - 9,6 → 9,8 - 9,8 → 9.9.1 |
| | 9,8 | directo |
| | 9,7 | directo |

Desde ONTAP 9,5

Las rutas de actualización de ONTAP 9,5 pueden variar en función de si se realiza una actualización automatizada o manual.

Rutas automatizadas

| Si su versión actual de ONTAP es... | Y su versión ONTAP de destino es... | Su ruta de actualización automatizada es... |
|-------------------------------------|-------------------------------------|--|
| 9,5 | 9.14.1 | multietapa - 9,5 → 9.9.1 (multi-hop directo, requiere imágenes para 9,7 y 9,9.1) - 9.9.1 → 9.13.1 - 9.13.1 → 9.14.1 |
| | 9.13.1 | multietapa - 9,5 → 9.9.1 (multi-hop directo, requiere imágenes para 9,7 y 9,9.1) - 9.9.1 → 9.13.1 |
| | 9.12.1 | multietapa - 9,5 → 9.9.1 (multi-hop directo, requiere imágenes para 9,7 y 9,9.1) - 9.9.1 → 9.12.1 |
| | 9.11.1 | multietapa - 9,5 → 9.9.1 (multi-hop directo, requiere imágenes para 9,7 y 9,9.1) - 9.9.1 → 9.11.1 |
| | 9.10.1 | multietapa - 9,5 → 9.9.1 (multi-hop directo, requiere imágenes para 9,7 y 9,9.1) - 9.9.1 → 9.10.1 |
| | 9.9.1 | salto múltiple directo (requiere imágenes para 9,7 y 9,9.1) |
| | 9,8 | multietapa - 9,5 → 9,7 - 9,7 → 9,8 |
| | 9,7 | directo |
| | 9,6 | directo |

Rutas de actualización manuales

| Si su versión actual de ONTAP es... | Y su versión ONTAP de destino es... | La ruta de actualización manual es... |
|-------------------------------------|-------------------------------------|---|
| 9,5 | 9.14.1 | multietapa - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.12.1 - 9.12.1 → 9.14.1 |
| | 9.13.1 | multietapa - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.12.1 - 9.12.1 → 9.13.1 |
| | 9.12.1 | multietapa - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.12.1 |
| | 9.11.1 | multietapa - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.11.1 |
| | 9.10.1 | multietapa - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.10.1 |
| | 9.9.1 | multietapa - 9,5 → 9,7 - 9,7 → 9.9.1 |
| | 9,8 | multietapa - 9,5 → 9,7 - 9,7 → 9,8 |
| | 9,7 | directo |
| | 9,6 | directo |

Desde ONTAP 9,4-9,0

Las rutas de actualización de ONTAP 9,4, 9,3, 9,2, 9,1 y 9,0 pueden variar en función de si se realiza una actualización automatizada o manual.

| Si su versión actual de ONTAP es... | Y su versión ONTAP de destino es... | Su ruta de actualización automatizada es... |
|-------------------------------------|-------------------------------------|---|
| 9,4 | 9.14.1 | multietapa - 9,4 → 9,5 - 9,5 → 9.9.1 (multi-hop directo, requiere imágenes para 9,7 y 9,9.1) - 9.9.1 → 9.13.1 - 9.13.1 → 9.14.1 |
| | 9.13.1 | multietapa - 9,4 → 9,5 - 9,5 → 9.9.1 (multi-hop directo, requiere imágenes para 9,7 y 9,9.1) - 9.9.1 → 9.13.1 |
| | 9.12.1 | multietapa - 9,4 → 9,5 - 9,5 → 9.9.1 (multi-hop directo, requiere imágenes para 9,7 y 9,9.1) - 9.9.1 → 9.12.1 |
| | 9.11.1 | multietapa - 9,4 → 9,5 - 9,5 → 9.9.1 (multi-hop directo, requiere imágenes para 9,7 y 9,9.1) - 9.9.1 → 9.11.1 |
| | 9.10.1 | multietapa - 9,4 → 9,5 - 9,5 → 9.9.1 (multi-hop directo, requiere imágenes para 9,7 y 9,9.1) - 9.9.1 → 9.10.1 |
| | 9.9.1 | multietapa - 9,4 → 9,5 - 9,5 → 9.9.1 (multi-hop directo, requiere imágenes para 9,7 y 9,9.1) |
| | 9,8 | multietapa - 9,4 → 9,5 - 9,5 → 9,8 (multi-hop directo, requiere imágenes para 9,7 y 9,8) |
| | 9,7 | multietapa - 9,4 → 9,5 - 9,5 → 9,7 |
| | 9,6 | multietapa - 9,4 → 9,5 - 9,5 → 9,6 |
| | 9,5 | directo |

| Si su versión actual de ONTAP es... | Y su versión ONTAP de destino es... | Su ruta de actualización automatizada es... |
|-------------------------------------|-------------------------------------|--|
| 9,3 | 9.14.1 | multietapa - 9,3 → 9,7 (multi-hop directo, requiere imágenes para 9,5 y 9,7) - 9,7 → 9.9.1 - 9.9.1 → 9.13.1 - 9.13.1 → 9.14.1 |
| | 9.13.1 | multietapa - 9,3 → 9,7 (multi-hop directo, requiere imágenes para 9,5 y 9,7) - 9,7 → 9.9.1 - 9.9.1 → 9.13.1 |
| | 9.12.1 | multietapa - 9,3 → 9,7 (multi-hop directo, requiere imágenes para 9,5 y 9,7) - 9,7 → 9.9.1 - 9.9.1 → 9.12.1 |
| | 9.11.1 | multietapa - 9,3 → 9,7 (multi-hop directo, requiere imágenes para 9,5 y 9,7) - 9,7 → 9.9.1 - 9.9.1 → 9.11.1 |
| | 9.10.1 | multietapa - 9,3 → 9,7 (multi-hop directo, requiere imágenes para 9,5 y 9,7) - 9,7 → 9.10.1 (multi-hop directo, requiere imágenes para 9,8 y 9.10.1) |
| | 9.9.1 | multietapa - 9,3 → 9,7 (multi-hop directo, requiere imágenes para 9,5 y 9,7) - 9,7 → 9.9.1 |
| | 9,8 | multietapa - 9,3 → 9,7 (multi-hop directo, requiere imágenes para 9,5 y 9,7) - 9,7 → 9,8 |
| | 9,7 | salto múltiple directo (requiere imágenes para 9,5 y 9,7) |
| | 9,6 | multietapa - 9,3 → 9,5 - 9,5 → 9,6 |
| | 9,5 | directo |
| | 9,4 | no disponible |

| Si su versión actual de ONTAP es... | Y su versión ONTAP de destino es... | Su ruta de actualización automatizada es... |
|-------------------------------------|-------------------------------------|---|
| 9,2 | | |

| | | |
|-------------------------------------|-------------------------------------|--|
| Si su versión actual de ONTAP es... | 9,7 | multietapa - 9,2 → 9,3 - 9,3 → 9,5 - 9,5 → 9,6 - 9,6 → 9,7 |
| | Y su versión ONTAP de destino es... | Su ruta de actualización es: 9,3 → 9,5 (actualización automatizada es para 9,5 y 9,7) |
| | 9,6 | multietapa - 9,2 → 9,3 - 9,3 → 9,5 - 9,5 → 9,6 |
| | 9,5 | multietapa - 9,3 → 9,5 - 9,5 → 9,6 |
| | 9,4 | no disponible |
| | 9,3 | directo |

| Si su versión actual de ONTAP es... | Y su versión ONTAP de destino es... | Su ruta de actualización automatizada es... |
|-------------------------------------|-------------------------------------|---|
| 9,1 | | |

| | | |
|-------------------------------------|-------------------------------------|---|
| Si su versión actual de ONTAP es... | 9,7 | multietapa - 9,1 → 9,3 - 9,3 → 9,7 (actualización automatizada, requiere imágenes para 9,5 y 9,7) |
| | 9,6 | multietapa - 9,1 → 9,3 - 9,3 → 9,6 (multi-hop directo, requiere imágenes para 9,5 y 9,6) |
| | 9,5 | multietapa - 9,1 → 9,3 - 9,3 → 9,5 |
| | 9,4 | no disponible |
| | 9,3 | directo |
| | 9,2 | no disponible |
| | Y su versión ONTAP de destino es... | Su ruta de actualización automatizada es para 9,5 y 9,7) |

| Si su versión actual de ONTAP es... | Y su versión ONTAP de destino es... | Su ruta de actualización automatizada es... |
|-------------------------------------|-------------------------------------|---|
| 9,0 | | |

| Si su versión actual de ONTAP es... | Y su versión ONTAP de destino es... | Para 9.5 de actualización automatizada es... |
|--|--|---|
| | | Para 9.7 de actualización automatizada es... |
| | | <ul style="list-style-type: none"> - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,7 (multi-hop directo, requiere imágenes para 9,5 y 9,7) - 9,7 → 9.9.1 |
| | 9,8 | multietapa <ul style="list-style-type: none"> - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,7 (multi-hop directo, requiere imágenes para 9,5 y 9,7) - 9,7 → 9,8 |
| | 9,7 | multietapa <ul style="list-style-type: none"> - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,7 (multi-hop directo, requiere imágenes para 9,5 y 9,7) |
| | 9,6 | multietapa <ul style="list-style-type: none"> - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,5 - 9,5 → 9,6 |
| | 9,5 | multietapa <ul style="list-style-type: none"> - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,5 |
| | 9,4 | no disponible |
| | 9,3 | multietapa <ul style="list-style-type: none"> - 9,0 → 9,1 - 9,1 → 9,3 |
| | 9,2 | no disponible |
| | 9,1 | directo |

Rutas de actualización manuales

| Si su versión actual de ONTAP es... | Y su versión ONTAP de destino es... | La ruta DE actualización DE ANDU es... |
|-------------------------------------|-------------------------------------|--|
| 9,4 | 9.14.1 | multietapa - 9,4 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.12.1 - 9.12.1 → 9.14.1 |
| | 9.13.1 | multietapa - 9,4 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.12.1 - 9.12.1 → 9.13.1 |
| | 9.12.1 | multietapa - 9,4 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.12.1 |
| | 9.11.1 | multietapa - 9,4 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.11.1 |
| | 9.10.1 | multietapa - 9,4 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.10.1 |
| | 9.9.1 | multietapa - 9,4 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 |
| | 9,8 | multietapa - 9,4 → 9,5 - 9,5 → 9,7 - 9,7 → 9,8 |
| | 9,7 | multietapa - 9,4 → 9,5 - 9,5 → 9,7 |
| | 9,6 | multietapa - 9,4 → 9,5 - 9,5 → 9,6 |
| | 9,5 | directo |

| Si su versión actual de ONTAP es... | Y su versión ONTAP de destino es... | La ruta DE actualización DE ANDU es... |
|-------------------------------------|-------------------------------------|--|
| 9,3 | 9.14.1 | multietapa - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.12.1 - 9.12.1 → 9.14.1 |
| | 9.13.1 | multietapa - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.12.1 - 9.12.1 → 9.13.1 |
| | 9.12.1 | multietapa - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.12.1 |
| | 9.11.1 | multietapa - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.11.1 |
| | 9.10.1 | multietapa - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.10.1 |
| | 9.9.1 | multietapa - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 |
| | 9,8 | multietapa - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9,8 |
| | 9,7 | multietapa - 9,3 → 9,5 - 9,5 → 9,7 |
| | 9,6 | multietapa - 9,3 → 9,5 - 9,5 → 9,6 |
| | 9,5 | directo |
| | 9,4 | no disponible |

| Si su versión actual de ONTAP es... | Y su versión ONTAP de destino es... | La ruta DE actualización DE ANDU es... |
|-------------------------------------|-------------------------------------|--|
| 9,2 | | |

| | | |
|--|--|---|
| | 9,7 | multietapa - 9,2 → 9,3 |
| Si su versión actual de ONTAP es... | Y su versión ONTAP de destino es... | La ruta DE actualización DE ANDU es... |
| | 9,6 | multietapa - 9,2 → 9,3 - 9,3 → 9,5 - 9,5 → 9,6 |
| | 9,5 | multietapa - 9,2 → 9,3 - 9,3 → 9,5 |
| | 9,4 | no disponible |
| | 9,3 | directo |

| Si su versión actual de ONTAP es... | Y su versión ONTAP de destino es... | La ruta DE actualización DE ANDU es... |
|-------------------------------------|-------------------------------------|--|
| 9,1 | | |

| | | |
|--|--|---|
| | 9,7 | multietapa - 9,1 → 9,3 - 9,5 → 9,7 |
| Si su versión actual de ONTAP es... | Y su versión ONTAP de destino es... | La ruta de actualización DE ANDU es... |
| | 9,6 | multietapa - 9,1 → 9,3 - 9,3 → 9,5 - 9,5 → 9,6 |
| | 9,5 | multietapa - 9,1 → 9,3 - 9,3 → 9,5 |
| | 9,4 | no disponible |
| | 9,3 | directo |
| | 9,2 | no disponible |

| Si su versión actual de ONTAP es... | Y su versión ONTAP de destino es... | La ruta DE actualización DE ANDU es... |
|-------------------------------------|-------------------------------------|--|
| 9,0 | | |

| | | |
|--|--|---|
| | | - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,5 |
| Si su versión actual de ONTAP es... | Y su versión ONTAP de destino es... | La ruta de actualización DE ANDU es... |
| | 9,8 | multietapa - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9,8 |
| | 9,7 | multietapa - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,5 - 9,5 → 9,7 |
| | 9,6 | multietapa - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,5 - 9,5 → 9,6 |
| | 9,5 | multietapa - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,5 |
| | 9,4 | no disponible |
| | 9,3 | multietapa - 9,0 → 9,1 - 9,1 → 9,3 |
| | 9,2 | no disponible |
| | 9,1 | directo |

Data ONTAP 8

Asegúrese de verificar que su plataforma puede ejecutar la versión de ONTAP de destino mediante el ["Hardware Universe de NetApp"](#).

Nota: la Guía de actualización de Data ONTAP 8.3 indica erróneamente que en un clúster de cuatro nodos, debe planificar la actualización del nodo que tenga el valor épsilon en último lugar. Esto ya no es un requisito para las actualizaciones a partir de Data ONTAP 8.2.3. Para obtener más información, consulte ["ID de error de NetApp Bugs Online: 805277"](#).

Desde Data ONTAP 8.3.x

Puede actualizar directamente a ONTAP 9.1 y, posteriormente, actualizar a versiones posteriores.

De versiones de Data ONTAP anteriores a 8.3.x, incluidas 8.2.x.

Primero es necesario actualizar a Data ONTAP 8.3.x y, después, actualizar a ONTAP 9.1 y, posteriormente, actualizar a versiones posteriores.

Compruebe la configuración de recuperación tras fallos de LIF

Antes de actualizar ONTAP, debe comprobar que las políticas de conmutación por error y los grupos de conmutación por error del clúster están configurados correctamente.

Durante el proceso de actualización, las LIF se migran en función del método de actualización. En función del método de actualización, es posible que se utilice la política de conmutación por error del LIF.

Si tiene 8 nodos o más en el clúster, la actualización automatizada se realiza mediante el método de lote. El método de actualización por lotes implica dividir el clúster en varios lotes de actualización, actualizar el conjunto de nodos del primer lote, actualizar sus partners de alta disponibilidad (ha) y, a continuación, repetir el proceso para los lotes restantes. En ONTAP 9.7 y versiones anteriores, si se utiliza el método por lotes, los LIF se migran al partner de alta disponibilidad del nodo que se actualiza. En ONTAP 9.8 y versiones posteriores, si se utiliza el método por lotes, los LIF se migran al otro grupo por lotes.

Si tiene menos de 8 nodos en el clúster, la actualización automatizada se realiza mediante el método de reversión. El método de actualización gradual implica iniciar una operación de conmutación al respaldo en cada nodo de un par de alta disponibilidad, actualizar el nodo que ha conmutado al nodo de respaldo, iniciar el retorno al nodo primario y, a continuación, repetir el proceso de cada par de alta disponibilidad del clúster. Si se usa el método de reversión, las LIF se migran al nodo de destino de conmutación por error tal como se define en la política de conmutación por error de LIF.

Pasos

1. Mostrar la política de recuperación tras fallos para cada LIF de datos:

| Si la versión de ONTAP es... | Utilice este comando |
|------------------------------|--|
| 9,6 o posterior | <code>network interface show -service-policy *data* -failover</code> |
| 9,5 o anterior | <code>network interface show -role data -failover</code> |

Este ejemplo muestra la configuración predeterminada de la conmutación por error de un clúster de dos nodos con dos LIF de datos:

```
cluster1::> network interface show -role data -failover
```

| Vserver | Logical Interface | Home Node:Port | Failover Policy | Failover Group |
|---------|-------------------|--|-----------------|----------------|
| vs0 | lif0 | node0:e0b | nextavail | system- |
| defined | | Failover Targets: node0:e0b, node0:e0c, node0:e0d, node0:e0e, node0:e0f, node1:e0b, node1:e0c, node1:e0d, node1:e0e, node1:e0f | | |
| vs1 | lif1 | node1:e0b | nextavail | system- |
| defined | | Failover Targets: node1:e0b, node1:e0c, node1:e0d, node1:e0e, node1:e0f, node0:e0b, node0:e0c, node0:e0d, node0:e0e, node0:e0f | | |

El campo **objetivos de conmutación por error** muestra una lista priorizada de destinos de conmutación por error para cada LIF. Por ejemplo, si 'lif0' conmuta por error desde su puerto raíz (e0b en node0), primero intenta conmutar por error al puerto e0c en node0. Si lif0 no puede conmutar al nodo de respaldo a e0c, intenta conmutar al puerto e0d en node0, etc.

2. Si la política de conmutación por error se establece en **disabled** para cualquier LIF, que no sea LIF de SAN, utilice el `network interface modify` comando para habilitar la conmutación al nodo de respaldo.
3. Para cada LIF, compruebe que el campo **objetivos de conmutación por error** incluye puertos de datos de un nodo diferente que permanecerán activos mientras se esté actualizando el nodo de inicio de la LIF.

Puede utilizar el `network interface failover-groups modify` comando para agregar un destino de conmutación por error al grupo de conmutación por error.

Ejemplo

```
network interface failover-groups modify -vserver vs0 -failover-group
fg1 -targets sti8-vsim-ucs572q:e0d,sti8-vsim-ucs572r:e0d
```

Información relacionada

["Gestión de redes y LIF"](#)

Comprobar la configuración de enrutamiento de SVM

Para evitar interrupciones, antes de actualizar el software ONTAP, debe asegurarse de que la ruta predeterminada de la SVM pueda alcanzar cualquier dirección de red que no sea accesible por una ruta más específica. Se recomienda configurar una ruta predeterminada para una SVM. Para obtener más información, consulte ["SU134: El acceso a la red puede verse interrumpido por una configuración de enrutamiento incorrecta en ONTAP"](#).

La tabla de enrutamiento de una SVM determina la ruta de red que la SVM utiliza para comunicarse con un destino. Es importante comprender cómo funcionan las tablas de enrutamiento para evitar problemas de red antes de que ocurran.

Las reglas de enrutamiento son las siguientes:

- ONTAP enruta el tráfico por la ruta disponible más específica.
- ONTAP enruta el tráfico por una ruta de puerta de enlace predeterminada (con 0 bits de máscara de red) como último recurso, cuando no hay más rutas específicas disponibles.

En el caso de rutas con el mismo destino, máscara de red y métrica, no hay garantía de que el sistema utilice la misma ruta después de un reinicio o después de una actualización. Esto puede ser especialmente un problema si ha configurado varias rutas predeterminadas.

Consideraciones especiales

Consideraciones especiales antes de una actualización de ONTAP

Ciertas configuraciones de clúster requieren que realice acciones específicas antes de iniciar una actualización del software de ONTAP. Por ejemplo, si tiene una configuración de SAN, debe verificar que cada host esté configurado con el número correcto de rutas directas e indirectas antes de comenzar la actualización.

Revise la siguiente tabla para determinar qué pasos adicionales debe tomar.

| Antes de actualizar ONTAP, pregúntese... | Si su respuesta es sí, entonces haga esto... |
|--|---|
| ¿Mi clúster está actualmente en estado de versión mixta? | Compruebe los requisitos de versión mixta |
| ¿Tengo una configuración de MetroCluster? | Consulte los requisitos específicos de actualización de las configuraciones de MetroCluster |
| ¿Tengo una configuración SAN? | Compruebe la configuración del host SAN |
| ¿Hay definidas relaciones de SnapMirror en mi clúster? | "Comprobar la compatibilidad de las versiones de ONTAP para las relaciones de SnapMirror" |
| ¿He definido relaciones de SnapMirror para tipo DP? ¿Estoy actualizando a ONTAP 9.12.1 o una versión posterior? | "Convierta las relaciones de tipo DP existentes a XDP" |
| ¿Uso el cifrado de almacenamiento de NetApp con servidores de gestión de claves externos? | Elimine todas las conexiones existentes del servidor de gestión de claves |

| Antes de actualizar ONTAP, pregúntese... | Si su respuesta es sí, entonces haga esto... |
|--|---|
| ¿He cargado grupos de red en SVM? | Verifique que el archivo netgroup está presente en cada nodo |
| ¿Tengo clientes LDAP que utilizan SSLv3? | Configure los clientes LDAP para que usen TLS |
| ¿Estoy utilizando protocolos orientados a sesiones? | Examinar las consideraciones relativas a los protocolos orientados a las sesiones |
| ¿Está habilitado el modo FIPS de SSL en un clúster donde las cuentas de administrador se autentican con una clave pública SSH? | Verifique el soporte del algoritmo de clave de host SSH |

Clústeres de ONTAP de versión mixta

Un clúster de ONTAP de versión mixta consta de nodos que ejecutan dos versiones principales de ONTAP diferentes durante un tiempo limitado. Por ejemplo, si un clúster actualmente consta de nodos que ejecutan ONTAP 9.8 y 9.12.1, el clúster es un clúster de una versión mixta. De igual forma, un clúster en el que nodos ejecuten ONTAP 9.9.1 y 9.13.1 sería un clúster de versiones mixtas. NetApp admite clústeres ONTAP de versión mixta durante períodos limitados y en situaciones específicas.

A continuación se muestran los casos más comunes en los que un clúster de ONTAP tendrá una versión mixta:

- Actualizaciones del software ONTAP en grandes clústeres
- Es necesario actualizar el software ONTAP cuando piensa añadir nodos nuevos a un clúster

La información se aplica a las versiones de ONTAP que admiten sistemas de plataformas NetApp, como los sistemas A-Series y C-Series de AFF, ASA, FAS y C-Series. La información no se aplica a las versiones de cloud de ONTAP (9.x.0) como 9.12.0.

Requisitos para clústeres de ONTAP de versión mixta

Si su clúster tiene que introducir una versión mixta de ONTAP, debe conocer los requisitos y las restricciones importantes.

- No puede haber más de dos versiones principales de ONTAP diferentes en un clúster en un momento dado. Por ejemplo, se admite ONTAP 9.9.1 y 9.13.1, pero ONTAP 9.9.1, 9.12.1 y 9.13.1 no lo es. Los clústeres que tienen nodos en ejecución con niveles de revisión P o D diferentes de la misma versión de ONTAP, como ONTAP 9.9.1P1 y 9.9.1P5, no se consideran clústeres de ONTAP de versiones mixtas.
- Mientras el clúster tiene una versión mixta, no debe introducir ningún comando que modifique la operación o la configuración del clúster, excepto los necesarios para la actualización o el proceso de migración de datos. Por ejemplo, no deben realizarse actividades como la migración LIF, las operaciones planificadas de conmutación por error de almacenamiento o la creación o eliminación de objetos a gran escala hasta que hayan finalizado la actualización y la migración de datos.
- Para un funcionamiento óptimo del clúster, la cantidad de tiempo que el clúster tenga el estado de versión mixta debe ser lo más breve posible. La cantidad máxima de tiempo que puede permanecer un clúster en una versión mixta depende de la versión de ONTAP más baja del clúster.

| Si la versión más baja de ONTAP que se ejecuta en el clúster de versiones mixtas es: | A continuación, puede permanecer en un estado de versión mixta durante un máximo de |
|--|---|
| ONTAP 9,8 o superior | 90 días |
| ONTAP 9,7 o inferior | 7 días |

- A partir de ONTAP 9,8, la diferencia de versión entre los nodos originales y los nuevos no puede ser superior a cuatro. Por ejemplo, un clúster ONTAP de versión mixta podría tener nodos que ejecuten ONTAP 9,8 y 9.12.1, o bien podría tener nodos que ejecuten ONTAP 9.9.1 y 9.13.1. Sin embargo, no se admitiría una versión mixta de un clúster de ONTAP con nodos que ejecuten ONTAP 9,8 y 9.13.1.

Si desea ver una lista completa de los clústeres de versiones mixtas compatibles, consulte ["rutas de actualización admitidas"](#). Todas las rutas de actualización *DIRECT* se admiten para clústeres de versiones mixtas.

Actualización de la versión de ONTAP de un clúster de gran tamaño

Una situación en la que se puede introducir un estado en un clúster de versiones mixtas implica actualizar la versión ONTAP de un clúster con varios nodos para aprovechar las funciones disponibles en versiones posteriores de ONTAP 9. Cuando necesite actualizar la versión de ONTAP de un clúster más grande, deberá introducir un estado de clúster de versiones mixtas durante un período de tiempo a medida que actualice cada nodo del clúster.

Añadir nuevos nodos a un clúster de ONTAP

Otra situación para introducir un estado de cluster de versiones mixtas implica la adición de nuevos nodos al clúster. Es posible añadir nodos nuevos al clúster para expandir su capacidad, o es posible añadir nodos nuevos como parte del proceso de reemplazar por completo las controladoras. En cualquier caso, debe habilitar la migración de sus datos desde controladoras existentes a los nodos nuevos en el sistema nuevo.

Si piensa agregar nodos nuevos al clúster y esos nodos requieren una versión mínima de ONTAP que sea posterior a la versión que se está ejecutando actualmente en el clúster, debe realizar las actualizaciones de software compatibles de los nodos existentes del clúster antes de agregar los nodos nuevos.

Lo ideal sería que actualizara todos los nodos existentes a la versión mínima de ONTAP que requieran los nodos que planea agregar al clúster. Sin embargo, si esto no es posible porque algunos de sus nodos existentes no admiten la versión posterior de ONTAP, deberá introducir un estado de versión mixta durante una cantidad limitada de tiempo como parte del proceso de actualización. Si tiene nodos que no admiten la versión mínima de ONTAP requerida por las controladoras nuevas, debe hacer lo siguiente:

1. ["Renovar"](#) Los nodos que no admiten la versión mínima de ONTAP requerida por las nuevas controladoras hasta la versión máxima de ONTAP que admiten.

Por ejemplo, si tiene un sistema FAS8080 con ONTAP 9,5 y va a añadir una nueva plataforma C-Series con ONTAP 9.12.1, debería actualizar su sistema FAS8080 a ONTAP 9,8 (que es la versión máxima de ONTAP que admite).

2. ["Añada los nodos nuevos al clúster"](#).
3. ["Migrar los datos"](#) de los nodos que se están quitando del clúster a los nodos recién añadidos.
4. ["Quite los nodos no compatibles del clúster"](#).
5. ["Renovar"](#) los nodos restantes del clúster a la misma versión de los nuevos nodos.

De manera opcional, actualice el clúster completo (incluidos los nodos nuevos) al ["última versión de parche recomendada"](#) De la versión de ONTAP que se ejecuta en los nodos nuevos.

Para obtener más información sobre la migración de datos, consulte:

- ["Cree un agregado y mueva volúmenes a los nuevos nodos"](#)
- ["Configuración de nuevas conexiones iSCSI para movimientos de volúmenes SAN"](#)
- ["Movimiento de volúmenes con cifrado"](#)

Requisitos de actualización de ONTAP para configuraciones de MetroCluster

Antes de actualizar el software ONTAP en una configuración MetroCluster, los clústeres deben cumplir ciertos requisitos.

- Ambos clústeres deben ejecutar la misma versión de ONTAP.

Puede comprobar la versión de ONTAP con el comando `version`.

- Si está realizando una actualización importante de ONTAP, la configuración de MetroCluster debe estar en modo normal.
- Si está realizando una actualización de ONTAP de parche, la configuración de MetroCluster puede estar en modo normal o de conmutación.
- Para todas las configuraciones, excepto clústeres de dos nodos, puede actualizar de forma no disruptiva ambos clústeres al mismo tiempo.

Para la actualización no disruptiva de clústeres de dos nodos, es necesario actualizar los clústeres de un nodo a uno.

- Los agregados de ambos clústeres no deben volver a asignar el estado de RAID.

Durante la reparación de MetroCluster, los agregados reflejados se resincronizan. Puede verificar si la configuración de MetroCluster está en este estado mediante la `storage aggregate plex show -in -progress true` comando. Si se sincroniza algún agregado, no se debe realizar una actualización hasta que se complete la resincronización.

- Se producirá un error en las operaciones de conmutación al nodo de respaldo negociadas mientras la actualización está en curso.

Para evitar problemas con las operaciones de actualización o reversión, no intente realizar una conmutación de sitios no planificada durante una operación de actualización o reversión a menos que todos los nodos de ambos clústeres estén ejecutando la misma versión de ONTAP.

Requisitos de configuración para el funcionamiento normal de MetroCluster

- Los LIF de SVM de origen deben estar activos y ubicados en sus nodos principales.

No es necesario que los LIF de datos de las SVM de destino estén en funcionamiento o que estén en sus nodos de inicio.

- Todos los agregados del sitio local deben estar en línea.
- Todos los volúmenes raíz y de datos que pertenecen a las SVM del clúster local deben estar en línea.

Requisitos de configuración para la conmutación de sitios de MetroCluster

- Todos los LIF deben estar activos y ubicados en sus nodos principales.
- Todos los agregados deben estar en línea, excepto los agregados raíz en el sitio de recuperación ante desastres.

Los agregados raíz del sitio de recuperación tras desastres están sin conexión durante determinadas fases de la conmutación.

- Todos los volúmenes deben estar en línea.

Información relacionada

["Verificación del estado de red y almacenamiento de las configuraciones de MetroCluster"](#)

Compruebe la configuración del host SAN antes de actualizar ONTAP

La actualización de ONTAP en un entorno SAN cambia qué rutas son directas. Antes de actualizar un clúster SAN, debe comprobar que cada host esté configurado con el número correcto de rutas directas e indirectas y que cada host esté conectado a las LIF correctas.

Pasos

1. En cada host, compruebe que se haya configurado un número suficiente de rutas directas e indirectas y que cada ruta esté activa.

Cada host debe tener una ruta a cada nodo del clúster.

2. Compruebe que cada host está conectado a una LIF en cada nodo.

Debe registrar la lista de iniciadores para la comparación después de la actualización.

| Durante... | Introduzca... |
|------------|---|
| ISCSI | <pre>iscsi initiator show -fields igroup,initiator-name,tpgroup</pre> |
| FC | <pre>fcp initiator show -fields igroup,wwpn,lif</pre> |

SnapMirror

Versiones de ONTAP compatibles para relaciones de SnapMirror

Los volúmenes de origen y destino deben ejecutar versiones de ONTAP compatibles antes de crear una relación de protección de datos de SnapMirror. Antes de actualizar ONTAP, debe comprobar que la versión actual de ONTAP sea compatible con la versión de ONTAP de destino para las relaciones de SnapMirror.

Relaciones de replicación unificadas

En lo que respecta a las relaciones de SnapMirror del tipo «'XDP», utilizando las versiones locales o de Cloud Volumes ONTAP:



A partir de ONTAP 9,9.0:

- Las versiones ONTAP 9.x,0 son versiones de solo cloud y son compatibles con los sistemas Cloud Volumes ONTAP. El asterisco (*) después de la versión indica una versión de sólo nube.
- Las versiones ONTAP 9.x,1 son versiones generales y son compatibles tanto con los sistemas locales como con los sistemas Cloud Volumes ONTAP.



La interoperabilidad es bidireccional.

Interoperabilidad para ONTAP versión 9,3 y posterior

| Versión ONTAP ... | Interactúa con estas versiones anteriores de ONTAP... | | | | | | | | | | | | | | | | | |
|-------------------|---|---------|--------|---------|--------|---------|--------|---------|--------|---------|-------|--------|-----|-----|-----|-----|-----|-----|
| | 9.14.1 | 9.14.0* | 9.13.1 | 9.13.0* | 9.12.1 | 9.12.0* | 9.11.1 | 9.11.0* | 9.10.1 | 9.10.0* | 9.9.1 | 9.9.0* | 9,8 | 9,7 | 9,6 | 9,5 | 9,4 | 9,3 |
| 9.14.1 | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | No | No | No | No | No | No |
| 9.14.0* | Sí | Sí | Sí | No | Sí | No | Sí | No | Sí | No | Sí | No | Sí | No | No | No | No | No |
| 9.13.1 | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | No | No | No | No | No |
| 9.13.0* | Sí | No | Sí | Sí | Sí | No | Sí | No | Sí | No | Sí | No | Sí | No | No | No | No | No |
| 9.12.1 | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | No | No | No | No |
| 9.12.0* | Sí | No | Sí | No | Sí | Sí | Sí | No | Sí | No | Sí | No | Sí | Sí | No | No | No | No |
| 9.11.1 | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | No | No | No |
| 9.11.0* | Sí | No | Sí | No | Sí | No | Sí | Sí | Sí | No | Sí | No | Sí | Sí | Sí | No | No | No |
| 9.10.1 | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | No | No |
| 9.10.0* | Sí | No | Sí | No | Sí | No | Sí | No | Sí | Sí | Sí | No | Sí | Sí | Sí | Sí | No | No |
| 9.9.1 | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | No | No |

| | | | | | | | | | | | | | | | | | | |
|--------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 9.9.0* | Sí | No | Sí | No | Sí | No | Sí | No | Sí | No | Sí | Sí | Sí | Sí | Sí | Sí | No | No |
| 9,8 | No | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | No | Sí |
| 9,7 | No | No | No | No | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | No | Sí |
| 9,6 | No | No | No | No | No | No | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | No | Sí |
| 9,5 | No | No | No | No | No | No | No | No | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí |
| 9,4 | No | No | No | No | No | No | No | No | No | No | No | No | No | No | No | Sí | Sí | Sí |
| 9,3 | No | No | No | No | No | No | No | No | No | No | No | No | Sí | Sí | Sí | Sí | Sí | Sí |

Relaciones de SnapMirror Synchronous



SnapMirror Synchronous no es compatible con las instancias de cloud de ONTAP.

| Versión ONTAP ... | Interactúa con estas versiones anteriores de ONTAP... | | | | | | | | | |
|-------------------|---|--------|--------|--------|--------|-------|-----|-----|-----|-----|
| | 9.14.1 | 9.13.1 | 9.12.1 | 9.11.1 | 9.10.1 | 9.9.1 | 9,8 | 9,7 | 9,6 | 9,5 |
| 9.14.1 | Sí | Sí | Sí | Sí | Sí | Sí | Sí | No | No | No |
| 9.13.1 | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | No | No |
| 9.12.1 | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | No | No |
| 9.11.1 | Sí | Sí | Sí | Sí | Sí | Sí | No | No | No | No |
| 9.10.1 | Sí | Sí | Sí | Sí | Sí | Sí | Sí | No | No | No |
| 9.9.1 | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | No | No |
| 9,8 | Sí | Sí | Sí | No | Sí | Sí | Sí | Sí | Sí | No |
| 9,7 | No | Sí | Sí | No | No | Sí | Sí | Sí | Sí | Sí |
| 9,6 | No | No | No | No | No | No | Sí | Sí | Sí | Sí |
| 9,5 | No | No | No | No | No | No | No | Sí | Sí | Sí |

Relaciones de recuperación ante desastres de SVM de SnapMirror

- Para los datos de recuperación ante desastres de SVM y la protección de SVM:

La recuperación ante desastres de SVM solo se admite entre clústeres que ejecutan la misma versión de ONTAP. **La independencia de versiones no es compatible con la replicación de SVM.**

- Para la recuperación ante desastres de SVM para la migración de SVM:
 - La replicación es compatible en una sola dirección de una versión anterior de ONTAP en origen para que la misma versión de ONTAP o una posterior en el destino.
- La versión de ONTAP en el clúster de destino no debe tener más de dos versiones locales principales más nuevas o dos versiones de cloud principales más recientes, como se muestra en la tabla a continuación.
 - La replicación no es compatible con los casos de uso de protección de datos a largo plazo.

El asterisco (*) después de la versión indica una versión de sólo nube.

Para determinar la compatibilidad, busque la versión de origen en la columna de la tabla izquierda y, a continuación, busque la versión de destino en la fila superior (DR/Migración para versiones similares y Migración sólo para versiones más recientes).

| Orig en | Destino | | | | | | | | | | | | | | | | | |
|---------|--|--|--|-----------|-----------|-----------|-----------|-------|---------|--------|---------|--------|---------|--------|---------|--------|---------|--------|
| | 9,3 | 9,4 | 9,5 | 9,6 | 9,7 | 9,8 | 9.9.0* | 9.9.1 | 9.10.0* | 9.10.1 | 9.11.0* | 9.11.1 | 9.12.0* | 9.12.1 | 9.13.0* | 9.13.1 | 9.14.0* | 9.14.1 |
| 9,3 | Recuperación antes de astr es/ Migración | Migración | Migración | Migración | Migración | | | | | | | | | | | | | |
| 9,4 | | Recuperación antes de astr es/ Migración | Migración | Migración | Migración | Migración | | | | | | | | | | | | |
| 9,5 | | | Recuperación antes de astr es/ Migración | Migración | Migración | Migración | Migración | | | | | | | | | | | |

| | | | | | | | | | | | | | | | | | |
|--------|--|--|--|---|---|---|---|-----------|-----------|-----------|-----------|--|--|--|--|--|--|
| 9,6 | | | | Recuperación antes de las pruebas/ Migración | Migración | Migración | Migración | Migración | | | | | | | | | |
| 9,7 | | | | | Recuperación antes de las pruebas/ Migración | Migración | Migración | Migración | Migración | | | | | | | | |
| 9,8 | | | | | | Recuperación antes de las pruebas/ Migración | Migración | Migración | Migración | Migración | | | | | | | |
| 9.9.0* | | | | | | | Recuperación antes de las pruebas/ Migración | Migración | Migración | Migración | Migración | | | | | | |

| | | | | | | | | | | | | | | | | | | |
|-------------|--|--|--|--|--|--|--|---------------------------------------|---------------------------------------|---------------------------------------|-----------|-----------|-----------|-----------|--|--|--|--|
| 9.9. 1 | | | | | | | | Recuperación antes astr es/ Migración | Migración | Migración | Migración | Migración | | | | | | |
| 9.10 .0* | | | | | | | | Recuperación antes astr es/ Migración | Migración | Migración | Migración | Migración | | | | | | |
| 9.10 .1 | | | | | | | | | Recuperación antes astr es/ Migración | Migración | Migración | Migración | Migración | | | | | |
| 9.11 .0* | | | | | | | | | | Recuperación antes astr es/ Migración | Migración | Migración | Migración | Migración | | | | |

| | | | | | | | | | | | | | | | | | |
|-------------|--|--|--|--|--|--|--|--|--|--|---|---|---|-----------|-----------|-----------|--|
| 9.11 .1 | | | | | | | | | | | Recuperación antes de las pruebas/ Migración | Migración | Migración | Migración | Migración | | |
| 9.12 .0* | | | | | | | | | | | Recuperación antes de las pruebas/ Migración | Migración | Migración | Migración | Migración | | |
| 9.12 .1 | | | | | | | | | | | | Recuperación antes de las pruebas/ Migración | Migración | Migración | Migración | Migración | |
| 9.13 .0* | | | | | | | | | | | | | Recuperación antes de las pruebas/ Migración | Migración | Migración | Migración | |

| | | | | | | | | | | | | | | | | | | |
|-------------|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|---|---|---|
| 9.13 .1 | | | | | | | | | | | | | | | | Recuperación antes de desastres/ Migración | Migración | Migración |
| 9.14 .0* | | | | | | | | | | | | | | | | | Recuperación antes de desastres/ Migración | Migración |
| 9.14 .1 | | | | | | | | | | | | | | | | | | Recuperación antes de desastres/ Migración |

Relaciones de recuperación ante desastres de SnapMirror

Para relaciones de SnapMirror del tipo «DP» y del tipo de política «duplicación asíncrona»:



Los reflejos de tipo DP no se pueden inicializar comenzando con ONTAP 9.11.1 y están completamente obsoletos en ONTAP 9.12.1. Para obtener más información, consulte ["Amortización de las relaciones de SnapMirror para la protección de datos"](#).



En la siguiente tabla, la columna de la izquierda indica la versión de ONTAP en el volumen de origen y la fila superior indica las versiones de ONTAP que se pueden tener en el volumen de destino.

| Origen | Destino | | | | | | | | | | | |
|--------|---------|--------|-------|-----|-----|-----|-----|-----|-----|-----|-----|----|
| | 9.11.1 | 9.10.1 | 9.9.1 | 9,8 | 9,7 | 9,6 | 9,5 | 9,4 | 9,3 | 9,2 | 9,1 | 9 |
| 9.11.1 | Sí | No | No | No | No | No | No | No | No | No | No | No |

| | | | | | | | | | | | | |
|--------|----|----|----|----|----|----|----|----|----|----|----|----|
| 9.10.1 | Sí | Sí | No | No | No | No | No | No | No | No | No | No |
| 9.9.1 | Sí | Sí | Sí | No | No | No | No | No | No | No | No | No |
| 9,8 | No | Sí | Sí | Sí | No | No | No | No | No | No | No | No |
| 9,7 | No | No | Sí | Sí | Sí | No | No | No | No | No | No | No |
| 9,6 | No | No | No | Sí | Sí | Sí | No | No | No | No | No | No |
| 9,5 | No | No | No | No | Sí | Sí | Sí | No | No | No | No | No |
| 9,4 | No | No | No | No | No | Sí | Sí | Sí | No | No | No | No |
| 9,3 | No | No | No | No | No | No | Sí | Sí | Sí | No | No | No |
| 9,2 | No | No | No | No | No | No | No | Sí | Sí | Sí | No | No |
| 9,1 | No | No | No | No | No | No | No | No | Sí | Sí | Sí | No |
| 9 | No | No | No | No | No | No | No | No | No | Sí | Sí | Sí |



La interoperabilidad no es bidireccional.

Convierta una relación de tipo DP existente a XDP

Si actualiza a ONTAP 9.12.1 o una versión posterior, debe convertir las relaciones de tipo DP a XDP antes de realizar la actualización. ONTAP 9.12.1 y las versiones posteriores no admiten relaciones de tipo DP. Puede convertir fácilmente una relación de tipo de DP existente a XDP para poder aprovechar las ventajas de la flexibilidad de versión de SnapMirror.

Acerca de esta tarea

- SnapMirror no convierte automáticamente las relaciones de tipo DP existentes a XDP. Para convertir la relación, debe romper y eliminar la relación existente, crear una nueva relación XDP y volver a sincronizar la relación. Para obtener información previa, consulte ["XDP sustituye a DP como la opción predeterminada de SnapMirror"](#).
- Al planificar la conversión, tenga en cuenta que la preparación en segundo plano y la fase de almacenamiento de datos de una relación de SnapMirror para XDP pueden llevar mucho tiempo. No es poco frecuente ver la relación de SnapMirror que informa sobre el estado "preparación" para un periodo de tiempo prolongado.



Después de convertir un tipo de relación de SnapMirror de DP a XDP, las configuraciones relacionadas con el espacio, como la configuración automática de tamaño y la garantía de espacio, ya no se replican en el destino.

Pasos

1. En el clúster de destino, compruebe que la relación SnapMirror sea del tipo DP, que el estado de mirroring sea en SnapMirror, que el estado de la relación sea inactivo y que la relación esté en buen estado:

```
snapmirror show -destination-path <SVM:volume>
```

En el siguiente ejemplo, se muestra el resultado de `snapmirror show` comando:


```
cluster_dst:>snapmirror show -destination-path svm_backup:volA_dst
```

```
Source Path: svm1:volA
Destination Path: svm_backup:volA_dst
Relationship Type: DP
SnapMirror Schedule: -
Tries Limit: -
Throttle (KB/sec): unlimited
Mirror State: Snapmirrored
Relationship Status: Idle
Transfer Snapshot: -
Snapshot Progress: -
Total Progress: -
Snapshot Checkpoint: -
Newest Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Newest Snapshot Timestamp: 06/27 10:00:55
Exported Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Exported Snapshot Timestamp: 06/27 10:00:55
Healthy: true
```



Puede que le resulte útil conservar una copia del `snapmirror show` salida de comando para realizar un seguimiento de la configuración de relaciones existente.

2. En los volúmenes de origen y destino, asegúrese de que ambos volúmenes tengan una copia Snapshot común:

```
volume snapshot show -vserver <SVM> -volume <volume>
```

En el siguiente ejemplo se muestra el `volume snapshot show` salida de los volúmenes de origen y destino:

```
cluster_src:> volume snapshot show -vserver svml -volume volA
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-----
svml volA
weekly.2014-06-09_0736 valid 76KB 0% 28%
weekly.2014-06-16_1305 valid 80KB 0% 29%
daily.2014-06-26_0842 valid 76KB 0% 28%
hourly.2014-06-26_1205 valid 72KB 0% 27%
hourly.2014-06-26_1305 valid 72KB 0% 27%
hourly.2014-06-26_1405 valid 76KB 0% 28%
hourly.2014-06-26_1505 valid 72KB 0% 27%
hourly.2014-06-26_1605 valid 72KB 0% 27%
daily.2014-06-27_0921 valid 60KB 0% 24%
hourly.2014-06-27_0921 valid 76KB 0% 28%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
valid 44KB 0% 19%
11 entries were displayed.
```

```
cluster_dest:> volume snapshot show -vserver svm_backup -volume volA_dst
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-----
svm_backup volA_dst
weekly.2014-06-09_0736 valid 76KB 0% 30%
weekly.2014-06-16_1305 valid 80KB 0% 31%
daily.2014-06-26_0842 valid 76KB 0% 30%
hourly.2014-06-26_1205 valid 72KB 0% 29%
hourly.2014-06-26_1305 valid 72KB 0% 29%
hourly.2014-06-26_1405 valid 76KB 0% 30%
hourly.2014-06-26_1505 valid 72KB 0% 29%
hourly.2014-06-26_1605 valid 72KB 0% 29%
daily.2014-06-27_0921 valid 60KB 0% 25%
hourly.2014-06-27_0921 valid 76KB 0% 30%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
```

3. Para garantizar que las actualizaciones programadas no se ejecuten durante la conversión, desactive la relación de tipo DP existente:

```
snapmirror quiesce -source-path <SVM:volume> -destination-path  
<SVM:volume>
```

Para obtener una sintaxis completa del comando, consulte ["página de manual"](#).



Se debe ejecutar este comando desde la SVM de destino o el clúster de destino.

En el siguiente ejemplo, se pausa la relación entre el volumen de origen volA encendido svm1 y el volumen de destino volA_dst encendido svm_backup:

```
cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
```

4. Rompa la relación de tipo de DP existente:

```
snapmirror break -destination-path <SVM:volume>
```

Para obtener una sintaxis completa del comando, consulte ["página de manual"](#).



Se debe ejecutar este comando desde la SVM de destino o el clúster de destino.

En el siguiente ejemplo, se rompe la relación entre el volumen de origen volA encendido svm1 y el volumen de destino volA_dst encendido svm_backup:

```
cluster_dst::> snapmirror break -destination-path svm_backup:volA_dst
```

5. Si la eliminación automática de las copias Snapshot está habilitada en el volumen de destino, desactívelo:

```
volume snapshot autodelete modify -vserver _SVM_ -volume _volume_  
-enabled false
```

En el ejemplo siguiente se deshabilita la eliminación automática de copias Snapshot en el volumen de destino volA_dst:

```
cluster_dst::> volume snapshot autodelete modify -vserver svm_backup  
-volume volA_dst -enabled false
```

6. Elimine la relación de tipo de DP existente:

```
snapmirror delete -destination-path <SVM:volume>
```

Para obtener una sintaxis completa del comando, consulte ["página de manual"](#).



Se debe ejecutar este comando desde la SVM de destino o el clúster de destino.

En el siguiente ejemplo, se elimina la relación entre el volumen de origen volA encendido svm1 y el volumen de destino volA_dst encendido svm_backup:

```
cluster_dst::> snapmirror delete -destination-path svm_backup:volA_dst
```

7. Libere la relación de recuperación ante desastres de la SVM de origen en el origen:

```
snapmirror release -destination-path <SVM:volume> -relationship-info  
-only true
```

En el ejemplo siguiente se libera la relación de recuperación de desastres de SVM:

```
cluster_src::> snapmirror release -destination-path svm_backup:volA_dst  
-relationship-info-only true
```

8. Puede utilizar la salida que ha retenido de `snapmirror show` Comando para crear la nueva relación de tipo XDP:

```
snapmirror create -source-path <SVM:volume> -destination-path  
<SVM:volume> -type XDP -schedule <schedule> -policy <policy>
```

La nueva relación debe usar el mismo volumen de origen y destino. Para obtener una sintaxis de comando completa, consulte la página man.



Se debe ejecutar este comando desde la SVM de destino o el clúster de destino.

En el siguiente ejemplo se crea una relación de recuperación de desastres de SnapMirror entre el volumen de origen volA encendido svm1 y el volumen de destino volA_dst encendido svm_backup con el valor predeterminado MirrorAllSnapshots política:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination  
-path svm_backup:volA_dst  
-type XDP -schedule my_daily -policy MirrorAllSnapshots
```

9. Resincronización de los volúmenes de origen y destino:

```
snapmirror resync -source-path <SVM:volume> -destination-path  
<SVM:volume>
```

Para mejorar el tiempo de resincronización, puede utilizar el `-quick-resync` opcional, pero debe tener en cuenta que se pueden perder ahorros en eficiencia del almacenamiento. Para obtener una sintaxis completa del comando, consulte la página man: "[Comando SnapMirror resync](#)".



Se debe ejecutar este comando desde la SVM de destino o el clúster de destino. Aunque la resincronización no requiere una transferencia básica, puede requerir mucho tiempo. Puede que desee ejecutar la resincronización en horas de menor actividad.

En el siguiente ejemplo, vuelva a establecer la relación entre el volumen de origen `volA` encendido `svm1` y el volumen de destino `volA_dst` encendido `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination  
-path svm_backup:volA_dst
```

10. Si ha deshabilitado la eliminación automática de copias Snapshot, vuelva a habilitarla:

```
volume snapshot autodelete modify -vserver <SVM> -volume <volume>  
-enabled true
```

Después de terminar

1. Utilice la `snapmirror show` Comando para verificar que la relación de SnapMirror se ha creado.
2. Una vez que el volumen de destino de SnapMirror XDP comienza a actualizar las copias snapshot tal como se define en la política de SnapMirror, utilice el resultado de `snapmirror list-destinations` Comando del clúster de origen para mostrar la nueva relación de XDP de SnapMirror.

Elimine las conexiones del servidor de gestión de claves externo existentes antes de actualizar ONTAP

Antes de actualizar ONTAP, si ejecuta ONTAP 9,2 o una versión anterior con el cifrado de almacenamiento de NetApp (NSE) y se actualiza a ONTAP 9,3 o posterior, debe utilizar la interfaz de línea de comandos (CLI) para eliminar cualquier conexión existente del servidor de gestión de claves externa (KMIP).

Pasos

1. Compruebe que las unidades NSE estén desbloqueadas, abiertas y configuradas con el ID seguro de fabricación predeterminado 0x0:

```
storage encryption disk show -disk *
```

2. Entre en el modo de privilegio avanzado:

```
set -privilege advanced
```

3. Utilice el ID seguro de fabricación predeterminado 0x0 para asignar la clave FIPS a los discos de cifrado automático (SED):

```
storage encryption disk modify -fips-key-id 0x0 -disk *
```

4. Compruebe que se haya completado la asignación de la clave FIPS a todos los discos:

```
storage encryption disk show-status
```

5. Verifique que el **mode** para todos los discos esté configurado en data

```
storage encryption disk show
```

6. Vea los servidores KMIP configurados:

```
security key-manager show
```

7. Elimine los servidores KMIP configurados:

```
security key-manager delete -address kmip_ip_address
```

8. Elimine la configuración del gestor de claves externo:

```
security key-manager delete-kmip-config
```



Este paso no quita los certificados de NSE.

El futuro

Una vez completada la actualización, debe hacerlo [Vuelva a configurar las conexiones del servidor KMIP](#).

Compruebe que el archivo netgroup está presente en todos los nodos antes de actualizar ONTAP

Antes de actualizar ONTAP, si ha cargado netgroups en máquinas virtuales de almacenamiento (SVM), debe verificar que el archivo netgroup esté presente en cada nodo. Si falta un archivo de grupo de red en un nodo, puede provocar un error en la actualización.

Pasos

1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Muestre el estado del grupo de red para cada SVM:

```
vserver services netgroup status
```

3. Compruebe que, en cada SVM, cada nodo muestra el mismo valor hash de archivo netgroup:

```
vserver services name-service netgroup status
```

De ser así, puede omitir el siguiente paso y continuar con la actualización o la reversión. De lo contrario, continúe con el siguiente paso.

4. En cualquier nodo del clúster, cargue manualmente el archivo netgroup:

```
vserver services netgroup load -vserver vserver_name -source uri
```

Este comando descarga el archivo netgroup en todos los nodos. Si ya existe un archivo de netgroup en un nodo, se sobrescribe.

Información relacionada

["Trabajar con netgroups"](#)

Configure los clientes LDAP para que utilicen TLS para obtener la mayor seguridad

Antes de actualizar ONTAP, debe configurar clientes LDAP mediante SSLv3 para establecer comunicaciones seguras con servidores LDAP con el fin de utilizar TLS. SSL no estará disponible después de la actualización.

De forma predeterminada, las comunicaciones LDAP entre las aplicaciones cliente y servidor no están cifradas. Debe desactivar el uso de SSL e imponer el uso de TLS.

Pasos

1. Compruebe que los servidores LDAP del entorno son compatibles con TLS.

Si no lo hacen, no continúe. Debe actualizar los servidores LDAP a una versión compatible con TLS.

2. Compruebe qué configuraciones del cliente LDAP de ONTAP tienen LDAP sobre SSL/TLS habilitado:

```
vserver services name-service ldap client show
```

Si no hay ninguno, puede omitir los pasos restantes. Sin embargo, debe considerar utilizar LDAP sobre TLS para mejorar la seguridad.

3. Para cada configuración de cliente LDAP, desactivar SSL para que aplique el uso de TLS:

```
vserver services name-service ldap client modify -vserver vserver_name  
-client-config ldap_client_config_name -allow-ssl false
```

4. Compruebe que ya no se permite el uso de SSL en ningún cliente LDAP:

```
vserver services name-service ldap client show
```

Información relacionada

["Gestión de NFS"](#)

Consideraciones sobre los protocolos orientados a las sesiones

Los clústeres y los protocolos orientados a la sesión pueden causar efectos adversos en clientes y aplicaciones en ciertas áreas, como el servicio de I/O durante las actualizaciones.

Si utiliza protocolos orientados a la sesión, tenga en cuenta lo siguiente:

- SMB

Si usted sirve recursos compartidos de disponibilidad continua (CA) con SMBv3, puede utilizar el sistema automatizado

Método de actualización no disruptivo (con System Manager o CLI) y no se producen interrupciones experimentado por el cliente.

Si presta servicio a recursos compartidos con SMBv1 o SMBv2, o recursos compartidos que no son de CA con SMBv3, las sesiones del cliente se interrumpen durante las operaciones de toma de control y reinicio de la actualización. Debe dirigir a los usuarios para que terminen sus sesiones antes de actualizarlas.

Hyper-V y SQL Server sobre SMB admiten operaciones no disruptivas (NDO). Si configuró una solución Hyper-V o SQL Server mediante SMB, los servidores de aplicaciones y las máquinas virtuales o bases de datos contenidas permanecen en línea y proporcionan disponibilidad continua durante la actualización de ONTAP.

- NFSv4. X

Los clientes de NFSv4.x podrán recuperarse automáticamente de las pérdidas de conexión sufridas durante la actualización con procedimientos de recuperación de NFSv4.x. Las aplicaciones pueden experimentar un retraso de I/O temporal durante este proceso.

- NDMP

Se pierde el estado y el usuario cliente debe volver a intentar la operación.

- Backups y restauraciones

Se pierde el estado y el usuario cliente debe volver a intentar la operación.



No inicie una copia de seguridad ni restaure durante o inmediatamente antes de una actualización. Si lo hace, se puede producir la pérdida de datos.

- Aplicaciones (por ejemplo, Oracle o Exchange)

Los efectos dependen de las aplicaciones. Para las aplicaciones basadas en tiempo de espera, es posible que pueda cambiar la configuración de tiempo de espera a más largo que el tiempo de reinicio de ONTAP

para minimizar los efectos adversos.

Verifique la compatibilidad con el algoritmo de clave de host SSH antes de actualizar ONTAP

Antes de actualizar ONTAP, si se habilita el modo FIPS SSL en un clúster donde las cuentas de administrador se autentican con una clave pública SSH, debe asegurarse de que el algoritmo de clave de host sea compatible con la versión de ONTAP de destino.

La siguiente tabla indica los algoritmos de tipo de clave de host que se admiten para las conexiones SSH de ONTAP. Estos tipos de claves no se aplican a la configuración de la autenticación pública SSH.

| Versión de ONTAP | Tipos de clave compatibles con el modo FIPS | Tipos de clave compatibles con el modo no FIPS |
|---------------------|---|--|
| 9.11.1 y posterior | ecdsa-sha2-nistp256 | ecdsa-sha2-nistp256 rsa-sha2-512 rsa-sha2-256 ssh-ed25519 ssh-dss ssh-rsa |
| 9.10.1 y anteriores | ecdsa-sha2-nistp256 ssh-ed25519 | ecdsa-sha2-nistp256 ssh-ed25519 ssh-dss ssh-rsa |



La compatibilidad con el algoritmo de clave de host ssh-ed25519 se elimina a partir de ONTAP 9.11.1.

Para obtener más información, consulte ["Configurar la seguridad de red con FIPS"](#).

Las cuentas de clave pública SSH existentes sin algoritmos de clave soportados deben volver a configurarse con un tipo de clave soportada antes de actualizar o se producirá un error en la autenticación del administrador.

["Obtenga más información sobre cómo habilitar cuentas de claves públicas de SSH."](#)

Reinicie el SP o BMC para preparar la actualización del firmware durante una actualización de ONTAP

No es necesario actualizar manualmente el firmware antes de proceder con una actualización de ONTAP. El firmware del clúster se incluye con el paquete de actualización de ONTAP y se copia en el dispositivo de arranque de cada nodo. El nuevo firmware se instala como parte del proceso de actualización.

El firmware de los siguientes componentes se actualiza automáticamente si la versión del clúster es más antigua que el firmware que se incluye con el paquete de actualización de ONTAP:

- BIOS/CARGADOR
- Service Processor (SP) o controlador de gestión de placa base (BMC)
- Bandeja de almacenamiento

- Disco
- Flash Cache

Para prepararse para una actualización fluida, debe reiniciar el SP o BMC antes de que comience la actualización.

Paso

1. Reinicie el SP o BMC antes de realizar la actualización:

```
system service-processor reboot-sp -node node_name
```

Solo reinicie un SP o BMC a la vez. Espere a que el SP o BMC reiniciado recicle por completo antes de reiniciar el siguiente.

También puede hacerlo ["actualice el firmware manualmente"](#) Entre actualizaciones de ONTAP. Si tiene Active IQ, puede ["Consulte la lista de versiones de firmware incluidas actualmente en la imagen ONTAP"](#).

Las versiones actualizadas del firmware están disponibles de la siguiente manera:

- ["Firmware del sistema \(BIOS, BMC, SP\)"](#)
- ["Firmware de la bandeja"](#)
- ["Firmware de disco y Flash Cache"](#)

Descargue la imagen del software ONTAP

Antes de actualizar ONTAP, primero debe descargar la imagen del software de ONTAP de destino desde el sitio de soporte de NetApp. Según la versión de ONTAP, puede descargar el software ONTAP en un servidor HTTPS, HTTP o FTP de la red o en una carpeta local.

| Si está ejecutando... | Puede descargar la imagen en esta ubicación... |
|-----------------------------------|---|
| ONTAP 9.6 y posteriores | <ul style="list-style-type: none"> • Un servidor HTTPS El certificado de CA del servidor debe instalarse en el sistema local. • Una carpeta local • Un servidor HTTP o FTP |
| ONTAP 9,4 y versiones posteriores | <ul style="list-style-type: none"> • Una carpeta local • Un servidor HTTP o FTP |
| ONTAP 9,0 y versiones posteriores | Un servidor HTTP o FTP |

Acerca de esta tarea

- Si realiza una actualización automatizada no disruptiva (ANDU) mediante un ["ruta de actualización directa de varios saltos"](#), usted necesita ["descargue"](#) El paquete de software para la versión de ONTAP intermedia y la versión de ONTAP de destino necesaria para la actualización. Por ejemplo, si va a actualizar de

ONTAP 9,8 a ONTAP 9.13.1, debe descargar los paquetes de software tanto para ONTAP 9.12.1 como para ONTAP 9.13.1. Consulte ["rutas de actualización admitidas"](#) para determinar si la ruta de actualización requiere la descarga de un paquete de software intermedio.

- Si actualiza un sistema con el cifrado de volúmenes de NetApp a ONTAP 9.5 o una versión posterior, debe descargar la imagen del software ONTAP para países no restringidos, que incluye el cifrado de volúmenes de NetApp.

Si utiliza la imagen del software de ONTAP para países restringidos a fin de actualizar un sistema con el cifrado de volúmenes de NetApp, el sistema produce una alarma y perderá el acceso a los volúmenes.

- No es necesario descargar un paquete de software independiente para su firmware. La actualización del firmware del clúster se incluye con el paquete de actualización de software ONTAP y se copia en el dispositivo de arranque de cada nodo. El nuevo firmware se instala como parte del proceso de actualización.

Pasos

1. Busque el software ONTAP de destino en la ["Descargas de software"](#) Del sitio de soporte de NetApp.

Para una actualización de ONTAP Select, seleccione **actualización de nodo de ONTAP Select**.

2. Copie la imagen del software (por ejemplo, 97_q_image.tgz) en la ubicación adecuada.

Según la versión de ONTAP, la ubicación será un directorio desde el que se servirá la imagen al sistema local o a una carpeta local del sistema de almacenamiento.

Métodos de actualización de ONTAP

Métodos de actualización del software ONTAP

Puede realizar una actualización automatizada del software ONTAP con System Manager. Como alternativa, puede realizar una actualización automatizada o manual con la interfaz de línea de comandos (CLI) de ONTAP. El método que utiliza para actualizar ONTAP depende de la configuración, la versión actual de ONTAP y el número de nodos del clúster. NetApp recomienda usar System Manager para realizar actualizaciones automatizadas a menos que la configuración requiera un enfoque diferente. Por ejemplo, si tiene una configuración de MetroCluster con 4 nodos que ejecuten ONTAP 9,3 o posterior, debería utilizar System Manager para llevar a cabo una actualización automatizada (a veces denominada actualización no disruptiva automatizada o ANDU). Si tiene una configuración de MetroCluster con nodos 8 que ejecutan ONTAP 9,2 o una versión anterior, debe usar la CLI para realizar una actualización manual.

Una actualización puede ejecutarse mediante el proceso de actualización gradual o el proceso de actualización en lote. Ambos elementos no disruptivos.

Para las actualizaciones automatizadas, ONTAP instala automáticamente la imagen ONTAP de destino en cada nodo, valida los componentes del clúster para garantizar que el clúster se pueda actualizar sin interrupciones y, a continuación, ejecuta una actualización en lote o en segundo plano en función del número de nodos. En el caso de las actualizaciones manuales, el administrador confirma manualmente que cada nodo del clúster está listo para la actualización y, a continuación, realiza los pasos necesarios para ejecutar una actualización gradual.

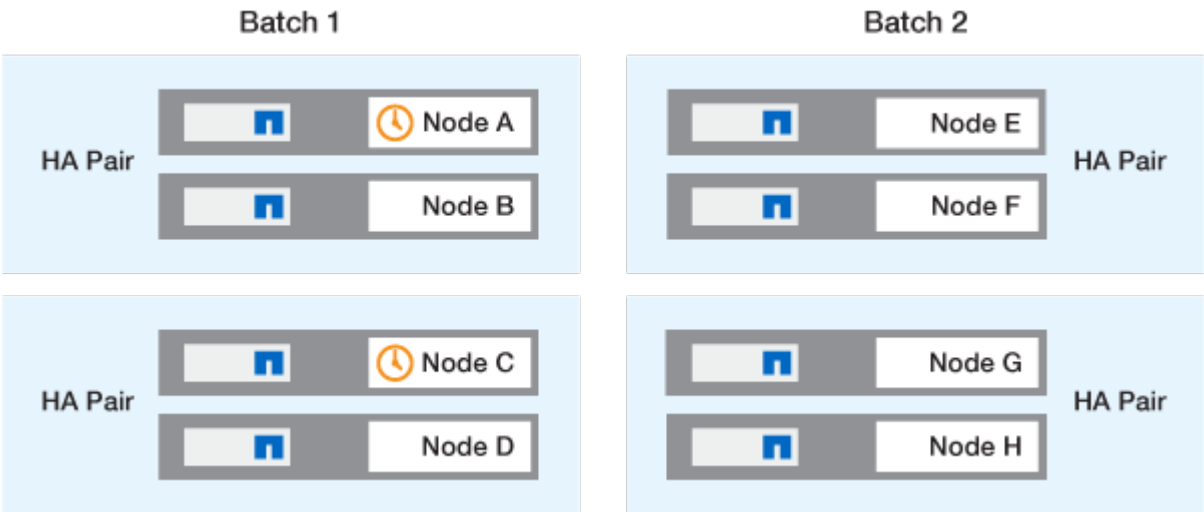
Actualizaciones graduales de ONTAP

El proceso de actualización gradual es la opción predeterminada para los clústeres con menos de 8 nodos. En el proceso de actualización gradual, un nodo se desconecta y se actualiza mientras su compañero toma el control de su almacenamiento. Cuando se completa la actualización del nodo, el nodo asociado le devuelve el control al nodo propietario original y el proceso se repite en el nodo asociado. Cada par de alta disponibilidad adicional se actualiza en secuencia hasta que todos los pares de alta disponibilidad ejecutan la versión de destino.

Actualizaciones en lotes de ONTAP

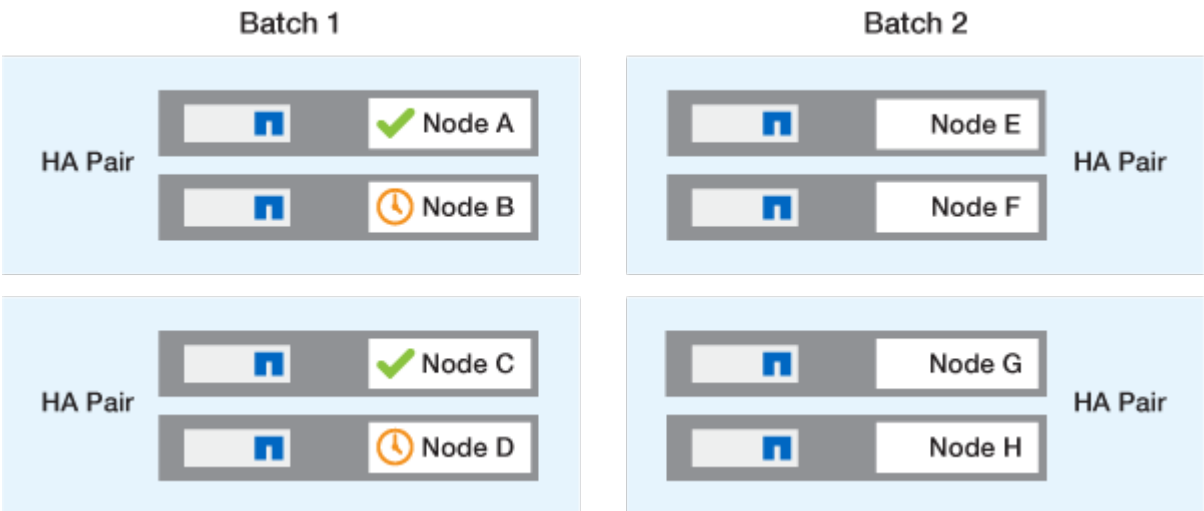
El proceso de actualización por lotes es el predeterminado para clústeres de 8 nodos o más. En el proceso de actualización por lotes, el clúster se divide en dos lotes. Cada lote contiene varios pares de alta disponibilidad. En el primer lote, el primer nodo de cada par de alta disponibilidad se actualiza simultáneamente con el primer nodo de los demás pares de alta disponibilidad del lote.

En el siguiente ejemplo, hay dos pares de alta disponibilidad en cada lote. Cuando comienza la actualización por lotes, los nodos A y C se actualizan simultáneamente.



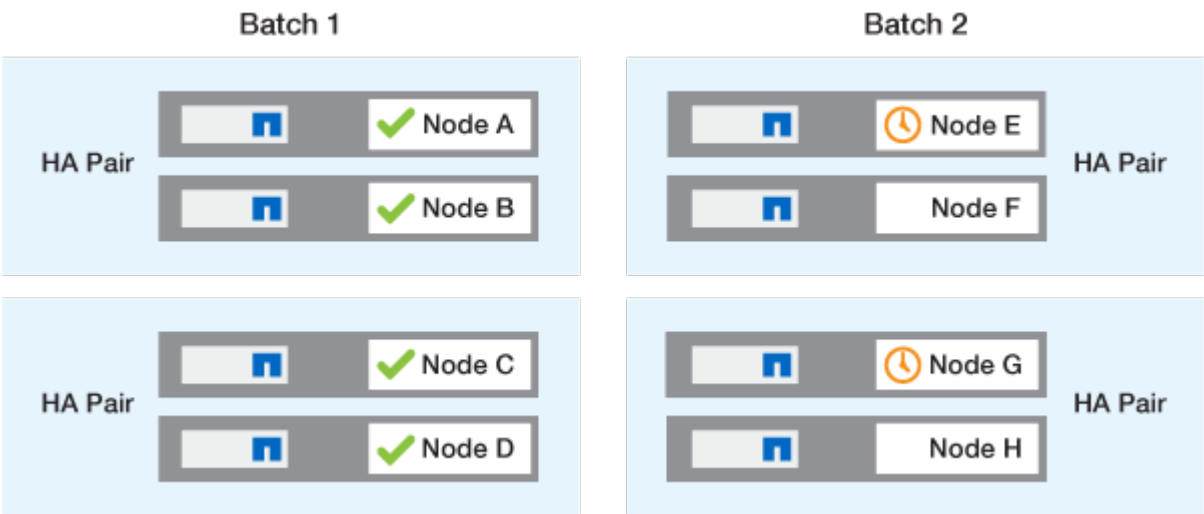
Una vez completada la actualización de los primeros nodos de cada par de alta disponibilidad, los nodos asociados del lote 1 se actualizan simultáneamente.

En el siguiente ejemplo, después de actualizar los nodos A y C, los nodos B y D se actualizan simultáneamente.



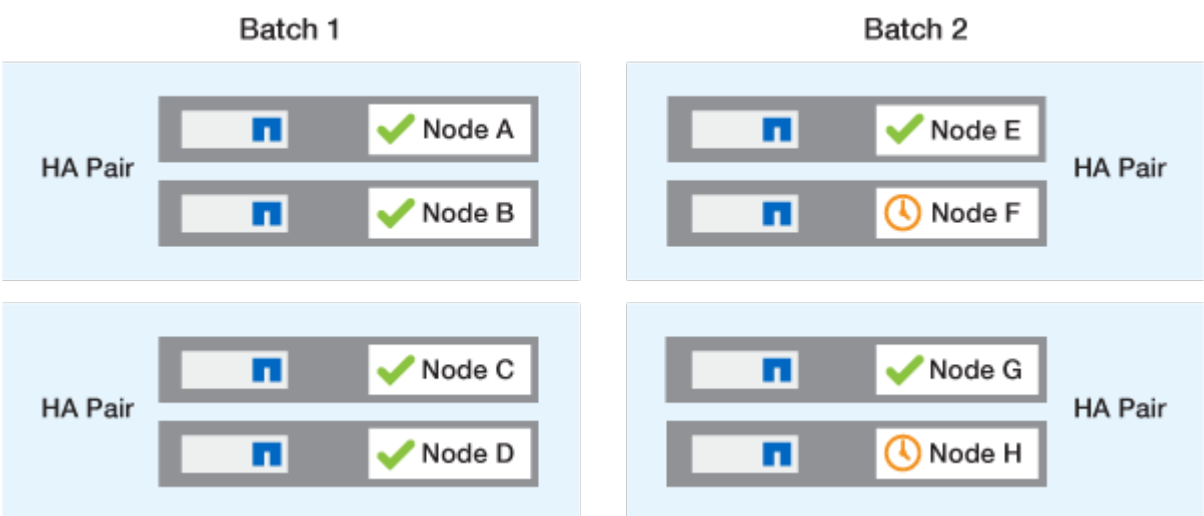
A continuación, el proceso se repite para los nodos en el lote 2. El primer nodo de cada par de alta disponibilidad se actualiza de forma simultánea con el primer nodo de los demás pares de alta disponibilidad del lote.

En el siguiente ejemplo, el nodo E y el nodo G se actualizan simultáneamente.



Una vez completada la actualización de los primeros nodos de cada par de alta disponibilidad, los nodos asociados del lote 2 se actualizan simultáneamente.

En el siguiente ejemplo, el nodo F y el nodo H se actualizan simultáneamente para completar el proceso de actualización por lotes.



Métodos de actualización de ONTAP recomendados según la configuración

Los métodos de actualización admitidos por la configuración se enumeran por orden de uso recomendado.

| Configuración | Versión de ONTAP | Número de nodos | Método de actualización recomendado |
|---------------|------------------|-----------------|---|
| Estándar | 9,0 o posterior | 2 o más | <ul style="list-style-type: none"> • Automatización no disruptiva gracias a System Manager • Automatización no disruptiva gracias a la interfaz de línea de comandos |
| Estándar | 9,0 o posterior | Único | "Interrupción automatizada" |
| MetroCluster | 9,3 o posterior | 8 | <ul style="list-style-type: none"> • Automatización no disruptiva gracias a la interfaz de línea de comandos • Manual no disruptivo para MetroCluster de 4 o 8 nodos con la CLI |
| MetroCluster | 9,3 o posterior | 2,4 | <ul style="list-style-type: none"> • Automatización no disruptiva gracias a System Manager • Automatización no disruptiva gracias a la interfaz de línea de comandos |
| MetroCluster | 9.2 o anterior | 4, 8 | Manual no disruptivo para MetroCluster de 4 o 8 nodos con la CLI |
| MetroCluster | 9.2 o anterior | 2 | Manual no disruptivo para MetroCluster de 2 nodos utilizando la línea de comandos |

ANDU El uso de System Manager es el método de actualización recomendado para todas las actualizaciones de revisiones, independientemente de la configuración.



A. **actualización manual disruptiva** se puede realizar en cualquier configuración. Sin embargo, no se debe realizar una actualización disruptiva a menos que se pueda desconectar el clúster durante la actualización. Si trabaja en un entorno SAN, debe estar preparado para apagar o suspender todos los clientes SAN antes de realizar una actualización disruptiva. Las actualizaciones disruptivas se realizan mediante la interfaz de línea de comandos de ONTAP.

Actualización automatizada y no disruptiva de ONTAP

Cuando realiza una actualización automatizada, ONTAP instala automáticamente la imagen de ONTAP de destino en cada nodo, valida que el clúster pueda actualizarse correctamente y, a continuación, ejecuta cualquiera de ellos [actualización por lotes o sucesivas](#) en el segundo plano según el número de nodos del clúster.

Si es compatible con su configuración, debe usar System Manager para realizar una actualización automatizada. Si la configuración no admite la actualización automatizada mediante System Manager, puede utilizar la interfaz de línea de comandos (CLI) de ONTAP para realizar una actualización automatizada.



Modificar el ajuste de `storage failover modify-auto-giveback` La opción de comando antes del inicio de una actualización automática no disruptiva (ANDU) no afecta al proceso de actualización. EL proceso ANDU ignora cualquier valor predefinido para esta opción durante la toma de control/devolución necesaria para la actualización. Por ejemplo, establecer `-autogiveback A False` antes de comenzar ANDU no interrumpe la actualización automática antes de la devolución.

Antes de empezar

- Usted debe ["prepare la actualización"](#).
- Usted debe ["Descargue la imagen del software ONTAP"](#) Para la versión de ONTAP objetivo.

Si está realizando una ["actualización directa de varios saltos"](#), Necesita descargar las dos imágenes ONTAP necesarias para su específico ["ruta de actualización"](#).

- Para cada pareja de alta disponibilidad, cada nodo debe tener uno o varios puertos en el mismo dominio de retransmisión.

Si tiene 8 nodos o más, se utiliza el método de actualización por lotes en la actualización automática no disruptiva. En ONTAP 9.7 y versiones anteriores, si se utiliza el método por lotes, los LIF se migran al partner de alta disponibilidad del nodo que se actualiza. Si los partners no tienen ningún puerto en el mismo dominio de retransmisión, la migración LIF falla.

En ONTAP 9.8 y versiones posteriores, si se utiliza el método por lotes, los LIF se migran al otro grupo por lotes.

- Si actualiza ONTAP en una configuración de MetroCluster FC, el clúster debe habilitarse para una conmutación de sitios no planificada automática.
- Si no tiene previsto supervisar el progreso del proceso de actualización, debería hacerlo ["Solicite notificaciones EMS de errores que puedan requerir intervención manual"](#).
- Si tiene un clúster de un solo nodo, siga el ["actualización automatizada y disruptiva"](#) proceso.

Las actualizaciones de los clústeres de un solo nodo causan interrupciones.

Ejemplo 2. Pasos

System Manager


1. Valide la imagen de destino de ONTAP:



Si está actualizando una configuración de MetroCluster, debe validar el clúster A y, a continuación, repetir el proceso de validación en el clúster B.

- a. Según la versión de ONTAP que esté ejecutando, realice uno de los pasos siguientes:

| Si está ejecutando... | Realice lo siguiente... |
|-----------------------|---|
| ONTAP 9,8 o posterior | Haga clic en Cluster > Overview . |
| ONTAP 9.5, 9.6 y 9.7 | Haga clic en Configuración > clúster > Actualizar . |
| ONTAP 9.4 o anterior | Haga clic en Configuración > actualización de clúster . |

- b. En la esquina derecha del panel **Overview**, haga clic en .
- c. Haga clic en **actualización de ONTAP**.
- d. En la pestaña **Cluster Update**, agregue una nueva imagen o seleccione una imagen disponible.

| Si desea... | Realice lo siguiente... |
|--|---|
| Agregue una nueva imagen de software desde una carpeta local Ya deberías tener "se ha descargado la imagen" al cliente local. | <ol style="list-style-type: none">i. En Imágenes de software disponibles, haga clic en Agregar desde local.ii. Busque la ubicación en la que guardó la imagen de software, seleccione la imagen y, a continuación, haga clic en Abrir. |
| Añada una nueva imagen de software desde un servidor HTTP o FTP | <ol style="list-style-type: none">i. Haga clic en Agregar desde el servidor.ii. En el cuadro de diálogo Agregar una nueva imagen de software, introduzca la URL del servidor HTTP o FTP en el que descargó la imagen del software ONTAP del sitio de soporte de NetApp. Para el FTP anónimo, debe especificar la dirección URL en el ftp://anonymous@ftpserver formato.iii. Haga clic en Agregar. |
| Seleccione una imagen disponible | Elija una de las imágenes mostradas. |

- e. Haga clic en **Validar** para ejecutar las comprobaciones de validación previas a la actualización.

Si se encuentran errores o advertencias durante la validación, se muestran junto con una lista de acciones correctivas. Debe resolver todos los errores antes de continuar con la actualización. Se recomienda también resolver las advertencias.

2. Haga clic en **Siguiente**.

3. Haga clic en **Actualizar**.

La validación se realizará de nuevo. Los errores o advertencias restantes se muestran junto con una lista de acciones correctivas. Es necesario corregir los errores antes de continuar con la actualización. Si la validación se completa con advertencias, corrija las advertencias o seleccione **Actualizar con advertencias**.



De manera predeterminada, ONTAP utiliza el "[proceso de actualización por lotes](#)" para actualizar clústeres con ocho o más nodos. A partir de ONTAP 9.10.1, si lo prefiere, puede seleccionar **Actualizar un par de alta disponibilidad a la vez** para anular el valor predeterminado y hacer que su clúster actualice un par de alta disponibilidad a la vez mediante el proceso de actualización gradual.

En el caso de las configuraciones de MetroCluster con más de 2 nodos, el proceso de actualización de ONTAP se inicia simultáneamente en los pares de alta disponibilidad en ambos sitios. Para una configuración de MetroCluster de 2 nodos, la actualización se inicia primero en el sitio donde no se inicia la actualización. La actualización en el sitio restante comienza después de que la primera actualización se haya completado por completo.

4. Si la actualización se detiene debido a un error, haga clic en el mensaje de error para ver los detalles y, a continuación, corrija el error y. "[reanude la actualización](#)".

Después de terminar

Cuando la actualización se haya completado correctamente, el nodo se reiniciará y se le redirigirá a la página de inicio de sesión de System Manager. Si el nodo tarda mucho tiempo en reiniciarse, debe actualizar el navegador.

CLI

1. Validar la imagen del software de destino ONTAP



Si va a actualizar una configuración de MetroCluster, primero debe ejecutar los siguientes pasos en el clúster A y, a continuación, ejecutar los mismos pasos en el clúster B.

a. Elimine el paquete de software de ONTAP anterior:

```
cluster image package delete -version previous_ONTAP_Version
```

b. Cargue la imagen de software ONTAP de destino en el repositorio de paquetes del cluster:

```
cluster image package get -url location
```

```
cluster1::> cluster image package get -url
http://www.example.com/software/9.13.1/image.tgz

Package download completed.
Package processing completed.
```

Si está realizando una "actualización directa de varios saltos", También es necesario cargar el paquete de software para la versión intermedia de ONTAP necesaria para su actualización. Por ejemplo, si está actualizando de 9,8 a 9.13.1, debe cargar el paquete de software para ONTAP 9.12.1 y a continuación utilizar el mismo comando para cargar el paquete de software de 9.13.1.

- c. Compruebe que el paquete de software esté disponible en el repositorio del paquete de clúster:

```
cluster image package show-repository
```

```
cluster1::> cluster image package show-repository
Package Version  Package Build Time
-----
9.13.1           MM/DD/YYYY 10:32:15
```

- d. Ejecute las comprobaciones automatizadas previas a la actualización:

```
cluster image validate -version package_version_number
```

Si está realizando una "actualización directa de varios saltos", Solo necesita utilizar el paquete ONTAP de destino para la verificación. No es necesario validar la imagen de actualización intermedia por separado. Por ejemplo, si va a actualizar de 9,8 a 9.13.1, use el paquete 9.13.1 para verificación. No es necesario validar el paquete 9.12.1 por separado.

```
cluster1::> cluster image validate -version 9.13.1

WARNING: There are additional manual upgrade validation checks that
must be performed after these automated validation checks have
completed...
```

- a. Supervise el progreso de la validación:

```
cluster image show-update-progress
```

- b. Complete todas las acciones necesarias identificadas por la validación.
- c. Si va a actualizar una configuración de MetroCluster, repita los pasos anteriores en el clúster B.

2. Genere un cálculo de actualización de software:

```
cluster image update -version package_version_number -estimate-only
```



Si va a actualizar una configuración de MetroCluster, puede ejecutar este comando en el clúster A o en el clúster B. No es necesario ejecutarlo en ambos clústeres.

La estimación de actualización de software muestra detalles sobre cada componente que se va a actualizar, así como la duración estimada de la actualización.

3. Realice la actualización de software:

```
cluster image update -version package_version_number
```

- Si está realizando una "[actualización directa de varios saltos](#)", Utilice la versión ONTAP de destino para el paquete_VERSION_NUMBER. Por ejemplo, si va a actualizar de ONTAP 9,8 a 9.13.1, utilice 9.13.1 como package_version_number.
- De manera predeterminada, ONTAP utiliza el "[proceso de actualización por lotes](#)" para actualizar clústeres con ocho o más nodos. Si lo prefiere, puede usar el `-force-rolling` parámetro para anular el proceso predeterminado y que el clúster actualice un nodo a la vez mediante el proceso de actualización gradual.
- Tras completar cada toma de control y devolución, la actualización espera durante 8 minutos para permitir que las aplicaciones cliente se recuperen desde la pausa en las operaciones de I/O que se producen durante la toma de control y el retorno al nodo primario. Si el entorno requiere más o menos tiempo para la estabilización de clientes, puede usar el `-stabilize-minutes` parámetro para especificar otra cantidad de tiempo de estabilización.
- Para las configuraciones MetroCluster con más de 4 nodos, la actualización automatizada comienza simultáneamente en los pares de alta disponibilidad en ambos sitios. Para una configuración MetroCluster de 2 nodos, la actualización se inicia en el sitio donde no se inicia la actualización. La actualización en el sitio restante comienza después de que la primera actualización se haya completado por completo.

```

cluster1::> cluster image update -version 9.13.1

Starting validation for this update. Please wait..

It can take several minutes to complete validation...

WARNING: There are additional manual upgrade validation checks...

Pre-update Check      Status      Error-Action
-----
.....
...
20 entries were displayed

Would you like to proceed with update ? {y|n}: y
Starting update...

cluster-1::>

```

4. Muestre el progreso de la actualización del clúster:

```
cluster image show-update-progress
```

Si va a actualizar una configuración de MetroCluster de 4 o 8 nodos, el `cluster image show-update-progress` el comando solo muestra el progreso del nodo en el que ejecuta el comando. Debe ejecutar el comando en cada nodo para ver el progreso de cada nodo.

5. Compruebe que la actualización se ha completado correctamente en cada nodo.

```
cluster image show-update-progress
```

```
cluster1::> cluster image show-update-progress
```

| Elapsed | | Estimated |
|--------------------|-----------|-----------|
| Update Phase | Status | Duration |
| Duration | | |
| ----- | ----- | ----- |
| ----- | | |
| Pre-update checks | completed | 00:10:00 |
| 00:02:07 | | |
| Data ONTAP updates | completed | 01:31:00 |
| 01:39:00 | | |
| Post-update checks | completed | 00:10:00 |
| 00:02:00 | | |

3 entries were displayed.

Updated nodes: node0, node1.

6. Active una notificación de AutoSupport:

```
autosupport invoke -node * -type all -message "Finishing_NDU"
```

Si el clúster no está configurado para enviar mensajes de AutoSupport, se guardará una copia de la notificación de forma local.

7. Si va a actualizar una configuración de MetroCluster FC de 2 nodos, compruebe que el clúster esté habilitado para la conmutación automática de sitios no planificada.



Si va a actualizar una configuración estándar, una configuración de IP de MetroCluster o una configuración de FC de MetroCluster superior a 2 nodos, no necesita realizar este paso.

a. Compruebe si la conmutación automática no planificada está habilitada:

```
metrocluster show
```

Si la conmutación automática no planificada está habilitada, aparecerá la siguiente instrucción en el resultado del comando:

```
AUSO Failure Domain      auso-on-cluster-disaster
```

a. Si la sentencia no aparece en la salida, habilite la conmutación automática no planificada:

```
metrocluster modify -auto-switchover-failure-domain auso-on-  
cluster-disaster
```

- b. Compruebe que se ha activado la conmutación automática no planificada:

```
metrocluster show
```

Reanude la actualización del software ONTAP tras un error en el proceso de actualización automatizada

Si una actualización automática del software ONTAP se detiene debido a un error, debe resolver el error y, a continuación, continuar con la actualización. Una vez resuelto el error, puede optar por continuar con el proceso de actualización automatizada o completar manualmente el proceso de actualización. Si decide continuar con la actualización automatizada, no realice ninguno de los pasos de actualización de forma manual.

Ejemplo 3. Pasos

System Manager

1. Según la versión de ONTAP que esté ejecutando, realice uno de los pasos siguientes:

| Si está ejecutando... | Realice lo siguiente... |
|-----------------------|--|
| ONTAP 9,8 o posterior | Haga clic en Cluster > Overview |
| ONTAP 9,7, 9,6 o 9,5 | Haga clic en Configuración > clúster > Actualizar. |
| ONTAP 9.4 o anterior | <ul style="list-style-type: none">• Haga clic en Configuración > actualización de clúster.• En la esquina derecha del panel Descripción general, haz clic en los tres puntos verticales azules y selecciona Actualización de ONTAP. |

2. Continúe la actualización automatizada o cancele la actualización y continúe manualmente.

| Si desea... | Realice lo siguiente... |
|--|-------------------------------|
| Reanude la actualización automatizada | Haga clic en Reanudar. |
| Cancele la actualización automatizada y continúe manualmente | Haga clic en Cancelar. |

CLI

1. Vea el error de actualización:

```
cluster image show-update-progress
```

2. Resuelva el error.
3. Reanude la actualización:

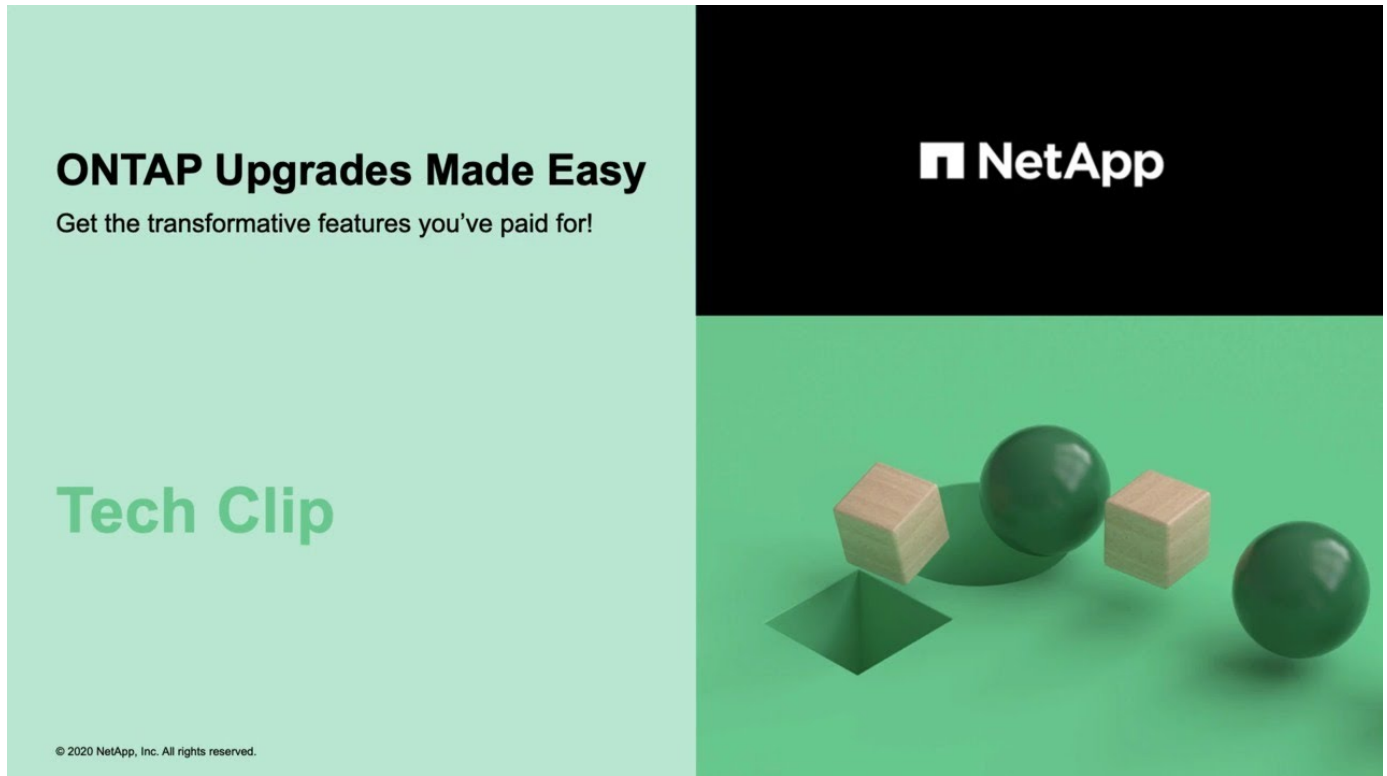
| Si desea... | Introduzca el siguiente comando... |
|--|--|
| Reanude la actualización automatizada | <pre>cluster image resume-update</pre> |
| Cancele la actualización automatizada y continúe manualmente | <pre>cluster image cancel-update</pre> |

Después de terminar

["Realice las comprobaciones posteriores a la actualización"](#).

Vídeo: Las actualizaciones se han realizado con facilidad

Eche un vistazo a las funcionalidades de actualización simplificadas de ONTAP de System Manager en ONTAP 9.8.



Información relacionada

- ["Inicie Active IQ"](#)
- ["Documentación de Active IQ"](#)

Actualizaciones manuales

Instale el paquete de software ONTAP para las actualizaciones manuales

Después de descargar el paquete de software de ONTAP para una actualización manual, debe instalarlo localmente antes de comenzar la actualización.

Pasos

1. Establezca el nivel de privilegio en avanzado, introduzca **y** cuando se le solicite continuar: `set -privilege advanced`

El aviso avanzado (*>) aparece.

2. Instale la imagen.

| Si tiene la siguiente configuración... | Se usa este comando... |
|---|--|
| <ul style="list-style-type: none"> • MetroCluster sin MetroCluster • MetroCluster de 2 nodos | <pre>system node image update -node * -package _location_ -replace -package true -setdefault true -background true</pre> <p><i>Location</i> puede ser un servidor Web o una carpeta local, según la versión de ONTAP. Consulte <code>system node image update manual</code> para más detalles.</p> <p>Este comando instala la imagen de software en todos los nodos simultáneamente. Para instalar la imagen en cada nodo de uno en uno, no especifique el <code>-background</code> parámetro.</p> |
| <ul style="list-style-type: none"> • MetroCluster de 4 nodos • Configuración de MetroCluster de 8 nodos | <pre>system node image update -node * -package location -replace -package true -background true -setdefault false</pre> <p>Debe emitir este comando en ambos clústeres.</p> <p>Este comando utiliza una consulta ampliada para cambiar la imagen de software de destino, que se instala como la imagen alternativa en cada nodo.</p> |

- Introduzca `y` para continuar cuando se le solicite.
- Compruebe que la imagen de software está instalada en cada nodo.

```
system node image show-update-progress -node *
```

Este comando muestra el estado actual de la instalación de la imagen de software. Debe continuar ejecutando este comando hasta que todos los nodos informen un **Estado de ejecución de salida**, y un **Estado de salida de éxito**.

El comando de actualización de imagen del nodo del sistema puede fallar y mostrar mensajes de error o advertencia. Después de resolver errores o advertencias, puede volver a ejecutar el comando.

Este ejemplo muestra un clúster de dos nodos en el que la imagen de software se instala correctamente en ambos nodos:

```
cluster1::*> system node image show-update-progress -node *
There is no update/install in progress
Status of most recent operation:
    Run Status:      Exited
    Exit Status:     Success
    Phase:           Run Script
    Exit Message:    After a clean shutdown, image2 will be set as
the default boot image on node0.
There is no update/install in progress
Status of most recent operation:
    Run Status:      Exited
    Exit Status:     Success
    Phase:           Run Script
    Exit Message:    After a clean shutdown, image2 will be set as
the default boot image on node1.
2 entries were acted on.
```

Actualización manual no disruptiva de ONTAP mediante la CLI (configuraciones estándar)

La actualización automatizada mediante System Manager es el método de actualización preferido. Si System Manager no admite la configuración, puede utilizar la interfaz de línea de comandos (CLI) de ONTAP para realizar una actualización manual no disruptiva. Para actualizar un clúster de dos o más nodos mediante el método manual no disruptivo, debe iniciar una operación de conmutación por error en cada nodo de un par de alta disponibilidad, actualizar el nodo «error», iniciar la devolución y, a continuación, repetir el proceso para cada pareja de alta disponibilidad del clúster.

Antes de empezar

Debe haber realizado una actualización satisfactoria "preparación" requisitos.

Actualizar el primer nodo de una pareja de alta disponibilidad

Puede actualizar el primer nodo de un par de alta disponibilidad iniciando la toma de control por parte del partner de nodo. El partner presta servicio a los datos del nodo mientras se actualiza el primer nodo.

Si realiza una actualización principal, el primer nodo que se va a actualizar debe ser el mismo nodo en el que haya configurado las LIF de datos para conectividad externa e instalado la primera imagen de ONTAP.

Después de actualizar el primer nodo, debe actualizar el nodo del compañero con la mayor rapidez posible. No permita que los dos nodos permanezcan en un "versión mixta" estado más largo de lo necesario.

Pasos

1. Actualice el primer nodo del clúster invocando un mensaje de AutoSupport:

```
autosupport invoke -node * -type all -message "Starting_NDU"
```

Esta notificación de AutoSupport incluye un registro del estado del sistema justo antes de la actualización. Guarda información útil sobre la solución de problemas en caso de que haya un problema con el proceso de actualización.

Si el clúster no está configurado para enviar mensajes de AutoSupport, se guardará una copia de la notificación de forma local.

2. Establezca el nivel de privilegio en avanzado, introduzca **y** cuando se le solicite continuar:

```
set -privilege advanced
```

El aviso avanzado (*>) aparece.

3. Establezca la nueva imagen del software ONTAP como la imagen predeterminada:

```
system image modify {-node nodenameA -iscurrent false} -isdefault true
```

El comando `system image modify` utiliza una consulta ampliada para cambiar la nueva imagen de software ONTAP (que se instala como imagen alternativa) a la imagen predeterminada del nodo.

4. Supervise el progreso de la actualización:

```
system node upgrade-revert show
```

5. Compruebe que la nueva imagen del software ONTAP está configurada como la imagen predeterminada:

```
system image show
```

En el siguiente ejemplo, `image2` es la nueva versión de ONTAP y se establece como la imagen predeterminada del nodo 0:

```
cluster1::*> system image show
```

| Node | Image | Is Default | Is Current | Version | Install Date |
|-------|--------|------------|------------|---------|-----------------|
| node0 | | | | | |
| | image1 | false | true | X.X.X | MM/DD/YYYY TIME |
| | image2 | true | false | Y.Y.Y | MM/DD/YYYY TIME |
| node1 | | | | | |
| | image1 | true | true | X.X.X | MM/DD/YYYY TIME |
| | image2 | false | false | Y.Y.Y | MM/DD/YYYY TIME |

4 entries were displayed.

6. Deshabilite la devolución automática del nodo del partner si está habilitada:

```
storage failover modify -node nodenameB -auto-giveback false
```

Si el clúster es un clúster de dos nodos, se muestra un mensaje que le advierte que al deshabilitar la devolución automática se impide que los servicios del clúster de gestión se conecten en el evento de un fallo alternativo. Introduzca `y` para continuar.

7. Compruebe que la devolución automática está deshabilitada para el partner de nodo:

```
storage failover show -node nodenameB -fields auto-giveback
```

```
cluster1::> storage failover show -node node1 -fields auto-giveback
node      auto-giveback
-----
node1     false
1 entry was displayed.
```

8. Ejecute el siguiente comando dos veces para determinar si el nodo que se va a actualizar está sirviendo a cualquier cliente

```
system node run -node nodenameA -command uptime
```

El comando `uptime` muestra el número total de operaciones que el nodo ha realizado para clientes NFS, SMB, FC e iSCSI desde que se inició por última vez el nodo. Para cada protocolo, debe ejecutar el comando dos veces para determinar si el número de operaciones está aumentando. Si aumentan, el nodo actualmente sirve clientes para ese protocolo. Si no aumentan, el nodo no ofrece actualmente clientes para ese protocolo.



Debe tomar una nota de cada protocolo que ha aumentado las operaciones de cliente de manera que, después de actualizar el nodo, pueda verificar que el tráfico del cliente se haya reanudado.

En el ejemplo siguiente se muestra un nodo con operaciones NFS, SMB, FC e iSCSI. Sin embargo, actualmente el nodo sólo ofrece clientes NFS e iSCSI.

```
cluster1::> system node run -node node0 -command uptime
2:58pm up 7 days, 19:16 800000260 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32810 iSCSI ops

cluster1::> system node run -node node0 -command uptime
2:58pm up 7 days, 19:17 800001573 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32815 iSCSI ops
```

9. Migre todos los LIF de datos del nodo:

```
network interface migrate-all -node nodenameA
```

10. Compruebe las LIF que ha migrado:

```
network interface show
```

Para obtener más información acerca de los parámetros que puede utilizar para comprobar el estado de LIF, consulte la página `show man` de la interfaz de red.

El ejemplo siguiente muestra que las LIF de datos de nodo 0 se migraron correctamente. Para cada LIF, los campos incluidos en este ejemplo le permiten comprobar el nodo y el puerto de inicio de la LIF, el nodo y el puerto actuales al que se ha migrado la LIF y el estado operativo y administrativo de la LIF.

```
cluster1::> network interface show -data-protocol nfs|cifs -role data
-home-node node0 -fields home-node,curr-node,curr-port,home-port,status-
admin,status-oper
vserver lif      home-node home-port curr-node curr-port status-oper
status-admin
-----
vs0      data001 node0      e0a      node1      e0a      up      up
vs0      data002 node0      e0b      node1      e0b      up      up
vs0      data003 node0      e0b      node1      e0b      up      up
vs0      data004 node0      e0a      node1      e0a      up      up
4 entries were displayed.
```

11. Inicie una toma de control:

```
storage failover takeover -ofnode nodenameA
```

No especifique el parámetro `-option Immediate` porque se requiere una toma de control normal para el nodo que se va a realizar la operación para arrancar en la nueva imagen de software. Si no ha migrado manualmente las LIF desde el nodo, migran automáticamente al partner de alta disponibilidad del nodo para garantizar que no hay interrupciones del servicio.

El primer nodo arranca hasta la espera del estado de devolución.



Si AutoSupport está habilitado, se envía un mensaje de AutoSupport que indica que el nodo está fuera del quórum del clúster. Puede ignorar esta notificación y continuar con la actualización.

12. Compruebe que la toma de control se ha realizado correctamente:

```
storage failover show
```

Es posible que aparezcan mensajes de error que indiquen problemas de versiones no coincidentes y de formato del buzón. Se trata del comportamiento esperado y representa un estado temporal en una actualización no disruptiva importante y no es perjudicial.

El siguiente ejemplo muestra que la toma de control se ha realizado correctamente. El nodo 0 tiene el estado esperando devolución y su partner está en el estado de toma de control.

```
cluster1::> storage failover show
```

| Node | Partner | Takeover Possible | State Description |
|-------|---------|----------------------|--|
| node0 | node1 | - | Waiting for giveback (HA mailboxes) |
| node1 | node0 | false | In takeover |

2 entries were displayed.

13. Espere al menos ocho minutos para que surtan efecto las siguientes condiciones:

- La multivía del cliente (si está implementada) se estabiliza.
- Los clientes se recuperan de la pausa en una operación de I/O que se produce durante la toma de control.

El tiempo de recuperación es específico del cliente y puede tardar más de ocho minutos, en función de las características de las aplicaciones cliente.

14. Devuelva los agregados al primer nodo:

```
storage failover giveback -ofnode nodenameA
```

La devolución devuelve primero el agregado raíz al nodo del partner y, después de que ese nodo haya terminado de arrancarse, devuelve los agregados que no son raíz y los LIF que se hayan establecido en revertir automáticamente. El nodo que se acaba de arrancar empieza a suministrar datos a los clientes desde cada agregado en cuanto se devuelva dicho agregado.

15. Compruebe que se han devuelto todos los agregados:

```
storage failover show-giveback
```

Si el campo Estado de devolución indica que no hay agregados que devolver, se devolverán todos los agregados. Si se vetó la devolución, el comando muestra el progreso de devolución y qué subsistema vetó la devolución.

16. Si no se ha devuelto ningún agregado, realice los siguientes pasos:

- a. Revise la solución de veto para determinar si desea abordar la condición "vertical" o anular el veto.
- b. Si es necesario, tratar la condición "veto" descrita en el mensaje de error, asegurándose de que las operaciones identificadas se cancelen con gracia.
- c. Vuelva a ejecutar el comando de recuperación tras fallos del almacenamiento.

Si ha decidido anular la condición "VETE", establezca el parámetro -override-vetoes en TRUE.

17. Espere al menos ocho minutos para que surtan efecto las siguientes condiciones:

- La multivía del cliente (si está implementada) se estabiliza.
- Los clientes se recuperan de la pausa en una operación de I/O que se produce durante la devolución.

El tiempo de recuperación es específico del cliente y puede tardar más de ocho minutos, en función de las características de las aplicaciones cliente.

18. Compruebe que la actualización se ha realizado correctamente para el nodo:

- a. Vaya al nivel de privilegio avanzado :

```
set -privilege advanced
```

- b. Compruebe que el estado de la actualización se haya completado para el nodo:

```
system node upgrade-revert show -node nodenameA
```

El estado debe aparecer como completo.

Si el estado no se completa, póngase en contacto con el soporte técnico.

- a. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

19. Compruebe que los puertos del nodo estén activos:

```
network port show -node nodenameA
```

Debe ejecutar este comando en un nodo que se haya actualizado a la versión superior de ONTAP 9.

En el ejemplo siguiente se muestra que todos los puertos del nodo están en funcionamiento:

```
cluster1::> network port show -node node0
```

| | | | | | | Speed |
|---------------------------|-------|---------|------------------|-------|-------|------------|
| (Mbps) | | | | | | |
| Node | Port | IPspace | Broadcast Domain | Link | MTU | Admin/Oper |
| ----- | ----- | ----- | ----- | ----- | ----- | |
| node0 | | | | | | |
| | e0M | Default | - | up | 1500 | auto/100 |
| | e0a | Default | - | up | 1500 | auto/1000 |
| | e0b | Default | - | up | 1500 | auto/1000 |
| | e1a | Cluster | Cluster | up | 9000 | auto/10000 |
| | e1b | Cluster | Cluster | up | 9000 | auto/10000 |
| 5 entries were displayed. | | | | | | |

20. Revierte los LIF al nodo:

```
network interface revert *
```

Este comando muestra las LIF que se han migrado del nodo.

```
cluster1::> network interface revert *  
8 entries were acted on.
```

21. Compruebe que los LIF de datos del nodo se hayan revertido correctamente al nodo y que estén en funcionamiento:

```
network interface show
```

En el ejemplo siguiente se muestra que todos los LIF de datos alojados en el nodo se han revertido correctamente al nodo y que su estado operativo está en funcionamiento:


```
cluster1::> network interface show
```

| Current Is | Logical | Status | Network | Current | |
|------------|-----------|------------|----------------|---------|------|
| Vserver | Interface | Admin/Oper | Address/Mask | Node | Port |
| Home | | | | | |
| vs0 | | | | | |
| | data001 | up/up | 192.0.2.120/24 | node0 | e0a |
| true | | | | | |
| | data002 | up/up | 192.0.2.121/24 | node0 | e0b |
| true | | | | | |
| | data003 | up/up | 192.0.2.122/24 | node0 | e0b |
| true | | | | | |
| | data004 | up/up | 192.0.2.123/24 | node0 | e0a |
| true | | | | | |

4 entries were displayed.

22. Si anteriormente ha determinado que este nodo sirve a clientes, compruebe que el nodo está proporcionando servicio para cada protocolo que estaba sirviendo anteriormente:

```
system node run -node nodenameA -command uptime
```

La operación se restablece a cero durante la actualización.

En el ejemplo siguiente se muestra que el nodo actualizado ha reanudado el servicio a sus clientes NFS e iSCSI:

```
cluster1::> system node run -node node0 -command uptime
3:15pm up 0 days, 0:16 129 NFS ops, 0 CIFS ops, 0 HTTP ops, 0 FCP
ops, 2 iSCSI ops
```

23. Vuelva a habilitar la devolución automática en el nodo del partner si estaba previamente deshabilitada:

```
storage failover modify -node nodenameB -auto-giveback true
```

Debe continuar para actualizar el partner de alta disponibilidad del nodo lo más rápido posible. Si debe suspender el proceso de actualización por cualquier motivo, ambos nodos de la pareja de alta disponibilidad deben ejecutar la misma versión de ONTAP.

Actualizar el nodo del partner en una pareja de alta disponibilidad

Después de actualizar el primer nodo de un par de alta disponibilidad, actualiza su compañero iniciando la toma de control sobre él. El primer nodo sirve los datos del partner mientras se actualiza el nodo del partner.

1. Establezca el nivel de privilegio en avanzado, introduzca **y** cuando se le solicite continuar:

```
set -privilege advanced
```

El aviso avanzado (*>) aparece.

2. Establezca la nueva imagen del software ONTAP como la imagen predeterminada:

```
system image modify {-node nodenameB -iscurrent false} -isdefault true
```

El comando `system image modify` utiliza una consulta ampliada para cambiar la nueva imagen de software ONTAP (que se instala como imagen alternativa) que es la imagen predeterminada del nodo.

3. Supervise el progreso de la actualización:

```
system node upgrade-revert show
```

4. Compruebe que la nueva imagen del software ONTAP está configurada como la imagen predeterminada:

```
system image show
```

En el siguiente ejemplo: `image2` Es la nueva versión de ONTAP y se establece como imagen predeterminada en el nodo:

```
cluster1::*> system image show
```

| Node | Image | Is Default | Is Current | Version | Install Date |
|-------|--------|---------------|---------------|---------|-----------------|
| node0 | | | | | |
| | image1 | false | false | X.X.X | MM/DD/YYYY TIME |
| | image2 | true | true | Y.Y.Y | MM/DD/YYYY TIME |
| node1 | | | | | |
| | image1 | false | true | X.X.X | MM/DD/YYYY TIME |
| | image2 | true | false | Y.Y.Y | MM/DD/YYYY TIME |

4 entries were displayed.

5. Deshabilite la devolución automática del nodo del partner si está habilitada:

```
storage failover modify -node nodenameA -auto-giveback false
```

Si el clúster es un clúster de dos nodos, se muestra un mensaje que le advierte que al deshabilitar la devolución automática se impide que los servicios del clúster de gestión se conecten en el evento de un

fallo alternativo. Introduzca y para continuar.

6. Compruebe que la devolución automática está deshabilitada para el nodo asociado:

```
storage failover show -node nodenameA -fields auto-giveback
```

```
cluster1::> storage failover show -node node0 -fields auto-giveback
node      auto-giveback
-----
node0     false
1 entry was displayed.
```

7. Ejecute el siguiente comando dos veces para determinar si el nodo que se va a actualizar está sirviendo a cualquier cliente:

```
system node run -node nodenameB -command uptime
```

El comando uptime muestra el número total de operaciones que el nodo ha realizado para clientes NFS, SMB, FC e iSCSI desde que se inició por última vez el nodo. Para cada protocolo, debe ejecutar el comando dos veces para determinar si el número de operaciones está aumentando. Si aumentan, el nodo actualmente sirve clientes para ese protocolo. Si no aumentan, el nodo no ofrece actualmente clientes para ese protocolo.

NOTA: Debe tomar nota de cada protocolo que tiene cada vez más operaciones de cliente para que después de actualizar el nodo, pueda verificar que el tráfico de cliente se ha reanudado.

En el ejemplo siguiente se muestra un nodo con operaciones NFS, SMB, FC e iSCSI. Sin embargo, actualmente el nodo sólo ofrece clientes NFS e iSCSI.

```
cluster1::> system node run -node node1 -command uptime
 2:58pm up 7 days, 19:16 800000260 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32810 iSCSI ops

cluster1::> system node run -node node1 -command uptime
 2:58pm up 7 days, 19:17 800001573 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32815 iSCSI ops
```

8. Migre todos los LIF de datos del nodo:

```
network interface migrate-all -node nodenameB
```

9. Compruebe el estado de cualquier LIF que haya migrado:

```
network interface show
```

Para obtener más información acerca de los parámetros que puede utilizar para comprobar el estado de LIF, consulte la página `show man` de la interfaz de red.

El ejemplo siguiente muestra que las LIF de datos del nodo 1 se migraron correctamente. Para cada LIF, los campos incluidos en este ejemplo le permiten comprobar el nodo y el puerto de inicio de la LIF, el nodo y el puerto actuales al que se ha migrado la LIF y el estado operativo y administrativo de la LIF.

```
cluster1::> network interface show -data-protocol nfs|cifs -role data
-home-node node1 -fields home-node,curr-node,curr-port,home-port,status-
admin,status-oper
vserver lif      home-node home-port curr-node curr-port status-oper
status-admin
-----
vs0      data001 node1      e0a      node0      e0a      up      up
vs0      data002 node1      e0b      node0      e0b      up      up
vs0      data003 node1      e0b      node0      e0b      up      up
vs0      data004 node1      e0a      node0      e0a      up      up
4 entries were displayed.
```

10. Inicie una toma de control:

```
storage failover takeover -ofnode nodenameB -option allow-version-
mismatch
```

No especifique el parámetro `-option Immediate` porque se requiere una toma de control normal para el nodo que se va a realizar la operación para arrancar en la nueva imagen de software. Si no ha migrado manualmente las LIF desde el nodo, migran automáticamente al partner de alta disponibilidad del nodo para que no haya interrupciones del servicio.

Aparece una advertencia. Debe entrar `y` para continuar.

El nodo que se ha tomado arranca hasta esperando el estado de devolución.



Si AutoSupport está habilitado, se envía un mensaje de AutoSupport que indica que el nodo está fuera del quórum del clúster. Puede ignorar esta notificación y continuar con la actualización.

11. Compruebe que la toma de control se ha realizado correctamente:

```
storage failover show
```

El siguiente ejemplo muestra que la toma de control se ha realizado correctamente. El nodo 1 está en

estado esperando devolución del nodo y su compañero está en estado de toma de control.

```
cluster1::> storage failover show
```

| Node | Partner | Takeover Possible | State Description |
|-------|---------|----------------------|--|
| node0 | node1 | - | In takeover |
| node1 | node0 | false | Waiting for giveback (HA mailboxes) |

2 entries were displayed.

12. Espere al menos ocho minutos para que surtan efecto las siguientes condiciones:

+

La multivía del cliente (si está implementada) se estabiliza.

Los clientes se recuperan de la pausa en la I/O que se produce durante la toma de control.

+

El tiempo de recuperación es específico del cliente y puede tardar más de ocho minutos, según las características de las aplicaciones cliente.

13. Devolver los agregados al nodo partner:

```
storage failover giveback -ofnode nodenameB
```

La operación de devolución devuelve en primer lugar el agregado raíz al nodo del partner y, después de que ese nodo haya finalizado el arranque, devuelve los agregados que no son raíz y los LIF que se hayan configurado para que se revierten automáticamente. El nodo que se acaba de arrancar empieza a suministrar datos a los clientes desde cada agregado en cuanto se devuelva dicho agregado.

14. Compruebe que se devuelven todos los agregados:

```
storage failover show-giveback
```

Si el campo Giveback Status indica que no hay agregados que devolver, se devuelven todos los agregados. Si se vetó la devolución, el comando muestra el progreso de devolución y qué subsistema vetó la operación de devolución.

15. Si no se devuelve ningún agregado, realice los siguientes pasos:

- Revise la solución de veto para determinar si desea abordar la condición "vertical" o anular el veto.
- Si es necesario, tratar la condición "veto" descrita en el mensaje de error, asegurándose de que las operaciones identificadas se cancelen con gracia.
- Vuelva a ejecutar el comando de recuperación tras fallos del almacenamiento.

Si ha decidido anular la condición "VETE", establezca el parámetro -override-vetoes en TRUE.

16. Espere al menos ocho minutos para que surtan efecto las siguientes condiciones:

- La multivía del cliente (si está implementada) se estabiliza.
- Los clientes se recuperan de la pausa en una operación de I/O que se produce durante la devolución.

El tiempo de recuperación es específico del cliente y puede tardar más de ocho minutos, en función de las características de las aplicaciones cliente.

17. Compruebe que la actualización se ha realizado correctamente para el nodo:

a. Vaya al nivel de privilegio avanzado :

```
set -privilege advanced
```

b. Compruebe que el estado de la actualización se haya completado para el nodo:

```
system node upgrade-revert show -node nodenameB
```

El estado debe aparecer como completo.

Si el estado no es completo, desde el nodo, ejecute el comando `system node upgrade-revert upgrade`. Si el comando no completa la actualización, póngase en contacto con el soporte técnico.

a. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

18. Compruebe que los puertos del nodo estén activos:

```
network port show -node nodenameB
```

Este comando debe ejecutarse en un nodo que se ha actualizado a ONTAP 9.4.

En el ejemplo siguiente se muestra que todos los puertos de datos del nodo están en funcionamiento:

```
cluster1::> network port show -node node1
```

| | | | | | | Speed |
|---------------------------|-------|---------|------------------|-------|-------|------------|
| (Mbps) | | | | | | |
| Node | Port | IPspace | Broadcast Domain | Link | MTU | Admin/Oper |
| ----- | ----- | ----- | ----- | ----- | ----- | ----- |
| node1 | | | | | | |
| | e0M | Default | - | up | 1500 | auto/100 |
| | e0a | Default | - | up | 1500 | auto/1000 |
| | e0b | Default | - | up | 1500 | auto/1000 |
| | e1a | Cluster | Cluster | up | 9000 | auto/10000 |
| | e1b | Cluster | Cluster | up | 9000 | auto/10000 |
| 5 entries were displayed. | | | | | | |

19. Revierte los LIF al nodo:

```
network interface revert *
```

Este comando muestra las LIF que se han migrado del nodo.

```
cluster1::> network interface revert *  
8 entries were acted on.
```

20. Compruebe que los LIF de datos del nodo se hayan revertido correctamente al nodo y que estén en funcionamiento:

```
network interface show
```

En el ejemplo siguiente se muestra que todos los LIF de datos alojados en el nodo se vuelven a restaurar correctamente al nodo y que su estado operativo es up:

```
cluster1::> network interface show
```

| | Logical | Status | Network | Current | |
|------------|-----------|------------|----------------|---------|-------|
| Current Is | | | | | |
| Vserver | Interface | Admin/Oper | Address/Mask | Node | Port |
| Home | | | | | |
| ----- | ----- | ----- | ----- | ----- | ----- |
| vs0 | | | | | |
| | data001 | up/up | 192.0.2.120/24 | node1 | e0a |
| true | | | | | |
| | data002 | up/up | 192.0.2.121/24 | node1 | e0b |
| true | | | | | |
| | data003 | up/up | 192.0.2.122/24 | node1 | e0b |
| true | | | | | |
| | data004 | up/up | 192.0.2.123/24 | node1 | e0a |
| true | | | | | |

4 entries were displayed.

21. Si anteriormente ha determinado que este nodo sirve a clientes, compruebe que el nodo está proporcionando servicio para cada protocolo que estaba sirviendo anteriormente:

```
system node run -node nodenameB -command uptime
```

La operación se restablece a cero durante la actualización.

En el ejemplo siguiente se muestra que el nodo actualizado ha reanudado el servicio a sus clientes NFS e iSCSI:

```
cluster1::> system node run -node node1 -command uptime
3:15pm up 0 days, 0:16 129 NFS ops, 0 CIFS ops, 0 HTTP ops, 0 FCP
ops, 2 iSCSI ops
```

22. Si este fue el último nodo del clúster que se actualizó, active una notificación de AutoSupport:

```
autosupport invoke -node * -type all -message "Finishing_NDU"
```

Esta notificación de AutoSupport incluye un registro del estado del sistema justo antes de la actualización. Guarda información útil sobre la solución de problemas en caso de que haya un problema con el proceso de actualización.

Si el clúster no está configurado para enviar mensajes de AutoSupport, se guardará una copia de la notificación de forma local.

23. Confirme que el nuevo software ONTAP se está ejecutando en ambos nodos de la pareja de alta

disponibilidad:

```
set -privilege advanced
```

```
system node image show
```

En el siguiente ejemplo, image2 es la versión actualizada de ONTAP y es la versión predeterminada en ambos nodos:

```
cluster1::*> system node image show
```

| Node | Image | Is Default | Is Current | Version | Install Date |
|-------|--------|------------|------------|---------|-----------------|
| node0 | image1 | false | false | X.X.X | MM/DD/YYYY TIME |
| | image2 | true | true | Y.Y.Y | MM/DD/YYYY TIME |
| node1 | image1 | false | false | X.X.X | MM/DD/YYYY TIME |
| | image2 | true | true | Y.Y.Y | MM/DD/YYYY TIME |

4 entries were displayed.

24. Vuelva a habilitar la devolución automática en el nodo del partner si estaba previamente deshabilitada:

```
storage failover modify -node nodenameA -auto-giveback true
```

25. Compruebe que el cluster está en quórum y que los servicios se están ejecutando mediante `cluster show y.. cluster ring show` comandos (nivel de privilegio avanzado).

Debe realizar este paso antes de actualizar cualquier par de alta disponibilidad adicional.

26. Vuelva al nivel de privilegio de administrador:

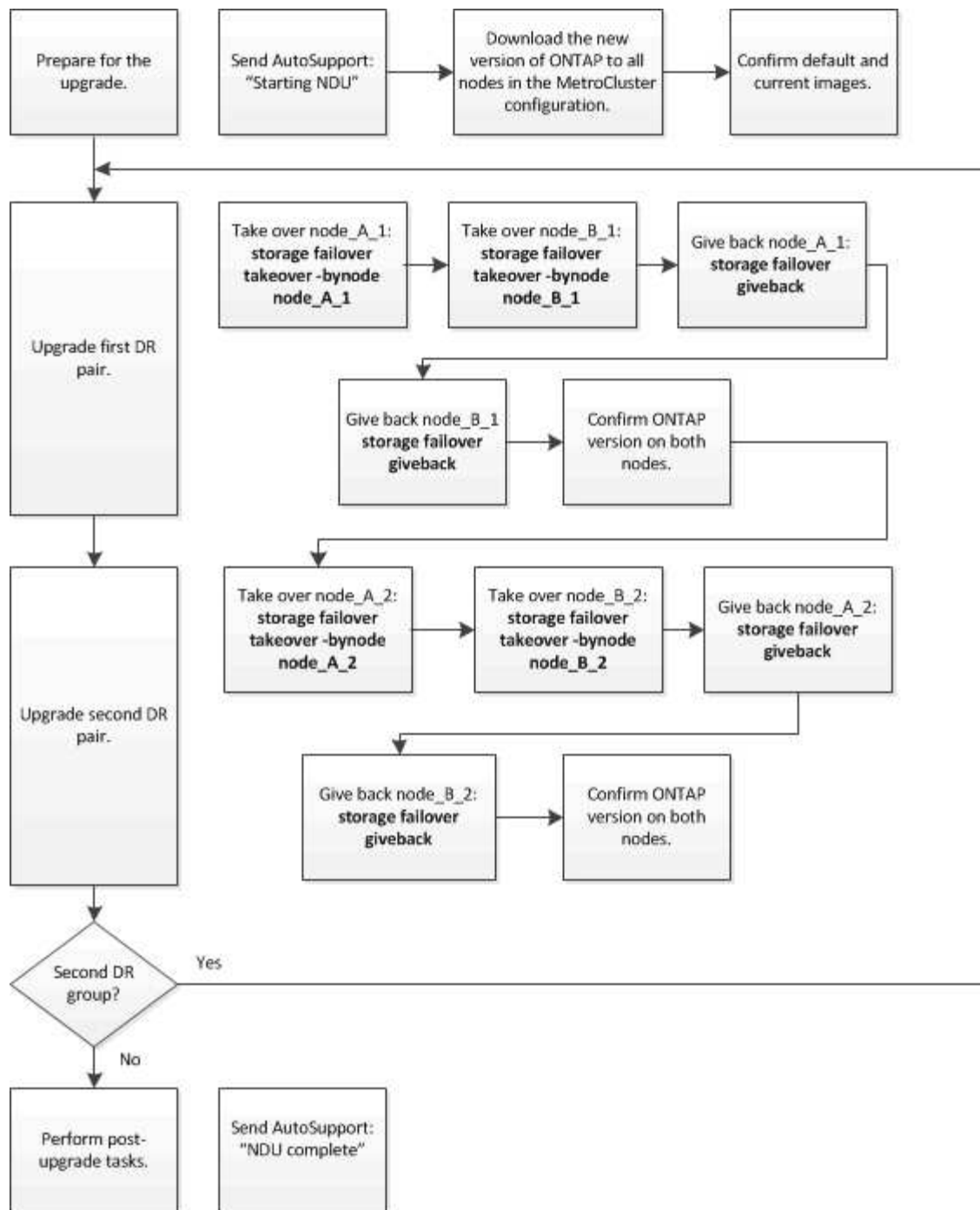
```
set -privilege admin
```

27. Actualice cualquier par de alta disponibilidad adicional.

Actualización manual de ONTAP no disruptiva de una configuración de MetroCluster de cuatro u ocho nodos mediante la CLI

Una actualización manual de una configuración de MetroCluster de cuatro u ocho nodos implica la preparación de la actualización, la actualización de los pares de recuperación ante desastres en cada uno o dos grupos de recuperación ante desastres simultáneamente y la realización de las tareas posteriores a la actualización.

- Esta tarea se aplica a las siguientes configuraciones:
 - Configuraciones IP o FC de MetroCluster de cuatro nodos que ejecuten ONTAP 9.2 o una versión anterior
 - Configuraciones de MetroCluster FC de ocho nodos, independientemente de la versión de ONTAP
- Si tiene una configuración MetroCluster de dos nodos, no utilice este procedimiento.
- Las siguientes tareas hacen referencia a las versiones anterior y nueva de ONTAP.
 - Al actualizar, la versión antigua es una versión anterior de ONTAP, con un número de versión inferior al de la nueva versión de ONTAP.
 - Al realizar la degradación, la versión anterior es una versión posterior de ONTAP, con un número de versión superior al de la nueva versión de ONTAP.
- En esta tarea se utiliza el siguiente flujo de trabajo de alto nivel:



Diferencias cuando se actualiza el software ONTAP en una configuración de MetroCluster de ocho o cuatro nodos

El proceso de actualización de software MetroCluster varía en función de si haya ocho o cuatro nodos en la configuración de MetroCluster.

Una configuración MetroCluster está compuesta por uno o dos grupos de recuperación ante desastres. Cada grupo de recuperación ante desastres consta de dos parejas de alta disponibilidad, un par de alta disponibilidad en cada clúster MetroCluster. Un MetroCluster de ocho nodos incluye dos grupos de recuperación ante desastres:



Actualiza un grupo de recuperación ante desastres cada vez.

Para configuraciones MetroCluster de cuatro nodos:

1. Actualizar grupo de DR uno:
 - a. Actualice NODE_A_1 y NODE_B_1.
 - b. Actualice NODE_A_2 y NODE_B_2.

Para configuraciones MetroCluster de ocho nodos, el procedimiento de actualización del grupo de recuperación ante desastres se realiza dos veces:

1. Actualizar grupo de DR uno:
 - a. Actualice NODE_A_1 y NODE_B_1.
 - b. Actualice NODE_A_2 y NODE_B_2.
2. Actualizar grupo DR dos:
 - a. Actualice NODE_A_3 y NODE_B_3.
 - b. Actualice NODE_A_4 y NODE_B_4.

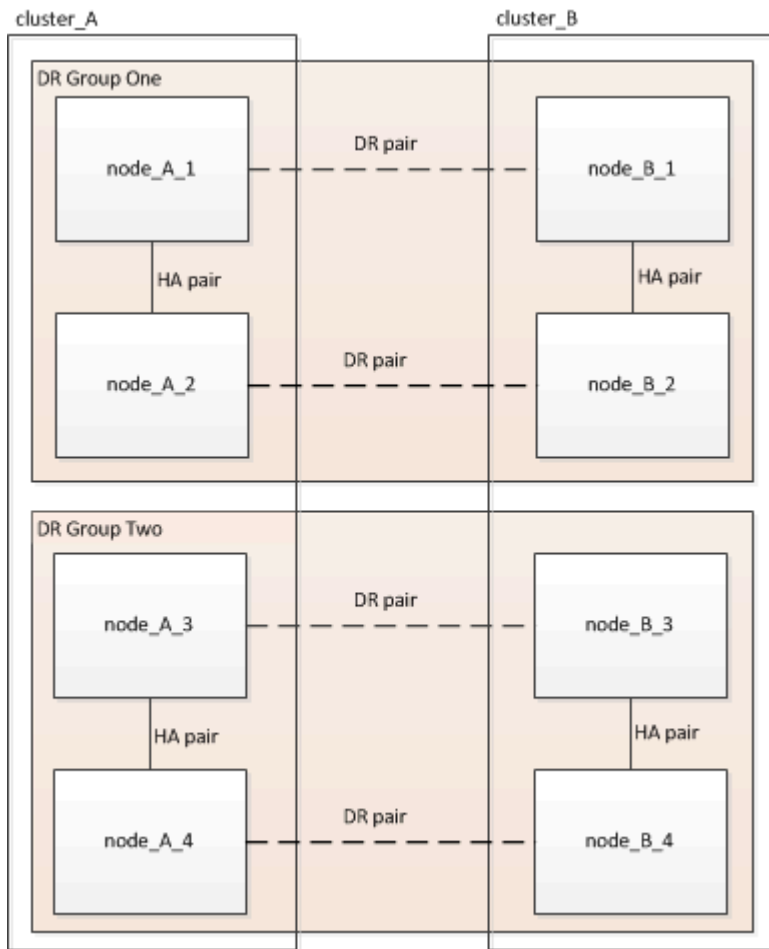
Preparar la actualización de un grupo de recuperación ante desastres de MetroCluster

Antes de actualizar el software ONTAP en los nodos, debe identificar las relaciones de recuperación ante desastres entre los nodos, enviar un mensaje de AutoSupport para iniciar una actualización y confirmar la versión de ONTAP que se está ejecutando en cada nodo.

Debe tener "descargado" y.. "instalado" las imágenes de software.

Esta tarea debe repetirse en cada grupo de recuperación ante desastres. Si la configuración del MetroCluster consta de ocho nodos, hay dos grupos de recuperación ante desastres. Por lo tanto, esta tarea debe repetirse en cada grupo de recuperación ante desastres.

Los ejemplos que se proporcionan en esta tarea utilizan los nombres que se muestran en la siguiente ilustración para identificar los clústeres y los nodos:



1. Identifique las parejas de recuperación ante desastres en la configuración:

```
metrocluster node show -fields dr-partner
```

```
cluster_A::> metrocluster node show -fields dr-partner
(metrocluster node show)
dr-group-id cluster      node      dr-partner
-----
1          cluster_A    node_A_1  node_B_1
1          cluster_A    node_A_2  node_B_2
1          cluster_B    node_B_1  node_A_1
1          cluster_B    node_B_2  node_A_2
4 entries were displayed.

cluster_A::>
```

2. Establezca el nivel de privilegio de admin en Advanced, introduciendo **y** cuando se le solicite continuar:

```
set -privilege advanced
```

El aviso avanzado (*>) aparece.

3. Confirme la versión de ONTAP en cluster_A:

```
system image show
```

```
cluster_A::*> system image show
Node      Image      Is      Is      Version  Install
          Image    Default Current Version  Date
-----
node_A_1
          image1   true    true    X.X.X    MM/DD/YYYY TIME
          image2   false   false   Y.Y.Y    MM/DD/YYYY TIME
node_A_2
          image1   true    true    X.X.X    MM/DD/YYYY TIME
          image2   false   false   Y.Y.Y    MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>
```

4. Confirme la versión en cluster_B:

```
system image show
```

```
cluster_B::*> system image show
```

| Node | Image | Is Default | Is Current | Version | Install Date |
|----------|--------|---------------|---------------|---------|-----------------|
| ----- | | | | | |
| node_B_1 | | | | | |
| | image1 | true | true | X.X.X | MM/DD/YYYY TIME |
| | image2 | false | false | Y.Y.Y | MM/DD/YYYY TIME |
| node_B_2 | | | | | |
| | image1 | true | true | X.X.X | MM/DD/YYYY TIME |
| | image2 | false | false | Y.Y.Y | MM/DD/YYYY TIME |

4 entries were displayed.

```
cluster_B::>
```

5. Active una notificación de AutoSupport:

```
autosupport invoke -node * -type all -message "Starting_NDU"
```

Esta notificación de AutoSupport incluye un registro del estado del sistema antes de la actualización. Guarda información útil sobre la solución de problemas si hay un problema con el proceso de actualización.

Si su clúster no está configurado para enviar mensajes de AutoSupport, se guardará una copia de la notificación de forma local.

6. Para cada nodo del primer conjunto, establezca la imagen del software ONTAP de destino como la imagen predeterminada:

```
system image modify {-node nodename -iscurrent false} -isdefault true
```

Este comando utiliza una consulta ampliada para cambiar la imagen de software de destino, que se instala como imagen alternativa, para que sea la imagen predeterminada del nodo.

7. Compruebe que la imagen del software ONTAP de destino esté establecida como la imagen predeterminada en cluster_A:

```
system image show
```

En el siguiente ejemplo, image2 es la nueva versión de ONTAP y se define como la imagen predeterminada en cada uno de los nodos del primer conjunto:

```
cluster_A::*> system image show
```

| Node | Image | Is Default | Is Current | Version | Install Date |
|----------|--------|---------------|---------------|---------|-----------------|
| ----- | | | | | |
| node_A_1 | image1 | false | true | X.X.X | MM/DD/YYYY TIME |
| | image2 | true | false | Y.Y.Y | MM/DD/YYYY TIME |
| node_A_2 | image1 | false | true | X.X.X | MM/DD/YYYY TIME |
| | image2 | true | false | Y.Y.Y | MM/DD/YYYY TIME |

2 entries were displayed.

- a. Compruebe que la imagen del software ONTAP de destino esté establecida como la imagen predeterminada en CLÚSTER_B:

```
system image show
```

En el siguiente ejemplo se muestra que la versión de destino está establecida como imagen predeterminada en cada uno de los nodos del primer conjunto:

```
cluster_B::*> system image show
```

| Node | Image | Is Default | Is Current | Version | Install Date |
|----------|--------|---------------|---------------|---------|-----------------|
| ----- | | | | | |
| node_A_1 | image1 | false | true | X.X.X | MM/DD/YYYY TIME |
| | image2 | true | false | Y.Y.Y | MM/YY/YYYY TIME |
| node_A_2 | image1 | false | true | X.X.X | MM/DD/YYYY TIME |
| | image2 | true | false | Y.Y.Y | MM/DD/YYYY TIME |

2 entries were displayed.

8. Determine si los nodos que se van a actualizar actualmente sirven a clientes dos veces para cada nodo:

```
system node run -node target-node -command uptime
```

El comando UpTime muestra el número total de operaciones que el nodo ha realizado para clientes NFS, CIFS, FC e iSCSI desde que se inició por última vez el nodo. Para cada protocolo, debe ejecutar el comando dos veces para determinar si el número de operaciones está aumentando. Si aumentan, el nodo actualmente sirve clientes para ese protocolo. Si no aumentan, el nodo no ofrece actualmente clientes para ese protocolo.



Debe tomar una nota de cada protocolo que ha aumentado las operaciones de cliente de manera que, una vez actualizado el nodo, pueda verificar que el tráfico del cliente se haya reanudado.

Este ejemplo muestra un nodo con operaciones NFS, CIFS, FC e iSCSI. Sin embargo, actualmente el nodo sólo ofrece clientes NFS e iSCSI.

```
cluster_x::> system node run -node node0 -command uptime
2:58pm up 7 days, 19:16 800000260 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32810 iSCSI ops

cluster_x::> system node run -node node0 -command uptime
2:58pm up 7 days, 19:17 800001573 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32815 iSCSI ops
```

Actualizar la primera pareja de recuperación ante desastres en un grupo de recuperación ante desastres de MetroCluster

Debe realizar una toma de control y una devolución de los nodos en el orden correcto para que la nueva versión de ONTAP sea la versión actual del nodo.

Todos los nodos deben ejecutar la versión anterior de ONTAP.

En esta tarea, se actualizan NODE_A_1 y NODE_B_1.

Si ha actualizado el software ONTAP en el primer grupo de recuperación ante desastres y ahora está actualizando el segundo grupo de recuperación ante desastres en una configuración MetroCluster de ocho nodos, en esta tarea debería actualizar NODE_A_3 y NODE_B_3.

1. Si el software MetroCluster Tiebreaker está habilitado, esta opción está deshabilitada.
2. Para cada nodo del par de alta disponibilidad, deshabilite el retorno automático:

```
storage failover modify -node target-node -auto-giveback false
```

Este comando se debe repetir para cada nodo de la pareja de ha.

3. Compruebe que la devolución automática está desactivada:

```
storage failover show -fields auto-giveback
```

Este ejemplo muestra que se ha deshabilitado la devolución automática de control en ambos nodos:

```
cluster_x::> storage failover show -fields auto-giveback
node      auto-giveback
-----
node_x_1  false
node_x_2  false
2 entries were displayed.
```

4. Asegúrese de que las I/O no superen el ~50 % en cada controladora y que el uso de CPU no supere el ~50 % por controladora.
5. Inicie la toma de control del nodo de destino en cluster_A:

No especifique el parámetro `-option Immediate` porque se requiere una toma de control normal para los nodos que se van a realizar la operación para arrancar en la nueva imagen de software.

- a. Asumir el control del partner de recuperación ante desastres en cluster_A (nodo_A_1):

```
storage failover takeover -ofnode node_A_1
```

El nodo arranca con el estado "esperando la devolución".



Si AutoSupport está habilitado, se envía un mensaje de AutoSupport que indica que los nodos no tienen quórum de clúster. Puede ignorar esta notificación y continuar con la actualización.

- b. Compruebe que la toma de control se ha realizado correctamente:

```
storage failover show
```

El siguiente ejemplo muestra que la toma de control se ha realizado correctamente. El nodo_A_1 está en el estado "esperando devolución" y el nodo_A_2 está en el estado "durante toma de control".

```
cluster1::> storage failover show
```

| Node | Partner | Takeover Possible | State Description |
|----------|----------|----------------------|-------------------------------------|
| node_A_1 | node_A_2 | - | Waiting for giveback (HA mailboxes) |
| node_A_2 | node_A_1 | false | In takeover |

2 entries were displayed.

6. Asumir el control del partner de recuperación ante desastres en cluster_B (nodo_B_1):

No especifique el parámetro `-option Immediate` porque se requiere una toma de control normal para los

nodos que se van a realizar la operación para arrancar en la nueva imagen de software.

- a. Asuma el control node_B_1:

```
storage failover takeover -ofnode node_B_1
```

El nodo arranca con el estado "esperando la devolución".



Si AutoSupport está habilitado, se envía un mensaje de AutoSupport que indica que los nodos no tienen quórum de clúster. Puede ignorar esta notificación y continuar con la actualización.

- b. Compruebe que la toma de control se ha realizado correctamente:

```
storage failover show
```

El siguiente ejemplo muestra que la toma de control se ha realizado correctamente. El nodo B_1 está en el estado "esperando devolución" y el nodo B_2 está en el estado "durante toma de control".

```
cluster1::> storage failover show
```

| Node | Partner | Takeover Possible | State Description |
|----------|----------|----------------------|-------------------------------------|
| node_B_1 | node_B_2 | - | Waiting for giveback (HA mailboxes) |
| node_B_2 | node_B_1 | false | In takeover |

2 entries were displayed.

7. Espere al menos ocho minutos para asegurarse de las siguientes condiciones:

- La multivía del cliente (si está implementada) se estabiliza.
- Los clientes se recuperan de la pausa en la I/O que se produce durante la toma de control.

El tiempo de recuperación es específico del cliente y puede tardar más de ocho minutos en función de las características de las aplicaciones cliente.

8. Devuelva los agregados a los nodos de destino:

Después de actualizar la configuración IP de MetroCluster a ONTAP 9.5 o una versión posterior, los agregados estarán en estado degradado durante un breve periodo de tiempo antes de volver a sincronizar y volver a un estado de reflejo.

- a. Proporcione los agregados al partner de recuperación ante desastres en cluster_A:

```
storage failover giveback -ofnode node_A_1
```

b. Proporcione los agregados al partner de recuperación ante desastres en cluster_B:

```
storage failover giveback -ofnode node_B_1
```

La operación de devolución devuelve primero el agregado raíz al nodo y, después de que el nodo haya terminado de arrancarse, devuelve los agregados que no son raíz.

9. Compruebe que todos los agregados se han devuelto emitiendo el siguiente comando en ambos clústeres:

```
storage failover show-giveback
```

Si el campo Estado de devolución indica que no hay agregados que devolver, se devolverán todos los agregados. Si se vetó la devolución, el comando muestra el progreso de devolución y qué subsistema vetó la devolución.

10. Si no se ha devuelto ningún agregado, realice lo siguiente:

- a. Revise la solución de veto para determinar si desea abordar la condición "vertical" o anular el veto.
- b. Si es necesario, tratar la condición "veto" descrita en el mensaje de error, asegurándose de que las operaciones identificadas se cancelen con gracia.
- c. Vuelva a introducir el comando de devolución del nodo de respaldo del almacenamiento.

Si ha decidido anular la condición "VETE", establezca el parámetro `-override-vetoes` en `TRUE`.

11. Espere al menos ocho minutos para asegurarse de las siguientes condiciones:

- La multivía del cliente (si está implementada) se estabiliza.
- Los clientes se recuperan de la pausa en la I/O que se produce durante la devolución.

El tiempo de recuperación es específico del cliente y puede tardar más de ocho minutos en función de las características de las aplicaciones cliente.

12. Establezca el nivel de privilegio de admin en Advanced, introduciendo **y** cuando se le solicite continuar:

```
set -privilege advanced
```

El aviso avanzado (*>) aparece.

13. Confirme la versión en cluster_A:

```
system image show
```

En el siguiente ejemplo se muestra que la impresora image2 del sistema debe ser la versión predeterminada y actual en node_A_1:

```
cluster_A::*> system image show
```

| Node | Image | Is Default | Is Current | Version | Install Date |
|----------|--------|------------|------------|---------|-----------------|
| ----- | | | | | |
| node_A_1 | | | | | |
| | image1 | false | false | X.X.X | MM/DD/YYYY TIME |
| | image2 | true | true | Y.Y.Y | MM/DD/YYYY TIME |
| node_A_2 | | | | | |
| | image1 | false | true | X.X.X | MM/DD/YYYY TIME |
| | image2 | true | false | Y.Y.Y | MM/DD/YYYY TIME |

4 entries were displayed.

```
cluster_A::>
```

14. Confirme la versión en cluster_B:

```
system image show
```

En el siguiente ejemplo se muestra que la imagen 2 del sistema (ONTAP 9.0.0) es la versión predeterminada y actual en node_A_1:

```
cluster_A::*> system image show
```

| Node | Image | Is Default | Is Current | Version | Install Date |
|----------|--------|------------|------------|---------|-----------------|
| ----- | | | | | |
| node_B_1 | | | | | |
| | image1 | false | false | X.X.X | MM/DD/YYYY TIME |
| | image2 | true | true | Y.Y.Y | MM/DD/YYYY TIME |
| node_B_2 | | | | | |
| | image1 | false | true | X.X.X | MM/DD/YYYY TIME |
| | image2 | true | false | Y.Y.Y | MM/DD/YYYY TIME |

4 entries were displayed.

```
cluster_A::>
```

Actualizar la segunda pareja de recuperación ante desastres en un grupo de recuperación ante desastres de MetroCluster

Debe realizar una toma de control y una devolución del nodo en el orden correcto para que la nueva versión de ONTAP sea la versión actual del nodo.

Debe haber actualizado el primer par DR (node_A_1 y node_B_1).

En esta tarea, se actualizan NODE_A_2 y NODE_B_2.

Si ha actualizado el software ONTAP en el primer grupo de recuperación ante desastres y ahora está actualizando el segundo grupo de recuperación ante desastres en una configuración MetroCluster de ocho nodos, en esta tarea está actualizando NODE_A_4 y NODE_B_4.

1. Migre todos los LIF de datos del nodo:

```
network interface migrate-all -node nodenameA
```

2. Inicie la toma de control del nodo de destino en cluster_A:

No especifique el parámetro -option Immediate porque se requiere una toma de control normal para los nodos que se van a realizar la operación para arrancar en la nueva imagen de software.

- a. Asuma el control del partner de recuperación ante desastres en cluster_A:

```
storage failover takeover -ofnode node_A_2 -option allow-version-mismatch
```



La allow-version-mismatch Esta opción no es necesaria para las actualizaciones de ONTAP 9.0 a ONTAP 9.1 o para cualquier actualización de parches.

El nodo arranca con el estado "esperando la devolución".

Si AutoSupport está habilitado, se envía un mensaje de AutoSupport que indica que los nodos no tienen quórum de clúster. Puede ignorar esta notificación y continuar con la actualización.

- b. Compruebe que la toma de control se ha realizado correctamente:

```
storage failover show
```

El siguiente ejemplo muestra que la toma de control se ha realizado correctamente. El nodo_A_2 está en el estado "esperando devolución" y el nodo_A_1 está en el estado "durante toma de control".


```
cluster1::> storage failover show
Node           Partner           Takeover
-----
node_A_1       node_A_2       false    In takeover
node_A_2       node_A_1       -        Waiting for giveback (HA
mailboxes)
2 entries were displayed.
```

3. Inicie la toma de control del nodo de destino en cluster_B:


No especifique el parámetro -option Immediate porque se requiere una toma de control normal para los

nodos que se van a realizar la operación para arrancar en la nueva imagen de software.

a. Asumir el control del partner de recuperación ante desastres en cluster_B (nodo_B_2):

| Si va a actualizar desde... | Introduzca este comando... |
|------------------------------|--|
| ONTAP 9.2 o ONTAP 9.1 | <div> storage failover takeover -ofnode node_B_2 </div> |
| ONTAP 9.0 o Data ONTAP 8.3.x | <div> storage failover takeover -ofnode node_B_2 -option allow-version-mismatch </div> <div>  La allow-version-mismatch Esta opción no es necesaria para las actualizaciones de ONTAP 9.0 a ONTAP 9.1 o para cualquier actualización de parches. </div> |

El nodo arranca con el estado "esperando la devolución".



Si AutoSupport está habilitado, se envía un mensaje de AutoSupport que indica que los nodos están fuera del quórum del clúster. Puede ignorar con toda tranquilidad esta notificación y continuar con la actualización.

b. Compruebe que la toma de control se ha realizado correctamente:

storage failover show

El siguiente ejemplo muestra que la toma de control se ha realizado correctamente. El nodo B_2 está en el estado "esperando devolución" y el nodo B_1 está en el estado "durante toma de control".

```

cluster1::> storage failover show
Node           Partner           Takeover
Possible State Description
-----
node_B_1       node_B_2           false    In takeover
node_B_2       node_B_1           -        Waiting for giveback (HA
mailboxes)
2 entries were displayed.
        
```

4. Espere al menos ocho minutos para asegurarse de las siguientes condiciones:

- La multivía del cliente (si está implementada) se estabiliza.
- Los clientes se recuperan de la pausa en la I/O que se produce durante la toma de control.

El tiempo de recuperación es específico del cliente y puede tardar más de ocho minutos en función de las características de las aplicaciones cliente.

5. Devuelva los agregados a los nodos de destino:

Después de actualizar la configuración IP de MetroCluster a ONTAP 9.5, los agregados estarán en estado degradado durante un breve periodo de tiempo antes de volver a sincronizar y a un estado reflejado.

a. Proporcione los agregados al partner de recuperación ante desastres en cluster_A:

```
storage failover giveback -ofnode node_A_2
```

b. Proporcione los agregados al partner de recuperación ante desastres en cluster_B:

```
storage failover giveback -ofnode node_B_2
```

La operación de devolución devuelve primero el agregado raíz al nodo y, después de que el nodo haya terminado de arrancarse, devuelve los agregados que no son raíz.

6. Compruebe que todos los agregados se han devuelto emitiendo el siguiente comando en ambos clústeres:

```
storage failover show-giveback
```

Si el campo Estado de devolución indica que no hay agregados que devolver, se devolverán todos los agregados. Si se vetó la devolución, el comando muestra el progreso de devolución y qué subsistema vetó la devolución.

7. Si no se ha devuelto ningún agregado, realice lo siguiente:

- Revise la solución de veto para determinar si desea abordar la condición "vertical" o anular el veto.
- Si es necesario, tratar la condición "veto" descrita en el mensaje de error, asegurándose de que las operaciones identificadas se cancelen con gracia.
- Vuelva a introducir el comando de devolución del nodo de respaldo del almacenamiento.

Si ha decidido anular la condición "VETE", establezca el parámetro `-override-vetoes` en TRUE.

8. Espere al menos ocho minutos para asegurarse de las siguientes condiciones:

- La multivía del cliente (si está implementada) se estabiliza.
- Los clientes se recuperan de la pausa en la I/O que se produce durante la devolución.

El tiempo de recuperación es específico del cliente y puede tardar más de ocho minutos en función de las características de las aplicaciones cliente.

9. Establezca el nivel de privilegio de admin en Advanced, introduciendo **y** cuando se le solicite continuar:


```
set -privilege advanced
```

El aviso avanzado (*>) aparece.

10. Confirme la versión en cluster_A:

```
system image show
```

El siguiente ejemplo muestra que la imagen 2 del sistema (imagen ONTAP de destino) es la versión predeterminada y actual en node_A_2:

```
cluster_B::*> system image show
```

| Node | Image | Is Default | Is Current | Version | Install Date |
|----------|--------|---------------|---------------|---------|-----------------|
| ----- | | | | | |
| node_A_1 | | | | | |
| | image1 | false | false | X.X.X | MM/DD/YYYY TIME |
| | image2 | true | true | Y.Y.Y | MM/DD/YYYY TIME |
| node_A_2 | | | | | |
| | image1 | false | false | X.X.X | MM/DD/YYYY TIME |
| | image2 | true | true | Y.Y.Y | MM/DD/YYYY TIME |

4 entries were displayed.

```
cluster_A::>
```

11. Confirme la versión en cluster_B:

```
system image show
```

El siguiente ejemplo muestra que System image2 (imagen ONTAP de destino) es la versión predeterminada y actual en NODE_B_2:

```
cluster_B::*> system image show
```

| Node | Image | Is Default | Is Current | Version | Install Date |
|----------|--------|---------------|---------------|---------|-----------------|
| ----- | | | | | |
| node_B_1 | | | | | |
| | image1 | false | false | X.X.X | MM/DD/YYYY TIME |
| | image2 | true | true | Y.Y.Y | MM/DD/YYYY TIME |
| node_B_2 | | | | | |
| | image1 | false | false | X.X.X | MM/DD/YYYY TIME |
| | image2 | true | true | Y.Y.Y | MM/DD/YYYY TIME |

4 entries were displayed.

```
cluster_A::>
```

12. Para cada nodo del par de alta disponibilidad, habilite la devolución automática:

```
storage failover modify -node target-node -auto-giveback true
```

Este comando se debe repetir para cada nodo de la pareja de ha.

13. Compruebe que la devolución automática está activada:

```
storage failover show -fields auto-giveback
```

Este ejemplo muestra que se ha habilitado la devolución automática de control en ambos nodos:

```
cluster_x::> storage failover show -fields auto-giveback
```

| node | auto-giveback |
|----------|---------------|
| ----- | |
| node_x_1 | true |
| node_x_2 | true |

2 entries were displayed.

Actualización no disruptiva de una configuración de MetroCluster de dos nodos en ONTAP 9,2 o versiones anteriores

La forma en que se actualiza una configuración de MetroCluster de dos nodos varía en función de su versión de ONTAP. Si ejecuta ONTAP 9,2 o una versión anterior, debe usar este procedimiento para realizar una actualización manual no disruptiva que incluya iniciar una conmutación de sitios negociada, actualizar el clúster en el sitio ««fallido»», iniciar una conmutación de retorno y, a continuación, repetir el proceso en el clúster en el otro sitio.

Si tiene una configuración MetroCluster de dos nodos que ejecute ONTAP 9,3 o una versión posterior, ejecute

un [Actualización automatizada mediante System Manager](#).

Pasos

1. Establezca el nivel de privilegio en avanzado, introduzca **y** cuando se le solicite continuar:

```
set -privilege advanced
```

El aviso avanzado (*>) aparece.

2. En el clúster que se va a actualizar, instale la nueva imagen de software ONTAP como predeterminada:

```
system node image update -package package_location -setdefault true  
-replace-package true
```

```
cluster_B::*> system node image update -package  
http://www.example.com/NewImage.tgz -setdefault true -replace-package  
true
```

3. Compruebe que la imagen del software de destino está definida como la imagen predeterminada:

```
system node image show
```

El siguiente ejemplo muestra eso NewImage se establece como la imagen predeterminada:

```
cluster_B::*> system node image show
```

| Node | Image | Is Default | Is Current | Version | Install Date |
|----------|----------|---------------|---------------|---------|-----------------|
| ----- | | | | | |
| node_B_1 | | | | | |
| | OldImage | false | true | X.X.X | MM/DD/YYYY TIME |
| | NewImage | true | false | Y.Y.Y | MM/DD/YYYY TIME |

2 entries were displayed.

4. Si la imagen del software de destino no está definida como la imagen predeterminada, cámbiela:

```
system image modify {-node * -iscurrent false} -isdefault true
```

5. Compruebe que todas las SVM del clúster tengan un estado de estado:

```
metrocluster vservers show
```

6. En el clúster que no se está actualizando, inicie una conmutación de sitios negociada:

```
metrocluster switchover
```

La operación puede llevar varios minutos. Puede usar el comando `MetroCluster operation show` para verificar que la conmutación se ha completado.

En el siguiente ejemplo, se realiza una conmutación negociada en el clúster remoto ("cluster_A"). Esto hace que el clúster local ("cluster_B") se detenga para que pueda actualizarlo.

```
cluster_A::> metrocluster switchover

Warning: negotiated switchover is about to start. It will stop all the
data
      Vservers on cluster "cluster_B" and
      automatically re-start them on cluster
      "cluster_A". It will finally gracefully shutdown
      cluster "cluster_B".
Do you want to continue? {y|n}: y
```

7. Compruebe que todas las SVM del clúster tengan un estado de estado:

```
metrocluster vservers show
```

8. Resincronizar los agregados de datos en el clúster de «surviving»:

```
metrocluster heal -phase aggregates
```

Después de actualizar la configuración IP de MetroCluster a ONTAP 9.5 o una versión posterior, los agregados estarán en estado degradado durante un breve periodo de tiempo antes de volver a sincronizar y volver a un estado de reflejo.

```
cluster_A::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

9. Compruebe que la operación de reparación se ha realizado correctamente:

```
metrocluster operation show
```

```
cluster_A::> metrocluster operation show
Operation: heal-aggregates
State: successful
Start Time: MM/DD/YYYY TIME
End Time: MM/DD/YYYY TIME
Errors: -
```

10. Resincronice los agregados raíz en el clúster «esencial»:

```
metrocluster heal -phase root-aggregates
```

```
cluster_A::> metrocluster heal -phase root-aggregates
[Job 131] Job succeeded: Heal Root Aggregates is successful.
```

11. Compruebe que la operación de reparación se ha realizado correctamente:

```
metrocluster operation show
```

```
cluster_A::> metrocluster operation show
Operation: heal-root-aggregates
State: successful
Start Time: MM/DD/YYYY TIME
End Time: MM/DD/YYYY TIME
Errors: -
```

12. En el clúster detenido, arranque el nodo desde el símbolo del sistema del CARGADOR:

```
boot_ontap
```

13. Espere a que termine el proceso de arranque y, a continuación, compruebe que todas las SVM del clúster estén en estado:

```
metrocluster vserver show
```

14. Haga una regreso desde el cluster «de la revolución»:

```
metrocluster switchback
```

15. Compruebe que la conmutación de estado se ha completado correctamente:

```
metrocluster operation show
```

```
cluster_A::> metrocluster operation show
Operation: switchback
State: successful
Start Time: MM/DD/YYYY TIME
End Time: MM/DD/YYYY TIME
Errors: -
```

16. Compruebe que todas las SVM del clúster tengan un estado de estado:

```
metrocluster vserver show
```

17. Repita todos los pasos anteriores en el otro clúster.

18. Compruebe que la configuración de MetroCluster sea correcta:

a. Compruebe la configuración:

```
metrocluster check run
```

```
cluster_A::> metrocluster check run
Last Checked On: MM/DD/YYYY TIME
Component          Result
-----
nodes              ok
lifs               ok
config-replication ok
aggregates         ok
4 entries were displayed.
```

Command completed. Use the "metrocluster check show -instance" command or sub-commands in "metrocluster check" directory for detailed results.

To check if the nodes are ready to do a switchover or switchback operation, run "metrocluster switchover -simulate" or "metrocluster switchback -simulate", respectively.

b. Si desea ver resultados más detallados, utilice el comando MetroCluster check run:

```
metrocluster check aggregate show
```

```
metrocluster check config-replication show
```

```
metrocluster check lif show
```

```
metrocluster check node show
```

c. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

d. Simule la operación switchover:

```
metrocluster switchover -simulate
```

e. Revise los resultados de la simulación de switchover:

```
metrocluster operation show
```

```
cluster_A::*> metrocluster operation show
  Operation: switchover
    State: successful
  Start time: MM/DD/YYYY TIME
    End time: MM/DD/YYYY TIME
    Errors: -
```

f. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

g. Repita estos mismos pasos en el otro clúster.

Después de terminar

Realice cualquier ["tareas posteriores a la actualización"](#).

Información relacionada

Actualización manual disruptiva de ONTAP mediante la interfaz de línea de comandos

Si puede desconectar el clúster para actualizar a una nueva versión de ONTAP, puede utilizar el método de actualización disruptiva. Este método tiene varios pasos:

Deshabilitar la conmutación por error de almacenamiento para cada pareja de alta disponibilidad, reiniciar cada nodo del clúster y, a continuación, volver a habilitar la conmutación por error del almacenamiento.

- Debe "descargue" y.. "instale" la imagen de software.
- Si opera en un entorno SAN, todos los clientes SAN deben cerrarse o suspenderse hasta que se complete la actualización.

Si los clientes SAN no se apagan o suspenden antes de una actualización disruptiva, los sistemas de archivos cliente y las aplicaciones sufren errores que pueden requerir recuperación manual una vez completada la actualización.

En una actualización disruptiva, se requiere un tiempo de inactividad porque la conmutación por error de almacenamiento está deshabilitada para cada par de alta disponibilidad y se actualiza cada nodo. Cuando se deshabilita la conmutación al respaldo de almacenamiento, cada nodo se comporta como un clúster de un solo nodo; es decir, los servicios del sistema asociados con el nodo se interrumpen mientras se tarda en reiniciar el sistema.

Pasos

1. Establezca el nivel de privilegio de admin en Advanced, introduciendo **y** cuando se le solicite continuar:

```
set -privilege advanced
```

El aviso avanzado (*>) aparece.

2. Establezca la nueva imagen del software ONTAP como la imagen predeterminada:

```
system image modify {-node * -iscurrent false} -isdefault true
```

Este comando utiliza una consulta ampliada para cambiar la imagen de software de ONTAP de destino (que se instala como imagen alternativa) y que sea la imagen predeterminada de cada nodo.

3. Compruebe que la nueva imagen del software ONTAP está configurada como la imagen predeterminada:

```
system image show
```

En el ejemplo siguiente, la imagen 2 es la nueva versión de ONTAP y se establece como la imagen predeterminada en ambos nodos:


```
cluster1::*> system image show
```

| Node | Image | Is Default | Is Current | Version | Install Date |
|-------|--------|---------------|---------------|---------|-----------------|
| ----- | | | | | |
| node0 | | | | | |
| | image1 | false | true | X.X.X | MM/DD/YYYY TIME |
| | image2 | true | false | Y.Y.Y | MM/DD/YYYY TIME |
| node1 | | | | | |
| | image1 | false | true | X.X.X | MM/DD/YYYY TIME |
| | image2 | true | false | Y.Y.Y | MM/DD/YYYY TIME |

4 entries were displayed.

4. Realice uno de los siguientes pasos:

| Si el clúster consta de... | Realice lo siguiente... |
|----------------------------|---|
| Un nodo | Continúe con el próximo paso. |
| Dos nodos | <p>a. Deshabilite alta disponibilidad del clúster:</p> <pre>cluster ha modify -configured false</pre> <p>Introduzca y para continuar cuando se le solicite.</p> <p>b. Desactive la conmutación por error del almacenamiento para el par de alta disponibilidad:</p> <pre>storage failover modify -node * -enabled false</pre> |
| Más de dos nodos | <p>Deshabilite la recuperación tras fallos del almacenamiento para cada pareja de alta disponibilidad del clúster:</p> <pre>storage failover modify -node * -enabled false</pre> |

5. Reiniciar un nodo en el clúster:

```
system node reboot -node nodename -ignore-quorum-warnings
```



No reinicie más de un nodo a la vez.

El nodo arranca la nueva imagen de ONTAP. Aparece la solicitud de inicio de sesión de ONTAP, que indica que el proceso de reinicio ha finalizado.

6. Después de que el nodo o el conjunto de nodos se haya reiniciado con la nueva imagen ONTAP, establezca el nivel de privilegio en AVANZADO:

```
set -privilege advanced
```

Introduzca **y** cuando se le solicite continuar

7. Confirme que el nuevo software se está ejecutando:

```
system node image show
```

En el siguiente ejemplo, image1 es la nueva versión de ONTAP y se establece como la versión actual del nodo 0:

```
cluster1::*> system node image show
```

| Node | Image | Is Default | Is Current | Version | Install Date |
|-------|--------|------------|------------|---------|-----------------|
| ----- | | | | | |
| node0 | | | | | |
| | image1 | true | true | X.X.X | MM/DD/YYYY TIME |
| | image2 | false | false | Y.Y.Y | MM/DD/YYYY TIME |
| node1 | | | | | |
| | image1 | true | false | X.X.X | MM/DD/YYYY TIME |
| | image2 | false | true | Y.Y.Y | MM/DD/YYYY TIME |

4 entries were displayed.

8. Compruebe que la actualización se haya realizado correctamente:

- a. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

- b. Compruebe que el estado de la actualización se haya completado para cada nodo:

```
system node upgrade-revert show -node nodename
```

El estado debe aparecer como completo.

Si el estado es no completo, ["Comuníquese con el soporte de NetApp"](#) inmediatamente.

- a. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

9. Repita los pasos 2 a 8 en cada nodo adicional.
10. Si el clúster consta de dos o más nodos, habilite la conmutación por error del almacenamiento para cada pareja de alta disponibilidad del clúster:

```
storage failover modify -node * -enabled true
```

11. Si el clúster consta de solo dos nodos, habilite la alta disponibilidad de los clústeres:

```
cluster ha modify -configured true
```

Qué hacer después de una actualización de ONTAP

Qué hacer después de una actualización de ONTAP

Después de actualizar ONTAP, hay varias tareas que debe realizar para verificar la disponibilidad del clúster.

1. ["Compruebe el clúster"](#).

Después de actualizar ONTAP, debe comprobar la versión del clúster, el estado del clúster y el estado del almacenamiento. Si utiliza una configuración de MetroCluster FC, también debe verificar que el clúster esté habilitado para la conmutación automática no planificada.

2. ["Compruebe que todas las LIF se encuentran en los puertos domésticos"](#).

Durante un reinicio, es posible que algunas LIF se hayan migrado a sus puertos de conmutación al respaldo asignados. Tras actualizar un clúster, debe habilitar y revertir cualquier LIF que no esté en sus puertos de inicio.

3. Verificación ["consideraciones especiales"](#) específicas de su clúster.

Si existen ciertas configuraciones en el clúster, es posible que deba realizar pasos adicionales después de actualizar.

4. ["Actualización del paquete de cualificación de disco \(DQP\)"](#).

El DQP no se actualiza como parte de una actualización de ONTAP.

Compruebe el clúster después de actualizar ONTAP

Después de actualizar ONTAP, compruebe la versión del clúster, el estado del clúster y el estado del almacenamiento. Para configuraciones de FC de MetroCluster, compruebe también que el clúster esté habilitado para la conmutación de sitios automática no planificada.

Comprobar la versión del clúster

Una vez que se hayan actualizado todos los pares de HA, debe usar el comando `version` para verificar que todos los nodos estén ejecutando la versión de destino.

La versión del clúster es la versión más baja de ONTAP que se ejecuta en cualquier nodo del clúster. Si la versión del clúster no es la versión de ONTAP de destino, puede actualizar el clúster.

1. Compruebe que la versión del clúster es la versión de ONTAP de destino:

```
version
```

2. Si la versión del clúster no es la versión de ONTAP de destino, debe comprobar el estado de actualización de todos los nodos:

```
system node upgrade-revert show
```

Compruebe el estado del clúster

Después de actualizar un clúster, debe comprobar que los nodos estén en buen estado y que sean elegibles para participar en el clúster, y que el clúster esté en quórum.

1. Compruebe que los nodos del clúster estén en línea y que puedan participar en el clúster:

```
cluster show
```

```
cluster1::> cluster show
Node                Health  Eligibility
-----
node0               true    true
node1               true    true
```

Si alguno de los nodos no es saludable o no apto, compruebe los registros de EMS en busca de errores y realice acciones correctivas.

2. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

3. Verifique los detalles de configuración de cada proceso RDB.

- Las épocas de la base de datos relacional y la base de datos deben coincidir para cada nodo.
- El maestro de quórum por anillo debe ser el mismo para todos los nodos.

Tenga en cuenta que cada anillo puede tener un maestro de quórum diferente.

| Para mostrar este proceso RDB: | Introduzca este comando... |
|--|---|
| Aplicación de gestión | <code>cluster ring show -unitname mgmt</code> |
| Base de datos de ubicación del volumen | <code>cluster ring show -unitname vlodb</code> |
| Administrador de interfaz virtual | <code>cluster ring show -unitname vifmgr</code> |
| Daemon de gestión de SAN | <code>cluster ring show -unitname bcomd</code> |

Este ejemplo muestra el proceso de la base de datos de ubicación del volumen:

```
cluster1::*> cluster ring show -unitname vlodb
Node      UnitName Epoch    DB Epoch DB Trnxs Master    Online
-----
node0     vlodb     154      154      14847   node0     master
node1     vlodb     154      154      14847   node0     secondary
node2     vlodb     154      154      14847   node0     secondary
node3     vlodb     154      154      14847   node0     secondary
4 entries were displayed.
```

4. Si va a trabajar en un entorno SAN, compruebe que cada nodo se encuentra en quórum DE SAN:

```
cluster kernel-service show
```

```
cluster1::*> cluster kernel-service show
Master          Cluster          Quorum          Availability
Operational
Node            Node            Status          Status          Status
-----
cluster1-01     cluster1-01     in-quorum       true
operational
cluster1-02     in-quorum       true
operational
2 entries were displayed.
```

Información relacionada

["Administración del sistema"](#)

Verifique que la conmutación de sitios automática no planificada está habilitada (solo configuraciones de MetroCluster FC).

Si el clúster está en una configuración de MetroCluster FC, debe verificar que la conmutación automática no planificada esté habilitada después de actualizar ONTAP.

Si está utilizando una configuración IP de MetroCluster, omita este procedimiento.

Pasos

1. Compruebe si la conmutación automática no planificada está habilitada:

```
metrocluster show
```

Si la conmutación automática no planificada está habilitada, aparecerá la siguiente instrucción en el resultado del comando:

```
AUSO Failure Domain  auso-on-cluster-disaster
```

2. Si la sentencia no aparece, active una conmutación automática no planificada:

```
metrocluster modify -auto-switchover-failure-domain auso-on-cluster-
disaster
```

3. Compruebe que se ha activado un switchover no planificado automático:

```
metrocluster show
```

Información relacionada

Verifique que todos los LIFS están en los puertos de inicio después de la actualización de ONTAP

Durante el reinicio que se produce como parte del proceso de actualización de ONTAP, es posible que algunas LIF se migren de sus puertos principales a los puertos de conmutación al nodo de respaldo asignados. Después de una actualización, debe activar y revertir los LIF que no estén en sus puertos principales.

Pasos

1. Mostrar el estado de todas las LIF:

```
network interface show -fields home-port,curr-port
```

Si **Status Admin** está "caído" o **is home** es "falso" para cualquier LIF, continúe con el siguiente paso.

2. Habilite las LIF de datos:

```
network interface modify {-role data} -status-admin up
```

3. Revertir los LIF a sus puertos raíz:

```
network interface revert *
```

4. Compruebe que todas las LIF se encuentran en sus puertos de inicio:

```
network interface show
```

Este ejemplo muestra que todas las LIF para SVM vs0 están en sus puertos iniciales.

```
cluster1::> network interface show -vserver vs0
```

| Vserver | Logical Interface | Status Admin/Oper | Network Address/Mask | Current Node | Current Port | Is Home |
|---------|-------------------|-------------------|----------------------|--------------|--------------|---------|
| vs0 | | | | | | |
| | data001 | up/up | 192.0.2.120/24 | node0 | e0e | true |
| | data002 | up/up | 192.0.2.121/24 | node0 | e0f | true |
| | data003 | up/up | 192.0.2.122/24 | node0 | e2a | true |
| | data004 | up/up | 192.0.2.123/24 | node0 | e2b | true |
| | data005 | up/up | 192.0.2.124/24 | node1 | e0e | true |
| | data006 | up/up | 192.0.2.125/24 | node1 | e0f | true |
| | data007 | up/up | 192.0.2.126/24 | node1 | e2a | true |
| | data008 | up/up | 192.0.2.127/24 | node1 | e2b | true |

8 entries were displayed.

Configuraciones especiales

Consideraciones especiales tras una actualización de ONTAP

Si se configura el clúster con alguna de las siguientes funciones, es posible que deba realizar pasos adicionales después de actualizar el software ONTAP.

| Pregúntese... | Si su respuesta es sí, entonces haga esto... |
|---|---|
| ¿He actualizado desde ONTAP 9,7 o anterior a ONTAP 9,8 o posterior? | Compruebe la configuración de red Quite el servicio LIF EMS de las políticas de servicio de red que no proporcionan accesibilidad al destino EMS |
| ¿Mi clúster está en una configuración MetroCluster? | Compruebe el estado de las redes y el almacenamiento |
| ¿Tengo una configuración SAN? | Compruebe su configuración SAN |
| ¿Actualizo desde ONTAP 9,3 o anterior? ¿Utilizo el cifrado del almacenamiento de NetApp? | Volver a configurar las conexiones del servidor KMIP |
| ¿Tengo reflejos de uso compartido de carga? | Reubicar los volúmenes de origen de reflejos de uso compartido de carga movidos |
| ¿Tengo cuentas de usuario para el acceso al procesador de servicio (SP) que se hayan creado antes de ONTAP 9,9.1? | Compruebe el cambio en las cuentas que pueden acceder a Service Processor |

Verifique la configuración de red después de una actualización de ONTAP desde ONTAP 9,7x o una versión anterior

Después de realizar una actualización desde ONTAP 9,7x o anterior a ONTAP 9,8 o posterior, debe verificar la configuración de red. Después de la actualización, ONTAP supervisa automáticamente la accesibilidad de la capa 2.

Paso

1. Compruebe que cada puerto tiene accesibilidad al dominio de retransmisión esperado:

```
network port reachability show -detail
```

El resultado del comando contiene resultados de accesibilidad. Use el árbol de decisión y la tabla siguientes para comprender los resultados de la accesibilidad (estado de la accesibilidad) y determinar qué hacer, si es que hay algo, a continuación.



| accesibilidad-estado | Descripción |
|----------------------|-------------|
|----------------------|-------------|

| | |
|-----------------------------|--|
| de acuerdo | <p>El puerto tiene capacidad de acceso de capa 2 a su dominio de difusión asignado.</p> <p>Si el reachability-status es "ok", pero hay "puertos inesperados", considere combinar uno o más dominios de difusión. Para obtener más información, consulte "Fusionar dominios de retransmisión".</p> <p>Si el reachability-status es "ok", pero hay "puertos inaccesibles", considere dividir uno o más dominios de difusión. Para obtener más información, consulte "Divida los dominios de retransmisión".</p> <p>Si el estado de accesibilidad es "correcto" y no hay puertos inesperados o no accesibles, la configuración es correcta.</p> |
| función mal configurada | <p>El puerto no tiene posibilidad de recurrir a la capa 2 a su dominio de difusión asignado; sin embargo, el puerto tiene capacidad de acceso de capa 2 a un dominio de difusión diferente.</p> <p>Puede reparar la accesibilidad del puerto. Cuando ejecute el siguiente comando, el sistema asignará el puerto al dominio de retransmisión al que se le habrá accesibilidad:</p> <pre>network port reachability repair -node -port</pre> <p>Para obtener más información, consulte "Reparar la accesibilidad del puerto".</p> |
| ausencia de accesibilidad | <p>El puerto no tiene posibilidad de recurrir a ningún dominio de difusión existente de capa 2.</p> <p>Puede reparar la accesibilidad del puerto. Cuando ejecute el siguiente comando, el sistema asignará el puerto a un dominio de retransmisión creado automáticamente en el espacio IP predeterminado:</p> <pre>network port reachability repair -node -port</pre> <p>Para obtener más información, consulte "Reparar la accesibilidad del puerto".</p> |
| accesibilidad multi-dominio | <p>El puerto tiene la habilidad de la capa 2 para su dominio de broadcast asignado; sin embargo, también tiene la habilidad de la capa 2 para al menos otro dominio de broadcast.</p> <p>Examine la configuración física del conmutador y la conectividad para determinar si es incorrecta o si el dominio de difusión asignado al puerto necesita combinarse con uno o más dominios de difusión.</p> <p>Para obtener más información, consulte "Fusionar dominios de retransmisión" o "Reparar la accesibilidad del puerto".</p> |
| desconocido | <p>Si el estado de accesibilidad es "desconocido", espere unos minutos y vuelva a intentar el comando.</p> |

Después de reparar un puerto, necesita comprobar y resolver las LIF y VLAN desplazadas. Si el puerto era parte de un grupo de interfaces, también necesita comprender lo que ha sucedido con ese grupo de

interfaces. Para obtener más información, consulte ["Reparar la accesibilidad del puerto"](#).

Quite el servicio LIF de EMS de las políticas de servicio de red

Si tiene mensajes del sistema de gestión de eventos (EMS) configurados antes de actualizar de ONTAP 9.7 o anterior a ONTAP 9.8 o posterior , después de la actualización, es posible que los mensajes de EMS no se envíen.

Durante la actualización, Management-ems, que es el servicio LIF de EMS, se agrega a todas las políticas de servicio existentes. Esto permite enviar mensajes de EMS desde cualquiera de las LIF asociadas con cualquiera de las políticas de servicio. Si la LIF seleccionada no tiene accesibilidad al destino de notificaciones de eventos, el mensaje no se entrega.

Para evitar esto, después de la actualización, debe eliminar el servicio LIF de EMS de las políticas de servicio de red que no proporcionan accesibilidad al destino.

Pasos

- 1. Identificar las LIF y las políticas de servicio de red asociadas mediante las cuales se pueden enviar mensajes de EMS:

```
network interface show -fields service-policy -services management-ems
```

| vserver | lif | service-policy |
|---------------------------|---------------|----------------------|
| cluster-1 | cluster_mgmt | |
| | | default-management |
| cluster-1 | node1-mgmt | |
| | | default-management |
| cluster-1 | node2-mgmt | |
| | | default-management |
| cluster-1 | inter_cluster | |
| | | default-intercluster |
| 4 entries were displayed. | | |

- 2. Compruebe cada LIF para obtener conectividad con el destino EMS:

```
network ping -lif lif_name -vserver svm_name -destination destination_address
```

Realice esto en cada nodo.

Ejemplos

```
cluster-1::> network ping -lif node1-mgmt -vserver cluster-1
-destination 10.10.10.10
10.10.10.10 is alive

cluster-1::> network ping -lif inter_cluster -vserver cluster-1
-destination 10.10.10.10
no answer from 10.10.10.10
```

3. Introduzca el nivel de privilegio avanzado:

```
set advanced
```

4. Para los LIF que no tienen habilidad, quite el servicio LIF Management-ems de las políticas de servicio correspondientes:

```
network interface service-policy remove-service -vserver svm_name
-policy service_policy_name -service management-ems
```

5. Compruebe que el LIF de ems de gestión solo esté asociado a las LIF que proporcionan accesibilidad al destino de EMS:

```
network interface show -fields service-policy -services management-ems
```

Enlaces relacionados

["LIF y políticas de servicio en ONTAP 9.6 y posteriores"](#)

Comprobar el estado de redes y almacenamiento de las configuraciones de MetroCluster tras una actualización de ONTAP

Después de actualizar un clúster de ONTAP en una configuración de MetroCluster, debe comprobar el estado de las LIF, los agregados y los volúmenes de cada clúster.

1. Compruebe el estado de la LIF:

```
network interface show
```

En un funcionamiento normal, los LIF de las SVM de origen deben tener el estado de administrador de en activo y estar ubicados en sus nodos raíz. Los LIF para las SVM de destino no necesitan estar en marcha o ubicados en sus nodos iniciales. Sin embargo, todos los LIF tienen el estado de administrador activo, pero no es necesario que estén ubicados en sus nodos iniciales.

```

cluster1::> network interface show

```

| Current Is | Logical | Status | Network | Current | |
|-------------|---------------------------------|------------|-----------------|-------------|-------|
| Vserver | Interface | Admin/Oper | Address/Mask | Node | Port |
| Home | | | | | |
| ----- | ----- | ----- | ----- | ----- | ----- |
| Cluster | | | | | |
| | cluster1-a1_clus1 | up/up | 192.0.2.1/24 | cluster1-01 | e2a |
| true | | | | | |
| | cluster1-a1_clus2 | up/up | 192.0.2.2/24 | cluster1-01 | e2b |
| true | | | | | |
| cluster1-01 | | | | | |
| | clus_mgmt | up/up | 198.51.100.1/24 | cluster1-01 | e3a |
| true | | | | | |
| | cluster1-a1_inet4_intercluster1 | up/up | 198.51.100.2/24 | cluster1-01 | e3c |
| true | | | | | |
| | ... | | | | |

```

27 entries were displayed.

```

2. Compruebe el estado de los agregados:

```
storage aggregate show -state !online
```

Este comando muestra todos los agregados que *not* están en línea. En el funcionamiento normal, todos los agregados ubicados en el sitio local deben estar en línea. Sin embargo, si la configuración de MetroCluster está de conmutación, los agregados raíz del sitio de recuperación ante desastres pueden estar sin conexión.

Este ejemplo muestra un clúster en funcionamiento normal:

```

cluster1::> storage aggregate show -state !online
There are no entries matching your query.

```

Este ejemplo muestra un clúster con conmutación de sitios, en el que los agregados raíz del sitio de recuperación ante desastres están sin conexión:

```
cluster1::> storage aggregate show -state !online
Aggregate      Size Available Used% State   #Vols  Nodes      RAID
Status
-----
-----
aggr0_b1
      0B      0B    0% offline    0 cluster2-01
raid_dp,
mirror
degraded
aggr0_b2
      0B      0B    0% offline    0 cluster2-02
raid_dp,
mirror
degraded
2 entries were displayed.
```

3. Compruebe el estado de los volúmenes:

```
volume show -state !online
```

Este comando muestra los volúmenes que *not* están en línea.

Si la configuración de MetroCluster tiene un funcionamiento normal (no está en estado de conmutación por sitios), el resultado debe mostrar todos los volúmenes que pertenecen a las SVM secundarias del clúster (los que tienen el nombre de SVM anexo con "-mc").

Esos volúmenes solo entran en línea en caso de que se produzca un cambio.

Este ejemplo muestra un clúster con un funcionamiento normal, en el cual los volúmenes del sitio de recuperación ante desastres no están en línea.

```
cluster1::> volume show -state !online
(volume show)
Vserver   Volume      Aggregate    State    Type    Size
Available Used%
-----
vs2-mc    vol1        aggr1_b1     -        RW      -
-         -
vs2-mc    root_vs2    aggr0_b1     -        RW      -
-         -
vs2-mc    vol2        aggr1_b1     -        RW      -
-         -
vs2-mc    vol3        aggr1_b1     -        RW      -
-         -
vs2-mc    vol4        aggr1_b1     -        RW      -
-         -
5 entries were displayed.
```

4. Compruebe que no haya volúmenes incoherentes:

```
volume show -is-inconsistent true
```

Consulte el artículo de la base de conocimientos ["Volumen que muestra una incoherencia de WAFL"](#) sobre la forma de abordar los volúmenes incoherentes.

Comprobar la configuración DE SAN tras una actualización

Tras una actualización de ONTAP, en un entorno SAN, debe verificar que cada iniciador que esté conectado a una LIF antes de que la actualización se haya reconectado correctamente a la LIF.

1. Compruebe que cada iniciador está conectado a la LIF correcta.

Debe comparar la lista de iniciadores con la lista que ha realizado durante la preparación de la actualización.

| Durante... | Introduzca... |
|------------|---|
| ISCSI | <pre>iscsi initiator show -fields igroup,initiator-name,tpgroup</pre> |

| Durante... | Introduzca... |
|------------|---|
| FC | <pre>fcf initiator show -fields igroup,wwpn,lif</pre> |

Vuelva a configurar las conexiones del servidor KMIP después de una actualización de ONTAP 9,2 o una versión anterior

Después de realizar la actualización desde ONTAP 9,2 o una versión anterior a ONTAP 9,3 o una versión posterior, debe volver a configurar todas las conexiones del servidor de gestión de claves externa (KMIP).

Pasos

1. Configure la conectividad del gestor de claves:

```
security key-manager setup
```

2. Añada sus servidores KMIP:

```
security key-manager add -address key_management_server_ip_address
```

3. Compruebe que los servidores KMIP están conectados:

```
security key-manager show -status
```

4. Consulte los servidores de claves:

```
security key-manager query
```

5. Cree una nueva clave de autenticación y contraseña:

```
security key-manager create-key -prompt-for-key true
```

La frase de contraseña debe tener un mínimo de 32 caracteres.

6. Consulte la nueva clave de autenticación:

```
security key-manager query
```

7. Asigne la nueva clave de autenticación a sus discos de cifrado automático (SED):

```
storage encryption disk modify -disk disk_ID -data-key-id key_ID
```



Asegúrese de que está utilizando la nueva clave de autenticación de su consulta.

8. Si es necesario, asigne una clave FIPS al SED:

```
storage encryption disk modify -disk disk_id -fips-key-id  
fips_authentication_key_id
```

Si la configuración de seguridad requiere el uso de claves diferentes para la autenticación de datos y la autenticación FIPS 140-2-2, debe crear una clave independiente para cada una. Si no es así, puede usar la misma clave de autenticación para el cumplimiento de FIPS que se usa para acceder a los datos.

Reubicar volúmenes de origen de reflejos de uso compartido de carga movidos después de una actualización de ONTAP

Después de actualizar ONTAP, tiene que mover los volúmenes de origen de reflejos de uso compartido de carga nuevamente a sus ubicaciones previas a la actualización.

Pasos

1. Identifique la ubicación a la que se va a mover el volumen de origen de reflejos de uso compartido de carga mediante el registro creado antes de mover el volumen de origen de reflejos de uso compartido de carga.
2. Mueva el volumen de origen de reflejos de uso compartido de carga de vuelta a su ubicación original:

```
volume move start
```

Cambio en las cuentas de usuario que pueden acceder a Service Processor

Si ha creado cuentas de usuario en ONTAP 9,8 o una versión anterior que pueden acceder al procesador de servicio (SP) con un rol no de administrador y actualiza a ONTAP 9.9.1 o una versión posterior, cualquier valor que no sea administrador en la `-role` el parámetro se modifica a `admin`.

Para obtener más información, consulte ["Cuentas que pueden acceder al SP"](#).

Actualice el paquete de cualificación de disco

Después de actualizar el software de ONTAP, debe descargar e instalar el paquete de cualificación de disco de ONTAP (DQP). El DQP no se actualiza como parte de una actualización de ONTAP.

El DQP contiene los parámetros adecuados para la interacción ONTAP con todas las unidades recién cualificadas. Si su versión del DQP no contiene información para una unidad recién cualificada, ONTAP no tendrá la información necesaria para configurar correctamente la unidad.

Se recomienda actualizar el DQP cada trimestre. También debe actualizar el DQP por los siguientes motivos:

- Siempre que se añada un nuevo tipo o tamaño de unidad a un nodo del clúster

Por ejemplo, si ya tiene unidades de 1 TB y añade unidades de 2 TB, debe comprobar la actualización más reciente del DQP.

- Cada vez que se actualiza el firmware de disco
- Siempre que estén disponibles los archivos DQP o firmware de disco más nuevos

Información relacionada

- ["Descargas de NetApp: Paquete de cualificación de disco"](#)
- ["Descargas de NetApp: Firmware de la unidad de disco"](#)

Firmware y actualizaciones del sistema

Descripción general de las actualizaciones del sistema y el firmware

En función de la versión de ONTAP, puede habilitar el firmware automático y las actualizaciones del sistema.

| Versión de ONTAP | Lo que se incluye en las actualizaciones automáticas |
|--------------------|--|
| 9.13.1 y posterior | <ul style="list-style-type: none">• Base de datos de zona horaria de ONTAP• Firmware de almacenamiento para dispositivos de almacenamiento, discos y bandejas de discos• Firmware del SP/BMC para los procesadores de servicio y los módulos BMC |
| 9.10.1 y posterior | <ul style="list-style-type: none">• Firmware de almacenamiento para dispositivos de almacenamiento, discos y bandejas de discos• Firmware del SP/BMC para los procesadores de servicio y los módulos BMC |
| 9.9.1 y anteriores | No admitido |

Si ejecuta ONTAP 9.9.1 o una versión anterior, o si no tiene ["actualizaciones automáticas del sistema"](#) habilitado, puede ["realice las actualizaciones de firmware manualmente"](#).

Si ejecuta ONTAP 9.12.1 o una versión anterior, o si no tiene ["actualizaciones automáticas del sistema"](#) Activado, puede actualizar la base de datos de zona horaria manualmente. Consulte el artículo de la base de conocimientos, ["Cómo actualizar la información de zona horaria en ONTAP 9"](#), para más detalles.

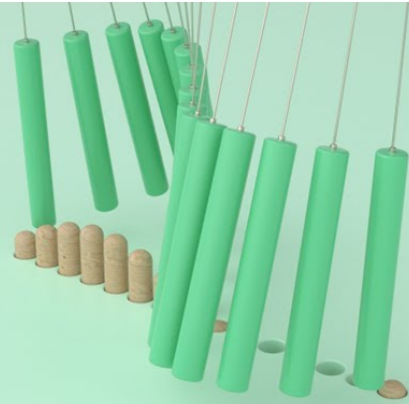
Vídeo: Función de actualización automática del firmware

Echa un vistazo a la función de actualización automática de firmware disponible a partir de ONTAP 9.10.1.



Automatic Firmware Update feature is available starting in ONTAP 9.10.1

By Jim Svesnik,
Quality Assurance Engineer



Cómo se programan las actualizaciones automáticas para la instalación

Todos los nodos elegibles del mismo clúster se agrupan para realizar actualizaciones automáticas. El plazo en el que se programan los nodos elegibles para la actualización automática varía en función del nivel de prioridad de la actualización y el porcentaje de sistemas del entorno que requieren la actualización.

Por ejemplo, si el 10% o menos de su total de sistemas son elegibles para una actualización sin prioridad, la actualización está programada para todos los sistemas elegibles dentro de 1 semana. Sin embargo, si el 76 % o más de sus sistemas totales pueden optar a una actualización sin prioridad, la actualización se escalonará en los sistemas aptos durante 8 semanas. Esta instalación escalonada ayuda a mitigar los riesgos de su entorno general si se produce un problema con una actualización que debe solucionarse.

El porcentaje del total de sistemas programados para actualizaciones automáticas por semana es el siguiente:

Para actualizaciones críticas

| % de sistemas que requieren actualización | % de actualizaciones que se producen en la semana 1 | % de actualizaciones que se producen en la semana 2 |
|---|---|---|
| 50 % o menos | 100 % | |
| Del 50 al 100 % | 30 % | 70 % |

Para actualizaciones de alta prioridad

| % de sistemas que requieren actualización | % de actualizaciones que se producen por semana | | | |
|---|---|----------|----------|----------|
| | semana 1 | semana 2 | semana 3 | semana 4 |
| 25% o menos | 100 % | | | |
| 26-50% | 30 % | 70 % | | |
| 50-100% | 10 % | 20 % | 30 % | 40 % |

Para actualizaciones de prioridad normales

| % de sistemas que requieren actualización | % de actualizaciones que se producen por semana | | | | | | | |
|---|---|----------|----------|----------|----------|----------|----------|----------|
| | semana 1 | semana 2 | semana 3 | semana 4 | semana 5 | semana 6 | semana 7 | semana 8 |
| 10% o menos | 100 % | | | | | | | |
| 11-20% | 30 % | 70 % | | | | | | |
| 21-50% | 10 % | 20 % | 30 % | 40 % | | | | |
| 51-75% | 5 % | 10 % | 15 % | 20 % | 20 % | 30 % | | |
| 76-100% | 5 % | 5 % | 10 % | 10 % | 15 % | 15 % | 20 % | 20 % |

Active las actualizaciones automáticas

A partir de ONTAP 9.10.1, puede habilitar las actualizaciones automáticas para permitir que ONTAP descargue e instale actualizaciones de firmware sin la intervención del usuario.

A partir de ONTAP 9.13.1, estas actualizaciones automáticas también incluyen actualizaciones automáticas de la base de datos de zona horaria.

Antes de empezar

Debe tener un derecho de soporte vigente. Esto se puede validar en el ["Sitio de soporte de NetApp"](#) En la página **Detalles del sistema**.

Acerca de esta tarea

Para habilitar las actualizaciones automáticas, primero debe habilitar AutoSupport con HTTPS. Si AutoSupport no está habilitado en el clúster, o si AutoSupport está habilitado en el clúster con otro protocolo de transporte, tendrá la opción de habilitarla con HTTPS durante este procedimiento.

Pasos

1. En System Manager, haga clic en **Eventos**.
2. En la sección **Overview**, junto a **Enable automatic update**, haz clic en **Actions>Enable**.

3. Si no dispone de AutoSupport con HTTPS habilitado, seleccione para habilitarlo.
4. Acepte los términos y condiciones y seleccione **Guardar**.


Información relacionada

["Solucione problemas de entrega de mensajes de AutoSupport a través de HTTP o HTTPS"](#)

Modificar actualizaciones automáticas

Cuando se habilitan las actualizaciones automáticas, de forma predeterminada, ONTAP detecta, descarga e instala automáticamente todas las actualizaciones de firmware recomendadas y, a partir de ONTAP 9.13.1, las actualizaciones de la base de datos de zona horaria de ONTAP. Si desea ver las actualizaciones recomendadas antes de instalarlas o si desea que las recomendaciones se descarten automáticamente, puede modificar el comportamiento predeterminado según sus preferencias.

Pasos

1. En System Manager, haga clic en **clúster > Configuración**.
2. En la sección **actualización automática**, haga clic en  para ver una lista de acciones.
3. Haga clic en **Editar configuración de actualización automática**.
4. Especifique las acciones por defecto que se van a realizar para cada tipo de evento.

Puede elegir actualizar automáticamente, mostrar notificaciones o descartar automáticamente las actualizaciones para cada tipo de evento.






La base de datos de zona horaria de ONTAP está controlada por el tipo de evento de ARCHIVOS DEL SISTEMA.


Administrar las actualizaciones automáticas recomendadas

El registro de actualización automática muestra una lista de recomendaciones de actualización y detalles sobre cada una, incluyendo una descripción, categoría, hora programada para la instalación, estado y cualquier error. Puede ver el log y, a continuación, decidir qué acción desea realizar para cada recomendación.

Pasos

1. Vea la lista de recomendaciones:

| Vista desde Configuración del clúster | Vista en la pestaña Actualización de firmware |
|--|--|
| a. Haga clic en clúster > Configuración . b. En la sección actualización automática , haga clic en  . A continuación, haga clic en Ver todas las actualizaciones automáticas . | a. Haga clic en Cluster > Overview . b. En la sección Descripción general , haga clic en más  . A continuación, haga clic en actualización de ONTAP . c. Seleccione la ficha actualización del firmware . d. En la ficha actualización del firmware , haga clic en más  . A continuación, haga clic en Ver todas las actualizaciones automáticas . |

2. Haga clic en  junto a la descripción para ver una lista de acciones que puede realizar con la recomendación.

Se puede realizar una de las siguientes acciones, según el estado de la recomendación:

| Si la actualización está en este estado... | Le permite... |
|--|--|
| No se ha programado | Actualizar: Inicia el proceso de actualización. Programación: Permite establecer una fecha para iniciar el proceso de actualización. Descartar: Elimina la recomendación de la lista. |
| Se ha programado | Actualizar: Inicia el proceso de actualización. Editar programación: Le permite modificar la fecha programada para iniciar el proceso de actualización. Cancelar programa: Cancela la fecha programada. |
| Ha sido despedido | Undismiss: Devuelve la recomendación a la lista. |
| Se está aplicando o se está descargando | Cancelar: Cancela la actualización. |

Actualice el firmware manualmente

A partir de ONTAP 9.9.1, si está registrado con **"Active IQ Unified Manager"**, Puede recibir alertas en System Manager que le informen cuando las actualizaciones de firmware de los dispositivos compatibles, como el disco, las bandejas de discos, el procesador de servicio (SP) o la controladora de gestión de placa base (BMC) están pendientes en el clúster.

Si está ejecutando ONTAP 9.8 o no está registrado en Active IQ Unified Manager, puede ir al sitio de soporte de NetApp para descargar las actualizaciones de firmware.

Antes de empezar

Para prepararse para una actualización de firmware fluida, debe reiniciar el SP o BMC antes de que comience la actualización. Puede utilizar el `system service-processor reboot-sp -node node_name` comando para reiniciar.

Pasos

Siga el procedimiento adecuado basado en su versión de ONTAP y si está registrado en Active IQ Unified Manager.

ONTAP 9.9.1 y versiones posteriores con Active IQ

1. En System Manager, vaya a **Dashboard**.

En la sección **Estado**, aparece un mensaje si hay alguna actualización de firmware recomendada para el clúster.

2. Haga clic en el mensaje de alerta.

La ficha **actualización del firmware** se muestra en la página **Actualizar**.

3. Haga clic en **Descarga desde el sitio de soporte de NetApp** para obtener la actualización de firmware que desee realizar.

Se mostrará el sitio de soporte de NetApp.

4. Inicie sesión en el sitio de soporte de NetApp y descargue el paquete de imagen de firmware necesario para la actualización.

5. Copie los archivos en un servidor HTTP o FTP de la red o en una carpeta local.

6. En System Manager, haga clic en **clúster > Descripción general**.

7. En la esquina derecha del panel **Descripción general**, haga clic en **más**  Y seleccione **actualización de ONTAP**.

8. Haga clic en **actualización del firmware**.

9. Según la versión de ONTAP, haga lo siguiente:

| ONTAP 9.9.1 y 9.10.0 | ONTAP 9.10.1 y posteriores |
|---|--|
| <ol style="list-style-type: none">a. Seleccione desde servidor o Cliente localb. Proporcione la URL del servidor o la ubicación del archivo. | <ol style="list-style-type: none">a. En la lista de actualizaciones recomendadas, selecciona Acciones.b. Haga clic en Actualizar para instalar la actualización inmediatamente o en Programar para programarla para más tarde. Si la actualización ya está programada, puedes Editar o Cancelar.c. Seleccione el botón Actualizar firmware. |

ONTAP 9,8 y posteriores sin Active IQ

1. Desplácese hasta la ["Sitio de soporte de NetApp"](#) e inicie sesión.
2. Seleccione el paquete de firmware que desea utilizar para actualizar el firmware del clúster.
3. Copie los archivos en un servidor HTTP o FTP de la red o en una carpeta local.
4. En System Manager, haga clic en **clúster > Descripción general**.
5. En la esquina derecha del panel **Descripción general**, haga clic en **más**  Y seleccione **actualización de ONTAP**.
6. Haga clic en **actualización del firmware**.

7. Según la versión de ONTAP, haga lo siguiente:

| ONTAP 9,8, 9.9.1 y 9.10.0 | ONTAP 9.10.1 y posteriores |
|---|--|
| <ol style="list-style-type: none">1. Seleccione desde servidor o Cliente local2. Proporcione la URL del servidor o la ubicación del archivo. | <ol style="list-style-type: none">1. En la lista de actualizaciones recomendadas, selecciona Acciones.2. Haga clic en Actualizar para instalar la actualización inmediatamente o en Programar para programarla para más tarde. Si la actualización ya está programada, puedes Editar o Cancelar.3. Seleccione el botón Actualizar firmware. |

Después de terminar

Puede supervisar o verificar las actualizaciones en **Resumen de actualización del firmware**. Para ver las actualizaciones que se han descartado o no se han podido instalar, haga clic en **Clúster > Configuración > Actualización automática > Ver todas las actualizaciones automáticas**.

Revierte ONTAP

Información general sobre revert ONTAP

Para realizar la transición de un clúster a una versión de ONTAP anterior, debe ejecutar una nueva versión.

La información de esta sección le guiará por los pasos que debe seguir antes y después de la reversión, incluidos los recursos que debe leer y las comprobaciones necesarias antes y después de la reversión que debe realizar.



Si necesita realizar la transición de un clúster de ONTAP 9.1 a ONTAP 9.0, debe utilizar el procedimiento de degradación documentado ["aquí"](#).

¿Necesito soporte técnico para revertir?

Es posible revertir sin ayuda en clústeres nuevos o de prueba. Debe llamar al soporte técnico para revertir los clústeres de producción. También debe llamar al soporte técnico si experimenta alguna de las siguientes situaciones:

- Está en un entorno de producción y la reversión falla o se encuentra con cualquier problema antes o después de la reversión, como:
 - El proceso de reversión falla y no puede finalizar.
 - El proceso de reversión finaliza, pero el clúster no se puede utilizar en un entorno de producción.
 - El proceso de reversión se finaliza y el clúster se pone en producción, pero no está satisfecho con su comportamiento.
- Creó volúmenes en ONTAP 9.5 o una versión posterior y debe revertir a una versión anterior. Los volúmenes que utilizan compresión adaptativa deben descomprimidos antes de revertir.

Rutas de reversión

La versión de ONTAP a la que se puede revertir varía según la versión de ONTAP que se esté ejecutando actualmente en los nodos. Puede utilizar el `system image show` Comando para determinar la versión de ONTAP que se ejecuta en cada nodo.

Estas directrices solo se refieren a versiones ONTAP en las instalaciones. Para obtener información acerca de cómo revertir la ONTAP en el cloud, consulte ["Revertir o degradar Cloud Volumes ONTAP"](#).

| Puede revertir de... | Para... |
|----------------------|------------------|
| ONTAP 9.14.1 | ONTAP 9.13.1 |
| ONTAP 9.13.1 | ONTAP 9.12.1 |
| ONTAP 9.12.1 | ONTAP 9.11.1 |
| ONTAP 9.11.1 | ONTAP 9.10.1 |
| ONTAP 9.10.1 | ONTAP 9.9.1 |
| ONTAP 9.9.1 | ONTAP 9,8 |
| ONTAP 9,8 | ONTAP 9,7 |
| ONTAP 9,7 | ONTAP 9,6 |
| ONTAP 9,6 | ONTAP 9,5 |
| ONTAP 9,5 | ONTAP 9,4 |
| ONTAP 9,4 | ONTAP 9,3 |
| ONTAP 9,3 | ONTAP 9,2 |
| ONTAP 9,2 | ONTAP 9,1 |
| ONTAP 9,1 o ONTAP 9 | Data ONTAP 8,3.x |



Si necesita cambiar de ONTAP 9.1 a 9.0, debe seguir el ["proceso de degradación"](#) aquí documentado.

¿Qué debería leer antes de revertir?

Recursos que debe revisar antes de revertir

Antes de revertir ONTAP, debe confirmar el soporte de hardware y revisar los recursos para saber cuáles son los problemas que se pueden encontrar o que son necesarios resolver.

1. Revise la ["Notas de la versión de ONTAP 9"](#) para la versión de destino.

En la sección ["Precauciones importantes"](#) se describen los posibles problemas que debe tener en cuenta antes de la degradación o la reversión.

2. Confirme que su plataforma de hardware es compatible con la versión de destino.

["Hardware Universe de NetApp"](#)

3. Confirme que su clúster y los switches de gestión son compatibles en la versión de destino.

Debe verificar que las versiones del software NX-OS (switches de red de clúster), IOS (switches de red de gestión) y archivo de configuración de referencia (RCF) sean compatibles con la versión de ONTAP a la que desea revertir.

["Descargas de NetApp: Switch Ethernet de Cisco"](#)

4. Si su clúster está configurado para SAN, confirme que la configuración SAN es totalmente compatible.

Deben ser compatibles todos los componentes DE SAN, como la versión de software de la ONTAP de destino, el sistema operativo y parches del host, el software de utilidades del host necesario y los controladores y firmware del adaptador.

["Herramienta de matriz de interoperabilidad de NetApp"](#)

Consideraciones sobre la reversión

Debe tener en cuenta los problemas y limitaciones de la reversión antes de iniciar una nueva versión de ONTAP.

- La reversión es disruptiva.

Durante la reversión no se puede acceder a ningún cliente. Si va a revertir un clúster de producción, asegúrese de incluir esta interrupción en su planificación.

- La reversión afecta a todos los nodos del clúster.

La reversión afecta a todos los nodos del clúster; sin embargo, la reversión debe realizarse y completarse en cada par de alta disponibilidad antes de que se reviertan otros pares de alta disponibilidad.

- La reversión se completa cuando todos los nodos ejecutan la nueva versión de destino.

Cuando el clúster tiene un estado de versión mixta, no debe introducir ningún comando que altere la operación o configuración del clúster, excepto si es necesario para cumplir con los requisitos de reversión; se permiten las operaciones de supervisión.



Si ha revertido algunos nodos, pero no todos, no intente actualizar el clúster de nuevo a la versión de origen.

- Al revertir un nodo, borra los datos almacenados en caché en un módulo Flash Cache.

Como no hay datos en caché en el módulo Flash Cache, el nodo admite solicitudes de lectura iniciales del disco, lo que provoca una disminución del rendimiento de lectura durante este período. El nodo vuelve a llenar la caché conforme sirve solicitudes de lectura.

- Una LUN de la que se realiza el backup a cinta que se ejecuta en ONTAP 9.x solo se puede restaurar a las versiones 9.x y posteriores, y no a una versión anterior.
- Si la versión actual de ONTAP admite la funcionalidad ACP (IBACP) en banda y se revierte a una versión de ONTAP que no admite IBACP, se deshabilita la ruta alternativa hacia la bandeja de discos.
- Si alguna de las máquinas virtuales de almacenamiento (SVM) utiliza LDAP, debe deshabilitarse la referencia de LDAP antes de volver a verla.
- En sistemas MetroCluster IP que usan switches compatibles con MetroCluster pero no validados con MetroCluster, la versión de ONTAP 9.7 a 9.6 resulta disruptiva, ya que no es compatible con sistemas que utilicen ONTAP 9.6 y versiones anteriores.

Cosas que verificar antes de revertir

Antes de revertir, debe comprobar el estado del clúster, el estado del almacenamiento y la hora del sistema. También debe eliminar todos los trabajos de clúster que se estén ejecutando y terminar correctamente las sesiones de SMB que no estén disponibles continuamente.

Compruebe el estado del clúster

Antes de revertir el clúster, debe comprobar que los nodos están en buen estado y que pueden participar en el clúster, así como que el clúster tiene quórum.

1. Compruebe que los nodos del clúster estén en línea y que puedan participar en el clúster: `cluster show`

```
cluster1::> cluster show
Node                Health  Eligibility
-----
node0               true    true
node1               true    true
```

Si alguno de los nodos no es saludable o no apto, compruebe los registros de EMS en busca de errores y realice acciones correctivas.

2. Establezca el nivel de privilegio en Advanced:

```
set -privilege advanced
```

Introduzca `y` para continuar.

3. Verifique los detalles de configuración de cada proceso RDB.

- Las épocas de la base de datos relacional y la base de datos deben coincidir para cada nodo.
- El maestro de quórum por anillo debe ser el mismo para todos los nodos.

Tenga en cuenta que cada anillo puede tener un maestro de quórum diferente.

| Para mostrar este proceso RDB: | Introduzca este comando... |
|--|---|
| Aplicación de gestión | <code>cluster ring show -unitname mgmt</code> |
| Base de datos de ubicación del volumen | <code>cluster ring show -unitname vlodb</code> |
| Administrador de interfaz virtual | <code>cluster ring show -unitname vifmgr</code> |
| Daemon de gestión de SAN | <code>cluster ring show -unitname bcomd</code> |

Este ejemplo muestra el proceso de la base de datos de ubicación del volumen:

```
cluster1::*> cluster ring show -unitname vlodb
Node      UnitName Epoch      DB Epoch DB Trnxs Master      Online
-----
node0     vlodb      154      154      14847   node0      master
node1     vlodb      154      154      14847   node0      secondary
node2     vlodb      154      154      14847   node0      secondary
node3     vlodb      154      154      14847   node0      secondary
4 entries were displayed.
```

4. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

5. Si va a trabajar en un entorno SAN, compruebe que cada nodo se encuentra en quórum DE SAN: `event log show -severity informational -message-name scsiblade.*`

El mensaje de evento `scsiblade` más reciente para cada nodo debe indicar que el `scsi-blade` está en quórum.

```
cluster1::*> event log show -severity informational -message-name
scsiblade.*
Time      Node      Severity      Event
-----
MM/DD/YYYY TIME node0      INFORMATIONAL scsiblade.in.quorum: The
scsi-blade ...
MM/DD/YYYY TIME node1      INFORMATIONAL scsiblade.in.quorum: The
scsi-blade ...
```

Información relacionada

Comprobación del estado del almacenamiento

Antes de revertir un clúster, debe comprobar el estado de los discos, los agregados y los volúmenes.

1. Compruebe el estado del disco:

| Para comprobar... | Realice lo siguiente... |
|---|---|
| Discos rotos | <ol style="list-style-type: none">a. Mostrar cualquier disco roto: <code>storage disk show -state broken</code>b. Retire o sustituya los discos rotos. |
| Discos sometidos a mantenimiento o reconstrucción | <ol style="list-style-type: none">a. Muestre cualquier disco en estado de mantenimiento, pendiente o reconstrucción: <code>`storage disk show -state maintenance</code> |
| pending | <code>reconstructing`</code> .. Espere a que la operación de mantenimiento o reconstrucción finalice antes de continuar. |

2. Compruebe que todos los agregados están en línea mostrando el estado del almacenamiento físico y lógico, incluidos los agregados de almacenamiento: `storage aggregate show -state !online`

Este comando muestra los agregados que *not* están en línea. Todos los agregados deben estar en línea antes y después de realizar una actualización o versión posterior principales.

```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

3. Verifique que todos los volúmenes estén en línea mostrando los volúmenes que *not* en línea: `volume show -state !online`

Todos los volúmenes deben estar en línea antes y después de realizar una actualización o versión posterior principales.

```
cluster1::> volume show -state !online
There are no entries matching your query.
```

4. Compruebe que no haya volúmenes incoherentes: `volume show -is-inconsistent true`

Consulte el artículo de la base de conocimientos "[Volumen que muestra una incoherencia de WAFL](#)" sobre la forma de abordar los volúmenes incoherentes.

Información relacionada

["Gestión de discos y agregados"](#)

Verificación de la hora del sistema

Antes de revertir, debe verificar que NTP está configurado y que la hora está sincronizada en todo el clúster.

1. Compruebe que el clúster esté asociado con un servidor NTP: `cluster time-service ntp server show`
2. Compruebe que cada nodo tiene la misma fecha y hora: `cluster date show`

```
cluster1::> cluster date show
Node          Date                Timezone
-----
node0         4/6/2013 20:54:38    GMT
node1         4/6/2013 20:54:38    GMT
node2         4/6/2013 20:54:38    GMT
node3         4/6/2013 20:54:38    GMT
4 entries were displayed.
```

Compruebe que no hay trabajos en ejecución

Antes de revertir el software ONTAP, debe comprobar el estado de los trabajos del clúster. Si cualquier trabajo de agregado, volumen, NDMP (volcado o restauración) o Snapshot (como crear, eliminar, mover, modificar, replicar, y los trabajos de montaje) están en ejecución o en cola, debe permitir que los trabajos finalicen correctamente o detener las entradas en cola.

1. Revise la lista de trabajos en ejecución o en cola de agregados, volúmenes o copias Snapshot: `job show`

```
cluster1::> job show
Job ID Name                Owing
Vserver      Node      State
-----
8629  Vol Reaper              cluster1  -      Queued
      Description: Vol Reaper Job
8630  Certificate Expiry Check
      cluster1  -      Queued
      Description: Certificate Expiry Check
.
.
.
```

2. Elimine cualquier trabajo que esté en ejecución o en cola de agregados, volúmenes o copias Snapshot:
`job delete -id job_id`

```
cluster1::> job delete -id 8629
```


3. Compruebe que no haya trabajos de agregado, volumen ni Snapshot en ejecución ni en la cola: `job show`

En este ejemplo, se han eliminado todos los trabajos en ejecución y en cola:

```
cluster1::> job show
```

| Job ID | Name | Owning Vserver | Node | State |
|---|-------------------------------|----------------|-------|---------|
| 9944 | SnapMirrorDaemon_7_2147484678 | cluster1 | node1 | Dormant |
| Description: Snapmirror Daemon for 7_2147484678 | | | | |
| 18377 | SnapMirror Service Job | cluster1 | node0 | Dormant |
| Description: SnapMirror Service Job | | | | |

2 entries were displayed

Sesiones SMB que deben finalizar

Antes de revertir, debe identificar y terminar con dignidad cualquier sesión SMB que no esté disponible de forma continua.

No es necesario terminar los recursos compartidos SMB disponibles de forma continua, a los que acceden los clientes de Hyper-V o Microsoft SQL Server con el protocolo SMB 3.0 antes de la actualización o la degradación.

1. Identifique cualquier sesión SMB establecida que no esté disponible continuamente: `vserver cifs session show -continuously-available No -instance`

Este comando muestra información detallada sobre cualquier sesión SMB que no tiene disponibilidad continua. Debe terminarlas antes de continuar con la degradación de ONTAP.

```
cluster1::> vserver cifs session show -continuously-available No
-instance

Node: node1
Vserver: vs1
Session ID: 1
Connection ID: 4160072788
Incoming Data LIF IP Address: 198.51.100.5
Workstation IP address: 203.0.113.20
Authentication Mechanism: NTLMv2
Windows User: CIFSLAB\user1
UNIX User: nobody
Open Shares: 1
Open Files: 2
Open Other: 0
Connected Time: 8m 39s
Idle Time: 7m 45s
Protocol Version: SMB2_1
Continuously Available: No
1 entry was displayed.
```

2. Si es necesario, identifique los archivos que están abiertos para cada sesión SMB que ha identificado:

```
vserver cifs session file show -session-id session_ID
```

```
cluster1::> vserver cifs session file show -session-id 1

Node:      node1
Vserver:   vs1
Connection: 4160072788
Session:   1
File      File      Open Hosting
Continuously
ID        Type      Mode Volume      Share      Available
-----
-----
1         Regular   rw   vol10      homedirshare   No
Path: \TestDocument.docx
2         Regular   rw   vol10      homedirshare   No
Path: \file1.txt
2 entries were displayed.
```

Autenticación NVMe en banda

Si va a revertir desde ONTAP 9.12.1 o posterior a ONTAP 9.12.0 o anterior, debe ["desactive la autenticación"](#)

en banda" antes de revertir. Si la autenticación en banda con DH-HMAC-CHAP no está desactivada, se producirá un error en la reversión.

¿Qué más debería comprobar antes de revertir?

Comprobaciones previas a la reversión

En función de su entorno, debe tener en cuenta ciertos factores antes de revertir. Empiece por revisar la siguiente tabla para ver qué consideraciones especiales debe tener en cuenta.

| Pregúntese... | Si su respuesta es sí, entonces haga esto... |
|---|--|
| ¿Mi clúster ejecuta SnapMirror? | <ul style="list-style-type: none">• Revisar las consideraciones de revertir sistemas con relaciones de SnapMirror síncrono• Consulte los requisitos de la modificación de versiones para relaciones de SnapMirror y SnapVault |
| ¿Mi clúster ejecuta SnapLock? | Establezca los períodos de compromiso automático |
| ¿Hay volúmenes FlexClone divididos? | Intercambio físico de bloques inverso |
| ¿Tengo volúmenes FlexGroup? | Deshabilite la funcionalidad Qtree |
| ¿Tengo servidores CIFS en modo grupo de trabajo? | Mover o eliminar servidores CIFS en modo Workgroup |
| ¿Tengo volúmenes deduplicados? | Comprobar que el volumen contiene suficiente espacio libre |
| ¿Tengo copias Snapshot? | Preparar copias de Snapshot |
| ¿Estoy volviendo a ONTAP 8.3.x? | Identifique las cuentas de usuario que utilizan la función hash SHA-2 |
| ¿La protección contra ransomware se configuró para ONTAP 9.11.1 o posterior? | Compruebe las licencias antiransomware |
| ¿Está configurado el acceso multiprotocolo de S3 para ONTAP 9.12.1 o posterior? | Quitar la configuración de bloque NAS de S3 |
| ¿Está configurada la conexión troncal de sesiones de NFSv4,1 para ONTAP 9.14.1 o posterior? | Elimine la configuración de troncalización de sesión NFSv4,1 |

Comprobaciones previas a la reversión de MetroCluster

Según la configuración de MetroCluster, debe tener en cuenta ciertos factores antes de revertir. Empiece por revisar la siguiente tabla para ver qué consideraciones especiales debe tener en cuenta.

| Pregúntese... | Si su respuesta es sí, entonces haga esto... |
|--|---|
| ¿Tengo una configuración MetroCluster de dos o cuatro nodos? | Deshabilitar la conmutación automática sin planificar |

| Pregúntese... | Si su respuesta es sí, entonces haga esto... |
|---|--|
| ¿Tengo una configuración MetroCluster IP o estructural de cuatro u ocho nodos que ejecute ONTAP 9.12.1 o posterior? | Deshabilite IPsec |

SnapMirror

Consideraciones que tener en cuenta para revertir sistemas con relaciones de SnapMirror síncrono

Debe estar al tanto de las consideraciones para las relaciones de SnapMirror síncrono antes de revertir de ONTAP 9.6 a ONTAP 9.5.

Antes de revertir, debe realizar los siguientes pasos si tiene relaciones de SnapMirror síncrono:

- Debe eliminar cualquier relación de SnapMirror Synchronous en la que el volumen de origen esté sirviendo datos mediante NFSv4 o SMB.

ONTAP 9.5 no admite NFSv4 y SMB.

- Debe eliminar todas las relaciones de SnapMirror síncrono en una puesta en marcha en cascada de reflejos.

No se admite una puesta en marcha en cascada de reflejos mediante relaciones de SnapMirror síncrono en ONTAP 9.5.

- Si las copias Snapshot comunes en ONTAP 9.5 no están disponibles durante la reversión, debe inicializar la relación de SnapMirror síncrono después de revertir.

Tras dos horas de actualización a ONTAP 9.6, las copias Snapshot comunes de ONTAP 9.5 se reemplazan automáticamente por las copias Snapshot comunes de ONTAP 9.6. Por lo tanto, no puede volver a sincronizar la relación de SnapMirror síncrono tras revertir si las copias Snapshot comunes de ONTAP 9.5 no están disponibles.

Requisitos de nueva versión para relaciones de SnapMirror y SnapVault

El comando de reversión del nodo del sistema le notifica cualquier relación de SnapMirror y SnapVault que sea necesario eliminar o reconfigurar para que se complete el proceso de nueva versión. Sin embargo, debe tener en cuenta estos requisitos antes de iniciar la reversión.

- Todas las relaciones de reflejo de protección de datos y SnapVault deben ponerse en modo inactivo y después romperse.

Una vez completada la reversión, puede volver a sincronizar y reanudar estas relaciones si existe una copia Snapshot común.

- Las relaciones de SnapVault no deben contener los siguientes tipos de políticas de SnapMirror:

- reflejo asíncrono

Debe eliminar cualquier relación que utilice este tipo de política.

- Reflejo de AndVault

Si alguna de estas relaciones existe, debe cambiar la política de SnapMirror a mirror-vault.

- Se deben eliminar todas las relaciones de reflejo con uso compartido de carga y los volúmenes de destino.
- Deben eliminarse las relaciones de SnapMirror con volúmenes de destino de FlexClone.
- Debe deshabilitarse la compresión de red para cada política de SnapMirror.
- La regla `all_source_snapshot` debe eliminarse de cualquier política de SnapMirror de tipo reflejo asíncrono.



Las operaciones de restauración de snapshot de archivo único (SFSR) y de restauración de snapshot de archivo parcial (PFSR) se obsoletos en el volumen raíz.

- Todas las operaciones de restauración de archivo único y de snapshot que se estén ejecutando actualmente deben completarse antes de que pueda continuar la reversión.

Puede esperar a que finalice la operación de restauración o anularla.

- Todas las operaciones incompletas de restauración de archivos individuales y Snapshot deben eliminarse mediante el comando `snapmirror restore`.

Configure periodos de confirmación automática para volúmenes SnapLock antes de revertir

Para revertir a ONTAP 9, el valor del período de compromiso automático para los volúmenes de SnapLock se debe establecer en horas, no días. Antes de intentar la reversión, debe comprobar el valor de compromiso automático de los volúmenes SnapLock y modificarlo de días a horas, de ser necesario.

1. Compruebe que haya volúmenes SnapLock en el clúster que tengan periodos de compromiso automático no compatibles:
`volume snaplock show -autocommit-period *days`
2. Modifique los periodos de compromiso automático no compatibles a horas:
`volume snaplock modify -vserver vs_server_name -volume volume_name -autocommit-period value hours`

Revierta el uso compartido de bloques físicos en volúmenes FlexClone separados

Si dividió un volumen FlexClone de su volumen principal, se deberá deshacer el uso compartido de cualquier bloque físico entre el clon y su volumen principal antes de revertir desde ONTAP 9.4 o una versión posterior de ONTAP.

Esta tarea solo es aplicable a sistemas AFF cuando se ha ejecutado la división en alguno de los volúmenes FlexClone.

1. Inicie sesión en el nivel de privilegio avanzado: `set -privilege advanced`
2. Identifique los volúmenes FlexClone divididos con bloques físicos compartidos: `volume clone sharing-by-split show`

```
cluster1::> volume clone sharing-by-split show
```

| Node | Vserver | Volume | Aggregate |
|-------|---------|------------|-----------|
| node1 | vs1 | vol_clone1 | aggr1 |
| node2 | vs2 | vol_clone2 | aggr2 |

2 entries were displayed.

3. Deshace el uso compartido de bloques físicos en todos los volúmenes FlexClone divididos por el clúster:
`volume clone sharing-by-split undo start-all`
4. Compruebe que no hay volúmenes FlexClone divididos con bloques físicos compartidos: `volume clone sharing-by-split show`

```
cluster1::> volume clone sharing-by-split show
```

This table is currently empty.

Deshabilite la funcionalidad Qtree en volúmenes FlexGroup antes de revertir

Los qtrees de volúmenes de FlexGroup no son compatibles antes de ONTAP 9.3. Debe deshabilitar la funcionalidad para qtrees en volúmenes de FlexGroup antes de revertir de ONTAP 9.3 a una versión anterior de ONTAP.

La funcionalidad Qtree se habilita al crear un qtree o si se modifican los atributos de estilo de seguridad y modo oplock del qtree predeterminado.

1. Identifique y elimine todos los qtrees no predeterminados en cada volumen de FlexGroup que estén habilitados con la funcionalidad Qtree:
 - a. Inicie sesión en el nivel de privilegio avanzado: `set -privilege advanced`
 - b. Compruebe si hay algún volumen de FlexGroup habilitado con la funcionalidad Qtree.

Para ONTAP 9.6 o posterior, utilice: `volume show -is-qtree-caching-enabled true`

Para ONTAP 9.5 o anterior, utilice: `volume show -is-flexgroup-qtree-enabled true`

```
cluster1::*> volume show -is-flexgroup-qtree-enabled true
```

| Vserver | Volume | Aggregate | State | Type | Size |
|-----------|--------|-----------|--------|------|-------|
| Available | Used% | | | | |
| vs0 | fg | - | online | RW | 320MB |
| 220.4MB | 31% | | | | |

- c. Elimine todos los qtrees no predeterminados de cada volumen de FlexGroup que estén habilitados con la funcionalidad de qtree: `volume qtree delete -vserver svm_name -volume volume_name`

```
-qtree qtree_name
```

Si la funcionalidad Qtree se encuentra habilitada porque se modificaron los atributos del qtree predeterminado y, si no tiene ningún qtree, puede omitir este paso.

```
cluster1::*> volume qtree delete -vserver vs0 -volume fg -qtree qtree4
WARNING: Are you sure you want to delete qtree qtree4 in volume fg
vserver vs0? {y|n}: y
[Job 38] Job is queued: Delete qtree qtree4 in volume fg vserver vs0.
```

2. Deshabilite la funcionalidad Qtree en cada volumen FlexGroup: `volume flexgroup qtree-disable -vserver svm_name -volume volume_name`

```
cluster1::*> volume flexgroup qtree-disable -vserver vs0 -volume fg
```

3. Identificar y eliminar cualquier copia de Snapshot que esté habilitada con la funcionalidad de qtree.

- a. Compruebe si hay alguna copia Snapshot habilitada con la funcionalidad para qtrees: `volume snapshot show -vserver vserver_name -volume volume_name -fields is-flexgroup-qtree-enabled`

```
cluster1::*> volume snapshot show -vserver vs0 -volume fg -fields is-
flexgroup-qtree-enabled
vserver volume snapshot is-flexgroup-qtree-enabled
-----
vs0      fg      fg_snap1 true
vs0      fg      daily.2017-09-27_0010 true
vs0      fg      daily.2017-09-28_0010 true
vs0      fg      snapmirror.0241f354-a865-11e7-a1c0-
00a098a71764_2147867740.2017-10-04_124524 true
```

- b. Elimine todas las copias Snapshot que están habilitadas con la funcionalidad para qtrees: `volume snapshot delete -vserver svm_name -volume volume_name -snapshot snapshot_name -force true -ignore-owners true`

Las copias Snapshot que deben eliminarse incluyen copias Snapshot regulares y las copias Snapshot realizadas para relaciones de SnapMirror. Si ha creado alguna relación de SnapMirror para los volúmenes de FlexGroup con un clúster de destino que ejecute ONTAP 9.2 o una versión anterior, debe eliminar todas las copias de Snapshot que se realizaron cuando se habilitó el volumen de FlexGroup de origen para la funcionalidad de qtree.

```
cluster1::> volume snapshot delete -vserver vs0 -volume fg -snapshot
daily.2017-09-27_0010 -force true -ignore-owners true
```

Información relacionada

["Gestión de volúmenes de FlexGroup"](#)

Identificar y mover servidores SMB en modo de grupo de trabajo

Antes de realizar una reversión, debe eliminar cualquier servidor SMB en modo de grupo de trabajo o moverlos a un dominio. El modo de grupo de trabajo no es compatible con las versiones de ONTAP anteriores a ONTAP 9.

1. Identificar cualquier servidor SMB con un estilo de autenticación de grupo de trabajo: `vserver cifs show`
2. Mueva o elimine los servidores identificados:

| Si va a... | A continuación, utilice este comando.... |
|--|--|
| Mover el servidor SMB del grupo de trabajo a un dominio de Active Directory: | <code>vserver cifs modify -vserver <i>vserver_name</i> -domain <i>domain_name</i></code> |
| Elimine el servidor SMB | <code>vserver cifs delete -vserver <i>vserver_name</i></code> |

3. Si eliminó el servidor SMB, introduzca el nombre de usuario del dominio y la contraseña de usuario.

Información relacionada

["Gestión de SMB"](#)

Verifique que los volúmenes deduplicados tengan suficiente espacio libre antes de revertir

Antes de revertir desde cualquier versión de ONTAP 9, debe asegurarse de que los volúmenes contengan espacio libre suficiente para la operación de reversión.

El volumen debe tener suficiente espacio para acomodar el ahorro que se obtuvo mediante la detección en línea de bloques de ceros. Consulte el artículo de la base de conocimientos ["Cómo observar ahorros de espacio gracias a la deduplicación, la compresión y la compactación en ONTAP 9"](#).

Si se habilitó tanto la deduplicación como la compresión de datos en un volumen que se desea revertir, se debe revertir la compresión de datos antes de revertir la deduplicación.

1. Use el comando `volume Efficiency show` con la opción `-fields` para ver el progreso de las operaciones de eficiencia que se están ejecutando en los volúmenes.

El siguiente comando muestra el progreso de las operaciones de eficiencia: `volume efficiency show -fields vserver,volume,progress`

2. Use el comando `volume Efficiency stop` con la opción `-all` para detener todas las operaciones de deduplicación activas y en cola.

El siguiente comando detiene todas las operaciones de deduplicación activas y en cola en el volumen `Vola`: `volume efficiency stop -vserver vs1 -volume Vola -all`

3. Utilice el comando `set -Privilege Advanced` para iniciar sesión en el nivel de privilegio avanzado.

4. La eficiencia de volumen se debe usar con la opción `-version` para degradar los metadatos de eficiencia de un volumen a una versión específica de ONTAP.

El siguiente comando revierte los metadatos de eficiencia del volumen Vola a ONTAP 9.x: `volume efficiency revert-to -vserver vs1 -volume VolA -version 9.x`



El comando de reversión de la eficiencia del volumen revierte los volúmenes presentes en el nodo en el que se ejecuta este comando. Este comando no revierte volúmenes entre nodos.

5. El comando `volume Efficiency show` se utiliza con la opción `-op-status` para supervisar el progreso de la degradación.

El siguiente comando supervisa y muestra el estado de la degradación: `volume efficiency show -vserver vs1 -op-status Downgrading`

6. Si la reversión no se realiza correctamente, use el comando `volume Efficiency show` con la opción `-instance` para ver por qué ha fallado la reversión.

El siguiente comando muestra información detallada sobre todos los campos: `volume efficiency show -vserver vs1 -volume voll - instance`

7. Una vez finalizada la operación de reversión, vuelva al nivel de privilegio de administrador: `set -privilege admin`

["Gestión de almacenamiento lógico"](#)

Prepare las copias Snapshot antes de revertir

Antes de revertir a una versión de ONTAP anterior, debe deshabilitar todas las políticas de copia de Snapshot y eliminar las copias de Snapshot que se crearon después de actualizar a la versión actual.

Si va a revertir en un entorno de SnapMirror, primero debe eliminar las siguientes relaciones de reflejo:

- Todas las relaciones de mirroring de uso compartido de carga
- Todas las relaciones de mirroring de protección de datos que se crearon en ONTAP 8.3.x.
- Todas las relaciones de mirroring de protección de datos si el clúster se volvió a crear en ONTAP 8.3.x.
 - a. Deshabilite las políticas de copia Snapshot para todas las SVM de datos: `volume snapshot policy modify -vserver * -enabled false`
 - b. Deshabilite las políticas de copia Snapshot para los agregados de cada nodo:
 - i. Identifique los agregados del nodo mediante el comando `run-nodenodenameaggr status`.
 - ii. Deshabilite la política de copia Snapshot de cada agregado: `run -node nodename aggr options aggr_name nosnap on`
 - iii. Repita este paso con cada uno de los nodos restantes.
 - c. Deshabilite las políticas de copia Snapshot para el volumen raíz de cada nodo:
 - i. Identifique el volumen raíz del nodo mediante el comando `run-nodenodesmalevol status`.

El volumen raíz se identifica por la palabra `root` en la columna `Options` del resultado del comando `vol status`.

```
vs1::> run -node node1 vol status
```

| Volume | State | Status | Options |
|--------|--------|-------------------------|-----------------|
| vol0 | online | raid_dp, flex 64-bit | root, nvfail=on |

- i. Deshabilite la política de copia Snapshot en el volumen raíz: `run -node nodename vol options root_volume_name nosnap on`
- ii. Repita este paso con cada uno de los nodos restantes.
- d. Elimine todas las copias Snapshot que se crearon después de actualizar a la versión actual:
 - i. Configure el nivel de privilegio en Advanced: `set -privilege advanced`
 - ii. Desactive las instantáneas: `snapshot policy modify -vserver * -enabled false`
 - iii. Elimine las copias Snapshot de la versión más reciente del nodo: `volume snapshot prepare-for-revert -node nodename`

Este comando elimina las copias Snapshot de una versión más reciente en cada volumen de datos, agregado raíz y volumen raíz.

Si alguna copia de Snapshot no se puede eliminar, el comando falla y notifica las acciones necesarias que debe realizar para poder eliminar las copias de Snapshot. Debe completar las acciones necesarias y volver a ejecutar el comando `prepare-for-revert` de la snapshot del volumen antes de continuar con el siguiente paso.

```
cluster1::*> volume snapshot prepare-for-revert -node node1
```

```
Warning: This command will delete all Snapshot copies that have the
format used by the current version of ONTAP. It will fail if any
Snapshot copy polices are enabled, or
if any Snapshot copies have an owner. Continue? {y|n}: y
```

- i. Compruebe que las copias Snapshot se han eliminado: `volume snapshot show -node nodename`

Si queda alguna copia Snapshot de la versión más reciente, obligue a eliminar: `volume snapshot delete {-fs-version 9.0 -node nodename -is-constituent true} -ignore-owners -force`

- ii. Repita este paso c para cada uno de los nodos restantes.
- iii. Vuelva al nivel de privilegio de administrador: `set -privilege admin`



Estos pasos deben ejecutarse en los dos clústeres de la configuración de MetroCluster.

Identifique las cuentas de usuario que utilizan la función hash SHA-2

Si va a revertir de ONTAP 9.1 o ONTAP 9.0 a ONTAP 8.3.x, los usuarios de cuentas SHA-2 ya no podrán autenticarse con sus contraseñas. Antes de revertir, debe identificar las cuentas de usuario que utilizan la función hash SHA-2, de modo que, después de revertir, pueda hacer que restablezcan sus contraseñas para utilizar el tipo de cifrado (MD5) admitido por la versión a la que se revierte.

1. Cambie a la configuración de privilegio a avanzado: `set -privilege advanced`
2. Identifique las cuentas de usuario que utilizan SHA-2 tiene función: `security login show -vserver * -username * -application * -authentication-method password -hash-function !md5`
3. Conserve el resultado del comando para utilizarlo después de la reversión.



Durante la reversión, se le pedirá que ejecute el comando `Advanced security login password-prepare-to-downgrade` Para restablecer su propia contraseña para utilizar la función hash MD5. Si su contraseña no está cifrada con MD5, el comando le solicita una nueva contraseña y la cifra con MD5, lo que permite autenticar su credencial después de la reversión.

Compruebe las licencias de protección contra ransomware autónomas antes de volver de ONTAP 9.11.1 o posterior

Si configuró la protección de ransomware autónoma (ARP) y revierte de ONTAP 9.11.1 o una versión posterior a ONTAP 9.10.1 o una versión anterior, puede experimentar mensajes de advertencia y funcionalidad ARP limitada.

En ONTAP 9.11.1, la licencia Anti-ransomware reemplazó la licencia de gestión de claves multi-tenant (MTKM). Si el sistema tiene la licencia Anti_ransomware pero no tiene licencia MT_EK_MGMT, verá una advertencia durante la reversión de que ARP no puede habilitarse en volúmenes nuevos al revertir.

Los volúmenes con protección existente seguirán funcionando normalmente después de la reversión y el estado ARP puede mostrarse con la interfaz de línea de comandos ONTAP. System Manager no puede mostrar el estado de ARP sin la licencia de MTKM.

Por lo tanto, si desea que ARP continúe después de revertir a ONTAP 9.10.1, asegúrese de que la licencia MTKM está instalada antes de revertir. ["Más información sobre las licencias de ARP."](#)

Quite la configuración de bloque NAS de S3 antes de revertir de ONTAP 9.12.1 o posterior

Si ha configurado el acceso de cliente S3 para datos de NAS, antes de revertir desde ONTAP 9.12.1 o posterior a ONTAP 9.11.1 o versiones anteriores, debe usar la interfaz de línea de comandos (CLI) de ONTAP para quitar la configuración de bucket NAS y para eliminar cualquier asignación de nombre (S3 usuarios para usuarios Windows o Unix).

Acerca de esta tarea

Las siguientes tareas se completan en segundo plano durante el proceso de reversión.

- Quite todas las creaciones de objetos singleton completadas parcialmente (es decir, todas las entradas de directorios ocultos).

- Quite todos los directorios ocultos; puede haber uno en cada volumen al que se pueda acceder desde la raíz de la exportación asignada desde el bloque NAS de S3.
- Retire la tabla de carga.
- Elimine los valores de usuario predeterminados de unix-user y Windows-default para todos los servidores S3 configurados.

Pasos

1. Eliminar la configuración del bucket NAS de S3:

```
vserver object-store-server bucket delete -vserver _svm_name_ -bucket
_s3_nas_bucket_name_
```

2. Eliminar asignaciones de nombres para UNIX:

```
vserver name-mapping delete -vserver _svm_name_ -direction s3-unix
```

3. Eliminar asignaciones de nombres para Windows:

```
vserver name-mapping delete -vserver _svm_name_ -direction s3-win
```

4. Quite los protocolos S3 de la SVM:

```
vserver remove-protocols -vserver <svm_name> -protocols s3
```

Elimine la configuración de trunking de sesión NFSv4,1 antes de revertir desde ONTAP 9.14.1 o una versión posterior

Si ha activado la conexión troncal para las conexiones de cliente y vuelve a una versión anterior a ONTAP 9.14.1, debe deshabilitar la conexión troncal en cualquier servidor NFSv4,1 antes de revertir.

Cuando introduzca la `revert-to` comando, verá un mensaje de advertencia para informarle de que deshabilite la conexión troncal antes de continuar.

Después de volver a una versión anterior de ONTAP, los clientes que utilizan conexiones troncalizadas vuelven a utilizar una única conexión. El rendimiento de sus datos se verá afectado, pero no habrá interrupción. El comportamiento de reversión es el mismo que modificar la opción de Trunking NFSv4,1 para la SVM de enabled a disabled.

Pasos

1. Desactive la troncalización en el servidor NFSv4,1:

```
vserver nfs modify -vserver svm_name -v4.1-trunking disabled
```

2. Compruebe que NFS está configurado como desee:

```
vserver nfs show -vserver svm_name
```

Deshabilite la conmutación de sitios no planificada automática antes de revertir las configuraciones de MetroCluster de dos y cuatro nodos

Antes de revertir una configuración de MetroCluster de dos o cuatro nodos, se debe deshabilitar la conmutación automática sin planificar (AUSO).

1. En los dos clústeres de MetroCluster, deshabilite la conmutación automática no planificada:

```
metrocluster modify -auto-switchover-failure-domain auso-disabled
```

Información relacionada

["Gestión y recuperación ante desastres de MetroCluster"](#)

Deshabilite IPsec antes de revertir las configuraciones de MetroCluster

Antes de revertir una configuración de MetroCluster, debe deshabilitar IPsec.

No puede revertir ONTAP en una configuración de MetroCluster que ejecute ONTAP 9.12.1 con IPsec habilitada. Antes de revertir, se realiza una comprobación para asegurarse de que no hay configuraciones IPsec en la configuración de MetroCluster. Debe eliminar cualquier configuración IPsec presente y deshabilitar IPsec antes de continuar con el proceso de reversión. Revertir ONTAP se bloquea si IPsec está habilitada, incluso cuando no se ha configurado ninguna directiva de usuario.

Descargue e instale la imagen del software de ONTAP

Primero, tiene que descargar el software ONTAP del sitio de soporte de NetApp; entonces puede instalarlo.

Descargue la imagen del software

Para degradar o revertir de ONTAP 9.4 y versiones posteriores, puede copiar la imagen del software ONTAP del sitio de soporte de NetApp a una carpeta local. Para una degradación o para revertir a ONTAP 9.3 o una versión anterior, debe copiar la imagen del software ONTAP en un servidor HTTP o FTP de la red.

Debe tener en cuenta la siguiente información importante:

- Las imágenes de software son específicas para los modelos de la plataforma.

Debe obtener la imagen correcta para su clúster. Las imágenes de software, la información de versión de firmware y el firmware más reciente para el modelo de su plataforma están disponibles en el sitio de soporte de NetApp.

- Las imágenes de software incluyen la versión más reciente del firmware del sistema disponible cuando se publicó una versión concreta de ONTAP.
- Si va a cambiar a un sistema con el cifrado de volúmenes de NetApp desde ONTAP 9.5 o posterior, debe descargar la imagen del software ONTAP para países no restringidos, que incluye el cifrado de volúmenes de NetApp.

Si utiliza la imagen de software de ONTAP para países restringidos a fin de degradar o revertir un sistema con el cifrado de volúmenes de NetApp, el sistema tendrá una alarma y perderá el acceso a los volúmenes.

- a. Busque el software ONTAP de destino en la ["Descargas de software"](#) Del sitio de soporte de NetApp.

b. Copie la imagen del software.

- Para ONTAP 9.3 o una versión anterior, copie la imagen de software (por ejemplo, 93_q_image.tgz) del sitio de soporte de NetApp en el directorio del servidor HTTP o FTP a partir del que se servirá la imagen.
- Para ONTAP 9.4 o posterior, copie la imagen de software (por ejemplo, 97_q_image.tgz) del sitio de soporte de NetApp en el directorio del servidor HTTP o FTP a partir del que se servirá la imagen o en una carpeta local.

Instale la imagen del software

Debe instalar la imagen de software de destino en los nodos del clúster.

- Si va a degradar o revertir un sistema con cifrado de volumen de NetApp desde ONTAP 9.5 o posterior, debe haber descargado la imagen del software ONTAP para países no restringidos, que incluye el cifrado de volúmenes de NetApp.

Si utiliza la imagen de software de ONTAP para países restringidos a fin de degradar o revertir un sistema con el cifrado de volúmenes de NetApp, el sistema tendrá una alarma y perderá el acceso a los volúmenes.

- a. Establezca el nivel de privilegio en avanzado, introduzca **y** cuando se le solicite continuar: `set -privilege advanced`

El aviso avanzado (*>) aparece.

- b. Instale la imagen de software en los nodos.

Este comando descarga e instala la imagen de software en todos los nodos al mismo tiempo. Para descargar e instalar la imagen en cada nodo de uno en uno, no especifique el parámetro `-background`.

- Si va a degradar o revertir una configuración que no sea de MetroCluster o una configuración de MetroCluster de dos nodos: `system node image update -node * -package location -replace-package true -setdefault true -background true`

Este comando utiliza una consulta ampliada para cambiar la imagen de software de destino, que se instala como imagen alternativa, para que sea la imagen predeterminada del nodo.

- Si va a revertir una configuración MetroCluster de cuatro u ocho nodos, debe emitir el siguiente comando en ambos clústeres: `system node image update -node * -package location -replace-package true true -background true -setdefault false`

Este comando utiliza una consulta ampliada para cambiar la imagen de software de destino, que se instala como la imagen alternativa en cada nodo.

- c. Introduzca **y** para continuar cuando se le solicite.

- d. Compruebe que la imagen de software se haya descargado e instalado en cada nodo: `system node image show-update-progress -node *`

Este comando muestra el estado actual de la descarga e instalación de la imagen de software. Debe continuar ejecutando este comando hasta que todos los nodos informen sobre un estado de ejecución de salida y un estado de salida correcto.

El comando de actualización de imagen del nodo del sistema puede fallar y mostrar mensajes de error

o advertencia. Después de resolver errores o advertencias, puede volver a ejecutar el comando.

Este ejemplo muestra un clúster de dos nodos en el cual la imagen de software se descarga y se instala correctamente en ambos nodos:

```
cluster1::*> system node image show-update-progress -node *
There is no update/install in progress
Status of most recent operation:
    Run Status:      Exited
    Exit Status:     Success
    Phase:           Run Script
    Exit Message:    After a clean shutdown, image2 will be set as
the default boot image on node0.
There is no update/install in progress
Status of most recent operation:
    Run Status:      Exited
    Exit Status:     Success
    Phase:           Run Script
    Exit Message:    After a clean shutdown, image2 will be set as
the default boot image on node1.
2 entries were acted on.
```

Revertir un clúster de ONTAP

Para desconectar el clúster y volver a una versión ONTAP anterior, debe deshabilitar la conmutación por error del almacenamiento y los LIF de datos, abordar las condiciones previas para la reversión, revertir la configuración del clúster y del sistema de archivos en un nodo y, a continuación, repetir el proceso para cada nodo adicional del clúster.

Debe haber completado la reversión "[verificaciones](#)" y.. "[comprobaciones previas](#)".

Al revertir un clúster se necesita que el clúster se desconecte durante la duración de la versión re.

1. Configure el nivel de privilegio en Advanced: `set -privilege advanced`

Introduzca **y** cuando se le solicite continuar.

2. Compruebe que el software ONTAP de destino está instalado: `system image show`

El siguiente ejemplo muestra que la versión 9.1 está instalada como imagen alternativa en ambos nodos:

```
cluster1::*> system image show
```

| Node | Image | Is Default | Is Current | Version | Install Date |
|-------|--------|---------------|---------------|---------|-----------------|
| node0 | image1 | true | true | 9.2 | MM/DD/YYYY TIME |
| | image2 | false | false | 9.1 | MM/DD/YYYY TIME |
| node1 | image1 | true | true | 9.2 | MM/DD/YYYY TIME |
| | image2 | false | false | 9.1 | MM/DD/YYYY TIME |

4 entries were displayed.

3. Deshabilite todas las LIF de datos del clúster: `network interface modify {-role data} -status-admin down`
4. Determinar si tiene relaciones de FlexCache entre clústeres: `flexcache origin show-caches -relationship-type inter-cluster`
5. Si hay destellos entre clústeres, deshabilite los datos del clúster de caché: `network interface modify -vserver vservice_name -lif lif_name -status-admin down`
6. Si el clúster consta de solo dos nodos, deshabilite el clúster de alta disponibilidad: `cluster ha modify -configured false`
7. deshabilite la recuperación tras fallos del almacenamiento para los nodos del par de alta disponibilidad de cualquiera de los nodos: `storage failover modify -node nodename -enabled false`

Solo tiene que deshabilitar la conmutación por error del almacenamiento una vez para el par de alta disponibilidad. Cuando deshabilita la conmutación al respaldo de almacenamiento para un nodo, la conmutación al respaldo de almacenamiento también se deshabilita en el compañero de nodo.

8. Inicie sesión en el nodo que desea revertir.

Para revertir un nodo, debe haber iniciado sesión en el clúster a través de la LIF de gestión del nodo del nodo.

9. Establezca la imagen de software ONTAP de destino del nodo en ser la imagen predeterminada: `system image modify -node nodename -image target_image -isdefault true`
10. Verifique que la imagen del software de ONTAP de destino se esté establecida como la imagen predeterminada del nodo que está revirtiendo: `system image show`

En el siguiente ejemplo, se muestra que la versión 9.1 se establece como la imagen predeterminada en el nodo 0:


```
cluster1::*> system image show
```

| Node | Image | Is Default | Is Current | Version | Install Date |
|-------|--------|------------|------------|---------|-----------------|
| node0 | image1 | false | true | 9.2 | MM/DD/YYYY TIME |
| | image2 | true | false | 9.1 | MM/DD/YYYY TIME |
| node1 | image1 | true | true | 9.2 | MM/DD/YYYY TIME |
| | image2 | false | false | 9.1 | MM/DD/YYYY TIME |

4 entries were displayed.

11. Si el clúster solo consta de dos nodos, compruebe que el nodo no esté configurado con *épsilon*:

a. Compruebe si el nodo está actualmente configurado con *épsilon*: `cluster show -node nodename`

En el siguiente ejemplo se muestra que el nodo está configurado con *épsilon*:

```
cluster1::*> cluster show -node node1
```

```
Node: node1
UUID: 026efc12-ac1a-11e0-80ed-0f7eba8fc313
Epsilon: true
Eligibility: true
Health: true
```

a. Si el nodo no está configurado con *épsilon*, márkelo como falso en el nodo para que se pueda transferir el valor *épsilon* al partner del nodo: `cluster modify -node nodenameA -epsilon false`

b. Transfiera el valor *épsilon* al partner del nodo marcando *épsilon* true en el nodo del partner: `cluster modify -node nodenameB -epsilon true`

12. Compruebe que el nodo esté listo para la nueva versión: `system node revert-to -node nodename -check-only true -version 9.x`

El parámetro `check-only` identifica las condiciones previas que se deben abordar antes de revertir, como los siguientes ejemplos:

- Deshabilitar la recuperación tras fallos del almacenamiento
- Deshabilitar la política de Snapshot
- Eliminar copias de Snapshot que se crearon después de actualizar a la versión posterior de ONTAP

13. Compruebe que se han tratado todas las condiciones previas: `system node revert-to -node nodename -check-only true -version 9.x`

14. Revierte la configuración del clúster del nodo: `system node revert-to -node nodename -version 9.x`

La opción `-version` hace referencia a la versión de destino. Por ejemplo, si el software que ha instalado y verificado es ONTAP 9.1, el valor correcto de la opción `-version` es 9.1.

La configuración del clúster se revierte y luego se cierra la sesión en el `clustershell`.

15. Vuelva a iniciar sesión en el `clustershell` y, a continuación, cambie al `nodeshell`: `run -node nodename`

Después de iniciar sesión de nuevo en el `clustershell`, puede tardar unos minutos antes de que esté listo para aceptar el comando `nodeshell`. Por lo tanto, si el comando falla, espere unos minutos y vuelva a intentarlo.

16. Revierte la configuración del sistema de archivos del nodo: `revert_to 9.x`

Este comando verifica que la configuración del sistema de archivos del nodo está lista para revertirse y después lo revierte. Si se identifican las condiciones previas, debe abordarlas y a continuación, vuelva a ejecutar el comando `revert_to`.



El uso de una consola del sistema para supervisar el proceso de reversión muestra más detalles que los que se ven en el infierno.

Si se cumple LA FUNCIÓN AUTOBOOT, cuando el comando finaliza, el nodo se reiniciará en ONTAP.

Si el INICIO AUTOMÁTICO es falso, cuando el comando finaliza el símbolo del sistema del CARGADOR se muestra. Introduzca `yes` para revertir y después usarlo `boot_ontap` para reiniciar manualmente el nodo.

17. Cuando el nodo se haya reiniciado, confirme que el nuevo software está en ejecución: `system node image show`

En el siguiente ejemplo, `image1` es la nueva versión de ONTAP y se establece como la versión actual del nodo 0:

```
cluster1::*> system node image show
```

| Node | Image | Is Default | Is Current | Version | Install Date |
|-------|--------|------------|------------|---------|-----------------|
| node0 | | | | | |
| | image1 | true | true | X.X.X | MM/DD/YYYY TIME |
| | image2 | false | false | Y.Y.Y | MM/DD/YYYY TIME |
| node1 | | | | | |
| | image1 | true | false | X.X.X | MM/DD/YYYY TIME |
| | image2 | false | true | Y.Y.Y | MM/DD/YYYY TIME |

4 entries were displayed.

18. Compruebe que el estado de reversión se ha completado para cada nodo: `system node upgrade-revert show -node nodename`

El estado debe aparecer como Finalizado, No Necesario o No hay ninguna entrada de tabla devuelta.

19. Repetición [\[step-6\]](#) por [\[step-16\]](#) En el otro nodo del par de alta disponibilidad.

- 20. Si el clúster consta de solo dos nodos, vuelva a habilitar el clúster de alta disponibilidad: `cluster ha modify -configured true`
- 21. vuelva a activar la recuperación tras fallos de almacenamiento en ambos nodos si se deshabilitó anteriormente: `storage failover modify -node nodename -enabled true`
- 22. Repetición [\[step-5\]](#) por [\[step-19\]](#) Para cada par de alta disponibilidad adicional y ambos clústeres en Configuración de MetroCluster.

¿Qué debo hacer luego de revertir mi clúster?

Verifique el estado del clúster y del almacenamiento después de la degradación o la reversión

Después de degradar o revertir un clúster, debe comprobar que los nodos estén en buen estado y que puedan participar en el clúster, así como que el clúster esté de quórum. También debe verificar el estado de los discos, los agregados y los volúmenes.

Compruebe el estado del clúster

- 1. Compruebe que los nodos del clúster estén en línea y que puedan participar en el clúster: `cluster show`

```
cluster1::> cluster show
Node                      Health  Eligibility
-----
node0                     true   true
node1                     true   true
```

Si alguno de los nodos no es saludable o no apto, compruebe los registros de EMS en busca de errores y realice acciones correctivas.

- 2. Establezca el nivel de privilegio en Advanced:
`set -privilege advanced`

Introduzca `y` para continuar.

- 3. Verifique los detalles de configuración de cada proceso RDB.
 - Las épocas de la base de datos relacional y la base de datos deben coincidir para cada nodo.
 - El maestro de quórum por anillo debe ser el mismo para todos los nodos.

Tenga en cuenta que cada anillo puede tener un maestro de quórum diferente.

| Para mostrar este proceso RDB: | Introduzca este comando... |
|--|---|
| Aplicación de gestión | <code>cluster ring show -unitname mgmt</code> |
| Base de datos de ubicación del volumen | <code>cluster ring show -unitname vldb</code> |
| Administrador de interfaz virtual | <code>cluster ring show -unitname vifmgr</code> |

| | |
|---------------------------------------|--|
| Para mostrar este proceso RDB: | Introduzca este comando... |
| Daemon de gestión de SAN | <code>cluster ring show -unitname bcomd</code> |

Este ejemplo muestra el proceso de la base de datos de ubicación del volumen:

```
cluster1::*> cluster ring show -unitname vlodb
```

| Node | UnitName | Epoch | DB Epoch | DB Trnxs | Master | Online |
|-------|----------|-------|----------|----------|--------|-----------|
| node0 | vlodb | 154 | 154 | 14847 | node0 | master |
| node1 | vlodb | 154 | 154 | 14847 | node0 | secondary |
| node2 | vlodb | 154 | 154 | 14847 | node0 | secondary |
| node3 | vlodb | 154 | 154 | 14847 | node0 | secondary |

4 entries were displayed.

4. Vuelva al nivel de privilegio de administrador: `set -privilege admin`
5. Si va a trabajar en un entorno SAN, compruebe que cada nodo se encuentra en quórum DE SAN: `event log show -severity informational -message-name scsiblade.*`

El mensaje de evento scsiblade más reciente para cada nodo debe indicar que el scsi-blade está en quórum.

```
cluster1::*> event log show -severity informational -message-name scsiblade.*
```

| Time | Node | Severity | Event |
|-----------------|-------|---------------|---|
| MM/DD/YYYY TIME | node0 | INFORMATIONAL | scsiblade.in.quorum: The scsi-blade ... |
| MM/DD/YYYY TIME | node1 | INFORMATIONAL | scsiblade.in.quorum: The scsi-blade ... |

Información relacionada

["Administración del sistema"](#)

Comprobación del estado del almacenamiento

Después de revertir o degradar un clúster, debe verificar el estado de los discos, agregados y volúmenes.

1. Compruebe el estado del disco:

| Para comprobar... | Realice lo siguiente... |
|---|---|
| Discos rotos | a. Mostrar cualquier disco roto: <code>storage disk show -state broken</code> b. Retire o sustituya los discos rotos. |
| Discos sometidos a mantenimiento o reconstrucción | a. Muestre cualquier disco en estado de mantenimiento, pendiente o reconstrucción: <code>`storage disk show -state maintenance</code> |
| pending | <code>reconstructing`</code> .. Espere a que la operación de mantenimiento o reconstrucción finalice antes de continuar. |

- Compruebe que todos los agregados están en línea mostrando el estado del almacenamiento físico y lógico, incluidos los agregados de almacenamiento: `storage aggregate show -state !online`

Este comando muestra los agregados que *not* están en línea. Todos los agregados deben estar en línea antes y después de realizar una actualización o versión posterior principales.

```
cluster1:> storage aggregate show -state !online
There are no entries matching your query.
```

- Verifique que todos los volúmenes estén en línea mostrando los volúmenes que *not* en línea: `volume show -state !online`

Todos los volúmenes deben estar en línea antes y después de realizar una actualización o versión posterior principales.

```
cluster1:> volume show -state !online
There are no entries matching your query.
```

- Compruebe que no haya volúmenes incoherentes: `volume show -is-inconsistent true`

Consulte el artículo de la base de conocimientos ["Volumen que muestra una incoherencia de WAFL"](#) sobre la forma de abordar los volúmenes incoherentes.

Información relacionada

["Gestión de discos y agregados"](#)

Permite el cambio automático para configuraciones de MetroCluster

En este tema, se proporciona información sobre las tareas adicionales que debe realizar tras la nueva versión de las configuraciones de MetroCluster.

- Habilitar la conmutación de sitios automática no planificada: `metrocluster modify -auto -switchover-failure-domain auto-on-cluster-disaster`

2. Validar la configuración de MetroCluster: `metrocluster check run`

Habilite y revierte las LIF a los puertos de inicio después de una reversión

Durante un reinicio, es posible que algunas LIF se hayan migrado a sus puertos de conmutación al respaldo asignados. Después de revertir un clúster, debe habilitar y revertir cualquier LIF que no esté en sus puertos iniciales.

El comando `network interface revert` revierte una LIF que no está actualmente de su puerto de inicio a su puerto de inicio, siempre y cuando el puerto de inicio esté operativo. Cuando se crea la LIF, se especifica el puerto inicial de una LIF; puede determinar el puerto inicial de una LIF mediante el comando `network interface show`.

1. Mostrar el estado de todas las LIF: `network interface show`

Este ejemplo muestra el estado de todas las LIF de una máquina virtual de almacenamiento (SVM).

```
cluster1::> network interface show -vserver vs0
```

| | Logical | Status | Network | Current | |
|------------|-----------|------------|----------------|---------|-------|
| Current Is | | | | | |
| Vserver | Interface | Admin/Oper | Address/Mask | Node | Port |
| Home | | | | | |
| ----- | ----- | ----- | ----- | ----- | ----- |
| vs0 | | | | | |
| | data001 | down/down | 192.0.2.120/24 | node0 | e0e |
| true | | | | | |
| | data002 | down/down | 192.0.2.121/24 | node0 | e0f |
| true | | | | | |
| | data003 | down/down | 192.0.2.122/24 | node0 | e2a |
| true | | | | | |
| | data004 | down/down | 192.0.2.123/24 | node0 | e2b |
| true | | | | | |
| | data005 | down/down | 192.0.2.124/24 | node0 | e0e |
| false | | | | | |
| | data006 | down/down | 192.0.2.125/24 | node0 | e0f |
| false | | | | | |
| | data007 | down/down | 192.0.2.126/24 | node0 | e2a |
| false | | | | | |
| | data008 | down/down | 192.0.2.127/24 | node0 | e2b |
| false | | | | | |

8 entries were displayed.

Si alguna LIF aparece con el estado Status Admin de down o with an is home status de false, continúe con el siguiente paso.

2. Habilite las LIF de datos: `network interface modify {-role data} -status-admin up`

```
cluster1::> network interface modify {-role data} -status-admin up
8 entries were modified.
```

3. Revertir los LIF a sus puertos raíz: `network interface revert *`

Este comando revierte todas las LIF a sus puertos principales.

```
cluster1::> network interface revert *
8 entries were acted on.
```

4. Compruebe que todas las LIF se encuentran en sus puertos de inicio: `network interface show`

Este ejemplo muestra que todas las LIF para SVM vs0 están en sus puertos iniciales.

```
cluster1::> network interface show -vserver vs0
```

| Current Is | Logical | Status | Network | Current | |
|------------|-----------|------------|----------------|---------|------|
| Vserver | Interface | Admin/Oper | Address/Mask | Node | Port |
| Home | | | | | |
| ----- | ----- | ----- | ----- | ----- | |
| vs0 | | | | | |
| true | data001 | up/up | 192.0.2.120/24 | node0 | e0e |
| true | data002 | up/up | 192.0.2.121/24 | node0 | e0f |
| true | data003 | up/up | 192.0.2.122/24 | node0 | e2a |
| true | data004 | up/up | 192.0.2.123/24 | node0 | e2b |
| true | data005 | up/up | 192.0.2.124/24 | node1 | e0e |
| true | data006 | up/up | 192.0.2.125/24 | node1 | e0f |
| true | data007 | up/up | 192.0.2.126/24 | node1 | e2a |
| true | data008 | up/up | 192.0.2.127/24 | node1 | e2b |

```
8 entries were displayed.
```

Habilite las políticas de copia Snapshot después de revertir

Después de revertir a una versión anterior de ONTAP, debe habilitar las políticas de

copia de Snapshot para comenzar de nuevo a crear copias de Snapshot.

Es posible volver a habilitar las programaciones de Snapshot que se deshabilitaron antes de revertir a una versión anterior de ONTAP.

1. Habilite políticas de copia Snapshot para todas las SVM de datos:

```
volume snapshot policy modify -vserver * -enabled true
```

```
snapshot policy modify pg-rpo-hourly -enable true
```

2. Para cada nodo, habilite la normativa de copia Snapshot del volumen raíz mediante el comando `run-nodenodenodenamovol optionsroot_vol_namenosnap off`.

```
cluster1::> run -node node1 vol options vol0 nosnap off
```

Verificar el acceso del cliente (SMB y NFS)

Para los protocolos configurados, probar el acceso desde los clientes SMB y NFS para verificar que se pueda acceder al clúster.

Verifique las entradas del firewall IPv6

Una nueva versión de cualquier versión de ONTAP 9 podría resultar en que falten entradas predeterminadas del firewall IPv6 para algunos servicios en las políticas del firewall. Debe comprobar que las entradas de firewall necesarias se han restaurado en el sistema.

1. Compruebe que todas las directivas de firewall son correctas comparándolas con las directivas predeterminadas: `system services firewall policy show`

En el siguiente ejemplo, se muestran las políticas predeterminadas:


```
cluster1::*> system services firewall policy show
```

| Policy | Service | Action | IP-List |
|---------|---------|--------|-----------------|
| ----- | | | |
| cluster | dns | allow | 0.0.0.0/0 |
| | http | allow | 0.0.0.0/0 |
| | https | allow | 0.0.0.0/0 |
| | ndmp | allow | 0.0.0.0/0 |
| | ntp | allow | 0.0.0.0/0 |
| | rsh | allow | 0.0.0.0/0 |
| | snmp | allow | 0.0.0.0/0 |
| | ssh | allow | 0.0.0.0/0 |
| | telnet | allow | 0.0.0.0/0 |
| data | dns | allow | 0.0.0.0/0, ::/0 |
| | http | deny | 0.0.0.0/0, ::/0 |
| | https | deny | 0.0.0.0/0, ::/0 |
| | ndmp | allow | 0.0.0.0/0, ::/0 |
| | ntp | deny | 0.0.0.0/0, ::/0 |
| | rsh | deny | 0.0.0.0/0, ::/0 |
| . | | | |
| . | | | |
| . | | | |

2. Agregue manualmente todas las entradas predeterminadas del firewall IPv6 que falten creando una nueva política de firewall: `system services firewall policy create`

```
cluster1::*> system services firewall policy create -policy newIPv6  
-service ssh -action allow -ip-list ::/0
```

3. Aplique la nueva política a la LIF para permitir el acceso a un servicio de red: `network interface modify`

```
cluster1::*> network interface modify -vserver VS1 -lif LIF1  
-firewall-policy newIPv6
```

Revertir la función hash de contraseña al tipo de cifrado admitido

Si vuelve de ONTAP 9.1 o ONTAP 9.0 a ONTAP 8.3.x, los usuarios de cuentas SHA-2 ya no pueden autenticarse con sus contraseñas. Las contraseñas deben restablecerse para utilizar el tipo de cifrado MDS.

1. Establezca una contraseña temporal para cada cuenta de usuario SHA-2 que usted tenga [identificado](#)

[antes de la reversión](#): `security login password -username user_name -vserver vserver_name`

2. Comunique la contraseña temporal a los usuarios afectados y haga que inicien sesión a través de una consola o sesión SSH para cambiar sus contraseñas según lo indique el sistema.

Consideraciones que tener en cuenta si actualizar manualmente el firmware del SP

Si la funcionalidad de actualización automática del SP está habilitada (por defecto), la degradación o la reversión a ONTAP 8.3.x no requiere una actualización manual del firmware del SP. El firmware del SP se actualiza automáticamente a la versión compatible más reciente compatible, compatible con la versión de ONTAP a la que se revierte o degradó.

Si la funcionalidad de actualización automática del SP está deshabilitada (no se recomienda), una vez que se complete el proceso de reversión o degradación de ONTAP, debe actualizar manualmente el firmware del SP a una versión compatible con la versión de ONTAP a la que se revierte o se degrada.

["Matriz de compatibilidad de BIOS/ONTAP de NetApp"](#)

["Descargas de NetApp: Diagnóstico y firmware del sistema"](#)

Cambio en las cuentas de usuario que pueden acceder a Service Processor

Si creó cuentas de usuario en ONTAP 9.8 o una versión anterior, actualice a ONTAP 9.9.1 o una versión posterior (cuando la `-role` parámetro se cambia a `admin`), y luego volvió a ONTAP 9.8 o anterior, el `-role` el parámetro se restaura a su valor original. No obstante, debe verificar que los valores modificados sean aceptables.

Durante la reversión, si se ha eliminado el rol de un usuario del SP, se registrará el mensaje `"rbac.spuser.role.notfound"` EMS".

Para obtener más información, consulte ["Cuentas que pueden acceder al SP"](#).

Administración de clústeres

Gestión de clústeres con System Manager

Información general de administración con System Manager

System Manager es una interfaz gráfica de gestión basada en HTML5 que permite utilizar un navegador web para gestionar sistemas de almacenamiento y objetos de almacenamiento (como discos, volúmenes y niveles de almacenamiento) y realizar tareas de gestión comunes relacionadas con los sistemas de almacenamiento.

Los procedimientos de esta sección ayudan a gestionar el clúster con System Manager en ONTAP 9.7 y versiones posteriores.



- System Manager se incluye con el software ONTAP como servicio web, habilitado de forma predeterminada, accesible mediante un navegador.
- El nombre de System Manager ha cambiado a partir de ONTAP 9.6. En ONTAP 9.5 y versiones anteriores se denominaba System Manager de OnCommand. A partir de ONTAP 9.6 y versiones posteriores, se denomina System Manager.
- Si utiliza la versión clásica de System Manager (disponible solo en ONTAP 9.7 y versiones anteriores), consulte ["System Manager Classic \(ONTAP de 9.0 a 9.7\)"](#)

Con la consola de System Manager, puede ver información de un vistazo sobre las alertas y notificaciones importantes, la eficiencia y la capacidad de los niveles de almacenamiento y volúmenes, los nodos disponibles en un clúster, el estado de los nodos de un par de alta disponibilidad, las aplicaciones y objetos más activos, y las métricas de rendimiento de un clúster o un nodo.

Con System Manager puede realizar muchas tareas comunes, como las siguientes:

- Cree un clúster, configure una red y configure detalles de soporte para el clúster.
- Configurar y gestionar objetos de almacenamiento, como discos, niveles locales, volúmenes, qtrees, y cuotas.
- Configure protocolos, como SMB y NFS, y aprovisiona el uso compartido de archivos.
- Configure protocolos como FC, FCoE, NVMe e iSCSI para el acceso en bloque.
- Cree y configure componentes de red, como subredes, dominios de retransmisión, interfaces de datos y gestión, y grupos de interfaces.
- Configurar y gestionar las relaciones de mirroring y almacenamiento remoto.
- Realizar operaciones de gestión de clústeres, nodos de almacenamiento y de máquinas virtuales de almacenamiento (máquinas virtuales de almacenamiento).
- Crear y configurar equipos virtuales de almacenamiento, gestionar objetos de almacenamiento asociados con equipos virtuales de almacenamiento y gestionar servicios de equipos virtuales de almacenamiento.
- Supervisar y gestionar las configuraciones de alta disponibilidad en un clúster.
- Configure los procesadores de servicio para iniciar sesión, administrar, supervisar y administrar el nodo de forma remota, independientemente del estado del nodo.

Terminología de System Manager

System Manager utiliza una terminología diferente a la CLI para algunas funcionalidades clave de ONTAP.

- **Nivel local:** Conjunto de unidades físicas de estado sólido o unidades de disco duro en las que almacena sus datos. Puede que los conozca como agregados. De hecho, si utiliza la CLI de ONTAP, verá el término *aggregate* que se utiliza para representar un nivel local.
- **Cloud Tier:** Almacenamiento en la nube utilizada por ONTAP cuando desea tener algunos de sus datos fuera de las instalaciones por una de las razones siguientes. Si estás pensando en la parte de la nube de un FabricPool, ya lo has descubierto. Y si utiliza un sistema StorageGRID, es posible que su cloud no esté fuera de las instalaciones. (Una experiencia similar al cloud en las instalaciones se llama *cloud privado*).
- **Storage VM:** Máquina virtual que se ejecuta en ONTAP y proporciona servicios de almacenamiento y datos a sus clientes. Puede que lo sepa como un SVM o un vserver.
- **Interfaz de red** - Una dirección y propiedades asignadas a un puerto de red física. Es posible que lo sepa como una *interfaz lógica (LIF)*.
- **Pausa:** Acción que detiene las operaciones. Antes de ONTAP 9.8, es posible que haya hecho referencia a *QUIESCE* en otras versiones de System Manager.

Utilice System Manager para acceder a un clúster

Si prefiere utilizar una interfaz gráfica en lugar de la interfaz de línea de comandos (CLI) para acceder y gestionar un clúster, puede hacerlo mediante System Manager, que se incluye con ONTAP como servicio web, se habilita de forma predeterminada y se puede acceder a él mediante un navegador.



A partir de ONTAP 9.12.1, System Manager está totalmente integrado con BlueXP.

Con BlueXP, puede gestionar su infraestructura multicloud híbrida desde un único plano de control sin perder la consola conocida de System Manager.

Consulte "[Integración de System Manager con BlueXP](#)".

Acerca de esta tarea

Puede usar una interfaz de red de gestión (LIF) clústeres o una interfaz de red de gestión de nodos (LIF) para acceder a System Manager. Para acceder de forma ininterrumpida a System Manager, debe usar una interfaz de red de gestión de clústeres (LIF).

Antes de empezar

- Debe tener una cuenta de usuario de clúster configurada con el rol «'admin'» y los tipos de aplicación «'http'» y «'Console'».
- Debe haber activado las cookies y los datos del sitio en el navegador.

Pasos

1. Dirija el explorador web a la dirección IP de la interfaz de red de gestión del clúster:


- Si utiliza IPv4: **`https://cluster-mgmt-LIF`**
- Si utiliza IPv6: **`https://[cluster-mgmt-LIF]`**




Solo se admite HTTPS para el acceso al explorador de System Manager.



Si el clúster utiliza un certificado digital autofirmado, es posible que el explorador muestre una advertencia que indica que el certificado no es de confianza. Puede reconocer el riesgo de continuar con el acceso o instalar un certificado digital firmado de entidad de certificación (CA) en el clúster para la autenticación del servidor.

2. **Opcional:** Si ha configurado un banner de acceso mediante la CLI, lea el mensaje que aparece en el cuadro de diálogo **Advertencia** y elija la opción necesaria para continuar.
- Esta opción no es compatible en sistemas donde está habilitada la autenticación del lenguaje de marcado de aserción de seguridad (SAML).
- Si no desea continuar, haga clic en **Cancelar** y cierre el navegador.
 - Si desea continuar, haga clic en **Aceptar** para ir a la página de inicio de sesión de System Manager.
3. Inicie sesión en System Manager con las credenciales de administrador del clúster.



A partir de ONTAP 9.11.1, cuando inicia sesión en System Manager, puede especificar la configuración regional. La configuración regional especifica determinadas configuraciones de localización, como el idioma, la moneda, el formato de fecha y hora, y configuraciones similares. Para ONTAP 9.10.1 y versiones anteriores, se detecta la configuración regional de System Manager desde el explorador. Para cambiar la configuración regional de System Manager, tiene que cambiar la configuración regional del navegador.

4. **Opcional:** A partir de ONTAP 9.12.1, puede especificar su preferencia por la apariencia de System Manager:
- a. En la esquina superior derecha de System Manager, haga clic en  para gestionar las opciones de usuario.
 - b. Coloque el interruptor de selección **tema del sistema** a su preferencia:

| Cambiar de posición | Configuración de apariencia |
|---|--|
|  (izquierda) | Tema claro (fondo claro con texto oscuro) |
| So (centro) | La opción predeterminada es la preferencia de tema establecida para las aplicaciones del sistema operativo (generalmente la configuración del tema para el explorador que se utiliza para acceder a System Manager). |
|  (derecha) | Tema oscuro (fondo oscuro con texto claro) |

Información relacionada

["Gestión del acceso a los servicios web"](#)

["Acceder al registro de un nodo, al volcado principal y a archivos MIB mediante un navegador web"](#)

Habilite nuevas funciones añadiendo claves de licencia


En versiones anteriores a ONTAP 9.10.1, las funciones de ONTAP se habilitan con claves de licencia y las funciones en ONTAP 9.10.1 y versiones posteriores se habilitan

con un archivo de licencia de NetApp. Puede añadir claves de licencia y archivos de licencia de NetApp mediante System Manager.

A partir de ONTAP 9.10.1, se puede usar System Manager para instalar un archivo de licencia de NetApp con el fin de habilitar varias funciones con licencia a la vez. El uso de un archivo de licencia de NetApp simplifica la instalación de la licencia porque ya no tiene que añadir claves de licencia de funciones independientes. Descargue el archivo de licencia de NetApp desde el sitio de soporte de NetApp.

Si ya tiene claves de licencia para algunas funciones y va a actualizar a ONTAP 9.10.1, puede seguir utilizando dichas claves de licencia.


Pasos

1. Seleccione **Cluster > Settings**.
2. En **Licencias**, seleccione .
3. Seleccione **examinar**. Elija el archivo de licencia de NetApp que descargó.
4. Si desea añadir claves de licencia, seleccione **usar claves de licencia de 28 caracteres** e introduzca las claves.

Descargue una configuración de clúster

A partir de ONTAP 9.11.1, puede usar System Manager para descargar la configuración de un clúster.

Pasos

1. Haga clic en **Cluster > Overview**.
2. Haga clic en  para mostrar el menú desplegable.
3. Seleccione **Descargar configuración**.
4. Seleccione los pares HA y, a continuación, haga clic en **Descargar**.

La configuración se descarga como una hoja de cálculo de Excel.

- La primera hoja contiene detalles del grupo.
- Las otras hojas contienen detalles de nodo.

Asigne etiquetas a un clúster

A partir de ONTAP 9.14.1, puede usar System Manager para asignar etiquetas a un clúster e identificar objetos como pertenecientes a una categoría, como proyectos o centros de costes.

Acerca de esta tarea

Puede asignar una etiqueta a un clúster. En primer lugar, debe definir y agregar la etiqueta. A continuación, también puede editar o eliminar la etiqueta.

Las etiquetas se pueden agregar al crear un clúster o se pueden añadir más adelante.

Usted define una etiqueta especificando una clave y asociando un valor a ella usando el formato “key:value”. Por ejemplo: “dispt:engineering” o “location:san-jose”.

Debe tenerse en cuenta lo siguiente al crear etiquetas:

- Las claves tienen una longitud mínima de un carácter y no pueden ser nulas. Los valores pueden ser nulos.
- Una clave se puede emparejar con varios valores separando los valores con una coma, por ejemplo, "location:san-jose,toronto"
- Las etiquetas se pueden usar para varios recursos.
- Las teclas deben comenzar por una letra minúscula.

Pasos


Para administrar etiquetas, realice los siguientes pasos:

1. En System Manager, haga clic en **Cluster** para ver la página de descripción general.

Las etiquetas se enumeran en la sección **Tags**.

2. Haga clic en **Administrar etiquetas** para modificar las etiquetas existentes o agregar otras nuevas.

Puede agregar, editar o eliminar las etiquetas.

| Para realizar esta acción... | Realice estos pasos... |
|------------------------------|--|
| Agregue una etiqueta | <ol style="list-style-type: none">a. Haga clic en Añadir etiqueta.b. Especifique una clave y su valor o valores (separe varios valores con comas).c. Haga clic en Guardar. |
| Editar una etiqueta | <ol style="list-style-type: none">a. Modifique el contenido en los campos Key y values (opcional).b. Haga clic en Guardar. |
| Eliminar una etiqueta | <ol style="list-style-type: none">a. Haga clic en  junto a la etiqueta que desea eliminar. |

Consulte y envíe sus casos de soporte

A partir de ONTAP 9.9.1, es posible ver casos de soporte de Active IQ asociados con el clúster. También puede copiar los detalles del clúster que necesita para enviar un nuevo caso de soporte en el sitio de soporte de NetApp.

A partir de ONTAP 9.10.1, puede habilitar el registro de telemetría, lo que ayuda al personal de soporte a solucionar problemas.



Para recibir alertas sobre las actualizaciones de firmware, debe registrarse en Active IQ Unified Manager. Consulte ["Recursos de documentación de Active IQ Unified Manager"](#).

Pasos

1. En System Manager, seleccione **Soporte**.

Se muestra una lista de los casos de soporte abiertos asociados con este clúster.

2. Haga clic en los siguientes enlaces para realizar los procedimientos:

- **Número de caso:** Consulte los detalles del caso.
- **Visite la página de soporte de NetApp:** Desplácese hasta la página de **My AutoSupport** en el sitio de soporte de NetApp para ver artículos de la base de conocimientos o enviar un nuevo caso de soporte.
- **Ver Mis casos:** Desplácese hasta la página **Mis casos** del sitio de soporte de NetApp.
- **Ver detalles del clúster:** Permite ver y copiar la información que necesitará cuando envíe un caso nuevo.

Active el registro de telemetría

A partir de ONTAP 9.10.1, puede utilizar System Manager para habilitar el registro de telemetría. Cuando se permite el registro de telemetría, a los mensajes registrados por System Manager se les da un identificador de telemetría específico que indica el proceso exacto que activó el mensaje. Todos los mensajes que se emiten relacionados con ese proceso tienen el mismo identificador, que consiste en el nombre del flujo de trabajo operativo y un número (por ejemplo, "add-volume-1941290").

Si experimenta problemas de rendimiento, puede habilitar el registro de telemetría, que permite al personal de soporte identificar más fácilmente el proceso específico para el que se emitió un mensaje. Cuando se agregan identificadores de telemetría a los mensajes, el archivo de registro sólo se amplía ligeramente.

Pasos

1. En System Manager, seleccione **Cluster > Settings**.
2. En la sección **Configuración de la interfaz de usuario**, haga clic en la casilla de verificación **permitir registro de telemetría**.



Gestionar el límite de capacidad máximo de una máquina virtual de almacenamiento en System Manager

A partir de ONTAP 9.13.1, puede usar System Manager para habilitar un límite de capacidad máxima para una máquina virtual de almacenamiento y establecer un umbral para desencadenar alertas cuando el almacenamiento utilizado alcanza un cierto porcentaje de la capacidad máxima.

Habilite un límite de capacidad máxima para una máquina virtual de almacenamiento

A partir de ONTAP 9.13.1, puede especificar la capacidad máxima que se puede asignar a todos los volúmenes en una máquina virtual de almacenamiento. Es posible habilitar la capacidad máxima al añadir una máquina virtual de almacenamiento o al editar una máquina virtual de almacenamiento existente.

Pasos


1. Seleccione **Almacenamiento > VM de almacenamiento**.
2. Realice una de las siguientes acciones:
 - Para añadir una máquina virtual de almacenamiento, haga clic en .
 - Para editar una máquina virtual de almacenamiento, haga clic en  Junto al nombre de la VM de almacenamiento, y luego haga clic en **Editar**.

3. Introduzca o modifique la configuración de la máquina virtual de almacenamiento y active la casilla de comprobación etiquetada como Enable Maximum Capacity limit.
4. Especifique el tamaño de capacidad máxima.
5. Especifique el porcentaje de la capacidad máxima que desea usar como umbral para activar alertas.
6. Haga clic en **Guardar**.

Edite el límite de capacidad máxima de una máquina virtual de almacenamiento

A partir de ONTAP 9.13.1, puede editar el límite de capacidad máxima de una máquina virtual de almacenamiento existente, si la [se habilitó el límite de capacidad máxima](#) ya.

Pasos

1. Seleccione **Almacenamiento > VM de almacenamiento**.
2. Haga clic en  Junto al nombre de la VM de almacenamiento, y luego haga clic en **Editar**.

La casilla de comprobación etiquetada para habilitar límite de capacidad máxima ya está activada.

3. Realice uno de los siguientes pasos:

| Acción | Pasos |
|---|--|
| Deshabilite el límite de capacidad máxima | <ol style="list-style-type: none"> 1. Desactive la casilla de verificación. 2. Haga clic en Guardar. |
| Modifique el límite de capacidad máxima | <ol style="list-style-type: none"> 1. Especifique el tamaño de capacidad máxima nuevo. (No es posible especificar un tamaño menor que el espacio ya asignado en la máquina virtual de almacenamiento). 2. Especifique el nuevo porcentaje de la capacidad máxima que desea usar como umbral para activar alertas. 3. Haga clic en Guardar. |

Información relacionada

- ["Vea el límite de capacidad máxima de una máquina virtual de almacenamiento"](#)
- ["Mediciones de capacidad en System Manager"](#)
- ["Gestione los límites de capacidad de SVM mediante la CLI de ONTAP"](#)

Supervise la capacidad en System Manager

Con System Manager, puede supervisar cuánta capacidad de almacenamiento se ha utilizado y cuánto sigue disponible para un clúster, un nivel local o una máquina virtual de almacenamiento.

Con cada versión de ONTAP, System Manager proporciona información de supervisión de la capacidad más sólida:

- A partir de ONTAP 9.10.1, System Manager le permite ver datos históricos sobre la capacidad del clúster y las proyecciones sobre cuánta capacidad se utilizará o estará disponible en el futuro. También se puede supervisar la capacidad de niveles y volúmenes locales.

- A partir de ONTAP 9.12.1, System Manager muestra la cantidad de capacidad comprometida para un nivel local.
- A partir de ONTAP 9.13.1, puede habilitar un límite de capacidad máxima para una máquina virtual de almacenamiento y establecer un umbral para activar alertas cuando el almacenamiento utilizado alcanza un cierto porcentaje de la capacidad máxima.



Las mediciones de capacidad usada se muestran de forma diferente según la versión de ONTAP. Más información en ["Mediciones de capacidad en System Manager"](#).

Ver la capacidad de un clúster

Es posible ver las mediciones de capacidad de un clúster en la consola de System Manager.

Antes de empezar

Para ver datos relacionados con la capacidad en el cloud, debe tener una cuenta con el asesor digital de Active IQ y estar conectada.

Pasos

1. En System Manager, haga clic en **Panel**.
2. En la sección **capacidad**, puede ver lo siguiente:
 - La capacidad total utilizada del clúster
 - La capacidad total disponible del clúster
 - Porcentajes de capacidad utilizada y disponible.
 - Ratio de reducción de datos.
 - La cantidad de capacidad utilizada en el cloud.
 - Historial de uso de capacidad.
 - Proyección del uso de la capacidad



En System Manager, las representaciones de capacidad no dan cuenta de las capacidades de niveles de almacenamiento raíz (agregado).

3. Haga clic en el gráfico para ver más detalles acerca de la capacidad del clúster.

Las mediciones de capacidad se muestran en dos gráficos de barras:

- En el gráfico superior se muestra la capacidad física: El tamaño del espacio físico usado, reservado y disponible.
- El gráfico inferior muestra la capacidad lógica: El tamaño de datos de clientes, copias Snapshot y clones, y el espacio total lógico utilizado.

Debajo de los gráficos de barras hay mediciones para la reducción de datos:

- Tasa de reducción de datos solo para los datos del cliente (no se incluyen copias Snapshot y clones).
- Tasa de reducción de datos general.

Para obtener más información, consulte ["Mediciones de capacidad en System Manager"](#).

Ver la capacidad de un nivel local

Se pueden ver detalles acerca de la capacidad de los niveles locales. A partir de ONTAP 9.12.1, la vista **Capacity** también incluye la cantidad de capacidad comprometida para un nivel local, lo que le permite determinar si necesita agregar capacidad al nivel local para acomodar la capacidad comprometida y evitar quedarse sin espacio libre.

Pasos

1. Haga clic en **almacenamiento > niveles**.
2. Seleccione el nombre del nivel local.
3. En la página **Descripción general**, en la sección **capacidad**, la capacidad se muestra en un gráfico de barras con tres mediciones:
 - Se utiliza y la capacidad reservada
 - Capacidad disponible
 - Capacidad comprometida (a partir de ONTAP 9.12.1)
4. Haga clic en el gráfico para ver detalles acerca de la capacidad del nivel local.

Las mediciones de capacidad se muestran en dos gráficos de barras:

- El gráfico de barras superior muestra la capacidad física: El tamaño del espacio físico utilizado, reservado y disponible.
- El gráfico de la barra inferior muestra la capacidad lógica: El tamaño de datos de clientes, copias Snapshot y clones, y el total del espacio lógico utilizado.

Debajo de los gráficos de barras se encuentran las relaciones de medición para la reducción de datos:

- Tasa de reducción de datos solo para los datos del cliente (no se incluyen copias Snapshot y clones).
- Tasa de reducción de datos general.

Para obtener más información, consulte ["Mediciones de capacidad en System Manager"](#).

Acciones opcionales

- Si la capacidad comprometida es mayor que la capacidad del nivel local, puede considerar la posibilidad de añadir capacidad al nivel local antes de que se quede sin espacio libre. Consulte ["Añada capacidad a un nivel local \(añada discos a un agregado\)"](#).
- También puede ver el almacenamiento que utilizan volúmenes específicos en el nivel local seleccionando la pestaña **Volúmenes**.

Vea la capacidad de los volúmenes en una máquina virtual de almacenamiento

Es posible ver cuánto almacenamiento utilizan los volúmenes en una máquina virtual de almacenamiento y cuánta capacidad sigue disponible. La medición total del almacenamiento utilizado y disponible se denomina «capacidad entre volúmenes».

Pasos

1. Selecciona **Almacenamiento > VM de almacenamiento**.
2. Haga clic en el nombre de la máquina virtual de almacenamiento.
3. Desplácese a la sección **Capacidad**, que muestra un gráfico de barras con las siguientes medidas:

- **Físico utilizado:** Suma del almacenamiento físico utilizado en todos los volúmenes de esta VM de almacenamiento.
- **Disponible:** Suma de la capacidad disponible en todos los volúmenes de esta VM de almacenamiento.
- **Lógico usado:** Suma del almacenamiento lógico usado en todos los volúmenes de esta VM de almacenamiento.

Para obtener más información sobre las mediciones, consulte ["Mediciones de capacidad en System Manager"](#).

Vea el límite de capacidad máxima de una máquina virtual de almacenamiento

A partir de ONTAP 9.13.1, puede ver el límite de capacidad máxima de una máquina virtual de almacenamiento.

Antes de empezar

Debe ["Habilite el límite de capacidad máxima de una máquina virtual de almacenamiento"](#) antes de poder verlo.

Pasos

1. Seleccione **Almacenamiento > VM de almacenamiento**.

Es posible ver las mediciones de capacidad máxima de dos maneras:

- En la fila de la VM de almacenamiento, vea la columna **Capacidad máxima** que contiene un gráfico de barras que muestra la capacidad utilizada, la capacidad disponible y la capacidad máxima.
- Haga clic en el nombre de la máquina virtual de almacenamiento. En la pestaña **Overview**, desplácese para ver los valores de umbral de alerta de capacidad máxima, capacidad asignada y capacidad en la columna izquierda.

Información relacionada

- ["Edite el límite de capacidad máxima de una máquina virtual de almacenamiento"](#)
- ["Mediciones de capacidad en System Manager"](#)

Vea las configuraciones de hardware para determinar los problemas

A partir de ONTAP 9,8, puede usar System Manager para ver la configuración de hardware en la red y determinar el estado de sus sistemas de hardware y las configuraciones de cableado.

Pasos

Para ver las configuraciones de hardware, realice los siguientes pasos:

1. En System Manager, seleccione **Cluster > hardware**.
2. Pase el ratón sobre los componentes para ver el estado y otros detalles.

Puede ver varios tipos de información:

- [Información acerca de las controladoras](#)
- [Información acerca de las bandejas de discos](#)

- [Información sobre los switches de almacenamiento](#)

3. A partir de ONTAP 9.12.1, puede ver la información del cableado en System Manager. Haga clic en la casilla de verificación **Mostrar cables** para ver el cableado y, a continuación, pase el ratón sobre un cable para ver su información de conectividad.

- [Información sobre el cableado](#)

Información acerca de las controladoras

Puede ver lo siguiente:

Nodos

Nodos:

- Se pueden ver las vistas frontal y trasera.
- Para los modelos con bandeja de discos interna, también se puede ver el diseño de discos en la vista frontal.
- Puede ver las siguientes plataformas:

| Plataforma | Admitido en System Manager en la versión de ONTAP... | | | | | | |
|-------------|--|--------|----------|----------|----------|-------|---------------------------------|
| | 9.14.1 | 9.13.1 | 9.12.1 | 9.11.1 | 9.10.1 | 9.9.1 | 9,8 (solo modo de vista previa) |
| AFF A150 | Sí | Sí | | | | | |
| AFF A220 | Sí | Sí | Sí | Sí | Sí | Sí | Sí |
| AFF A250 | Sí | Sí | Sí | Sí | Sí | Sí | |
| AFF A300 | Sí | Sí | Sí | Sí | Sí | Sí | Sí |
| AFF A320 | Sí | Sí | Sí | Sí | Sí | Sí | |
| AFF A400 | Sí | Sí | Sí | Sí | Sí | Sí | Sí |
| AFF A700 | Sí | Sí | Sí | Sí | Sí | Sí | Sí |
| AFF A700s | Sí | Sí | Sí | Sí | Sí | Sí | |
| AFF A800 | Sí | Sí | Sí | Sí | Sí | Sí | |
| C190 de AFF | Sí | Sí | Sí | Sí | Sí | Sí | Sí |
| AFF C250 | Sí | Sí | Sí y#42; | Sí y#42; | Sí y#42; | | |
| AFF C400 | Sí | Sí | Sí y#42; | Sí y#42; | Sí y#42; | | |
| AFF C800 | Sí | Sí | Sí y#42; | Sí y#42; | Sí y#42; | | |
| ASAA150 | Sí | Sí | | | | | |
| ASAA250 | Sí | Sí | | | | | |

| | | | | | | | |
|----------|----|----|----|----|----|----|--|
| ASA A400 | Sí | Sí | | | | | |
| ASA A800 | Sí | Sí | | | | | |
| ASA A900 | Sí | Sí | | | | | |
| ASA C250 | Sí | Sí | | | | | |
| ASA C400 | Sí | Sí | | | | | |
| ASA C800 | Sí | Sí | | | | | |
| FAS500f | Sí | Sí | Sí | Sí | Sí | Sí | |
| FAS2720 | Sí | Sí | Sí | Sí | | | |
| FAS2750 | Sí | Sí | Sí | Sí | | | |
| FAS8300 | Sí | Sí | Sí | Sí | | | |
| FAS8700 | Sí | Sí | Sí | Sí | | | |
| FAS9000 | Sí | Sí | Sí | Sí | | | |
| FAS9500 | Sí | Sí | Sí | Sí | | | |

Puertos

Puertos:

- Verá un puerto resaltado en rojo si está inactivo.
- Al pasar el ratón sobre el puerto, puede ver el estado de un puerto y otros detalles.
- No es posible ver los puertos de consola.

Notas:

- Para ONTAP 9.10.1 y versiones anteriores, verá los puertos SAS resaltados en rojo cuando estén deshabilitados.
- A partir de ONTAP 9.11.1, verá los puertos SAS resaltados en rojo solo si están en estado de error o si un puerto cableado que se está utilizando se desconecta. Los puertos aparecen en blanco si están sin conexión y desconectados.

FRU

FRU:

La información sobre las FRU solo aparece cuando el estado de una FRU no es óptimo.

- PSU fallido en nodos o chasis.
- Temperaturas altas detectadas en los nodos.
- Los ventiladores fallidos en los nodos o chasis.

Tarjetas adaptadoras

Tarjetas adaptadoras:

- Las tarjetas con campos de número de pieza definidos se muestran en las ranuras si se han insertado tarjetas externas.
- Los puertos se muestran en las tarjetas.
- Para una tarjeta compatible, puede ver imágenes de esa tarjeta. Si la tarjeta no está en la lista de números de pieza compatibles, aparecerá un gráfico genérico.

Información acerca de las bandejas de discos

Puede ver lo siguiente:

Bandejas de discos

Bandejas de discos:

- Puede mostrar las vistas frontal y trasera.
- Es posible ver los siguientes modelos de bandeja de discos:

| | |
|-------------------------------------|--|
| Si el sistema se está ejecutando... | Luego, puede usar System Manager para ver... |
| ONTAP 9.9.1 y versiones posteriores | Todas las bandejas con <i>NOT</i> se han designado como «fin de servicio» o «fin de la disponibilidad» |
| ONTAP 9,8 | DS4243, DS4486, DS212C, DS2246, DS224C, Y NS224 |

Puertos de la bandeja

Puertos de estante:

- Puede ver el estado del puerto.
- Puede ver la información del puerto remoto si el puerto está conectado.

FRU de bandeja

FRU de estante:

- Se muestra la información sobre los fallos de PSU.

Información sobre los switches de almacenamiento

Puede ver lo siguiente:

Switches de almacenamiento

Interruptores de almacenamiento:

- La pantalla muestra los switches que actúan como switches de almacenamiento que se usan para conectar las bandejas a los nodos.
- A partir de ONTAP 9.9.1, System Manager muestra información sobre un switch que actúa como un switch de almacenamiento y un clúster, lo que también se puede compartir entre los nodos de una pareja de alta disponibilidad.
- Se muestra la siguiente información:
 - Nombre del switch
 - Dirección IP
 - Número de serie
 - Versión de SNMP
 - Versión del sistema
- Puede ver los siguientes modelos de switch de almacenamiento:

| Si el sistema se está ejecutando... | Luego, puede usar System Manager para ver... |
|-------------------------------------|---|
| ONTAP 9.11.1 o posterior | Cisco Nexus 3232C Cisco Nexus 9336C-FX2 Mellanox SN2100 |
| ONTAP 9.9.1 y 9.10.1 | Cisco Nexus 3232C Cisco Nexus 9336C-FX2 |
| ONTAP 9,8 | Cisco Nexus 3232C |

Puertos del switch de almacenamiento

Puertos del conmutador de almacenamiento

- Se muestra la siguiente información:
 - Nombre de la identidad
 - Índice de identidad
 - Estado
 - Conexión remota
 - Otros detalles

Información sobre el cableado

A partir de ONTAP 9.12.1, se puede ver la siguiente información sobre el cableado:

- **Cableado** entre controladores, interruptores y estantes cuando no se utilizan puentes de almacenamiento
- **Conectividad** que muestra los ID y las direcciones MAC de los puertos en cada extremo del cable

Gestione nodos mediante System Manager

En System Manager, puede añadir nodos a un clúster y cambiarles el nombre. También puede reiniciar, tomar el control y devolver nodos.

Añada nodos a un clúster

Puede aumentar el tamaño y las funcionalidades del clúster añadiendo nodos nuevos.

Antes de comenzar

Ya debe haber cableado los nodos nuevos al clúster.

Acerca de esta tarea

Hay procesos distintos para trabajar con System Manager en ONTAP 9,7 o ONTAP 9,8 y versiones posteriores.

Procedimiento de ONTAP 9,8 y posterior

Añadir nodos a un clúster con System Manager (ONTAP 9,8 y posteriores)

Pasos

1. Seleccione **Cluster > Overview**.

Las nuevas controladoras se muestran como nodos conectados a la red de clúster, pero no en el clúster.

2. Seleccione **Agregar**.

- Los nodos se añaden al clúster.
- El almacenamiento se asigna de forma implícita.

Procedimiento de ONTAP 9,7

Añadir nodos a un clúster con el Administrador del sistema (ONTAP 9,7)

Pasos

1. Seleccione **(Volver a la versión clásica)**.
2. Selecciona **Configuraciones > Expansión de clúster**.

System Manager detecta automáticamente los nuevos nodos.


3. Selecciona **Cambiar a la nueva experiencia**.
4. Selecciona **Cluster > Overview** para ver los nuevos nodos.

Apague, reinicie o edite el procesador de servicio

Cuando reinicia o apaga un nodo, su compañero de alta disponibilidad ejecuta automáticamente una toma de control.

Pasos

1. Seleccione **Cluster > Overview**.

2. En **Nodos**, seleccione .
3. Seleccione el nodo y luego seleccione **Apagar**, **Reiniciar** o **Editar Procesador de Servicio**.


Si un nodo se ha reiniciado y está esperando devolución, la opción **Giveback** también está disponible.

Si selecciona **Editar procesador de servicio**, puede elegir **Manual** para introducir la dirección IP, la máscara de subred y la puerta de enlace, o puede elegir **DHCP** para la configuración dinámica del host.

Cambie el nombre de los nodos

A partir de ONTAP 9.14.1, se puede cambiar el nombre de un nodo desde la página de resumen del clúster.

Pasos

1. Seleccione **Cluster**. Se muestra la página de descripción general del clúster.
2. Desplácese hacia abajo hasta la sección **Nodos**.
3. Junto al nodo al que desea cambiar el nombre, seleccione , Y seleccione **Renombrar**.
4. Modifique el nombre del nodo y, a continuación, seleccione **Renombrar**.

Gestión de licencias

Información general de las licencias de ONTAP

Una licencia es un registro de uno o más derechos de software. A partir de ONTAP 9.10.1, todas las licencias se proporcionan como archivo de licencia de NetApp (NLF), que es un solo archivo que admite varias funciones. A partir de mayo de 2023, todos los sistemas AFF (tanto A-series como C-series) y los sistemas FAS se venden con la suite de software ONTAP One o la suite de software básico ONTAP. A partir de junio de 2023, todos los sistemas ASA se venden con ONTAP One para SAN. Cada suite de software se entrega como un único NLF, en sustitución de los paquetes NLF independientes que se introdujeron primero en ONTAP 9.10.1.

Licencias incluidas con ONTAP One

ONTAP One contiene todas las funciones con licencia disponibles. Contiene una combinación de los contenidos del paquete Core anterior, el bundle de protección de datos, el bundle de seguridad y cumplimiento de normativas, el bundle de cloud híbrido y el bundle de cifrado, como se muestra en la tabla. El cifrado no está disponible en países restringidos.

| Nombre de grupo anterior | Claves ONTAP incluidas |
|--------------------------|------------------------|
| Bundle principal | FlexClone |
| | SnapRestore |
| | NFS, SMB, S3 |
| | FC, iSCSI |
| | NVMe-oF |

| | |
|--|---|
| Bundle de seguridad y cumplimiento de normativas | Protección autónoma de ransomware |
| | MTKM |
| | SnapLock |
| Bundle de protección de datos | SnapMirror (asíncrono, síncrono, continuidad del negocio) |
| | SnapCenter |
| | S3 SnapMirror para destinos NetApp |
| Bundle de cloud híbrido | SnapMirror Cloud |
| | SnapMirror de S3 para destinos que no son de NetApp |
| Bundle de cifrado | Cifrado de volúmenes de NetApp |
| | Módulo de plataforma de confianza |

Licencias no incluidas con ONTAP One

ONTAP One no incluye ninguno de los servicios proporcionados en cloud de NetApp, como los siguientes:

- Organización en niveles de BlueXP
- Cloud Insights
- Backup de BlueXP
- Regulación de datos

ONTAP One para sistemas existentes

Si tiene sistemas existentes que se encuentran actualmente en soporte de NetApp pero no se han actualizado a ONTAP One, las licencias existentes en esos sistemas siguen siendo válidas y siguen funcionando según lo previsto. Por ejemplo, si la licencia de SnapMirror ya está instalada en sistemas existentes, no es necesario actualizar a ONTAP One para obtener una nueva licencia de SnapMirror. Sin embargo, si no tiene instalada una licencia de SnapMirror en un sistema ya existente, la única forma de obtener dicha licencia consiste en actualizar a ONTAP One por una tarifa adicional.

A partir de junio de 2023, los sistemas ONTAP que utilizan claves de licencia de 28 caracteres también pueden ["Actualizar al paquete de compatibilidad ONTAP One o ONTAP Base"](#).

Licencias incluidas con ONTAP Base

Base de ONTAP es una suite de software opcional que es una alternativa a ONTAP One para los sistemas ONTAP. Es para casos de uso específicos en los que no se necesitan tecnologías de protección de datos como SnapMirror y SnapCenter, así como funciones de seguridad como ransomware autónomo, como sistemas que no son de producción para entornos de prueba o desarrollo dedicados. No se pueden añadir licencias adicionales a la base de ONTAP. Si desea añadir licencias, como SnapMirror, debe actualizar a ONTAP One.

| | |
|--------------------------|------------------------|
| Nombre de grupo anterior | Claves ONTAP incluidas |
|--------------------------|------------------------|

| | |
|-------------------|-----------------------------------|
| Bundle principal | FlexClone |
| | SnapRestore |
| | NFS, SMB, S3 |
| | FC, iSCSI |
| | NVMe-oF |
| Bundle de cifrado | Cifrado de volúmenes de NetApp |
| | Módulo de plataforma de confianza |

Licencias incluidas con ONTAP One para SAN

ONTAP One para SAN está disponible para los sistemas ASA A-series y C-series. Se trata de la única suite de software disponible para SAN. ONTAP One para SAN contiene las siguientes licencias:

| |
|---|
| Claves ONTAP incluidas |
| FlexClone |
| SnapRestore |
| FC, iSCSI |
| NVMe-oF |
| MTKM |
| SnapLock |
| SnapMirror (asíncrono, síncrono, continuidad del negocio) |
| SnapCenter |
| SnapMirror Cloud |
| Cifrado de volúmenes de NetApp |
| Módulo de plataforma de confianza |

Otros métodos de entrega de licencias

En ONTAP 8.2 a ONTAP 9.9.1, las claves de licencia se entregan como cadenas de 28 caracteres y hay una clave por función ONTAP. Utilice la interfaz de línea de comandos de ONTAP para instalar claves de licencia si utiliza ONTAP 8,2 a través de ONTAP 9,9.1.



ONTAP 9.10.1 admite la instalación de claves de licencia de 28 caracteres mediante System Manager o la CLI. Sin embargo, si se instala una licencia NLF para una función, no es posible instalar una clave de licencia de 28 caracteres en el archivo de licencia de NetApp para la misma función. Para obtener información sobre la instalación de NLF o claves de licencia mediante System Manager, consulte ["Instalar licencias de ONTAP"](#).

Información relacionada

["Cómo obtener una licencia de ONTAP One cuando el sistema ya tiene NLF"](#)

["Cómo comprobar las autorizaciones de software de ONTAP y las claves de licencia relacionadas a través del sitio de soporte"](#)

Descargue los archivos de licencia de NetApp (NLF) desde el sitio de soporte de NetApp

Si el sistema ejecuta ONTAP 9.10.1 o una versión posterior, puede actualizar los archivos de licencia del paquete en los sistemas existentes descargando NLF para ONTAP One o ONTAP Core desde el sitio de soporte de NetApp.



Las licencias de SnapMirror Cloud y S3 de SnapMirror no se incluyen con ONTAP One. Forman parte del paquete de compatibilidad ONTAP One, que puede obtener de forma gratuita si tiene ONTAP One y. "[solicite por separado](#)".

Pasos

Puede descargar archivos de licencia de ONTAP One para sistemas con paquetes de archivos de licencia de NetApp existentes y para sistemas con claves de licencia de 28 caracteres que se han convertido a archivos de licencia de NetApp en sistemas que ejecutan ONTAP 9.10.1 y versiones posteriores. Por un cargo, también puede actualizar los sistemas de la base ONTAP a ONTAP One.

Actualice NLF existente

1. Póngase en contacto con su equipo de ventas de NetApp y solicite el paquete de archivos de licencia que desee actualizar o convertir (por ejemplo, ONTAP Base to ONTAP One o el paquete central y el paquete de protección de datos a ONTAP One).

Cuando se procese su solicitud, recibirá un correo electrónico de netappsw@netapp.com con el asunto «Notificación de licencias de software de NetApp para el n.o de SO [número de SO]» y el correo electrónico incluirá un archivo adjunto en PDF que incluya el número de serie de su licencia.

2. Inicie sesión en la ["Sitio de soporte de NetApp"](#).
3. Seleccione **Sistemas > Licencias de software**.
4. En el menú, elija **Número de serie**, ingrese el número de serie que recibió y haga clic en **Nueva búsqueda**.
5. Localice el paquete de licencias que desea convertir.
6. Haga clic en **Obtener archivo de licencia de NetApp** para cada paquete de licencia y descargue los NLF cuando estén disponibles.
7. ["Instale"](#) El archivo ONTAP One.

Actualizar NLF convertido desde clave de licencia

1. Inicie sesión en la ["Sitio de soporte de NetApp"](#).
2. Seleccione **Sistemas > Licencias de software**.
3. En el menú, elija **Número de serie**, ingrese el número de serie del sistema y haga clic en **Nueva búsqueda**.
4. Localice la licencia que desea convertir, y en la columna **Elegibilidad** haga clic en **Comprobar**.
5. En el formulario **Comprobar elegibilidad**, haz clic en **Generar licencias para 9,10.x y posteriores**.
6. Cierre el formulario **Comprobar elegibilidad**.

Tendrá que esperar al menos 2 horas para que se generen las licencias.

7. Repita los pasos 1 a 3.
8. Busque la licencia de ONTAP One, haga clic en **Obtener archivo de licencia de NetApp** y elija el método de entrega.
9. ["Instale"](#) El archivo ONTAP One.

Instalar licencias de ONTAP

Puede instalar los archivos de licencia de NetApp (NLF) y las claves de licencia mediante System Manager, que es el método preferido para instalar NLF, o bien puede utilizar la interfaz de línea de comandos de ONTAP para instalar las claves de licencia. En ONTAP 9.10.1 y versiones posteriores, las funciones se habilitan con un archivo de licencia de NetApp, y en versiones anteriores a ONTAP 9.10.1, las funciones de ONTAP se habilitan con claves de licencia.

Pasos

Si ya lo ha hecho ["Archivos de licencia de NetApp descargados"](#) O las claves de licencia, puede usar System

Manager o la interfaz de línea de comandos de ONTAP para instalar NLF y las claves de licencia de 28 caracteres.

System Manager: ONTAP 9,8 y versiones posteriores

- 1. Seleccione **Cluster > Settings**.
- 2. En **Licencias**, seleccione ➔.
- 3. Seleccione **examinar**. Elija el archivo de licencia de NetApp que descargó.
- 4. Si desea añadir claves de licencia, seleccione **usar claves de licencia de 28 caracteres** e introduzca las claves.

System Manager: ONTAP 9,7 y versiones anteriores

- 1. Selecciona **Configuración > Clúster > Licencias**.
- 2. En **Licencias**, seleccione ➔.
- 3. En la ventana **Paquetes**, haga clic en **Agregar**.
- 4. En el cuadro de diálogo **Agregar paquetes de licencia**, haga clic en **elegir archivos** para seleccionar el archivo de licencia de NetApp que ha descargado y, a continuación, haga clic en **Agregar** para cargar el archivo en el clúster.

CLI

- 1. Añada una o más claves de licencia:

```
system license add
```

En el siguiente ejemplo se instalan las licencias del nodo local «/mroot/etc/lic_file» si el archivo existe en esta ubicación:

```
cluster1::> system license add -use-license-file true
```

En el siguiente ejemplo se agrega una lista de licencias con las claves
AA
AA

```
cluster1::> system license add -license-code  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA, BBBB BBBB BBBB BBBB BBBB BBBB BBBB
```

Información relacionada

["Página man para el comando system license add"](#).

Gestione licencias de ONTAP

Puede usar System Manager o la interfaz de línea de comandos de ONTAP para ver y gestionar las licencias instaladas en el sistema, incluida la visualización del número de

serie de la licencia, la comprobación del estado de una licencia y la eliminación de una licencia.

Ver detalles de una licencia

Pasos

La forma de ver los detalles de una licencia depende de la versión de ONTAP que esté usando y de si utiliza System Manager o la CLI de ONTAP.

System Manager: ONTAP 9,8 y versiones posteriores

1. Para ver detalles sobre una licencia de función específica, selecciona **Clúster > Configuración**.
2. En **Licencias**, seleccione ➔.
3. Selecciona **Features**.
4. Busque la función con licencia que desea ver y seleccionar ▼ para ver los detalles de la licencia.

System Manager: ONTAP 9,7 y versiones anteriores

1. Selecciona **Configuración > Clúster > Licencias**.
2. En la ventana **licencias**, realice la acción correspondiente:
3. Haga clic en la ficha **Detalles**.

CLI

1. Mostrar detalles sobre una licencia instalada:

```
system license show
```

Eliminar una licencia

System Manager: ONTAP 9,8 y versiones posteriores

1. Para eliminar una licencia, selecciona **Clúster > Configuración**.
2. En **Licencias**, seleccione ➔.
3. Selecciona **Features**.
4. Seleccione la función con licencia que desea eliminar y * Eliminar clave heredada *.

System Manager: ONTAP 9,7 y versiones anteriores

1. Selecciona **Configuración > Clúster > Licencias**.
2. En la ventana **licencias**, realice la acción correspondiente:

| Si desea... | Realice lo siguiente... |
|--|---|
| Eliminar un paquete de licencia específico de un nodo o una licencia maestra | Haga clic en la ficha Detalles . |
| Elimine un paquete de licencia específico en todos los nodos del clúster | Haga clic en la ficha Paquetes . |

3. Seleccione el paquete de licencia de software que desea eliminar y, a continuación, haga clic en **Eliminar**.

Sólo puede eliminar un paquete de licencia cada vez.

4. Active la casilla de verificación de confirmación y, a continuación, haga clic en **Eliminar**.

CLI

1. Eliminar una licencia:

```
system license delete
```

En el ejemplo siguiente se elimina una licencia llamada CIFS y el número de serie 1-81-00000000000000000000123456 del clúster:

```
cluster1::> system license delete -serial-number 1-81-  
00000000000000000000123456 -package CIFS
```

El siguiente ejemplo elimina del clúster todas las licencias bajo la licencia instalada Core Bundle para el número de serie 123456789:

```
cluster1::> system license delete { -serial-number 123456789  
-installed-license "Core Bundle" }
```

Información relacionada

Tipos de licencia y método con licencia

Comprender los tipos de licencia y el método con licencia le ayuda a gestionar las licencias de un clúster.

Tipos de licencia

Un paquete puede tener uno o varios de los siguientes tipos de licencia instalados en el clúster. La `system license show` el comando muestra los tipos o tipos de licencia instalados para un paquete.

- Licencia estándar (`license`)

Una licencia estándar es una licencia de bloqueo de nodo. Se emite para un nodo con un número de serie de sistema específico (también conocido como *Controller serial number*). Una licencia estándar solo es válida para el nodo que tenga el número de serie coincidente.

La instalación de una licencia estándar de bloqueo de nodo da derecho a un nodo a la funcionalidad con licencia. Para que el clúster utilice funcionalidad con licencia, debe tener licencia al menos un nodo para la funcionalidad. Es posible que no cumpla las normativas para utilizar la funcionalidad con licencia en un nodo que no tenga derechos para la funcionalidad.

- Licencia de sitio (`site`)

Una licencia de sitio no está vinculada a un número de serie de sistema específico. Cuando instala una licencia de sitio, todos los nodos del clúster tienen derecho a la funcionalidad con licencia. La `system license show` comando muestra las licencias de sitio bajo el número de serie del clúster.

Si su clúster tiene una licencia de sitio y quita un nodo del clúster, el nodo no lleva consigo la licencia del sitio y ya no puede optar a la funcionalidad con licencia. Si agrega un nodo a un clúster que tiene una licencia de sitio, el nodo tendrá automáticamente derecho a la funcionalidad concedida por la licencia del sitio.

- Licencia de evaluación (`demo`)

Una licencia de evaluación es una licencia temporal que expira después de un cierto período de tiempo (indicado por el `system license show`). Le permite probar ciertas funcionalidades de software sin tener que adquirir derechos. Es una licencia para todo el clúster y no está vinculada a un número de serie específico de un nodo.

Si su clúster tiene una licencia de evaluación de un paquete y quita un nodo del clúster, el nodo no lleva con ella la licencia de evaluación.

Método con licencia

Es posible instalar una licencia para todo el clúster (el `site` o `demo` escriba) y una licencia de bloqueo de nodo (el `license` escriba) para un paquete. Por lo tanto, un paquete instalado puede tener varios tipos de licencia en el clúster. Sin embargo, para el clúster, sólo hay un método *licensy* para un paquete. La `licensed method` del `system license status show` comando muestra el derecho que se está utilizando para un paquete. El comando determina el método con licencia de la siguiente manera:

- Si un paquete solo tiene un tipo de licencia instalado en el clúster, el tipo de licencia instalada es el método con licencia.
- Si un paquete no tiene licencias instaladas en el clúster, el método con licencia es `none`.
- Si un paquete tiene varios tipos de licencia instalados en el clúster, el método con licencia se determina en el siguiente orden de prioridad del tipo de licencia: `site`, `license`, y `demo`.

Por ejemplo:

- Si tiene una licencia de sitio, una licencia estándar y una licencia de evaluación de un paquete, el método con licencia del paquete en el clúster es `site`.
- Si tiene una licencia estándar y una licencia de evaluación de un paquete, el método con licencia del paquete en el clúster es `license`.
- Si solo tiene una licencia de evaluación de un paquete, el método con licencia del paquete en el clúster es `demo`.

Comandos para gestionar licencias

Es posible usar la CLI de ONTAP `system license` comandos para gestionar las licencias de funciones para el clúster. Utilice la `system feature-usage` comandos para supervisar el uso de funciones.

En la siguiente tabla, se enumeran algunos de los comandos comunes de la CLI para gestionar licencias y los enlaces a las páginas manuales de comandos para obtener información adicional.

| Si desea... | Se usa este comando... |
|--|--|
| Muestre todos los paquetes que requieren licencias y el estado actual de su licencia, incluidos los siguientes: <ul style="list-style-type: none"> • El nombre del paquete • El método con licencia • La fecha de caducidad, si procede | "show-status de la licencia del sistema" |
| Muestra o elimina licencias caducadas o no utilizadas | "limpieza de la licencia del sistema" |
| Mostrar un resumen del uso de las funciones en el clúster por nodo | "resumen del uso de funciones del sistema" |
| Muestre el estado de uso de las funciones en el clúster por nodo y por semana | "show-history de uso de funciones del sistema" |

| Si desea... | Se usa este comando... |
|--|---|
| Muestra el estado del riesgo de autorización de licencia de cada paquete de licencia | "exposición de riesgo de derecho de licencia del sistema" |

Información relacionada

["Comandos de ONTAP 9"](#)

["Artículo de la base de conocimientos: Información general sobre licencias de ONTAP 9.10.1 y posterior"](#)

["Utilice System Manager para instalar un archivo de licencia de NetApp"](#)

Gestión de clústeres con la CLI

Información general de administración con la interfaz de línea de comandos

Los sistemas ONTAP pueden administrarse con la interfaz de línea de comandos (CLI). Puede usar las interfaces de gestión ONTAP, acceder al clúster, gestionar nodos y mucho más.

Debe utilizar estos procedimientos en las siguientes circunstancias:

- Desea comprender la gama de funcionalidades de administrador de ONTAP.
- Desea utilizar la CLI, no System Manager ni una herramienta de secuencias de comandos automatizadas.

Información relacionada

Para obtener más detalles sobre la sintaxis y el uso de la CLI, consulte

["Referencia de páginas del manual de ONTAP 9"](#) documentación.

Administradores de clústeres y SVM

Administradores de clústeres y SVM

Los administradores de clúster administran todo el clúster y las máquinas virtuales de almacenamiento (SVM, antes denominadas Vserver) que contiene. Los administradores de SVM solo administran sus propias SVM de datos.

Los administradores del clúster pueden administrar todo el clúster y sus recursos. También pueden configurar SVM de datos y delegar la administración de SVM a los administradores de SVM. Las funcionalidades específicas que tienen los administradores de clúster dependen de sus roles de control de acceso. De forma predeterminada, un administrador de clúster con el nombre de cuenta o el nombre de la función «'admin'» tiene todas las funcionalidades necesarias para gestionar el clúster y las SVM.

Los administradores de SVM solo pueden administrar sus propios recursos de red y almacenamiento de SVM, como volúmenes, protocolos, LIF y servicios. Las funcionalidades específicas que tienen los administradores de SVM dependen de los roles de control de acceso que asignan los administradores del clúster.



La interfaz de línea de comandos (CLI) de ONTAP sigue utilizando el término `vserver` en la salida y `vserver` como comando o nombre de parámetro no se ha modificado.

Gestione el acceso a System Manager

Puede habilitar o deshabilitar el acceso de un navegador web a System Manager. También puede ver el registro de System Manager.

Puede controlar el acceso de un navegador web a System Manager mediante `vserver services web modify -name sysmgr -vserver cluster_name -enabled[true|false]`.

El registro de System Manager se registra en la `/mroot/etc/log/mlog/sysmgr.log` Archivos del nodo que aloja la LIF de gestión del clúster en el momento en que se accede a System Manager. Puede ver los archivos de registro mediante un explorador. El registro de System Manager también se incluye en los mensajes de AutoSupport.

Qué es el servidor de administración de clústeres

El servidor de gestión de clústeres, también llamado *adminSVM*, es una implementación de máquinas virtuales de almacenamiento (SVM) especializada que presenta el clúster como una única entidad gestionable. Además de servir como dominio administrativo de nivel superior, el servidor de gestión de clústeres posee recursos que no pertenecen lógicamente a una SVM de datos.

El servidor de gestión de clústeres está siempre disponible en el clúster. Puede acceder al servidor de gestión de clústeres mediante la LIF de gestión de la consola o el clúster.

En caso de fallo del puerto de red inicial, el LIF de gestión de clústeres conmuta automáticamente a otro nodo del clúster. En función de las características de conectividad del protocolo de gestión que utilice, es posible que note la conmutación por error o no. Si utiliza un protocolo sin conexión (por ejemplo, SNMP) o tiene una conexión limitada (por ejemplo, HTTP), no es probable que note la conmutación por error. Sin embargo, si utiliza una conexión a largo plazo (por ejemplo, SSH), deberá volver a conectarse al servidor de gestión de clústeres después de la conmutación al respaldo.

Cuando se crea un clúster, se configuran todas las características de la LIF de gestión del clúster, incluida su dirección IP, máscara de red, puerta de enlace y puerto.

A diferencia de una SVM de datos o una SVM de nodo, un servidor de gestión de clústeres no tiene un volumen raíz o volúmenes de usuario host (aunque puede alojar volúmenes del sistema). Además, un servidor de gestión de clústeres solo puede tener LIF del tipo de gestión de clústeres.

Si ejecuta el `vserver show` comando, el servidor de gestión de clústeres aparece en la lista de resultados de ese comando.

Tipos de SVM

Un clúster consta de cuatro tipos de SVM que ayudan a gestionar el clúster y sus recursos y el acceso a los datos a los clientes y las aplicaciones.

Un clúster contiene los siguientes tipos de SVM:

- SVM de administrador

El proceso de configuración del clúster crea automáticamente la SVM de administrador para el clúster. La SVM de administrador representa el clúster.

- SVM de nodo

Se crea una SVM de nodo cuando el nodo se une al clúster y la SVM de nodo representa los nodos individuales del clúster.

- SVM del sistema (avanzada)

Una SVM del sistema se crea automáticamente para las comunicaciones a nivel de clúster en un espacio IP.

- SVM de datos

Una SVM de datos representa los servicios de datos de las SVM. Tras la configuración del clúster, un administrador de clúster debe crear las SVM de datos y añadir volúmenes a estas SVM para facilitar el acceso a los datos desde el clúster.

Un clúster debe tener al menos una SVM de datos para servir datos a sus clientes.



A menos que se especifique lo contrario, el término SVM hace referencia a una SVM de datos (que sirve datos).

En la CLI, las SVM se muestran como Vserver.

Acceder al clúster mediante la CLI (solo administradores de clúster)

Acceda al clúster mediante el puerto serie

Puede acceder al clúster directamente desde una consola conectada al puerto de serie de un nodo.

Pasos

1. En la consola, pulse Intro.

El sistema responde con la solicitud de inicio de sesión.

2. En la solicitud de inicio de sesión, realice una de las siguientes acciones:

| Para acceder al clúster con... | Introduzca el siguiente nombre de cuenta... |
|--|---|
| La cuenta de clúster predeterminada | admin |
| Una cuenta de usuario administrativo alternativa | <i>username</i> |

El sistema responde con el aviso de contraseña.

3. Introduzca la contraseña de la cuenta de usuario administrador o administrativa y, a continuación, pulse Intro.

Acceda al clúster mediante SSH

Puede emitir solicitudes de SSH al clúster para realizar tareas administrativas. De forma predeterminada, SSH está habilitado.

Lo que necesitará

- Debe tener una cuenta de usuario configurada para usar `ssh` como método de acceso.

La `-application` parámetro de `security login` los comandos especifican el método de acceso para una cuenta de usuario. La `security login` ["páginas de manual"](#) contienen información adicional.

- Si utiliza una cuenta de usuario de dominio de Active Directory (AD) para acceder al clúster, debe haberse configurado un túnel de autenticación del clúster a través de una máquina virtual de almacenamiento habilitada para CIFS, y la cuenta de usuario de dominio de AD también se debe haber añadido al clúster con `ssh` como método de acceso y `domain` como método de autenticación.
- Si utiliza conexiones IPv6, IPv6 ya debe estar configurado y habilitado en el clúster, y las políticas de firewall ya deben estar configuradas con direcciones IPv6.

La `network options ipv6 show` Command muestra si IPv6 está habilitado. La `system services firewall policy show` comando muestra las directivas de firewall.

Acerca de esta tarea

- Debe utilizar un cliente OpenSSH 5.7 o posterior.
- Solo se admite el protocolo SSH v2; no se admite SSH v1.
- ONTAP admite un máximo de 64 sesiones de SSH simultáneas por nodo.

Si el LIF de gestión del clúster reside en el nodo, comparte este límite con la LIF de gestión del nodo.

Si la tasa de conexiones entrantes es superior a 10 por segundo, el servicio se deshabilitará temporalmente durante 60 segundos.

- ONTAP solo admite los algoritmos de cifrado AES y 3DES (también conocidos como *cifrados*) para SSH.

AES es compatible con una longitud de clave de 128, 192 y 256 bits. 3DES tiene una longitud de clave de 56 bits como EN EL DES original, pero se repite tres veces.

- Cuando el modo FIPS está activado, los clientes SSH deben negociar con los algoritmos de clave pública del algoritmo de firma digital de curva elíptica (ECDSA) para que la conexión sea exitosa.
- Si desea acceder a la CLI de ONTAP desde un host de Windows, puede utilizar una herramienta de otro proveedor, como PuTTY.
- Si utiliza un nombre de usuario de Windows AD para iniciar sesión en ONTAP, debe usar las mismas letras mayúsculas o minúsculas que se usaron cuando se crearon el nombre de usuario y el nombre de dominio de AD en ONTAP.

Los nombres de usuario y de dominio DE AD no distinguen mayúsculas de minúsculas. Sin embargo, los nombres de usuario de ONTAP distinguen mayúsculas de minúsculas. La discrepancia entre el nombre de usuario creado en ONTAP y el nombre de usuario creado en AD provoca un error de inicio de sesión.

Opciones de autenticación SSH

- A partir de ONTAP 9.3, puede hacerlo ["Habilite la autenticación multifactor SSH"](#) para cuentas de

administrador local.

Cuando la autenticación multifactor en SSH está habilitada, los usuarios se autentican mediante una clave pública y una contraseña.

- A partir de ONTAP 9.4, puede hacerlo ["Habilite la autenticación multifactor SSH"](#) Para usuarios remotos LDAP y NIS.
- A partir de ONTAP 9.13.1, opcionalmente puede añadir validación de certificados al proceso de autenticación SSH para mejorar la seguridad de inicio de sesión. Para hacer esto, ["Asocie un certificado X,509 a la clave pública"](#) que utiliza una cuenta. Si inicia sesión mediante SSH con una clave pública SSH y un certificado X,509, ONTAP comprueba la validez del certificado X,509 antes de autenticarse con la clave pública SSH. El inicio de sesión SSH se rechaza si ese certificado caduca o se revoca y la clave pública SSH se deshabilita automáticamente.
- A partir de ONTAP 9.14.1, puede agregar opcionalmente la autenticación de dos factores Cisco Duo al proceso de autenticación SSH para mejorar la seguridad de inicio de sesión. Tras iniciar sesión por primera vez después de habilitar la autenticación de Cisco Duo, los usuarios deberán inscribir un dispositivo para que sirva como autenticador para las sesiones SSH. Consulte ["Configurar Cisco Duo 2FA para inicios de sesión SSH"](#) Para obtener más información sobre la configuración de la autenticación SSH de Cisco Duo para ONTAP.

Pasos

1. Desde un host de administración, introduzca el `ssh` comando en uno de los siguientes formatos:

- `ssh username@hostname_or_IP [command]`
- `ssh -l username hostname_or_IP [command]`

Si utiliza una cuenta de usuario de dominio de AD, debe especificar *username* en el formato de *domainname\AD_accountname* (con barras diagonales dobles después del nombre de dominio) o `"domainname\AD_accountname"` (entre comillas dobles y con una sola barra diagonal inversa después del nombre de dominio).

hostname_or_IP Es el nombre de host o la dirección IP de la LIF de gestión de clústeres o una LIF de gestión de nodos. Se recomienda utilizar la LIF de gestión del clúster. Es posible usar una dirección IPv4 o IPv6.

command No es necesario para las sesiones interactivas con SSH.

Ejemplos de solicitudes SSH

Los siguientes ejemplos muestran cómo la cuenta de usuario denominada «joe» puede emitir una solicitud SSH para acceder a un clúster cuya LIF de gestión de clústeres sea 10.72.137.28:

```
$ ssh joe@10.72.137.28
Password:
cluster1::> cluster show
Node           Health  Eligibility
-----
node1           true   true
node2           true   true
2 entries were displayed.
```

```
$ ssh -l joe 10.72.137.28 cluster show
Password:
Node                Health  Eligibility
-----
node1                true   true
node2                true   true
2 entries were displayed.
```

Los siguientes ejemplos muestran cómo la cuenta de usuario denominada «john» del dominio denominado «DOMAIN1» puede emitir una solicitud SSH para acceder a un clúster cuya LIF de gestión de clústeres sea 10.72.137.28:

```
$ ssh DOMAIN1\\john@10.72.137.28
Password:
cluster1::> cluster show
Node                Health  Eligibility
-----
node1                true   true
node2                true   true
2 entries were displayed.
```

```
$ ssh -l "DOMAIN1\john" 10.72.137.28 cluster show
Password:
Node                Health  Eligibility
-----
node1                true   true
node2                true   true
2 entries were displayed.
```

En el siguiente ejemplo, se muestra cómo la cuenta de usuario llamada «joe» puede emitir una solicitud MFA de SSH para acceder a un clúster cuyo LIF de gestión de clústeres sea 10.72.137.32:

```
$ ssh joe@10.72.137.32
Authenticated with partial success.
Password:
cluster1::> cluster show
Node                Health  Eligibility
-----
node1                true   true
node2                true   true
2 entries were displayed.
```

Información relacionada

["Autenticación de administrador y RBAC"](#)

Seguridad de inicio de sesión SSH

A partir de ONTAP 9.5, puede ver información acerca de inicios de sesión anteriores, intentos fallidos de inicio de sesión y cambios en sus privilegios desde el último inicio de sesión correcto.

La información relacionada con la seguridad se muestra cuando inicia sesión correctamente como usuario administrador de SSH. Se le ha alertado de las siguientes condiciones:

- La última vez que se inició sesión en su nombre de cuenta.
- Número de intentos de inicio de sesión fallidos desde el último inicio de sesión correcto.
- Si el rol ha cambiado desde el último inicio de sesión (por ejemplo, si el rol de la cuenta del administrador ha cambiado de "admin" a "backup").
- Si las funcionalidades de adición, modificación o eliminación del rol se modificaron desde el último inicio de sesión.



Si alguna de las informaciones mostradas es sospechosa, debe ponerse en contacto inmediatamente con su departamento de seguridad.

Para obtener esta información al iniciar sesión, se deben cumplir los siguientes requisitos previos:

- Su cuenta de usuario SSH debe estar aprovisionada en ONTAP.
- Se debe crear el inicio de sesión de seguridad SSH.
- Su intento de inicio de sesión debe ser correcto.

Restricciones y otras consideraciones sobre la seguridad de inicio de sesión SSH

Las siguientes restricciones y consideraciones se aplican a la información de seguridad de inicio de sesión SSH:

- La información solo está disponible para inicios de sesión basados en SSH.
- En el caso de las cuentas admin basadas en grupos, como las cuentas LDAP/NIS y AD, los usuarios pueden ver la información de inicio de sesión SSH si el grupo al que pertenecen se aprovisiona como una cuenta de administrador en ONTAP.

Sin embargo, estos usuarios no pueden mostrar alertas sobre los cambios en el rol de la cuenta de usuario. Además, los usuarios que pertenecen a un grupo AD aprovisionado como cuenta de administrador en ONTAP no pueden ver el número de intentos de inicio de sesión fallidos que se produjeron desde la última vez que se iniciaron sesión.

- La información que se mantiene para un usuario se elimina cuando la cuenta de usuario se elimina de ONTAP.
- La información no se muestra para las conexiones con aplicaciones distintas de SSH.

Ejemplos de información de seguridad de inicio de sesión SSH

Los siguientes ejemplos muestran el tipo de información que se muestra después de iniciar sesión.

- Este mensaje se muestra después de cada inicio de sesión correcto:

```
Last Login : 7/19/2018 06:11:32
```

- Estos mensajes se muestran si no se han podido iniciar sesión desde la última sesión correcta:

```
Last Login : 4/12/2018 08:21:26
Unsuccessful login attempts since last login - 5
```

- Estos mensajes se muestran si no se ha podido iniciar sesión y los privilegios se han modificado desde el último inicio de sesión correcto:

```
Last Login : 8/22/2018 20:08:21
Unsuccessful login attempts since last login - 3
Your privileges have changed since last login
```

Active el acceso Telnet o RSH al clúster

Como práctica recomendada de seguridad, Telnet y RSH están desactivados en la directiva de firewall de administración predefinida (`mgmt`). Para permitir que el clúster acepte solicitudes Telnet o RSH, debe crear una nueva política de firewall de administración que tenga habilitada Telnet o RSH y, a continuación, asociar la nueva directiva con la LIF de administración de clústeres.

Acerca de esta tarea

ONTAP evita el cambio de políticas de firewall predefinidas, pero puede crear una nueva política clonando los predefinidos `mgmt`. Política de firewall de administración y, a continuación, habilitar Telnet o RSH bajo la nueva directiva. Sin embargo, Telnet y RSH no son protocolos seguros, por lo que se debe considerar el uso de SSH para acceder al clúster. SSH proporciona un shell remoto seguro y una sesión de red interactiva.

Siga estos pasos para activar el acceso Telnet o RSH a los clústeres:

Pasos

1. Entre en el modo de privilegio avanzado:
`set advanced`
2. Activar un protocolo de seguridad (RSH o Telnet):
`security protocol modify -application security_protocol -enabled true`
3. Cree una nueva política de firewall de administración basada en `mgmt` política de firewall de gestión:
`system services firewall policy clone -policy mgmt -destination-policy policy-name`
4. Active Telnet o RSH en la nueva política de firewall de administración:
`system services firewall policy create -policy policy-name -service security_protocol -action allow -ip-list ip_address/netmask`
Para permitir todas las direcciones IP, debe especificar `-ip-list 0.0.0.0/0`

5. Asocie la nueva política con la LIF de gestión del clúster:

```
network interface modify -vserver cluster_management_LIF -lif cluster_mgmt  
-firewall-policy policy-name
```

Acceda al clúster mediante Telnet

Puede enviar solicitudes Telnet al clúster para realizar tareas administrativas. Telnet está desactivado de forma predeterminada.

Lo que necesitará

Para poder utilizar Telnet para acceder al clúster se deben cumplir las siguientes condiciones:

- Debe tener una cuenta de usuario local de clúster configurada para utilizar Telnet como método de acceso.

La `-application` parámetro de `security login` los comandos especifican el método de acceso para una cuenta de usuario. Para obtener más información, consulte `security login` páginas de manual.

- Telnet debe estar activado en la política de firewall de gestión que utilizan las LIF de administración del clúster o nodo para que las solicitudes Telnet puedan pasar por el firewall.

De forma predeterminada, Telnet está desactivado. La `system services firewall policy show` con el `-service telnet` Parámetro muestra si Telnet se ha activado en una directiva de firewall. Para obtener más información, consulte `system services firewall policy` páginas de manual.

- Si utiliza conexiones IPv6, IPv6 ya debe estar configurado y habilitado en el clúster, y las políticas de firewall ya deben estar configuradas con direcciones IPv6.

La `network options ipv6 show` Command muestra si IPv6 está habilitado. La `system services firewall policy show` comando muestra las directivas de firewall.

Acerca de esta tarea

- Telnet no es un protocolo seguro.

Debe considerar utilizar SSH para acceder al clúster. SSH proporciona un shell remoto seguro y una sesión de red interactiva.

- ONTAP admite un máximo de 50 sesiones Telnet simultáneas por nodo.

Si el LIF de gestión del clúster reside en el nodo, comparte este límite con la LIF de gestión del nodo.

Si la tasa de conexiones próximas es superior a 10 por segundo, el servicio se deshabilitará temporalmente durante 60 segundos.

- Si desea acceder a la CLI de ONTAP desde un host de Windows, puede utilizar una herramienta de otro proveedor, como PuTTY.

Pasos

1. Desde un host de administración, introduzca el siguiente comando:

```
telnet hostname_or_IP
```

hostname_or_IP Es el nombre de host o la dirección IP de la LIF de gestión de clústeres o una LIF de

gestión de nodos. Se recomienda utilizar la LIF de gestión del clúster. Es posible usar una dirección IPv4 o IPv6.

Ejemplo de una solicitud Telnet

El siguiente ejemplo muestra cómo el usuario llamado "joe", que se ha configurado con acceso Telnet, puede emitir una solicitud Telnet para acceder a un clúster cuya LIF de administración de clúster es 10.72.137.28:

```
admin_host$ telnet 10.72.137.28
Data ONTAP
login: joe
Password:
cluster1::>
```

Acceda al clúster mediante RSH

Puede emitir solicitudes RSH al clúster para realizar tareas administrativas. RSH no es un protocolo seguro y está deshabilitado de forma predeterminada.

Lo que necesitará

Para poder utilizar RSH, se deben cumplir las siguientes condiciones:

- Es necesario tener una cuenta de usuario local de clúster que se haya configurado para utilizar RSH como método de acceso.

La `-application` parámetro de `security login` los comandos especifican el método de acceso para una cuenta de usuario. Para obtener más información, consulte `security login` páginas de manual.

- RSH ya debe estar habilitado en la directiva de firewall de gestión que utilizan las LIF de administración de clúster o nodo para que las solicitudes RSH puedan atravesar el firewall.

De forma predeterminada, RSH está desactivado. La `system services firewall policy show` con el `-service rsh` Parámetro muestra si RSH se ha habilitado en una directiva de firewall. Para obtener más información, consulte `system services firewall policy` páginas de manual.

- Si utiliza conexiones IPv6, IPv6 ya debe estar configurado y habilitado en el clúster, y las políticas de firewall ya deben estar configuradas con direcciones IPv6.

La `network options ipv6 show` Command muestra si IPv6 está habilitado. La `system services firewall policy show` comando muestra las directivas de firewall.

Acerca de esta tarea

- RSH no es un protocolo seguro.

Debe considerar utilizar SSH para acceder al clúster. SSH proporciona un shell remoto seguro y una sesión de red interactiva.

- ONTAP admite un máximo de 50 sesiones de RSH simultáneas por nodo.

Si el LIF de gestión del clúster reside en el nodo, comparte este límite con la LIF de gestión del nodo.

Si la tasa de conexiones próximas es superior a 10 por segundo, el servicio se deshabilitará temporalmente durante 60 segundos.

Pasos

1. Desde un host de administración, introduzca el siguiente comando:

```
rsh hostname_or_IP -l username:passwordcommand
```

hostname_or_IP Es el nombre de host o la dirección IP de la LIF de gestión de clústeres o una LIF de gestión de nodos. Se recomienda utilizar la LIF de gestión del clúster. Es posible usar una dirección IPv4 o IPv6.

command Es el comando que desea ejecutar a través de RSH.

Ejemplo de una solicitud RSH

El siguiente ejemplo muestra cómo el usuario llamado "joe", que se ha configurado con acceso RSH, puede emitir una solicitud RSH para ejecutar el `cluster show` comando:

```
admin_host$ rsh 10.72.137.28 -l joe:password cluster show
```

| Node | Health | Eligibility |
|-------|--------|-------------|
| node1 | true | true |
| node2 | true | true |

2 entries were displayed.

```
admin_host$
```

Use la interfaz de línea de comandos de ONTAP

Mediante la interfaz de línea de comandos de la ONTAP

La interfaz de línea de comandos (CLI) de ONTAP proporciona una vista basada en comandos de la interfaz de gestión. Introduzca los comandos en el símbolo del sistema de almacenamiento, y los resultados de los comandos se muestran en el texto.

El símbolo del sistema de la CLI se representa como `cluster_name::>`.

Si se configura el nivel de privilegio (es decir, el `-privilege` parámetro de `set` comando) a `advanced`, el símbolo del sistema incluye un asterisco (*), por ejemplo:

```
cluster_name::*>
```

Acerca de los distintos shell para los comandos de la CLI (solo administradores de clúster)

El clúster tiene tres shell diferentes para los comandos de la CLI, el *clustershell*, el *nodeshell* y el *systemshell*. Los shells son para propósitos diferentes, y cada uno tiene un conjunto de comandos diferente.

- Clustershell es el shell nativo que se inicia automáticamente cuando se inicia sesión en el clúster.

Se proporcionan todos los comandos que necesita para configurar y gestionar el clúster. Ayuda de CLI de clustershell (desencadenado por `?` en el símbolo del sistema clustershell) muestra los comandos clustershell disponibles. La `man command_name` en el clustershell muestra la página `man` del comando clustershell especificado.

- El nodesinferno es un shell especial para comandos que sólo tienen efecto a nivel de nodo.

El nodesinferno es accesible a través del `system node run` comando.

La ayuda de la CLI de Nodesinferno (activada por `?` o `help` en el prompt de nodeshell) muestra los comandos nodeshell disponibles. La `man command_name` comando en el nodeshell muestra la página `man` para el comando nodeshell especificado.

Muchos comandos y opciones de nodeshell utilizados comúnmente se tunean o se alian en el clustershell y pueden ejecutarse también desde el clustershell.

- El shell del sistema es un shell de bajo nivel que se utiliza sólo para fines de diagnóstico y solución de problemas.

El shell del sistema y la cuenta asociada "diag" están destinados a fines de diagnóstico de bajo nivel. Su acceso requiere el nivel de privilegio de diagnóstico y se reserva únicamente para que el soporte técnico realice tareas de solución de problemas.

Acceso a comandos y opciones nodeshell en el clustershell

Los comandos y opciones de Nodeshell son accesibles a través de Nodeshell:

```
system node run -node nodename
```

Muchos comandos y opciones de nodeshell utilizados comúnmente se tunean o se alian en el clustershell y pueden ejecutarse también desde el clustershell.

Se puede acceder a las opciones de Nodeshell que son compatibles con el clustershell mediante el `vserver options clustershell` comando. Para ver estas opciones, puede realizar una de las siguientes acciones:

- Consulte la CLI de clustershell con `vserver options -vserver nodename_or_clustername -option-name ?`
- Acceda a `vserver options` Manual en la CLI de clustershell con `man vserver options`

Si introduce un comando u opción nodeshell u legacy en clustershell y el comando u opción tiene un comando clustershell equivalente, ONTAP le informa del comando clustershell para utilizarlo.

Si introduce un comando u opción nodeshell u heredado que no está soportado en clustershell, ONTAP le informa del estado "no soportado" para el comando u opción.

Mostrar los comandos nodeshell disponibles

Puede obtener una lista de los comandos nodeshell disponibles utilizando la ayuda de la CLI de nodeshell.

Pasos

1. Para acceder a nodeshell, introduzca el siguiente comando en el símbolo del sistema del clustershell:


```
system node run -node {nodename|local}
```

local es el nodo que utilizó para acceder al clúster.



La `system node run` el comando tiene un comando de alias, `run`.

2. Introduzca el siguiente comando en el nodeshell para ver la lista de comandos nodeshell disponibles:

```
[commandname] help
```

``_commandname_`` es el nombre del comando cuya disponibilidad desea mostrar. Si no incluye ``_commandname_``, La CLI muestra todos los comandos nodeshell disponibles.

Introduzca `exit` O bien escriba `Ctrl-d` para volver a la CLI del clustershell.

Ejemplo de visualización de comandos nodeshell disponibles

En el ejemplo siguiente se accede al nodo `nodesinfierno` de un nodo llamado 2 y se muestra información sobre el comando nodeshell `environment`:

```
cluster1::> system node run -node node2
Type 'exit' or 'Ctrl-D' to return to the CLI

node2> environment help
Usage: environment status |
      [status] [shelf [<adapter>[.<shelf-number>]]] |
      [status] [shelf_log] |
      [status] [shelf_stats] |
      [status] [shelf_power_status] |
      [status] [chassis [all | list-sensors | Temperature | PSU 1 |
PSU 2 | Voltage | SYS FAN | NVRAM6-temperature-3 | NVRAM6-battery-3]]
```

Métodos para navegar por los directorios de comandos de la CLI

Los comandos de la CLI se organizan en una jerarquía por directorios de comandos. Puede ejecutar comandos en la jerarquía introduciendo la ruta completa del comando o navegando por la estructura del directorio.

Al utilizar la CLI, puede acceder a un directorio de comandos escribiendo el nombre del directorio en el símbolo del sistema y pulsando Entrar. A continuación, el nombre del directorio se incluye en el texto del indicador para indicar que está interactuando con el directorio de comandos apropiado. Para avanzar más en la jerarquía de comandos, escriba el nombre de un subdirectorio de comandos seguido de la tecla Intro. El nombre del subdirectorio se incluye entonces en el texto del indicador y el contexto se desplaza a ese subdirectorio.

Puede navegar por varios directorios de comandos introduciendo el comando entero. Por ejemplo, puede

mostrar información sobre las unidades de disco introduciendo el `storage disk show` en el símbolo del sistema. También es posible ejecutar el comando navegando por un directorio de comandos cada vez, tal y como se muestra en el ejemplo siguiente:

```
cluster1::> storage
cluster1::storage> disk
cluster1::storage disk> show
```

Los comandos se pueden abreviar introduciendo sólo el número mínimo de letras de un comando que hace que el comando sea único en el directorio actual. Por ejemplo, para abreviar el comando en el ejemplo anterior, es posible introducir `st d sh`. También puede utilizar la tecla TAB para expandir comandos abreviados y mostrar los parámetros de un comando, incluidos los valores de parámetros predeterminados.

Puede utilizar el `top` comando para ir al nivel superior de la jerarquía de comandos y el `up` command o. . . comando para subir un nivel en la jerarquía de comandos.



Los comandos y las opciones de comando precedidos de un asterisco (*) en la CLI sólo se pueden ejecutar en el nivel de privilegio avanzado o superior.

Reglas para especificar valores en la CLI

La mayoría de comandos incluyen uno o más parámetros requeridos o opcionales. Tendrá que especificar un valor para muchos de ellos. Existen algunas reglas para especificar valores en la CLI.

- Un valor puede ser un número, un especificador booleano, una selección de una lista enumerada de valores predefinidos o una cadena de texto.

Algunos parámetros pueden aceptar una lista de dos o más valores separados por coma. No es necesario que las listas de valores separadas por comas estén entre comillas (" "). Siempre que especifique texto, un espacio o un carácter de consulta (cuando no sea una consulta o un texto que empiece por un símbolo de menor que o mayor que), debe colocar comillas delante y detrás de la entidad.

- La CLI interpreta un signo de interrogación (" ? ") como el comando para mostrar información de ayuda de un comando determinado.
- Parte del texto introducido en la CLI, como los nombres de comandos, los parámetros y ciertos valores, no distingue mayúsculas de minúsculas.

Por ejemplo, cuando se introducen valores de parámetros para el `vserver cifs` comandos, se ignora la capitalización. Sin embargo, la mayoría de los valores de parámetros, como los nombres de los nodos, las máquinas virtuales de almacenamiento (SVM), los agregados, los volúmenes e las interfaces lógicas, distinguen mayúsculas de minúsculas.

- Si desea borrar el valor de un parámetro que toma una cadena o una lista, debe especificar un conjunto vacío de comillas (" ") o un guión ("-").
- El signo hash (" # "), también conocido como símbolo almohadilla, indica un comentario para una entrada de línea de comandos; si se utiliza, deberá aparecer después del último parámetro en una línea de comandos.

La CLI ignora el texto entre " # " y el final de la línea.

En el ejemplo siguiente, se crea una SVM con un comentario de texto. A continuación, la SVM se modifica para eliminar el comentario.

```
cluster1::> vserver create -vserver vs0 -subtype default -rootvolume
root_vs0
-aggregate aggr1 -rootvolume-security-style unix -language C.UTF-8 -is
-repository false -ipspace ipspaceA -comment "My SVM"
cluster1::> vserver modify -vserver vs0 -comment ""
```

En el siguiente ejemplo, un comentario de la línea de comandos que utiliza el signo «»#» indica lo que hace el comando.

```
cluster1::> security login create -vserver vs0 -user-or-group-name new-
admin
-application ssh -authmethod password #This command creates a new user
account
```

Métodos para ver el historial de comandos y volver a emitir comandos

Cada sesión de la CLI conserva un historial de todos los comandos emitidos en ella. Puede ver el historial de comandos de la sesión en la que está actualmente. También puede volver a emitir comandos.

Para ver el historial de comandos, puede utilizar `history` comando.

Para volver a emitir un comando, puede utilizar el `redo` comando con uno de los siguientes argumentos:

- Cadena que coincide con parte de un comando anterior

Por ejemplo, si el único `volume` el comando que ha ejecutado es `volume show`, puede utilizar la `redo volume` para volver a ejecutar el comando.

- El código numérico de un comando anterior, según se indica en la `history` comando

Por ejemplo, puede usar el `redo 4` comando para volver a emitir el cuarto comando en la lista de historial.

- Un desplazamiento negativo desde el final de la lista de historial

Por ejemplo, puede usar el `redo -2` comando para volver a emitir el comando que ejecutó hace dos comandos.

Por ejemplo, para rehacer el mandato que es tercero desde el final del historial de comandos, debe introducir el siguiente comando:

```
cluster1::> redo -3
```

Métodos abreviados de teclado para editar comandos de la CLI

El comando en el símbolo del sistema actual es el comando activo. El uso de métodos abreviados de teclado permite editar el comando activo rápidamente. Estos métodos abreviados de teclado son similares a los del shell `tcsh` de UNIX y al editor Emacs.

La tabla siguiente enumera los métodos abreviados de teclado para editar los comandos de la CLI. "Ctrl-" indica que mantiene pulsada la tecla Ctrl mientras escribe el carácter especificado después de ella. "Esc-" indica que pulsa y suelta la tecla Esc y, a continuación, escribe el carácter especificado después de ella.

| Si desea... | Usar el siguiente método abreviado de teclado... |
|--|--|
| Mueva el cursor hacia atrás un carácter | Ctrl-B |
| Flecha hacia atrás | Mueva el cursor hacia delante un carácter |
| Ctrl-F | Flecha hacia delante |
| Mueva el cursor hacia atrás una palabra | ESC-B |
| Mueva el cursor hacia delante una palabra | ESC-F |
| Mueva el cursor al principio de la línea | Ctrl-a |
| Mueva el cursor al final de la línea | Ctrl-E |
| Quite el contenido de la línea de comandos desde el principio de la línea hasta el cursor y guárdelo en el búfer de corte. El búfer de corte actúa como memoria temporal, similar a lo que se llama un <i>portapapeles</i> en algunos programas. | Ctrl-U |
| Quite el contenido de la línea de comandos del cursor al final de la línea y guárdelo en el búfer de corte | Ctrl-K |
| Quite el contenido de la línea de comandos del cursor al final de la siguiente palabra y guárdelo en el búfer de corte | ESC-D. |
| Quite la palabra que hay delante del cursor y guárdela en el búfer de corte | Ctrl-W. |
| Yank el contenido del búfer de corte y empújelo en la línea de comandos del cursor | Ctrl-y |
| Elimine el carácter situado delante del cursor | Ctrl-H |
| Retroceso | Elimine el carácter en el que se encuentra el cursor |

| Si desea... | Usar el siguiente método abreviado de teclado... |
|--|---|
| Ctrl-D. | Borrar la línea |
| Ctrl-C | Borre la pantalla |
| Ctrl-L | Reemplace el contenido actual de la línea de comandos por la entrada anterior de la lista de historial. Con cada repetición del método abreviado de teclado, el cursor de historial se desplaza a la entrada anterior. |
| Ctrl-P | ESC-P |
| Flecha arriba | Reemplace el contenido actual de la línea de comandos por la siguiente entrada de la lista de historial. Con cada repetición del método abreviado de teclado, el cursor de historial se desplaza a la siguiente entrada. |
| Ctrl-N | ESC-N |
| Flecha abajo | Expandir un comando parcialmente introducido o mostrar una entrada válida desde la posición de edición actual |
| Pestaña | Ctrl-I. |
| Mostrar la ayuda sensible al contexto | ? |
| Escapar del mapeo especial del signo de interrogación ("?") character. For instance, to enter a question mark into a command's argument, press Esc and then the "?" carácter. | ESC-? |
| Inicie la salida TTY | Ctrl-Q |
| Detenga la salida TTY | Ctrl-S |

Uso de niveles de privilegios administrativos

Los comandos y parámetros de ONTAP se definen en tres niveles de privilegio: *Admin*, *Advanced* y *Diagnostic*. Los niveles de privilegio reflejan los niveles de habilidad requeridos para realizar las tareas.

- **admin**

La mayoría de los comandos y parámetros están disponibles en este nivel. Se utilizan para tareas comunes o rutinarias.

- **avanzado**

Los comandos y los parámetros en este nivel se utilizan con poca frecuencia, requieren conocimientos avanzados y pueden ocasionar problemas si se utilizan de forma inadecuada.

Los comandos o parámetros avanzados solo se utilizan con la recomendación de personal de soporte.

- **diagnóstico**

Los comandos y los parámetros de diagnóstico son potencialmente perjudiciales. Solo el personal de soporte los utiliza para diagnosticar y solucionar problemas.

Configure el nivel de privilegio en la CLI

Puede establecer el nivel de privilegio en la CLI mediante el `set` comando. Los cambios en la configuración del nivel de privilegio se aplican solo a la sesión en la que se encuentra. No se conservan entre sesiones.

Pasos

1. Para configurar el nivel de privilegio en la CLI, utilice el `set` con el `-privilege` parámetro.

Ejemplo de configuración del nivel de privilegio

En el ejemplo siguiente se establece el nivel de privilegio en Advanced y luego en admin:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by NetApp personnel.
Do you wish to continue? (y or n): y
cluster1::*> set -privilege admin
```

Configure las preferencias de visualización en la CLI de

Puede configurar las preferencias de visualización para una sesión CLI mediante el `set` comando y. `rows` comando. Las preferencias que establezca se aplican solo a la sesión en la que se encuentra. No se conservan entre sesiones.

Acerca de esta tarea

Puede configurar las siguientes preferencias de visualización de la CLI:

- El nivel de privilegio de la sesión de comandos
- Si se emiten confirmaciones para comandos potencialmente disruptivos
- Si es así `show` los comandos muestran todos los campos
- El carácter o caracteres que se van a utilizar como separador de campo

- La unidad predeterminada al informar de tamaños de datos
- El número de filas que muestra la pantalla en la sesión CLI actual antes de que la interfaz detenga la salida

Si no se especifica el número preferido de filas, se ajusta automáticamente en función de la altura real del terminal. Si la altura real no está definida, el número predeterminado de filas es 24.

- El nodo o la máquina virtual de almacenamiento predeterminado (SVM)
- Si un comando continúe debería detenerse si encuentra un error

Pasos

1. Para configurar las preferencias de visualización de la CLI, use la `set` comando.

Para establecer el número de filas que muestra la pantalla en la sesión CLI actual, también puede utilizar `rows` comando.

Para obtener más información, consulte las páginas de manual de `set` comando y `rows` comando.

Ejemplo de configuración de preferencias de visualización en la CLI

En el siguiente ejemplo se establece una coma como separador de campo, establece GB como unidad de tamaño de datos predeterminada y establece el número de filas en 50:

```
cluster1::> set -showseparator "," -units GB
cluster1::> rows 50
```

Métodos de uso de operadores de consulta

La interfaz de administración admite consultas y patrones de estilo UNIX y comodines para permitir que coincida con varios valores en argumentos de parámetro-comando.

En la siguiente tabla se describen los operadores de consulta admitidos:

| Operador | Descripción |
|----------|---|
| * | Comodín que coincide con todas las entradas. Por ejemplo, el comando <code>volume show -volume *tmp*</code> muestra una lista de todos los volúmenes cuyos nombres incluyen la cadena <code>tmp</code> . |
| ! | NO es el operador. Indica un valor que no debe coincidir; por ejemplo, <code>!vs0</code> indica que no coincide con el valor <code>vs0</code> . |
| | |

| Operador | Descripción |
|---|--|
| O operador. Separa dos valores que se van a comparar ; por ejemplo, `*vs0 | vs2* coincide con vs0 o vs2. Puede especificar varias sentencias OR; por ejemplo, `a |
| b* | *c* coincide con la entrada a, cualquier entrada que comience con b, y cualquier entrada que incluya c. |
| .. | Operador de gama. Por ejemplo: 5..10 coincide con cualquier valor de 5 para 10, inclusive. |
| < | Operador menos que. Por ejemplo: <20 coincide con cualquier valor menor que 20. |
| > | Mayor que el operador. Por ejemplo: >5 coincide con cualquier valor mayor que 5. |
| <= | Operador menor que o igual que. Por ejemplo: ≤5 coincide con cualquier valor que sea menor o igual que 5. |
| >= | Operador mayor que o igual que. Por ejemplo: ≥5 coincide con cualquier valor que sea mayor o igual que 5. |
| {query} | Consulta ampliada. Se debe especificar una consulta ampliada como primer argumento después del nombre del comando, antes que los demás parámetros. Por ejemplo, el comando <code>volume modify {-volume *tmp*} -state offline</code> establece offline todos los volúmenes cuyos nombres incluyen la cadena tmp. |

Si desea analizar los caracteres de consulta como literales, debe incluir los caracteres entre comillas dobles (por ejemplo, "<10", "0..100", "*abc*", o "a|b") para devolver los resultados correctos.

Debe escribir los nombres de archivo sin procesar entre comillas dobles para evitar la interpretación de

caracteres especiales. Esto también se aplica a los caracteres especiales utilizados por el clustershell.

Puede utilizar varios operadores de consulta en una sola línea de comandos. Por ejemplo, el comando `volume show -size >1GB -percent-used <50 -vserver !vs1` Muestra todos los volúmenes de más de 1 GB, menos del 50% utilizados y no de la máquina virtual de almacenamiento (SVM) denominada «vs1».

Información relacionada

["Métodos abreviados de teclado para editar comandos de la CLI"](#)

Métodos de uso de consultas extendidas

Puede utilizar consultas ampliadas para hacer coincidir y realizar operaciones en objetos que tienen valores especificados.

Las consultas extendidas se especifican encerrándolas entre corchetes (`{}`). Se debe especificar una consulta ampliada como primer argumento después del nombre del comando, antes que los demás parámetros. Por ejemplo, para establecer sin conexión todos los volúmenes cuyos nombres incluyen la cadena `tmp`, ejecute el comando en el ejemplo siguiente:

```
cluster1::> volume modify {-volume *tmp*} -state offline
```

Las consultas ampliadas son generalmente útiles sólo con `modify` y `delete` comandos. No tienen sentido en `create` o `show` comandos.

La combinación de consultas y operaciones de modificación es una herramienta útil. Sin embargo, puede causar confusión y errores si se implementa incorrectamente. Por ejemplo, mediante el (privilegio avanzado) `system node image modify` el comando para establecer la imagen de software predeterminada de un nodo establece automáticamente la otra imagen de software que no es la predeterminada. El comando del siguiente ejemplo es efectivamente una operación nula:

```
cluster1::*> system node image modify {-isdefault true} -isdefault false
```

Este comando establece la imagen predeterminada actual como la imagen no predeterminada y, a continuación, establece la nueva imagen predeterminada (la imagen no predeterminada anterior) en la imagen no predeterminada, lo que resulta en la retención de la configuración predeterminada original. Para realizar la operación correctamente, puede utilizar el comando tal como se indica en el ejemplo siguiente:

```
cluster1::*> system node image modify {-iscurrent false} -isdefault true
```

Métodos para personalizar la salida del comando show mediante campos

Cuando utilice la `-instance` parámetro con a `show` comando para mostrar detalles, la salida puede ser larga e incluir más información de la necesaria. La `-fields` parámetro de un `show` command le permite mostrar únicamente la información que especifique.

Por ejemplo, ejecutando `volume show -instance` es probable que dé lugar a varias pantallas de

información. Puede utilizar `volume show -fields fieldname[,fieldname...]` personalizar la salida de modo que incluya sólo el campo o campos especificados (además de los campos predeterminados que siempre se muestran). Puede utilizar `-fields ?` para mostrar campos válidos para un `show` comando.

En el siguiente ejemplo, se muestra la diferencia de resultado entre `-instance` y la `-fields` parámetro:

```
cluster1::> volume show -instance

Vserver Name: cluster1-1
Volume Name: vol0
Aggregate Name: aggr0
Volume Size: 348.3GB
Volume Data Set ID: -
Volume Master Data Set ID: -
Volume State: online
Volume Type: RW
Volume Style: flex
...
Space Guarantee Style: volume
Space Guarantee in Effect: true
...
Press <space> to page down, <return> for next line, or 'q' to quit...
...
cluster1::>

cluster1::> volume show -fields space-guarantee,space-guarantee-enabled

vserver  volume  space-guarantee  space-guarantee-enabled
-----  -
cluster1-1 vol0    volume          true
cluster1-2 vol0    volume          true
vs1      root_vol
          volume          true
vs2      new_vol
          volume          true
vs2      root_vol
          volume          true
...
cluster1::>
```

Acerca de los parámetros posicionales

Puede aprovechar la funcionalidad de parámetro posicional de la CLI de ONTAP para aumentar la eficiencia de la entrada de comandos. Puede consultar un comando para identificar parámetros que son posicionales para el comando.

Qué es un parámetro posicional

- Un parámetro posicional es un parámetro que no requiere que especifique el nombre del parámetro antes de especificar el valor del parámetro.
- Un parámetro posicional se puede intersperlevar con parámetros no posicionales en la entrada del comando, siempre y cuando observe su secuencia relativa con otros parámetros posicionales en el mismo comando, como se indica en la **command_name ?** salida.
- Un parámetro posicional puede ser un parámetro obligatorio u opcional para un comando.
- Un parámetro puede ser posicional para un comando pero no posicional para otro.



No se recomienda utilizar la funcionalidad del parámetro posicional en los scripts, especialmente cuando los parámetros posicionales son opcionales para el comando o tienen parámetros opcionales listados antes de ellos.

Identificar un parámetro posicional

Puede identificar un parámetro posicional en la **command_name ?** resultado del comando. Un parámetro posicional tiene corchetes que rodean su nombre de parámetro, en uno de los siguientes formatos:

- `[-parameter_name] parameter_value` muestra un parámetro requerido que es posicional.
- `[[[-parameter_name] parameter_value]` muestra un parámetro opcional que es posicional.

Por ejemplo, cuando se muestra como lo siguiente en el **command_name ?** salida, el parámetro es posicional para el comando que aparece en:

- `[-lif] <lif-name>`
- `[[[-lif] <lif-name>]`

Sin embargo, cuando se muestra como lo siguiente, el parámetro no es posicional para el comando que aparece en:

- `-lif <lif-name>`
- `[-lif <lif-name>]`

Ejemplos de uso de parámetros posicionales

En el siguiente ejemplo, la **volume create ?** la salida muestra que tres parámetros son posicionales para el comando: `-volume`, `-aggregate`, y `-size`.

```

cluster1::> volume create ?
    -vserver <vserver name>                Vserver Name
    [-volume] <volume name>                Volume Name
    [-aggregate] <aggregate name>          Aggregate Name
    [[-size] {<integer>[KB|MB|GB|TB|PB]]]  Volume Size
    [ -state {online|restricted|offline|force-online|force-offline|mixed} ]
                                           Volume State (default: online)
    [ -type {RW|DP|DC} ]                   Volume Type (default: RW)
    [ -policy <text> ]                     Export Policy
    [ -user <user name> ]                  User ID
    ...
    [ -space-guarantee|-s {none|volume} ]   Space Guarantee Style (default:
volume)
    [ -percent-snapshot-space <percent> ]   Space Reserved for Snapshot
Copies
    ...

```

En el siguiente ejemplo, la `volume create` el comando se especifica sin aprovechar la funcionalidad del parámetro posicional:

```

cluster1::> volume create -vserver svml -volume vol1 -aggregate aggr1 -size 1g
-percent-snapshot-space 0

```

Los siguientes ejemplos utilizan la funcionalidad del parámetro posicional para aumentar la eficiencia de la entrada de comando. Los parámetros posicionales se intersitan con parámetros no posicionales en el `volume create` y los valores de parámetro posicionales se especifican sin los nombres de parámetro. Los parámetros posicionales se especifican en la misma secuencia indicada por el **volume create ?** salida. Es decir, el valor para `-volume` se especifica antes de la de `-aggregate`, que a su vez se especifica antes de la de `-size`.

```

cluster1::> volume create vol2 aggr1 1g -vserver svml -percent-snapshot-space 0

```

```

cluster1::> volume create -vserver svml vol3 -snapshot-policy default aggr1
-nvfail off 1g -space-guarantee none

```

Métodos para acceder a páginas manuales de ONTAP

Las páginas del manual de ONTAP (`man`) explican cómo usar los comandos de la CLI de ONTAP. Estas páginas están disponibles en la línea de comandos y también se publican en release-specific *command references*.

En la línea de comandos de la ONTAP, utilice `man command_name` comando para mostrar la página manual del comando especificado. Si no especifica un nombre de comando, se muestra el índice de la página manual. Puede utilizar el `man man comando` para ver información acerca de `man comando` mismo. Puede salir de una página de manual introduciendo `q`.

Consulte la [Referencia de comandos para su versión de ONTAP 9](#) Obtener más información acerca de los comandos de ONTAP a nivel de administrador y avanzado que se encuentran disponibles en su versión.

Gestionar sesiones CLI

Puede grabar una sesión de CLI en un archivo con un límite de nombre y tamaño especificado y, a continuación, cargarlo a un destino FTP o HTTP. También puede mostrar o eliminar archivos en los que haya grabado previamente las sesiones de la CLI.

Registre una sesión de la CLI

Un registro de una sesión CLI termina cuando se detiene la grabación o finaliza la sesión CLI, o cuando el archivo alcanza el límite de tamaño especificado. El límite de tamaño de archivo predeterminado es de 1 MB. El límite máximo de tamaño de archivo es 2 GB.

La grabación de una sesión CLI es útil, por ejemplo, si está solucionando problemas y desea guardar información detallada o si desea crear un registro permanente del uso de espacio en un momento determinado.

Pasos

1. Inicie la grabación de la sesión de CLI actual en un archivo:

```
system script start
```

Para obtener más información acerca del uso de `system script start` consulte la página [man](#).

ONTAP inicia la grabación de la sesión CLI en el archivo especificado.

2. Continúe con la sesión de la CLI.
3. Cuando termine, detenga la grabación de la sesión:

```
system script stop
```

Para obtener más información acerca del uso de `system script stop` consulte la página [man](#).

ONTAP deja de grabar la sesión CLI.

Comandos para gestionar registros de sesiones de la CLI

Utilice la `system script` Comandos para gestionar registros de sesiones de la CLI.

| Si desea... | Se usa este comando... |
|--|----------------------------------|
| Inicie la grabación de la sesión CLI actual en un archivo especificado | <code>system script start</code> |
| Detenga la grabación de la sesión CLI actual | <code>system script stop</code> |
| Muestra información acerca de los registros de sesiones de la CLI | <code>system script show</code> |

| Si desea... | Se usa este comando... |
|---|-----------------------------------|
| Cargue un registro de una sesión CLI en un destino FTP o HTTP | <code>system script upload</code> |
| Eliminar un registro de una sesión de la CLI | <code>system script delete</code> |

Información relacionada

["Comandos de ONTAP 9"](#)

Comandos para gestionar el tiempo de espera automático de las sesiones de la CLI

El valor de tiempo de espera especifica cuánto tiempo permanece inactiva una sesión CLI antes de que se finalice automáticamente. El valor de tiempo de espera de la CLI se encuentra en todo el clúster. Es decir, cada nodo de un clúster utiliza el mismo valor de tiempo de espera de la CLI.

De manera predeterminada, el tiempo de espera automático de las sesiones de la CLI es de 30 minutos.

Utilice la `system timeout` Comandos para gestionar el tiempo de espera automático de las sesiones de la CLI.

| Si desea... | Se usa este comando... |
|---|------------------------------------|
| Muestre el período de tiempo de espera automático para sesiones de la CLI | <code>system timeout show</code> |
| Modifique el período de tiempo de espera automático para sesiones de la CLI | <code>system timeout modify</code> |

Información relacionada

["Comandos de ONTAP 9"](#)

Gestión de clústeres (solo administradores de clústeres)

Muestra información sobre los nodos de un clúster

Puede mostrar los nombres de nodo, si los nodos están en buen estado y si pueden participar en el clúster. En el nivel de privilegio avanzado, también puede mostrar si un nodo está configurado con épsilon.

Pasos

1. Para mostrar información sobre los nodos de un clúster, utilice el `cluster show` comando.

Si desea que la salida muestre si un nodo está configurado con épsilon, ejecute el comando en el nivel de privilegio avanzado.

Ejemplos de mostrar los nodos en un clúster

En el siguiente ejemplo se muestra información sobre todos los nodos de un clúster de cuatro nodos:

```
cluster1::> cluster show
```

| Node | Health | Eligibility |
|-------|--------|-------------|
| node1 | true | true |
| node2 | true | true |
| node3 | true | true |
| node4 | true | true |

En el siguiente ejemplo, se muestra información detallada acerca del nodo denominado «'1'» en el nivel de privilegio avanzado:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> cluster show -node node1

      Node: node1
Node UUID: a67f9f34-9d8f-11da-b484-000423b6f094
  Epsilon: false
Eligibility: true
      Health: true
```

Mostrar los atributos del clúster

Puede mostrar el identificador único (UUID) de un clúster, el nombre, el número de serie, la ubicación y la información de contacto.

Pasos

1. Para mostrar los atributos de un clúster, utilice el `cluster identity show` comando.

Ejemplo de mostrar atributos de clúster

En el siguiente ejemplo se muestra el nombre, el número de serie, la ubicación y la información de contacto de un clúster.

```
cluster1::> cluster identity show

      Cluster UUID: 1cd8a442-86d1-11e0-ae1c-123478563412
      Cluster Name: cluster1
Cluster Serial Number: 1-80-123456
      Cluster Location: Sunnyvale
      Cluster Contact: jsmith@example.com
```

Modifique los atributos del clúster

Puede modificar los atributos de un clúster, como el nombre del clúster, la ubicación y la información de contacto, según sea necesario.

Acerca de esta tarea

No puede cambiar el UUID de un clúster, que se establece cuando se crea el clúster.

Pasos

1. Para modificar los atributos del clúster, utilice el `cluster identity modify` comando.

La `-name` el parámetro especifica el nombre del clúster. La `cluster identity modify` la página man describe las reglas para especificar el nombre del clúster.

La `-location` el parámetro especifica la ubicación del clúster.

La `-contact` parámetro especifica la información de contacto, como un nombre o una dirección de correo electrónico.

Ejemplo de cambio de nombre de un clúster

El siguiente comando cambia el nombre del clúster actual ("`cluster1`") a «`cluster2`»:

```
cluster1:> cluster identity modify -name cluster2
```

Mostrar el estado de los anillos de replicación del clúster

Puede mostrar el estado de los anillos de replicación del clúster para ayudarle a diagnosticar problemas en todo el clúster. Si su clúster tiene problemas, es posible que el personal de soporte le solicite que realice esta tarea para ayudarle en las tareas de solución de problemas.

Pasos

1. Para mostrar el estado de los anillos de replicación del clúster, utilice `cluster ring show` comando en el nivel de privilegio avanzado.

Ejemplo de mostrar el estado de la replicación de anillo del clúster

En el ejemplo siguiente se muestra el estado del anillo de replicación VLDB en un nodo llamado `node0`:


```

cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you wish to continue? (y or n): y

cluster1::*> cluster ring show -node node0 -unitname vldb
      Node: node0
    Unit Name: vldb
      Status: master
        Epoch: 5
Master Node: node0
  Local Node: node0
      DB Epoch: 5
DB Transaction: 56
  Number Online: 4
      RDB UUID: e492d2c1-fc50-11e1-bae3-123478563412

```

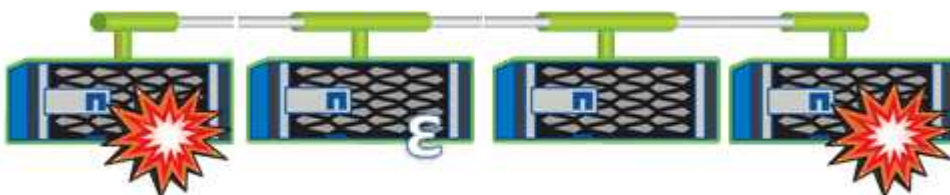
Acerca del quórum y del épsilon

El quórum y el épsilon son medidas importantes para el estado y la función de los clusters, que, en su conjunto, indican cómo abordan los clusters los desafíos potenciales de comunicaciones y conectividad.

Quórum es una condición previa para un clúster en pleno funcionamiento. Cuando un clúster se encuentra en quórum, una mayoría simple de nodos está en buen estado y puede comunicarse entre sí. Cuando se pierde quorum, el clúster pierde la capacidad de realizar las operaciones normales del clúster. Sólo una colección de nodos puede tener quórum a la vez porque todos los nodos comparten colectivamente una única vista de los datos. Por lo tanto, si dos nodos sin comunicación tienen permiso para modificar los datos de maneras divergentes, ya no es posible reconciliar los datos en una única vista de datos.

Cada nodo del cluster participa en un protocolo de votación que selecciona un nodo *master*; cada nodo restante es un *secundario*. El nodo maestro es responsable de sincronizar la información en todo el clúster. Cuando se forma el quórum, se mantiene mediante una votación continua. Si el nodo maestro se desconecta y el clúster aún se mantiene quórum, los nodos que permanecen en línea eligen un nuevo maestro.

Dado que en un cluster existe la posibilidad de empate con un número par de nodos, uno de ellos tiene un peso adicional fraccionario al votar llamado *épsilon*. Si falla la conectividad entre dos partes iguales de un clúster de gran tamaño, el grupo de nodos que contienen épsilon mantendrá el quórum, suponiendo que todos los nodos estén en buen estado. Por ejemplo, en la siguiente ilustración se muestra un clúster de cuatro nodos en el que dos de los nodos fallan. Sin embargo, dado que uno de los nodos supervivientes tiene épsilon, el cluster permanece en quórum aunque no hay una mayoría simple de nodos sanos.



Cuando se crea el clúster, se asigna automáticamente al primer nodo *épsilon*. Si el nodo que contiene *épsilon* se queda poco saludable, supera a su *partner* de alta disponibilidad o lo hace su *partner* de alta disponibilidad, se asignará el valor *épsilon* automáticamente a un nodo sano en una pareja de alta disponibilidad diferente.

Desconectar un nodo puede afectar a la capacidad del clúster para permanecer de quórum. Por lo tanto, ONTAP emite un mensaje de advertencia si se intenta una operación que impide que el clúster se quorum o si se elimina una interrupción del servicio de una pérdida de quórum. Puede deshabilitar los mensajes de advertencia de quórum mediante el `cluster quorum-service options modify` comando en el nivel de privilegio avanzado.

En general, suponiendo que haya una conectividad fiable entre los nodos del clúster, un clúster más grande es más estable que un clúster más pequeño. En un cluster de 24 nodos es más fácil mantener el requisito de quórum de la mayoría simple de la mitad de los nodos más con *épsilon* que en un cluster de dos nodos.

Un clúster de dos nodos presenta algunos retos únicos para mantener el quórum. Los clústeres de dos nodos utilizan *cluster ha*, en los que ninguno de los nodos está configurado con *épsilon*; en su lugar, se sondean ambos nodos continuamente para garantizar que, si uno de ellos falla, el otro tenga acceso completo de lectura/escritura a los datos, así como acceso a interfaces lógicas y funciones de gestión.

¿Qué volúmenes del sistema son

Los volúmenes del sistema son volúmenes FlexVol que contienen metadatos especiales, como metadatos para registros de auditoría de servicios de archivos. Estos volúmenes son visibles en el clúster para que pueda tener totalmente en cuenta el uso del almacenamiento de en el clúster.

Los volúmenes del sistema son propiedad del servidor de gestión del clúster (también llamado SVM de administrador) y se crean automáticamente cuando la auditoría de servicios de archivos está habilitada.

Para ver los volúmenes del sistema, se puede utilizar la `volume show` no se permite la mayoría de las demás operaciones de volumen. Por ejemplo, no puede modificar un volumen del sistema mediante el `volume modify` comando.

Este ejemplo muestra cuatro volúmenes del sistema en la SVM de administrador, que se crearon automáticamente cuando se habilitó la auditoría de servicios de archivos para una SVM de datos en el clúster:

```
cluster1::> volume show -vserver cluster1
```

| Vserver | Volume | Aggregate | State | Type | Size | Available |
|----------|--|-----------|--------|------|-------|-----------|
| Used% | | | | | | |
| ----- | ----- | ----- | ----- | ---- | ----- | ----- |
| ----- | | | | | | |
| cluster1 | MDV_aud_1d0131843d4811e296fc123478563412 | aggr0 | online | RW | 2GB | 1.90GB |
| 5% | | | | | | |
| cluster1 | MDV_aud_8be27f813d7311e296fc123478563412 | root_vs0 | online | RW | 2GB | 1.90GB |
| 5% | | | | | | |
| cluster1 | MDV_aud_9dc4ad503d7311e296fc123478563412 | aggr1 | online | RW | 2GB | 1.90GB |
| 5% | | | | | | |
| cluster1 | MDV_aud_a4b887ac3d7311e296fc123478563412 | aggr2 | online | RW | 2GB | 1.90GB |
| 5% | | | | | | |

4 entries were displayed.

Gestione los nodos

Añada nodos al clúster

Después de crear un clúster, puede ampliarlo añadiendo nodos a él. Solo añade un nodo a la vez.

Lo que necesitará

- Si va a añadir nodos a un clúster de varios nodos, todos los nodos existentes del clúster deben estar en buen estado (indicado por `cluster show`).
- Si va a añadir nodos a un clúster de dos nodos sin switches, debe convertir un clúster de dos nodos sin switches en un clúster conectado a switches mediante un switch de clúster compatible con NetApp.

La funcionalidad de clúster sin switch solo se admite en un clúster de dos nodos.

- Si va a añadir un segundo nodo a un clúster de un solo nodo, debe haber instalado el segundo nodo y debe haber configurado la red de clúster.
- Si el clúster tiene habilitada la configuración automática de SP, la subred especificada para el SP debe tener recursos disponibles para permitir que el nodo de unión utilice la subred especificada para configurar automáticamente el SP.
- Debe haber recopilado la siguiente información para la LIF de gestión de nodos del nuevo nodo:
 - Puerto
 - Dirección IP
 - Máscara de red
 - Pasarela predeterminada

Acerca de esta tarea

Los nodos deben tener números pares para que puedan formar pares de alta disponibilidad. Después de comenzar a añadir un nodo al clúster, debe completar el proceso. El nodo debe formar parte del clúster antes de poder empezar a añadir otro nodo.

Pasos

1. Encienda el nodo que desea añadir al clúster.

El nodo arranca y se inicia el Asistente de configuración de nodos en la consola.

```
Welcome to node setup.
```

```
You can enter the following commands at any time:
```

```
"help" or "?" - if you want to have a question clarified,
```

```
"back" - if you want to change previously answered questions, and
```

```
"exit" or "quit" - if you want to quit the setup wizard.
```

```
Any changes you made before quitting will be saved.
```

```
To accept a default or omit a question, do not enter a value.
```

```
Enter the node management interface port [e0M]:
```

2. Salga del asistente de configuración de nodos: `exit`

Se cerrará el asistente de configuración de nodos y aparecerá una solicitud de inicio de sesión con la advertencia de que no ha completado las tareas de configuración.

3. Inicie sesión en la cuenta de administrador con el `admin` nombre de usuario.
4. Inicie el asistente Cluster Setup:

```
cluster setup
```

```
::> cluster setup
```

Welcome to the cluster setup wizard.

You can enter the following commands at any time:

"help" or "?" - if you want to have a question clarified,
"back" - if you want to change previously answered questions, and
"exit" or "quit" - if you want to quit the cluster setup wizard.
Any changes you made before quitting will be saved.

You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value....

Use your web browser to complete cluster setup by accessing
`https://<node_mgmt_or_e0M_IP_address>`

Otherwise, press Enter to complete cluster setup using the
command line interface:



Para obtener más información sobre cómo configurar un clúster mediante la GUI de configuración, consulte ["System Manager" ayuda en línea](#).

5. Presione Enter para usar la CLI para completar esta tarea. Cuando se le solicite crear un nuevo clúster o unirse a uno existente, introduzca **join**.

```
Do you want to create a new cluster or join an existing cluster?
{create, join}:
join
```

Si la versión de ONTAP que se ejecuta en el nodo nuevo es diferente a la versión que se ejecuta en el clúster existente, el sistema informa de **A. System checks Error: Cluster join operation cannot be performed at this time error**. Este es el comportamiento esperado. Para continuar, ejecute el `add-node -allow-mixed-version-join new_node_name` comando en el nivel de privilegio avanzado de un nodo existente del clúster.

6. Siga las instrucciones para configurar el nodo y unirlo al clúster:
 - Para aceptar el valor predeterminado de una petición de datos, pulse Intro.
 - Para introducir su propio valor para una petición de datos, introduzca el valor y, a continuación, pulse Intro.
7. Repita los pasos anteriores para cada nodo adicional que desee añadir.

Después de terminar

Después de añadir nodos al clúster, debe habilitar la conmutación por error del almacenamiento para cada pareja de alta disponibilidad.

Información relacionada

["Clústeres de ONTAP de versión mixta"](#)

Quite los nodos del clúster

Es posible eliminar nodos no deseados de un clúster, de uno en uno. Después de quitar un nodo, también debe quitar su compañero de conmutación al nodo de respaldo. Si va a quitar un nodo, sus datos se vuelven inaccesibles o se borran.

Antes de empezar

Debe cumplir las siguientes condiciones antes de quitar nodos del clúster:

- Más de la mitad de los nodos del clúster deben estar en buen estado.
- Debe haberse evacuado todos los datos del nodo que desea quitar.
 - Esto podría incluir ["purgado de datos desde un volumen cifrado"](#).
- Todos los volúmenes que no son raíz fueron ["movido"](#) desde agregados que pertenecen al nodo.
- Se han encontrado todos los agregados que no son raíz ["eliminado"](#) desde el nodo.
- Si el nodo tiene discos de estándar de procesamiento de información federal (FIPS) o discos de cifrado automático (SED), ["se ha eliminado el cifrado del disco"](#) volviendo a poner los discos en modo sin protección.
 - Puede que también desee ["Desinfecte unidades FIPS o SED"](#).
- LIF de datos han sido ["eliminado"](#) o ["reubicado"](#) desde el nodo.
- Se han realizado las LIF de gestión del clúster ["reubicado"](#) desde el nodo y los puertos de inicio se han cambiado.
- Todas las LIF de interconexión de clústeres se han establecido ["quitada"](#).
 - Cuando elimina las LIF de interconexión de clústeres, se muestra una advertencia que puede ignorarse.
- La recuperación tras fallos del almacenamiento ha sido ["deshabilitado"](#) para el nodo.
- Todas las reglas de recuperación tras fallos de LIF han sido ["modificado"](#) para quitar los puertos del nodo.
- Todas las VLAN del nodo han sido ["eliminado"](#).
- Si tiene LUN en el nodo que se va a quitar, debería ["Modifique la lista nodos de generación de informes de asignación de LUN selectiva \(SLM\)"](#) antes de quitar el nodo.

Si no elimina el nodo y su partner de alta disponibilidad de la lista Reporting-Nodes de SLM, se puede perder el acceso a las LUN que anteriormente existían en el nodo aunque los volúmenes que contenían dichas LUN se hayan movido a otro nodo.

Se recomienda emitir un mensaje de AutoSupport para notificar al soporte técnico de NetApp que se está realizando la eliminación de nodos.

Nota: no debe realizar operaciones como `cluster remove-node`, `cluster unjoin`, y `node rename` Cuando hay una actualización automática de ONTAP en curso.

Acerca de esta tarea

- Si ejecuta un clúster de versión mixta, puede eliminar el último nodo de versión baja con uno de los comandos de privilegio avanzados desde ONTAP 9.3:

- ONTAP 9.3: `cluster unjoin -skip-last-low-version-node-check`
- ONTAP 9.4 y posteriores: `cluster remove-node -skip-last-low-version-node-check`
- Si desune 2 nodos de un clúster de 4 nodos, la alta disponibilidad de clúster se habilita automáticamente en los dos nodos que quedan.



Antes de quitar un nodo del clúster, se deben hacer inaccesibles a todos los datos del sistema y del usuario de todos los discos que están conectados al nodo. Si un nodo se desunió incorrectamente desde un clúster, póngase en contacto con el soporte de NetApp para obtener ayuda con las opciones de recuperación.

Pasos

1. Cambie el nivel de privilegio a avanzado:

```
set -privilege advanced
```

2. Compruebe si un nodo del clúster contiene épsilon:

```
cluster show -epsilon true
```

3. Si un nodo del clúster contiene épsilon y ese nodo se va a desunir, mueva épsilon a un nodo que no se va a desvincular:

- a. Mueva épsilon del nodo que se va a desunir

```
cluster modify -node <name_of_node_to_be_unjoined> -epsilon false
```

- b. Mueva épsilon a un nodo que no se va a desunir:

```
cluster modify -node <node_name> -epsilon true
```

4. Identifique el nodo maestro actual:

```
cluster ring show
```

El nodo principal es el nodo que contiene procesos como «mgmt», «vldb», «vifmgr», «bcomd» y «crs».

5. Si el nodo que desea quitar es el nodo maestro actual, habilite otro nodo del clúster para que se seleccione como nodo maestro:

- a. Haga que el nodo maestro actual no sea apto para participar en el cluster:

```
cluster modify - node <node_name> -eligibility false
```

Cuando el nodo maestro deja de ser elegible, el quórum del clúster selecciona uno de los nodos restantes como el nuevo nodo principal.

- b. Haga que el nodo maestro anterior sea apto para participar de nuevo en el clúster:

```
cluster modify - node <node_name> -eligibility true
```

6. Inicie sesión en la LIF de gestión de nodos remotos o en la LIF de gestión de clústeres en un nodo que no sea el que se está quitando.
7. Quite el nodo del clúster:

| Para esta versión de ONTAP... | Se usa este comando... |
|-----------------------------------|---------------------------------|
| ONTAP 9,3 | <pre>cluster unjoin</pre> |
| ONTAP 9,4 y versiones posteriores | <pre>cluster remove-node*</pre> |

Si tiene un clúster de versiones mixtas y va a eliminar el último nodo de la versión inferior, use el `-skip-last-low-version-node-check` parámetro con estos comandos.

El sistema le informa de lo siguiente:

- También debe quitar del clúster el compañero de conmutación al nodo de respaldo.
- Una vez que se ha eliminado el nodo y antes de poder volver a unirse a un clúster, debe utilizar la opción del menú de arranque (4) limpiar la configuración e inicializar todos los discos u opción (9) Configurar la partición avanzada de unidades para borrar la configuración del nodo e inicializar todos los discos.

Se genera un mensaje de fallo si tiene condiciones que debe abordar antes de quitar el nodo. Por ejemplo, el mensaje podría indicar que el nodo tiene recursos compartidos que debe quitar o que el nodo está en una configuración de alta disponibilidad de clúster o en una configuración de recuperación tras fallos de almacenamiento que debe deshabilitar.

Si el nodo es el maestro de quórum, el clúster perderá brevemente y volverá al quórum. Esta pérdida de quórum es temporal y no afecta a ninguna operación de datos.

8. Si un mensaje de fallo indica condiciones de error, solucione esas condiciones y vuelva a ejecutar el `cluster remove-node` o `cluster unjoin` comando.

El nodo se reinicia automáticamente después de que se quita correctamente del clúster.

9. Si va a reutilizar el nodo, borre la configuración del nodo e inicialice todos los discos:
- a. Durante el proceso de inicio, pulse Ctrl-C para mostrar el menú de inicio cuando se le solicite.
 - b. Seleccione la opción del menú de inicio (4) Limpiar configuración e inicializar todos los discos.
10. Volver al nivel de privilegio de administrador:


```
set -privilege admin
```

11. Repita los pasos anteriores para eliminar el partner de conmutación por error del clúster.

Acceda a los archivos log, core dump y MIB de un nodo mediante un navegador web

La infraestructura del procesador de servicio (`spi`) El servicio web está habilitado de forma predeterminada para habilitar un explorador web para acceder a los archivos log, core dump y MIB de un nodo en el clúster. Todavía es posible acceder a los archivos incluso cuando el nodo está inactivo, siempre que su partner haga el control del nodo.

Lo que necesitará

- El LIF de gestión del clúster debe estar activo.

Puede utilizar la LIF de gestión del clúster o de un nodo para acceder al `spi` servicio web. Sin embargo, se recomienda utilizar el LIF de gestión del clúster.

La `network interface show` El comando muestra el estado de todas las LIF del clúster.

- Se debe usar una cuenta de usuario local para acceder al `spi` servicio web, las cuentas de usuario de dominio no son compatibles.
- Si su cuenta de usuario no tiene la función «admin» (que tiene acceso a la `spi` servicio web de forma predeterminada), la función de control de acceso debe tener acceso a `spi` servicio web.

La `vserver services web access show` el comando muestra qué funciones tienen acceso a qué servicios web.

- Si no está utilizando la cuenta de usuario «admin» (que incluye la `http` método de acceso de forma predeterminada), la cuenta de usuario debe configurarse con el `http` método de acceso.

La `security login show` el comando muestra los métodos de acceso e inicio de sesión de las cuentas de usuario, así como sus roles de control de acceso.

- Si desea utilizar HTTPS para obtener acceso web seguro, debe habilitarse SSL y debe instalarse un certificado digital.

La `system services web show` el comando muestra la configuración del motor de protocolo web en el nivel del clúster.

Acerca de esta tarea

La `spi` el servicio web está activado de forma predeterminada y el servicio se puede desactivar manualmente (`vserver services web modify -vserver * -name spi -enabled false`).

La función «admin» tiene acceso a la `spi` servicio web de forma predeterminada y el acceso se puede deshabilitar manualmente (`services web access delete -vserver cluster_name -name spi -role admin`).

Pasos

1. Dirija el navegador web al `spi` Dirección URL del servicio web en uno de los siguientes formatos:

- `http://cluster-mgmt-LIF/spi/`
- `https://cluster-mgmt-LIF/spi/`

`cluster-mgmt-LIF` Es la dirección IP de la LIF de gestión del clúster.

2. Cuando el navegador lo solicite, introduzca su cuenta de usuario y contraseña.

Una vez autenticada su cuenta, el explorador mostrará vínculos a `/mroot/etc/log/`, `/mroot/etc/crash/`, y. `/mroot/etc/mib/` directorios de cada nodo del clúster.

Acceda a la consola del sistema de un nodo

Si un nodo está colgado en el menú de inicio o en el símbolo del sistema del entorno de arranque, sólo puede acceder a él a través de la consola del sistema (también llamada la *consola serie*). Puede acceder a la consola del sistema de un nodo desde una conexión SSH al SP del nodo o al clúster.

Acerca de esta tarea

Tanto el SP como los ONTAP ofrecen comandos que le permiten acceder a la consola del sistema. Sin embargo, desde SP, solo puede acceder a la consola del sistema de su propio nodo. Desde el clúster, puede acceder a la consola del sistema de cualquier nodo del clúster.

Pasos

1. Acceda a la consola del sistema de un nodo:

| Si se encuentra en... | Introduzca este comando... |
|-----------------------|--------------------------------------|
| CLI de SP del nodo | <code>system console</code> |
| CLI de ONTAP | <code>system node run-console</code> |

2. Inicie sesión en la consola del sistema cuando se le solicite que lo haga.
3. Para salir de la consola del sistema, pulse Ctrl-D.

Ejemplos de acceso a la consola del sistema

En el siguiente ejemplo se muestra el resultado de introducir el `system console` Comando en el símbolo de sistema "P 2". La consola del sistema indica que el nodo 2 está colgando en el indicador de entorno de inicio. La `boot_ontap` El comando se introduce en la consola para arrancar el nodo en ONTAP. A continuación, se pulsa Ctrl-D para salir de la consola y volver al SP.

```

SP node2> system console
Type Ctrl-D to exit.

LOADER>
LOADER> boot_ontap

...
*****
*
* Press Ctrl-C for Boot Menu. *
*
*****
...

```

(Ctrl-D se pulsa para salir de la consola del sistema.)

```

Connection to 123.12.123.12 closed.
SP node2>

```

En el siguiente ejemplo se muestra el resultado de introducir el `system node run-console` Desde ONTAP para acceder a la consola del sistema del nodo 2, que está en la solicitud del entorno de arranque. La `boot_ontap` El comando se introduce en la consola para arrancar el nodo 2 en ONTAP. A continuación, se pulsa Ctrl-D para salir de la consola y volver a ONTAP.

```

cluster1::> system node run-console -node node2
Pressing Ctrl-D will end this session and any further sessions you might
open on top of this session.
Type Ctrl-D to exit.

LOADER>
LOADER> boot_ontap

...
*****
*
* Press Ctrl-C for Boot Menu. *
*
*****
...

```

(Ctrl-D se pulsa para salir de la consola del sistema.)

```

Connection to 123.12.123.12 closed.
cluster1::>

```

Gestione volúmenes raíz del nodo y agregados raíz

El volumen raíz de un nodo es un volumen FlexVol que se instala de fábrica o mediante el software de configuración. Está reservado para los archivos del sistema, los archivos de registro y los archivos de núcleo. El nombre del directorio es `/mroot`, a la que sólo se puede acceder a través del shell del sistema mediante el soporte técnico. El tamaño mínimo para el volumen raíz de un nodo depende del modelo de plataforma.

Reglas que rigen la descripción general de los volúmenes raíz del nodo y los agregados raíz

El volumen raíz de un nodo contiene directorios y archivos especiales para ese nodo. El agregado raíz contiene el volumen raíz. Algunas reglas rigen el volumen raíz y el agregado raíz de un nodo.

- Las siguientes reglas rigen el volumen raíz del nodo:
 - A menos que el soporte técnico le indique que lo haga, no modifique la configuración ni el contenido del volumen raíz.
 - No almacenar datos de usuario en el volumen raíz.

El almacenamiento de datos de usuario en el volumen raíz aumenta el tiempo de devolución del almacenamiento entre nodos de un par de alta disponibilidad.

- Puede mover el volumen raíz a otro agregado. Consulte [\[relocate-root\]](#).
- El agregado raíz está dedicado únicamente al volumen raíz del nodo.

ONTAP impide la creación de otros volúmenes en el agregado raíz.

"Hardware Universe de NetApp"

Libere espacio en el volumen raíz de un nodo

Aparece un mensaje de advertencia cuando el volumen raíz de un nodo se ha llenado o casi llenado. El nodo no puede funcionar correctamente cuando su volumen raíz está lleno. Puede liberar espacio en el volumen raíz de un nodo si elimina los archivos de volcado principales, los archivos de seguimiento de paquetes y las copias Snapshot de volumen raíz.

Pasos

1. Muestra los archivos de volcado de memoria del nodo y sus nombres:

```
system node coredump show
```

2. Elimine los archivos de volcado de memoria no deseados del nodo:

```
system node coredump delete
```

3. Accede a la Nodessinfierno:

```
system node run -node nodename
```

nodename es el nombre del nodo cuyo espacio del volumen raíz desea liberar.

4. Cambie al nivel de privilegio avanzado nodessinfierno desde el nodessinfierno:

priv set advanced

5. Mostrar y eliminar los archivos de seguimiento de paquetes del nodo a través de nodeshell:

a. Muestre todos los archivos del volumen raíz del nodo:

```
ls /etc
```

b. Si hay archivos de seguimiento de paquetes (*.trc) se encuentran en el volumen raíz del nodo, elimínelos de forma individual:

```
rm /etc/log/packet_traces/file_name.trc
```

6. Identificar y eliminar las copias snapshot del volumen raíz del nodo a través del infierno:

a. Identifique el nombre del volumen raíz:

```
vol status
```

El volumen raíz se indica mediante la palabra «'root'» de la columna «'Options'» de la `vol status` resultado del comando.

En el siguiente ejemplo, el volumen raíz es `vol0`:

```
node1*> vol status
```

| Volume | State | Status | Options |
|--------|--------|-------------------------|-----------------|
| vol0 | online | raid_dp, flex 64-bit | root, nvfail=on |

a. Mostrar copias Snapshot de volumen raíz:

```
snap list root_vol_name
```

b. Elimine las copias Snapshot de volumen raíz que no desee:

```
snap delete root_vol_namesnapshot_name
```

7. Salga de nodeshell y vuelva al clustershell:

```
exit
```

Reubique los volúmenes raíz en nuevos agregados

El procedimiento de reemplazo raíz migra el agregado raíz actual a otro conjunto de discos sin interrupciones.

Acerca de esta tarea

La conmutación por error del almacenamiento debe estar habilitada para reubicar los volúmenes raíz. Puede utilizar el `storage failover modify -node nodename -enable true` comando para habilitar la conmutación al nodo de respaldo.

Puede cambiar la ubicación del volumen raíz a un nuevo agregado en las siguientes situaciones:

- Cuando los agregados raíz no se encuentran en el disco que prefiere
- Cuando desee reorganizar los discos conectados al nodo
- Cuando realice el reemplazo de una bandeja de bandejas de discos EOS

Pasos

1. Configure el nivel de privilegio en Advanced:

```
set privilege advanced
```

2. Reubicar el agregado raíz:

```
system node migrate-root -node nodename -disklist disklist -raid-type raid-type
```

- **-nodo**

Especifica el nodo que posee el agregado raíz que desea migrar.

- **-disklist**

Especifica la lista de discos en los que se creará el nuevo agregado raíz. Todos los discos deben ser repuestos y ser propiedad del mismo nodo. El número mínimo de discos necesario depende del tipo de RAID.

- **-raid-type**

Especifica el tipo de RAID del agregado raíz. El valor predeterminado es `raid-dp`.

3. Supervise el progreso del trabajo:

```
job show -id jobid -instance
```

Resultados

Si todas las comprobaciones previas se realizan correctamente, el comando inicia un trabajo de reemplazo de volumen raíz y sale del mismo. Espere que el nodo se reinicie.

Inicie o detenga una descripción general del nodo

Es posible que deba iniciar o detener un nodo por motivos de mantenimiento o solución de problemas. Puede hacerlo desde la CLI de ONTAP, el símbolo del sistema del entorno de arranque o desde la CLI de SP.

Con el comando CLI del SP `system power off` o `system power cycle` Para apagar o encender un nodo, es posible que un apagado incorrecto del nodo (también llamado *dirty shutdown*) y no es un sustituto de un apagado correcto usando la ONTAP `system node halt` comando.

Reinicie un nodo en el símbolo del sistema

Puede reiniciar un nodo en modo normal desde el símbolo del sistema. Un nodo se configura para arrancar desde el dispositivo de arranque, como una tarjeta PC CompactFlash.

Pasos

1. Si el clúster contiene cuatro o más nodos, compruebe que el nodo que se va a reiniciar no tenga épsilon:

a. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

b. Determine qué nodo tiene épsilon:

```
cluster show
```

En el siguiente ejemplo, se muestra «1'» con épsilon:

```
cluster1::*> cluster show
Node           Health Eligibility Epsilon
-----
node1          true  true      true
node2          true  true      false
node3          true  true      false
node4          true  true      false
4 entries were displayed.
```

a. Si el nodo que se va a reiniciar está configurado con épsilon, elimine épsilon del nodo:

```
cluster modify -node node_name -epsilon false
```

b. Asigne épsilon a un nodo diferente que permanecerá activo:

```
cluster modify -node node_name -epsilon true
```

c. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

2. Utilice la `system node reboot` comando para reiniciar el nodo.

Si no especifica el `-skip-lif-migration` Parámetro, el comando intenta migrar LIF de datos y de gestión del clúster de forma síncrona a otro nodo antes del reinicio. Si la migración de LIF falla o se agota el tiempo de espera, se anula el proceso de reinicio y ONTAP muestra un error para indicar el error de migración de la LIF.

```
cluster1::> system node reboot -node node1 -reason "software upgrade"
```

El nodo inicia el proceso de reinicio. Aparece la solicitud de inicio de sesión de ONTAP, que indica que el proceso de reinicio ha finalizado.

Arranque ONTAP en el símbolo del sistema del entorno de arranque

Puede arrancar la versión actual o la versión de backup de ONTAP cuando se encuentra en el símbolo del sistema de un entorno de arranque de un nodo.

Pasos

1. Acceda al símbolo del sistema del entorno de arranque desde el símbolo del sistema del sistema de almacenamiento mediante el `system node halt` comando.

La consola del sistema de almacenamiento muestra el símbolo del sistema del entorno de arranque.

2. En el símbolo del sistema de entorno de arranque, introduzca uno de los siguientes comandos:

| Para arrancar... | Introduzca... |
|---|---------------------------|
| La versión actual de ONTAP | <code>boot_ontap</code> |
| La imagen principal de ONTAP desde el dispositivo de arranque | <code>boot_primary</code> |
| La imagen de copia de seguridad de ONTAP desde el dispositivo de arranque | <code>boot_backup</code> |

Si no está seguro de qué imagen usar, debe usar `boot_ontap` en primer lugar.

Apague un nodo

Puede apagar un nodo si deja de responder o si el personal de soporte le dirige a hacerlo como parte de los esfuerzos de solución de problemas.

Pasos

1. Si el clúster contiene cuatro o más nodos, compruebe que el nodo que desea apagar no tenga épsilon:
 - a. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

- b. Determine qué nodo tiene épsilon:

```
cluster show
```

En el siguiente ejemplo, se muestra «1'» con épsilon:

```
cluster1::*> cluster show
Node           Health Eligibility Epsilon
-----
node1          true   true      true
node2          true   true      false
node3          true   true      false
node4          true   true      false
4 entries were displayed.
```

- a. Si el nodo que desea apagar está configurado con épsilon, elimine épsilon del nodo:


```
cluster modify -node node_name -epsilon false
```

b. Asigne `epsilon` a un nodo diferente que permanecerá activo:

```
cluster modify -node node_name -epsilon true
```

c. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

2. Utilice la `system node halt` comando para apagar el nodo.

Si no especifica el `-skip-lif-migration` Parámetro, el comando intenta migrar LIF de datos y de gestión del clúster de forma síncrona a otro nodo antes del apagado. Si la migración de LIF falla o se agota el tiempo, el proceso de apagado se cancela y ONTAP muestra un error para indicar el error de migración de la LIF.

Puede activar manualmente un volcado de memoria con el apagado mediante ambos `-dump` parámetro.

En el siguiente ejemplo se apaga el nodo llamado «'1'» para realizar tareas de mantenimiento del hardware:

```
cluster1::> system node halt -node node1 -reason 'hardware maintenance'
```

Gestione un nodo mediante el menú de arranque

Puede utilizar el menú de arranque para corregir problemas de configuración en un nodo, restablecer la contraseña de administrador, inicializar discos, restablecer la configuración del nodo y restaurar la información de configuración del nodo al dispositivo de arranque.



Si un par de alta disponibilidad está usando ["Cifrar unidades SAS o NVMe \(SED, NSE, FIPS\)"](#), debe seguir las instrucciones del tema ["Devolver una unidad FIPS o SED al modo sin protección"](#) Para todas las unidades dentro de la pareja de ha antes de inicializar el sistema (opciones de arranque 4 o 9). Si las unidades se reasignan, es posible que no se produzcan pérdidas de datos futuras.

Pasos

1. Reinicie el nodo para acceder al menú de arranque mediante el `system node reboot` en el símbolo del sistema.

El nodo inicia el proceso de reinicio.

2. Durante el proceso de reinicio, pulse Ctrl-C para mostrar el menú de inicio cuando se le solicite hacerlo.

El nodo muestra las siguientes opciones para el menú de arranque:


```
(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set onboard key management recovery secrets.
(11) Configure node for external key management.
Selection (1-11)?
```



Opción de menú de inicio (2) Boot without /etc/rc es obsoleto y no tiene ningún efecto en el sistema.

3. Seleccione una de las siguientes opciones introduciendo el número correspondiente:

| Para... | Seleccione... |
|--|-----------------------|
| Siga arrancando el nodo en el modo normal | 1) arranque normal |
| Cambie la contraseña del nodo, que es también la contraseña de la cuenta "admin" | 3) Cambiar contraseña |

| Para... | Seleccione... |
|---|---|
| Inicialice los discos del nodo y cree un volumen raíz para el nodo | <p>4) limpiar la configuración e inicializar todos los discos</p> <div>  <p>Esta opción de menú borra todos los datos de los discos del nodo y restablece la configuración del nodo a la configuración predeterminada de fábrica.</p> </div> <p>Solo seleccione este elemento de menú después de que el nodo se haya quitado de un clúster (desUnido) y no se haya Unido a otro clúster.</p> <p>Para un nodo con bandejas de discos internas o externas, se inicializa el volumen raíz en los discos internos. Si no hay bandejas de discos internas, se inicializa el volumen raíz en los discos externos.</p> <p>Para un sistema que ejecuta la virtualización FlexArray con bandejas de discos internas o externas, los LUN de cabina no se inicializan. Se inicializan todos los discos nativos de bandejas internas o externas.</p> <p>Para un sistema que ejecuta virtualización FlexArray solo con LUN de cabina y sin bandejas de discos internas o externas, se inicializa el volumen raíz en LOS LUN de la cabina de almacenamiento; consulte "Instalando FlexArray".</p> <p>Si el nodo que desea inicializar tiene discos particionados para la partición de datos raíz, los discos deben desparticionarse antes de poder inicializarse, consulte 9) Configurar la partición avanzada de discos y "Gestión de discos y agregados".</p> |
| Realizar operaciones de mantenimiento de agregados y discos y obtener información detallada sobre agregados y discos. | <p>5) arranque en modo de mantenimiento</p> <p>Para salir del modo de mantenimiento, utilice <code>halt</code> comando.</p> |
| Restaurar la información de configuración desde el volumen raíz del nodo al dispositivo de arranque, como una tarjeta PC CompactFlash | <p>6) Actualizar flash desde la configuración de la copia de seguridad</p> <p>ONTAP almacena alguna información de configuración del nodo en el dispositivo de arranque. Cuando se reinicia el nodo, se realiza automáticamente una copia de seguridad de la información del dispositivo de arranque en el volumen raíz del nodo. Si el dispositivo de arranque se daña o necesita reemplazarse, debe utilizar esta opción de menú para restaurar la información de configuración desde el volumen raíz del nodo al dispositivo de arranque.</p> |

| Para... | Seleccione... |
|---|--|
| Instale el nuevo software en el nodo | <p>7) instale primero el nuevo software</p> <p>Si el software ONTAP en el dispositivo de arranque no incluye compatibilidad con la cabina de almacenamiento que desea usar para el volumen raíz, puede usar esta opción de menú para obtener una versión del software que admite la cabina de almacenamiento e instalarla en el nodo.</p> <p>Esta opción de menú solo se utiliza para instalar una versión más reciente del software ONTAP en un nodo que no tiene instalado ningún volumen raíz. No utilice esta opción de menú para actualizar ONTAP.</p> |
| Reiniciar el nodo | 8) Reiniciar nodo |
| Desparticionar todos los discos y eliminar su información de propiedad o limpiar la configuración e inicializar el sistema con discos completos o particionados | <p>9) Configurar la partición avanzada de discos</p> <p>A partir de ONTAP 9.2, la opción Advanced Drive Partitioning ofrece funciones adicionales de gestión para los discos configurados para la partición de datos raíz o datos raíz. Las siguientes opciones están disponibles en Boot Option 9:</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>(9a) Unpartition all disks and remove their ownership information.</p> <p>(9b) Clean configuration and initialize system with partitioned disks.</p> <p>(9c) Clean configuration and initialize system with whole disks.</p> <p>(9d) Reboot the node.</p> <p>(9e) Return to main boot menu.</p> </div> |

Mostrar atributos de nodo

Puede mostrar los atributos de uno o más nodos del clúster, por ejemplo, el nombre, el propietario, la ubicación, número de modelo, número de serie, cuánto tiempo se ha ejecutado el nodo, estado y elegibilidad para participar en un clúster.

Pasos

1. Para mostrar los atributos de un nodo especificado o acerca de todos los nodos de un clúster, utilice el `system node show` comando.

Ejemplo de mostrar información acerca de un nodo

En el siguiente ejemplo, se muestra información detallada acerca de los nodos 1:

```
cluster1::> system node show -node node1
      Node: node1
      Owner: Eng IT
      Location: Lab 5
      Model: model_number
      Serial Number: 12345678
      Asset Tag: -
      Uptime: 23 days 04:42
      NVRAM System ID: 118051205
      System ID: 0118051205
      Vendor: NetApp
      Health: true
      Eligibility: true
      Differentiated Services: false
      All-Flash Optimized: true
      Capacity Optimized: false
      QLC Optimized: false
      All-Flash Select Optimized: false
      SAS2/SAS3 Mixed Stack Support: none
```

Modifique los atributos del nodo

Puede modificar los atributos de un nodo según sea necesario. Los atributos que puede modificar incluyen la información del propietario del nodo, la información de ubicación, la etiqueta de activo y la elegibilidad para participar en el clúster.

Acerca de esta tarea

La elegibilidad de un nodo para participar en el clúster puede modificarse en el nivel de privilegio avanzado mediante el `-eligibility` parámetro de `system node modify` o `cluster modify` comando. Si establece la idoneidad de un nodo `false`, el nodo se vuelve inactivo en el clúster.



No puede modificar la idoneidad del nodo de forma local. Debe modificarse desde un nodo diferente. La elegibilidad del nodo tampoco se puede modificar con una configuración de alta disponibilidad de clúster.



Debe evitar establecer la idoneidad de un nodo `false`, excepto en situaciones como restaurar la configuración del nodo o el mantenimiento prolongado de los nodos. El acceso a datos DE SAN y NAS al nodo puede verse afectado cuando el nodo no cumple con los requisitos.

Pasos

1. Utilice la `system node modify` comando para modificar los atributos de un nodo.

Ejemplo de modificación de atributos de nodo

El siguiente comando modifica los atributos del nodo `"1"`. El propietario del nodo se establece en `"Joe Smith"` y su etiqueta de activo se establece en `"js1234"`:

```
cluster1::> system node modify -node node1 -owner "Joe Smith" -assettag js1234
```

Cambie el nombre de un nodo

Es posible cambiar el nombre de un nodo según sea necesario.

Pasos

1. Para cambiar el nombre de un nodo, utilice `system node rename` comando.

La `-newname` el parámetro especifica el nuevo nombre del nodo. La `system node rename` la página man describe las reglas para especificar el nombre del nodo.

Si desea cambiar el nombre de varios nodos en el clúster, debe ejecutar el comando de cada nodo individualmente.



El nombre de nodo no puede ser «'todos'» porque «'todos'» es un nombre reservado del sistema.

Ejemplo de cambio de nombre de un nodo

El siguiente comando cambia el nombre del nodo "1" a "nodo 1a":

```
cluster1::> system node rename -node node1 -newname node1a
```

Gestione clústeres de un solo nodo

Un clúster de un solo nodo es una implementación especial de un clúster que se ejecuta en un nodo independiente. No se recomiendan los clústeres de un solo nodo porque no proporcionan redundancia. Si el nodo se cae, se pierde el acceso a los datos.



Para la tolerancia a fallos y las operaciones no disruptivas, es muy recomendable configurar el clúster con ["Alta disponibilidad \(parejas de alta disponibilidad\)"](#).

Si decide configurar o actualizar un clúster de un solo nodo, debe tener en cuenta lo siguiente:

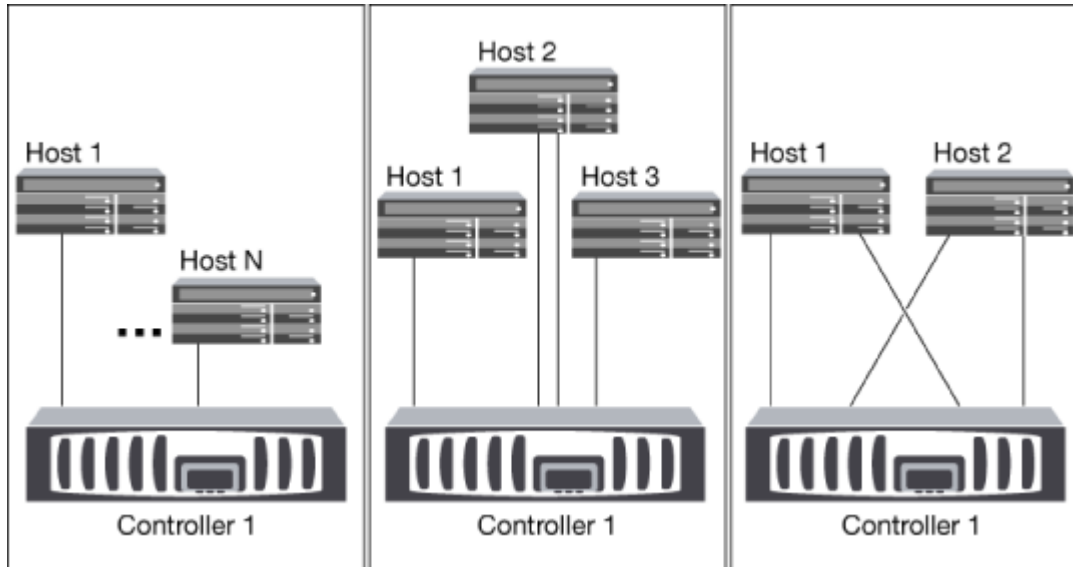
- El cifrado de volúmenes raíz no se admite en clústeres de un solo nodo.
- Si quita nodos para que tengan un clúster de un solo nodo, debe modificar los puertos de clúster para que proporcionen el tráfico de datos. Para ello, modifique los puertos de clúster para que sean puertos de datos y, a continuación, cree LIF de datos en los puertos de datos.
- Para los clústeres de un solo nodo, se puede especificar el destino del backup de configuración durante la configuración del software. Una vez completada la configuración, estas configuraciones se pueden modificar con los comandos de la ONTAP.
- Si hay varios hosts que se conectan al nodo, cada host se puede configurar con un sistema operativo diferente, como Windows o Linux. Si hay varias rutas desde el host hasta la controladora, debe habilitarse ALUA en el host.

Formas de configurar hosts SAN iSCSI con nodos únicos

Es posible configurar hosts SAN iSCSI para que se conecten directamente a un solo nodo o para conectarse a través de uno o varios switches IP. El nodo puede tener varias conexiones iSCSI al switch.

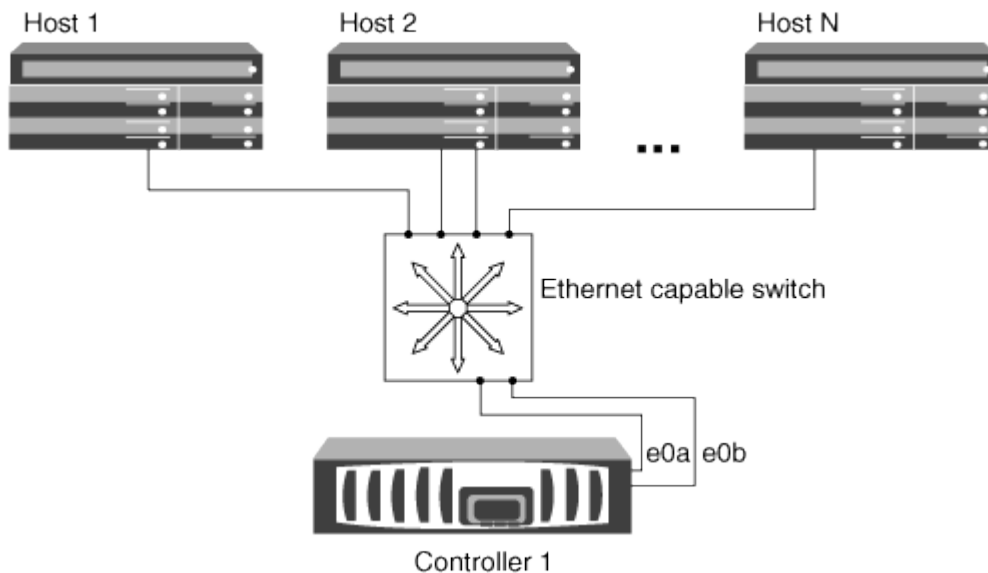
Configuraciones de conexión directa de un solo nodo

En configuraciones de nodo único de conexión directa, uno o varios hosts están conectados directamente al nodo.



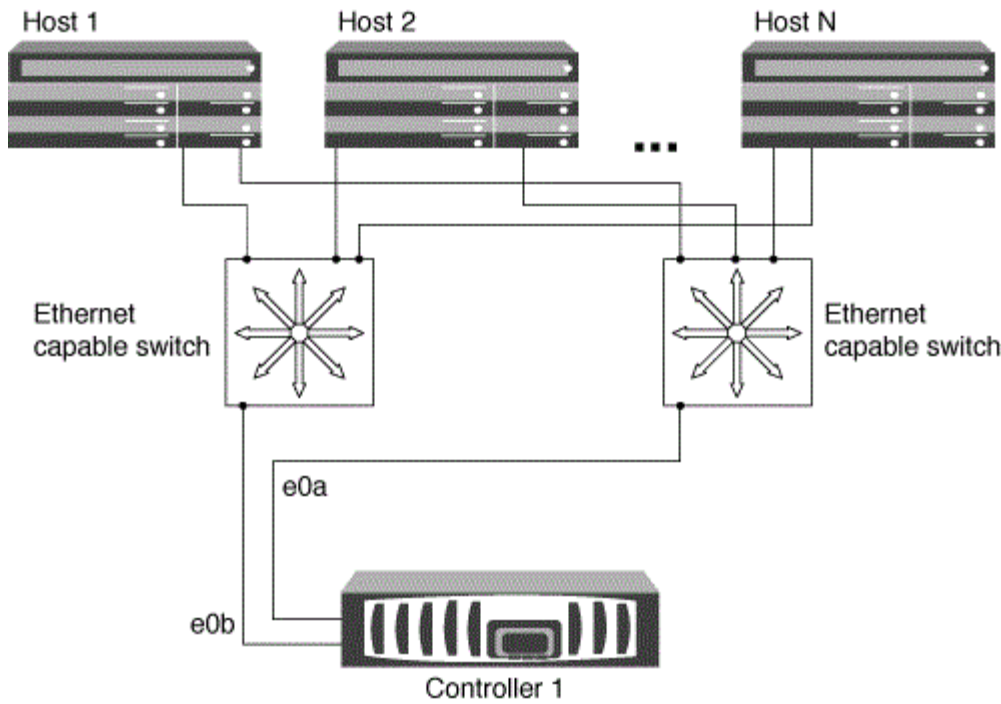
Configuraciones de red única de nodo único

En configuraciones de nodo único de red, un switch conecta un nodo único a uno o varios hosts. Dado que hay un único switch, esta configuración no es completamente redundante.



Configuraciones de un solo nodo en red múltiples

En configuraciones de varios nodos de una sola red, dos o más switches conectan un solo nodo a uno o varios hosts. Dado que hay varios switches, esta configuración es completamente redundante.



Formas de configurar hosts SAN FC y FC-NVMe con nodos únicos

Puede configurar hosts SAN FC y FC-NVMe con nodos únicos a través de una o varias estructuras. Se requiere virtualización de N-Port ID (NPIV) y debe habilitarse en todos los switches de FC de la estructura. No puede conectar directamente hosts SAN FC o FC-NMVE a nodos individuales sin usar un switch FC.

Configuraciones de nodo único con estructura única

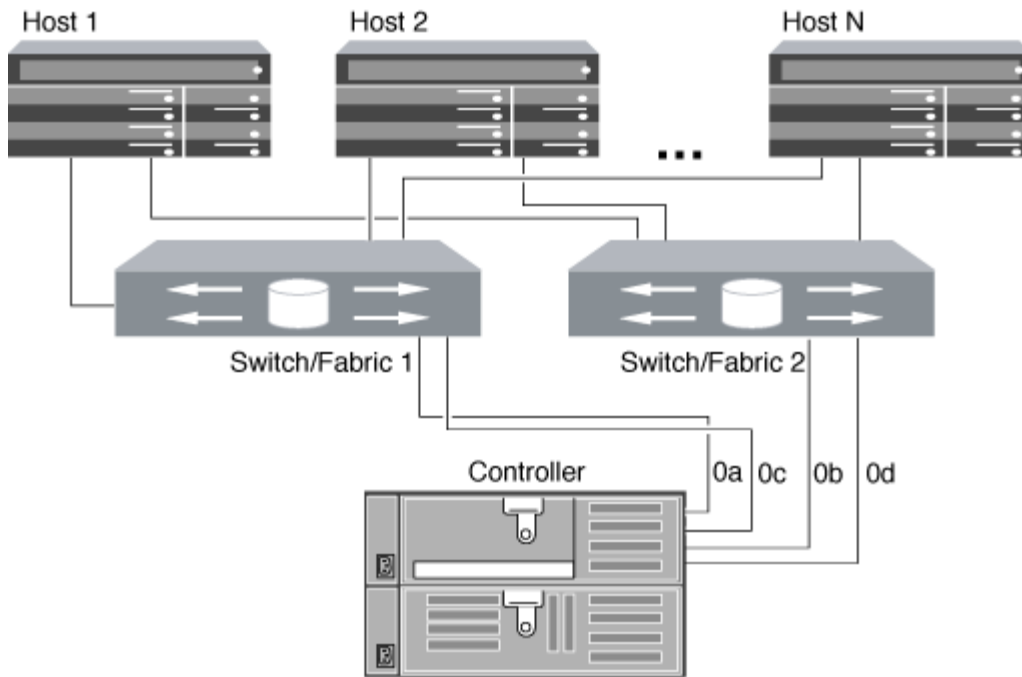
En configuraciones de estructura única de nodo único, hay un switch que conecta un nodo único a uno o varios hosts. Dado que hay un único switch, esta configuración no es completamente redundante.

En configuraciones de estructura única de nodo único, no es necesario el software multivía si solo tiene una ruta desde el host al nodo.

Configuraciones de nodo único estructura múltiple

En configuraciones de nodo único de estructura múltiple, hay dos o más switches que conectan un único nodo a uno o varios hosts. Para mayor simplicidad, la siguiente figura muestra una configuración de un solo nodo de estructura múltiple con dos estructuras, pero puede tener dos o más estructuras en cualquier configuración de estructura múltiple. En esta figura, el controlador de almacenamiento está montado en el chasis superior y el chasis inferior puede estar vacío o tener un módulo IOMX, como lo hace en este ejemplo.

Los puertos de destino FC (0a, 0c, 0b, 0d) en las ilustraciones son ejemplos. Los números de puerto reales varían según el modelo de su nodo de almacenamiento y si usa adaptadores de expansión.



Información relacionada

["Informe técnico de NetApp 4684: Implementación y configuración de SAN modernas con NVMe-oF"](#)

Actualización de ONTAP para clúster de un solo nodo

A partir de ONTAP 9,2, se puede usar la interfaz de línea de comandos de ONTAP para realizar una actualización automatizada de un clúster de un solo nodo. Como los clústeres de un solo nodo carecen de redundancia, las actualizaciones son siempre disruptivas. Las actualizaciones disruptivas no pueden llevarse a cabo mediante System Manager.

Antes de empezar

Debe completar la actualización ["preparación"](#) pasos.

Pasos

1. Elimine el paquete de software de ONTAP anterior:

```
cluster image package delete -version previous_package_version
```

2. Descargue el paquete de software de ONTAP de destino:

```
cluster image package get -url location
```

```
cluster1::> cluster image package get -url
http://www.example.com/software/9.7/image.tgz
```

```
Package download completed.
Package processing completed.
```

3. Compruebe que el paquete de software esté disponible en el repositorio del paquete de clúster:

```
cluster image package show-repository
```

```
cluster1:> cluster image package show-repository
Package Version  Package Build Time
-----
9.7              M/DD/YYYY 10:32:15
```

4. Compruebe que el clúster esté listo para actualizarse:

```
cluster image validate -version package_version_number
```

```
cluster1:> cluster image validate -version 9.7
```

```
WARNING: There are additional manual upgrade validation checks that must
be performed after these automated validation checks have completed...
```

5. Supervise el progreso de la validación:

```
cluster image show-update-progress
```

6. Complete todas las acciones necesarias identificadas por la validación.

7. Opcionalmente, genere un cálculo de actualización de software:

```
cluster image update -version package_version_number -estimate-only
```

El cálculo aproximado de actualización de software muestra detalles sobre cada componente que se va a actualizar y la duración estimada de la actualización.

8. Realice la actualización de software:

```
cluster image update -version package_version_number
```



Si se encuentra un problema, la actualización se detiene y le solicita que realice una acción correctiva. Puede utilizar el comando `cluster image show-update-progress` para ver detalles sobre cualquier problema y el progreso de la actualización. Una vez que corrija el problema, puede reanudar la actualización mediante el comando `cluster image resume-update`.

9. Muestre el progreso de la actualización del clúster:

```
cluster image show-update-progress
```

El nodo se reinicia como parte de la actualización y no se puede acceder a él mientras se reinicia.

10. Activar una notificación:

```
autosupport invoke -node * -type all -message "Finishing_Upgrade"
```

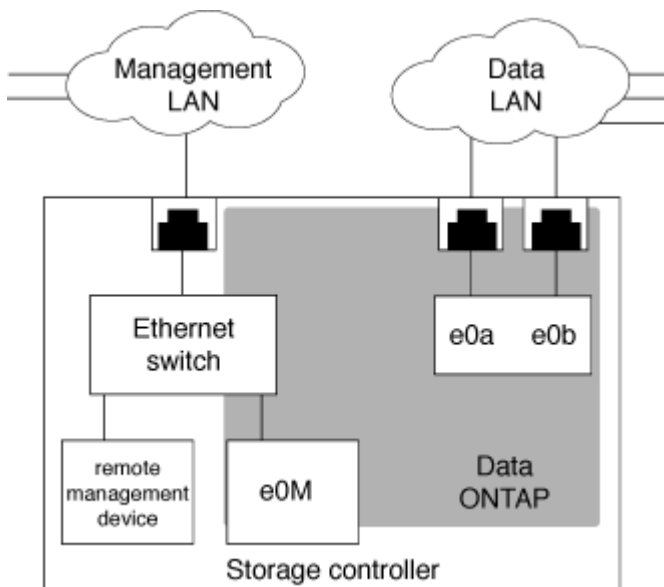
Si el clúster no está configurado para enviar mensajes, se guardará localmente una copia de la notificación.

Configure la red del SP/BMC

Aísle el tráfico de red de gestión

Se recomienda configurar el SP/BMC y la interfaz de gestión de e0M en una subred dedicada al tráfico de gestión. La ejecución del tráfico de datos por la red de gestión puede provocar problemas de degradación y de enrutamiento del rendimiento.

El puerto Ethernet de gestión de la mayoría de las controladoras de almacenamiento (indicado con un icono de llave en la parte posterior del chasis) está conectado a un switch Ethernet interno. El switch interno proporciona conectividad al SP/BMC y a la interfaz de gestión e0M, la cual puede utilizar para acceder al sistema de almacenamiento mediante protocolos TCP/IP como Telnet, SSH y SNMP.



Si tiene pensado utilizar tanto el dispositivo de gestión remota como e0M, debe configurarlos en la misma subred IP. Dado que estas son interfaces de bajo ancho de banda, la práctica recomendada es configurar SP/BMC y e0M en una subred dedicada al tráfico de gestión.

Si no puede aislar el tráfico de gestión o si su red de gestión dedicada es excepcionalmente grande, debe intentar mantener el volumen de tráfico de red lo más bajo posible. Un ingreso excesivo de tráfico de difusión o multidifusión puede degradar el rendimiento del SP/BMC.



Algunas controladoras de almacenamiento, como AFF A800, tienen dos puertos externos, uno para BMC y el otro para e0M. Para estas controladoras, no es necesario configurar BMC y e0M en la misma subred IP.

Consideraciones que tener en cuenta para la configuración de red del SP/BMC

Es posible habilitar la configuración de red automática a nivel de clúster para el SP (recomendado). También puede dejar deshabilitada la configuración automática de red de SP (predeterminado) y gestionar la configuración de red de SP manualmente en el nivel de nodo. Existen algunas consideraciones para cada caso.



Este tema se aplica tanto al SP como al BMC.

La configuración de red automática del SP permite al SP utilizar recursos de dirección (incluida la dirección IP, la máscara de subred y la dirección de puerta de enlace) desde la subred especificada para configurar su red automáticamente. Con la configuración de red automática de SP, no es necesario asignar manualmente las direcciones IP para el SP de cada nodo. De forma predeterminada, la configuración de red automática del SP está deshabilitada; esto se debe a que para habilitar la configuración es necesario que la subred se utilice para la configuración en el clúster primero.

Si habilita la configuración de red automática del SP, se aplican las siguientes situaciones y consideraciones:

- Si el SP nunca se ha configurado, la red del SP se configura automáticamente de acuerdo con la subred especificada para la configuración de red automática del SP.
- Si el SP se ha configurado manualmente o si la configuración de red del SP existente se basa en una subred diferente, la red de SP de todos los nodos del clúster se reconfiguran en función de la subred que especifique en la configuración de red automática de SP.

La reconfiguración puede dar como resultado que se asigne a SP otra dirección, lo que puede afectar a la configuración de DNS y a su capacidad de resolver los nombres de host de SP. Como resultado, es posible que deba actualizar la configuración de DNS.

- Un nodo que se une al clúster utiliza la subred especificada para configurar su red de SP automáticamente.
- La `system service-processor network modify` El comando no le permite cambiar la dirección IP del SP.

Cuando la configuración de red automática del SP está habilitada, el comando solo le permite habilitar o deshabilitar la interfaz de red del SP.

- Si la configuración de red automática del SP se habilitó anteriormente, al deshabilitar la interfaz de red del SP, se libera el recurso de dirección asignado y se vuelve a la subred.
- Si deshabilita la interfaz de red de SP y vuelve a habilitarla, el SP podría volver a configurarse con una dirección diferente.

Si la configuración de red automática del SP está deshabilitada (por defecto), se aplican las siguientes situaciones y consideraciones:

- Si el SP nunca se ha configurado, la configuración de red IPv4 de SP establece de manera predeterminada el uso de DHCP IPv4 e IPv6 está deshabilitado.

Un nodo que se une al clúster también utiliza DHCP IPv4 para la configuración de red del SP de forma predeterminada.

- La `system service-processor network modify` Command le permite configurar la dirección IP del SP de un nodo.

Aparece un mensaje de advertencia cuando intenta configurar manualmente la red del SP con direcciones asignadas a una subred. Si ignora la advertencia y continúa con la asignación manual de direcciones, podría producirse un escenario con direcciones duplicadas.

Si la configuración de red automática del SP se deshabilita después de haberse habilitado previamente, se aplican las siguientes situaciones y consideraciones:

- Si la configuración de red automática del SP tiene deshabilitada la familia de direcciones IPv4, la red IPv4 de SP debe utilizar DHCP de manera predeterminada y la `system service-processor network modify` El comando le permite modificar la configuración IPv4 de SP para nodos individuales.
- Si la configuración de red automática del SP tiene la familia de direcciones IPv6 deshabilitada, la red IPv6 del SP también está deshabilitada y el `system service-processor network modify` Comando le permite habilitar y modificar la configuración de IPv6 de SP para nodos individuales.

Habilite la configuración de red automática de SP/BMC

Habilitar el SP para utilizar la configuración de red automática es preferible de configurar manualmente la red del SP. Dado que la configuración de red automática del SP es de todo el clúster, no es necesario que gestione manualmente la red del SP para nodos individuales.



Esta tarea se aplica tanto al SP como al BMC.

- La subred que desea utilizar para la configuración de red automática del SP ya debe estar definida en el clúster y no debe haber conflictos de recursos con la interfaz de red del SP.

La `network subnet show` comando muestra información de subred para el clúster.

El parámetro que fuerza la asociación de subred (el `-force-update-lif-associations` parámetro de `network subnet` Comandos) solo es compatible en los LIF de red y no en la interfaz de red del SP.

- Si desea utilizar conexiones IPv6 para el SP, IPv6 ya debe estar configurado y habilitado para ONTAP.

La `network options ipv6 show` El comando muestra el estado actual de la configuración de IPv6 para ONTAP.

Pasos

1. Especifique la familia de direcciones IPv4 o IPv6 y el nombre de la subred que desea que utilice el SP con el `system service-processor network auto-configuration enable` comando.
2. Muestra la configuración de red automática del SP mediante el `system service-processor network auto-configuration show` comando.
3. Si posteriormente desea deshabilitar o volver a habilitar la interfaz de red IPv4 o IPv6 del SP para todos los nodos que están en quórum, utilice el `system service-processor network modify` con el `-address-family [IPv4|IPv6]` y `-enable [true|false]` parámetros.

Cuando se habilita la configuración de red automática del SP, no es posible modificar la dirección IP de SP para un nodo que está en quórum. Solo puede habilitar o deshabilitar la interfaz de red IPv4 o IPv6 del SP.

Si un nodo no tiene quórum, puede modificar la configuración de red de SP del nodo, incluida la dirección IP de SP, ejecutando `system service-processor network modify` En el nodo y confirme que desea anular la configuración de red automática del SP para el nodo. Sin embargo, cuando el nodo se une al quórum, la reconfiguración automática del SP se lleva a cabo para el nodo según la subred especificada.

Configure la red SP/BMC manualmente

Si no tiene configurada la configuración de red automática para el SP, debe configurar manualmente la red de SP de un nodo para que el SP pueda accederse a través de una dirección IP.

Lo que necesitará

Si desea utilizar conexiones IPv6 para el SP, IPv6 ya debe estar configurado y habilitado para ONTAP. La `network options ipv6` Los comandos gestionan la configuración de IPv6 para ONTAP.



Esta tarea se aplica tanto al SP como al BMC.

Puede configurar el SP para que use IPv4, IPv6 o ambos. La configuración IPv4 del SP es compatible con las direcciones estáticas y DHCP, y la configuración IPv6 del SP solo admite direcciones estáticas.

Si se ha configurado la configuración de red automática del SP, no es necesario configurar manualmente la red del SP para nodos individuales y el `system service-processor network modify` El comando le permite habilitar o deshabilitar la interfaz de red del SP.

Pasos

1. Configure la red del SP para un nodo mediante el `system service-processor network modify` comando.
 - La `-address-family` El parámetro especifica si se va a modificar la configuración de IPv4 o IPv6 del SP.
 - La `-enable` El parámetro habilita la interfaz de red de la familia de direcciones IP especificada.
 - La `-dhcp` El parámetro especifica si se debe utilizar la configuración de red desde el servidor DHCP o la dirección de red que se proporcione.

Puede habilitar DHCP (a modo de configuración `-dhcp` para v4) Sólo si está utilizando IPv4. No se puede habilitar DHCP para las configuraciones IPv6.

- La `-ip-address` El parámetro especifica la dirección IP pública del SP.

Aparece un mensaje de advertencia cuando intenta configurar manualmente la red del SP con direcciones asignadas a una subred. Si ignora la advertencia y continúa con la asignación manual de direcciones, podría producirse una asignación de direcciones duplicada.

- La `-netmask` El parámetro especifica la máscara de red del SP (si se utiliza IPv4).
- La `-prefix-length` El parámetro especifica la longitud del prefijo de red de la máscara de subred del SP (si se utiliza IPv6).

- La `-gateway` El parámetro especifica la dirección IP de pasarela del SP.
2. Configure la red SP para los nodos restantes del clúster repitiendo el paso 1.
 3. Mostrar la configuración de red del SP y comprobar el estado de configuración del SP mediante el `system service-processor network show` con el `-instance 0`. `-field setup-status` parámetros.

El estado de configuración de SP para un nodo puede ser uno de los siguientes:

- `not-setup` — no configurado
- `succeeded` — Configuración correcta
- `in-progress` — Configuración en curso
- `failed` — error de configuración

Ejemplo de configuración de la red del SP

En el ejemplo siguiente se configura el SP de un nodo para utilizar IPv4, habilita el SP y muestra la configuración de red del SP para comprobar los ajustes:

```

cluster1::> system service-processor network modify -node local
-address-family IPv4 -enable true -ip-address 192.168.123.98
-netmask 255.255.255.0 -gateway 192.168.123.1

cluster1::> system service-processor network show -instance -node local

Node: node1
Address Type: IPv4
Interface Enabled: true
Type of Device: SP
Status: online
Link Status: up
DHCP Status: none
IP Address: 192.168.123.98
MAC Address: ab:cd:ef:fe:ed:02
Netmask: 255.255.255.0
Prefix Length of Subnet Mask: -
Router Assigned IP Address: -
Link Local IP Address: -
Gateway IP Address: 192.168.123.1
Time Last Updated: Thu Apr 10 17:02:13 UTC 2014
Subnet Name: -
Enable IPv6 Router Assigned Address: -
SP Network Setup Status: succeeded
SP Network Setup Failure Reason: -

1 entries were displayed.

cluster1::>

```

Modifique la configuración del servicio API del SP

La API del SP es una API de red segura que permite a ONTAP comunicarse con el SP a través de la red. Puede cambiar el puerto utilizado por el servicio API del SP, renovar los certificados que el servicio utiliza para la comunicación interna o deshabilitar el servicio por completo. Sólo es necesario modificar la configuración en situaciones raras.

Acerca de esta tarea

- El servicio API del SP utiliza el puerto 50000 de forma predeterminada.

Puede cambiar el valor del puerto si, por ejemplo, está en una configuración de red donde puerto 50000 se utiliza para la comunicación por otra aplicación de red, o bien desea diferenciar el tráfico de otras aplicaciones y el tráfico generado por el servicio API de SP.

- Los certificados SSL y SSH que utiliza el servicio API del SP son internos al clúster y no se distribuyen externamente.

En el caso improbable de que los certificados se vean comprometidos, puede renovarlos.

- El servicio API del SP está habilitado de forma predeterminada.

Solo tiene que deshabilitar el servicio API de SP en situaciones raras, como en una LAN privada en la que el SP no está configurado o utilizado y desea deshabilitar el servicio.

Si el servicio API del SP está deshabilitado, la API no acepta ninguna conexión entrante. Además, la funcionalidad como las actualizaciones del firmware del SP basadas en la red y la recopilación de registros del SP basado en la red «sistema inactivo» deja de estar disponible. El sistema cambia a utilizar la interfaz de serie.

Pasos

1. Cambie al nivel de privilegio avanzado mediante el `set -privilege advanced` comando.
2. Modifique la configuración del servicio API del SP:

| Si desea... | Usar el siguiente comando... |
|---|---|
| Cambie el puerto que utiliza el servicio API del SP | <code>system service-processor api-service modify</code> con la <code>-port {49152..'65535'parámetro }</code> |
| Renueve los certificados SSL y SSH que utiliza el servicio API de SP para la comunicación interna | <ul style="list-style-type: none">• Para uso de ONTAP 9.5 o posterior <code>system service-processor api-service renew-internal-certificate</code>• Para ONTAP 9.4 y versiones anteriores• <code>system service-processor api-service renew-certificates</code> <p>Si no se especifica ningún parámetro, solo se renuevan los certificados del host (incluidos los certificados de cliente y de servidor).</p> <p>Si la <code>-renew-all true</code> Se especifica el parámetro, se renuevan los certificados del host y el certificado de CA raíz.</p> |
| com | |
| Deshabilite o vuelva a habilitar el servicio API de SP | <code>system service-processor api-service modify</code> con la <code>-is-enabled {true</code> |

3. Muestra la configuración del servicio API del SP mediante el `system service-processor api-service show` comando.

Gestione nodos de forma remota usando SP/BMC

Gestione un nodo de forma remota mediante la información general de SP/BMC

Puede gestionar un nodo de forma remota mediante una controladora integrada, denominada Service Processor (SP) o una controladora de gestión de placa base (BMC). Este controlador de administración remota está incluido en todos los modelos de plataforma actuales. La controladora sigue operativa a pesar del estado operativo del nodo.

Las siguientes plataformas son compatibles con BMC en lugar de SP:

- FAS 8700
- FAS 8300
- Fas27x0
- AFF A800
- AFF A700s
- AFF A400
- AFF A320
- AFF A220
- C190 de AFF

Acerca del SP

Service Processor (SP) es un dispositivo de gestión remota que le permite acceder, supervisar y solucionar problemas de un nodo de forma remota.

Las funcionalidades clave del SP incluyen lo siguiente:

- SP le permite acceder a un nodo remotamente para realizar diagnósticos, apagarlo, restablecerlo o reiniciarlo, al margen del estado de la controladora del nodo.

SP recibe alimentación de un voltaje de reserva, que está disponible siempre que el nodo tenga alimentación de entrada de al menos una de sus fuentes de alimentación.

Puede iniciar sesión en SP con una aplicación cliente Secure Shell desde un host de administración. A continuación, puede usar la interfaz de línea de comandos de SP para supervisar el nodo y solucionar remotamente los problemas. Además, puede usar SP para acceder a la consola de serie y ejecutar comandos de ONTAP de manera remota.

Puede acceder al SP desde la consola de serie o acceder a la consola de serie desde el SP. SP le permite abrir una sesión de CLI de SP y una sesión de la consola independiente de manera simultánea.

Por ejemplo, cuando un sensor de temperatura se vuelve extremadamente alto o bajo, ONTAP activa el SP para apagar la placa base correctamente. La consola de serie deja de responder, pero puede pulsar Ctrl-G en la consola para acceder a la CLI de SP. A continuación, puede utilizar la `system power on` o `system power cycle` Desde el SP para encender o apagar y encender el nodo.

- El SP supervisa los sensores de entorno y registra los eventos para ayudarle a realizar acciones de servicio eficaces y oportunas.

El SP supervisa los sensores de entorno como las temperaturas de los nodos, las tensiones, las corrientes

y las velocidades del ventilador. Cuando un sensor medioambiental ha alcanzado una condición fuera de lo normal, el SP registra las lecturas anormales, notifica al ONTAP del problema y envía alertas y notificaciones «de sistema inactivo» según sea necesario a través de un mensaje de AutoSupport, independientemente de si el nodo puede enviar mensajes de AutoSupport.

El SP también registra eventos como el progreso del arranque, los cambios de la unidad reemplazable del sector (FRU), los eventos generados por ONTAP y el historial de comandos de SP. Puede invocar manualmente un mensaje de AutoSupport para incluir los archivos de registro de SP que se recopilan desde un nodo especificado.

Además de generar estos mensajes en nombre de un nodo que está inactivo y asociar información de diagnóstico adicional a mensajes de AutoSupport, el SP no tiene ningún efecto en la funcionalidad AutoSupport. La configuración de AutoSupport y el comportamiento del contenido de los mensajes se heredan de ONTAP.



El SP no confía en el `-transport` ajuste de parámetros de `system node autosupport modify` comando para enviar notificaciones. El SP solo utiliza el protocolo simple de transporte de correo (SMTP) y requiere que la configuración de AutoSupport del host incluya la información del host de correo.

Si SNMP está activado, el SP genera capturas SNMP a los hosts de capturas configurados para todos los eventos de «sistema inactivo».

- El SP tiene un búfer de memoria no volátil que almacena hasta 4,000 eventos en un registro de eventos del sistema (SEL) para ayudarle a diagnosticar problemas.

El SEL almacena cada entrada del registro de auditoría como evento de auditoría. Se almacena en la memoria flash integrada del SP. El SP envía automáticamente la lista de eventos desde el SEL a los destinatarios especificados a través de un mensaje de AutoSupport.

El SEL contiene la información siguiente:

- Eventos de hardware detectados por el SP: Por ejemplo, estado del sensor acerca de suministros de energía, voltaje u otros componentes
- Errores detectados por el SP: Por ejemplo, un error de comunicación, un fallo en el ventilador o un error de memoria o CPU
- Eventos de software críticos enviados al SP por el nodo, por ejemplo, un pánico, un error de comunicación, un error de arranque o un «sistema inactivo» activado por el usuario como resultado de la emisión del SP `system reset` o `system power cycle` comando
- El SP supervisa la consola de serie independientemente de si los administradores han iniciado sesión o están conectados a la consola.

Cuando se envían mensajes a la consola, el SP los almacena en el registro de la consola. El registro de la consola se mantiene siempre que el SP reciba energía de alguno de los suministros del nodo. Dado que el SP funciona con voltaje de reserva, permanece disponible incluso si se somete al nodo a un ciclo de encendido y apagado, o si directamente se apaga.

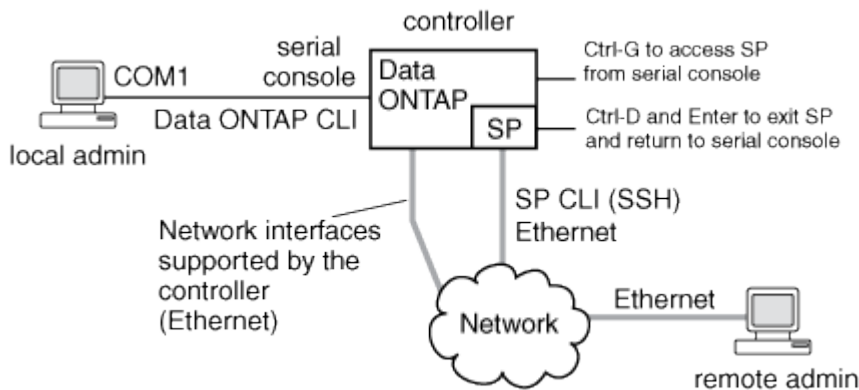
- La toma de control asistida por hardware está disponible si el SP está configurado.
- El servicio API del SP permite a ONTAP comunicarse con el SP a través de la red.

El servicio mejora la gestión de ONTAP del SP gracias a la compatibilidad con las funcionalidades basadas en la red, como el uso de la interfaz de red para la actualización del firmware del SP, lo cual permite a un nodo acceder a la funcionalidad del SP de otro nodo o a la consola del sistema, y cargar el

registro de SP desde otro nodo.

Para modificar la configuración del servicio API del SP, es posible cambiar el puerto que utiliza el servicio, renovar los certificados SSL y SSH que utiliza el servicio para la comunicación interna o deshabilitar el servicio por completo.

En el siguiente diagrama se muestra el acceso a ONTAP y al SP de un nodo. Para acceder a la interfaz del SP a través del puerto Ethernet (indicado con un icono de llave en la parte posterior del chasis):



Lo que hace el controlador de administración de la placa base

A partir de ONTAP 9.1, en algunas plataformas de hardware, el software se personaliza para admitir un nuevo controlador incorporado en el denominado controlador de administración de la placa base (BMC). El BMC tiene comandos de interfaz de línea de comandos (CLI) que puede utilizar para administrar el dispositivo de forma remota.

BMC funciona de forma similar con Service Processor (SP) y utiliza muchos de los mismos comandos. El BMC le permite hacer lo siguiente:

- Configure los valores de red del BMC.
- Acceda a un nodo de forma remota y realice tareas de gestión de nodos como diagnosticar, apagar, aplicar ciclos de apagado y encendido o reiniciar el nodo.

Existen algunas diferencias entre el SP y BMC:

- El BMC controla por completo el control medioambiental de los elementos de la fuente de alimentación, los elementos de refrigeración, los sensores de temperatura, los sensores de tensión y los sensores de corriente. El BMC informa de la información del sensor a ONTAP a través de IPMI.
- Algunos de los comandos de almacenamiento y alta disponibilidad son diferentes.
- El BMC no envía mensajes de AutoSupport.

Las actualizaciones automáticas del firmware también están disponibles cuando se ejecuta ONTAP 9.2 GA o posterior con los siguientes requisitos:

- Se debe instalar la revisión de firmware de BMC 1.15 o posterior.



Se requiere una actualización manual para actualizar el firmware de BMC de 1.12 a 1.15 o posterior.

- El BMC se reinicia automáticamente después de finalizar una actualización de firmware.



Las operaciones de nodos no se ven afectadas durante el reinicio de BMC.

Métodos para gestionar actualizaciones del firmware del SP/BMC

ONTAP incluye una imagen de firmware del SP que se denomina *baseline*. Si una nueva versión del firmware del SP se encuentra disponible posteriormente, tiene la opción de descargarlo y actualizar el firmware del SP a la versión descargada sin actualizar la versión de ONTAP.



Este tema se aplica tanto al SP como al BMC.

ONTAP ofrece los siguientes métodos para gestionar las actualizaciones del firmware del SP:

- La funcionalidad de actualización automática del SP está habilitada de forma predeterminada, lo que permite que el firmware del SP se actualice automáticamente en las siguientes situaciones:

- Al actualizar a una nueva versión de ONTAP

El proceso de actualización de ONTAP incluye automáticamente la actualización del firmware del SP, siempre y cuando la versión del firmware del SP incluida con ONTAP sea más reciente que la versión del SP que se ejecuta en el nodo.



ONTAP detecta una actualización automática del SP con errores y activa una acción correctiva para volver a intentar la actualización automática del SP hasta tres veces. Si los tres reintentos fallan, vea el enlace del artículo de la base de conocimientos: [Falla la actualización del SP de SPAutoUpgradeFailedMajorAlert de supervisión Health - Mensaje de AutoSupport](#).

- Cuando descarga una versión del firmware del SP desde el sitio de soporte de NetApp y la versión descargada es posterior a la que ejecuta el SP actualmente
- Al degradar o revertir a una versión anterior de ONTAP

El firmware del SP se actualiza automáticamente a la versión compatible más reciente compatible, compatible con la versión de ONTAP a la que se revierte o degradó. No es necesaria una actualización manual del firmware del SP.

Tiene la opción de deshabilitar la funcionalidad de actualización automática del SP mediante el `system service-processor image modify` comando. Sin embargo, se recomienda dejar la funcionalidad habilitada. Al deshabilitar la funcionalidad, puede haber combinaciones no cualificadas entre la imagen ONTAP y la imagen del firmware del SP.

- ONTAP le permite activar una actualización de SP manualmente y especificar cómo debe realizarse la actualización mediante el `system service-processor image update` comando.

Puede especificar las siguientes opciones:

- El paquete de firmware del SP que se va a utilizar (`-package`)

Puede actualizar el firmware del SP en un paquete descargado especificando el nombre del archivo

del paquete. Avance `system image package show` El comando muestra todos los archivos de paquetes (incluidos los archivos del paquete de firmware del SP) disponibles en un nodo.

- Si se utiliza el paquete de firmware del SP de referencia para la actualización del SP (`-baseline`)

Puede actualizar el firmware del SP a la versión de referencia que se incluye en el paquete con la versión actualmente en ejecución de ONTAP.



Si utiliza algunas de las opciones o parámetros de actualización más avanzadas, es posible que los ajustes de configuración del BMC se borren temporalmente. Tras el reinicio, ONTAP puede tardar hasta 10 minutos en restaurar la configuración del BMC.

- ONTAP le permite mostrar el estado de la última actualización del firmware del SP activada desde ONTAP mediante el `system service-processor image update-progress show` comando.

Cualquier conexión existente con el SP finaliza cuando se actualiza el firmware del SP. Este es el caso si la actualización del firmware del SP se activa de forma automática o manual.

Información relacionada

["Descargas de NetApp: Diagnóstico y firmware del sistema"](#)

Cuando SP/BMC utiliza la interfaz de red para las actualizaciones de firmware

Una actualización del firmware del SP que se activa desde ONTAP con el SP que ejecuta la versión 1.5, 2.5, 3.1 o posterior admite el uso de un mecanismo de transferencia de archivos basado en IP a través de la interfaz de red del SP.



Este tema se aplica tanto al SP como al BMC.

Una actualización del firmware del SP a través de la interfaz de red es más rápida que una actualización a través de la interfaz de serie. Reduce la ventana de mantenimiento durante la cual se actualiza el firmware del SP y también no es disruptivo para el funcionamiento de ONTAP. Las versiones del SP compatibles con esta funcionalidad se incluyen en ONTAP. También están disponibles en el sitio de soporte de NetApp y se pueden instalar en controladoras que ejecuten una versión compatible de ONTAP.

Cuando está ejecutando SP versión 1.5, 2.5, 3.1 o posterior, se aplican los siguientes comportamientos de actualización del firmware:

- Una actualización del firmware del SP que es *automáticamente* activada por ONTAP de forma predeterminada a la utilización de la interfaz de red para la actualización; sin embargo, la actualización automática del SP cambia a utilizar la interfaz de serie para la actualización del firmware si se da alguna de las condiciones siguientes:
 - La interfaz de red del SP no está configurada o no está disponible.
 - Se produce un error en la transferencia del archivo basado en IP.
 - El servicio API del SP está deshabilitado.

Independientemente de la versión del SP que esté ejecutando, una actualización del firmware del SP activada desde la CLI de SP siempre utiliza la interfaz de red del SP para la actualización.

Información relacionada

["Descargas de NetApp: Diagnóstico y firmware del sistema"](#)

Cuentas que pueden acceder al SP

Cuando intenta acceder al SP, se le solicita la credencial de. Las cuentas de usuario del clúster que se crean con la `service-processor` El tipo de aplicación tiene acceso a la CLI del SP en cualquier nodo del clúster. Las cuentas de usuario del SP se gestionan desde ONTAP y se autentican mediante contraseña. A partir de ONTAP 9.9.1, las cuentas de usuario del SP deben tener el `admin` función.

Las cuentas de usuario para acceder al SP se gestionan desde ONTAP en lugar de desde la CLI de SP. Una cuenta de usuario del clúster puede acceder al SP si se crea con el `-application` parámetro de `security login create` comando establecido en `service-processor` y la `-authmethod` parámetro establecido en `password`. El SP solo admite la autenticación por contraseña.

Debe especificar el `-role` Parámetro al crear una cuenta de usuario del SP.

- En ONTAP 9.9.1 y versiones posteriores, es necesario especificar `admin` para la `-role` y cualquier modificación en una cuenta requiere el `admin` función. Ya no se permiten otras funciones por motivos de seguridad.
 - Si va a actualizar a ONTAP 9.9.1 o versiones posteriores, consulte ["Cambio en las cuentas de usuario que pueden acceder a Service Processor"](#).
 - Si va a revertir a ONTAP 9.8 o versiones anteriores, consulte ["Compruebe las cuentas de usuario que pueden acceder a Service Processor"](#).
- En ONTAP 9.8 y versiones anteriores, cualquier rol puede acceder al SP, pero `admin` es recomendable.

De forma predeterminada, la cuenta de usuario del clúster denominada «'admin'» incluye `service-processor` Tipo de aplicación y tiene acceso al SP.

ONTAP evita la creación de cuentas de usuario con nombres reservados para el sistema (como «'root'» y «'naroot'»). No puede utilizar un nombre reservado con el sistema para acceder al clúster ni a SP.

Puede mostrar cuentas de usuario actuales del SP mediante el `-application service-processor` parámetro de `security login show` comando.

Acceda al SP/BMC desde un host de administración

Puede iniciar sesión en el SP de un nodo desde un host de administración para realizar tareas de gestión de nodos de forma remota.

Lo que necesitará

Deben cumplirse las siguientes condiciones:

- El host de administración que utiliza para acceder al SP debe admitir SSHv2.
- Su cuenta de usuario ya debe estar configurada para acceder al SP.

Para acceder al SP, su cuenta de usuario debe haberse creado con el `-application` parámetro de `security login create` comando establecido en `service-processor` y la `-authmethod` parámetro establecido en `password`.



Esta tarea se aplica tanto al SP como al BMC.

Si el SP está configurado para utilizar una dirección IPv4 o IPv6, y si cinco intentos de inicio de sesión SSH desde un host fallan consecutivamente en un plazo de 10 minutos, el SP rechaza las solicitudes de inicio de sesión de SSH y suspende la comunicación con la dirección IP del host durante 15 minutos. La comunicación se reanuda a partir de 15 minutos, y puede intentar iniciar sesión de nuevo en el SP.

ONTAP le impide crear o utilizar nombres reservados del sistema (como «'root'» y «'naroot'») para acceder al clúster o al SP.

Pasos

1. Desde el host de administración, inicie sesión en el SP:

```
ssh username@SP_IP_address
```

2. Cuando se le solicite, escriba la contraseña para `username`.

Aparece el aviso de SP, lo que indica que tiene acceso a la CLI de SP.

Ejemplos de acceso a SP desde un host de administración

En el ejemplo siguiente se muestra cómo iniciar sesión en el SP con una cuenta de usuario `joe`, que se ha configurado para acceder al SP.

```
[admin_host]$ ssh joe@192.168.123.98
joe@192.168.123.98's password:
SP>
```

Los siguientes ejemplos muestran cómo usar la dirección global de IPv6 o la dirección anunciada por el enrutador de IPv6 para iniciar sesión en el SP en un nodo que tiene SSH configurado para IPv6 y el SP configurado para IPv6.

```
[admin_host]$ ssh joe@fd22:8b1e:b255:202::1234
joe@fd22:8b1e:b255:202::1234's password:
SP>
```

```
[admin_host]$ ssh joe@fd22:8b1e:b255:202:2a0:98ff:fe01:7d5b
joe@fd22:8b1e:b255:202:2a0:98ff:fe01:7d5b's password:
SP>
```

Acceda a SP/BMC desde la consola del sistema

Puede acceder al SP desde la consola del sistema (también llamada *consola* de serie) para realizar tareas de supervisión o solución de problemas.

Acerca de esta tarea

Esta tarea se aplica tanto al SP como al BMC.

Pasos

1. Acceda a la CLI de SP desde la consola del sistema de con Ctrl-G en el símbolo del sistema de.
2. Inicie sesión en la CLI del SP cuando se le solicite.

Aparece el aviso de SP, lo que indica que tiene acceso a la CLI de SP.

3. Salga de la CLI de SP y vuelva a la consola del sistema pulsando Ctrl-D y, a continuación, pulse Intro.

Ejemplo de acceder a la CLI de SP desde la consola del sistema

En el siguiente ejemplo, se muestra el resultado de pulsar Ctrl-G desde la consola del sistema para acceder a la CLI de SP. La `help system power` Comando se introduce en el símbolo del sistema del SP, seguido de Ctrl-D y, a continuación, Intro para volver a la consola del sistema.

```
cluster1::>
```

(Pulse Ctrl-G para acceder a la CLI de SP).

```
Switching console to Service Processor
Service Processor Login:
Password:
SP>
SP> help system power
system power cycle - power the system off, then on
system power off - power the system off
system power on - power the system on
system power status - print system power status
SP>
```

(Pulse Ctrl-D y, a continuación, Intro para volver a la consola del sistema.)

```
cluster1::>
```

Relación entre la CLI de SP, la consola de SP y las sesiones de la consola del sistema

Puede abrir una sesión CLI de SP para gestionar un nodo de forma remota y abrir una sesión de la consola de SP independiente para acceder a la consola del nodo. La sesión de la consola del SP refleja el resultado que se muestra en una sesión simultánea de la consola del sistema. El SP y la consola del sistema tienen entornos de shell independientes con autenticación de inicio de sesión independiente.

Comprender cómo se relacionan la CLI de SP, la consola de SP y las sesiones de consola del sistema le ayuda a gestionar un nodo de forma remota. A continuación se describe la relación entre las sesiones:

- Solo un administrador puede iniciar sesión en la sesión CLI de SP a la vez; sin embargo, el SP permite abrir una sesión CLI de SP y una sesión de la consola de SP independiente de manera simultánea.

El CLI del SP se indica con el aviso del SP (`SP>`). Desde una sesión CLI de SP, puede utilizar el SP

`system console` Comando para iniciar una sesión de la consola del SP. Al mismo tiempo, puede iniciar una sesión CLI de SP independiente a través de SSH. Si pulsa Ctrl-D para salir de la sesión de la consola del SP, volverá automáticamente a la sesión CLI del SP. Si ya existe una sesión CLI del SP, un mensaje le pregunta si desea terminar la sesión CLI del SP existente. Si introduce «y», se finaliza la sesión CLI del SP existente, lo que le permite volver desde la consola del SP a la CLI del SP. Esta acción se registra en el registro de eventos del SP.

En una sesión CLI de ONTAP que está conectada a través de SSH, puede cambiar a la consola del sistema de un nodo ejecutando el ONTAP `system node run-console` desde otro nodo.

- Por motivos de seguridad, la sesión CLI de SP y la sesión de la consola del sistema de tienen autenticaciones de inicio de sesión independientes.

Cuando inicia una sesión de la consola del SP desde la CLI del SP (mediante el SP `system console`), se le solicita la credencial de la consola del sistema. Cuando accede a la CLI de SP desde una sesión de la consola del sistema (pulsando Ctrl-G), se le solicita la credencial de CLI de SP.

- La sesión de la consola de SP y la sesión de la consola del sistema de tienen entornos de shell independientes.

La sesión de la consola del SP refleja el resultado que se muestra en una sesión de la consola del sistema simultánea. Sin embargo, la sesión de la consola del sistema simultáneas no refleja la sesión de la consola del SP.

La sesión de la consola de SP no refleja el resultado de sesiones SSH simultáneas.

Gestione las direcciones IP que pueden acceder al SP

De forma predeterminada, el SP acepta solicitudes de conexión SSH de los hosts de administración de cualquier dirección IP. Puede configurar el SP para aceptar solicitudes de conexión SSH desde solo los hosts de administración que tienen las direcciones IP especificadas. Los cambios que haga se aplican al acceso SSH al SP de cualquier nodo del clúster.

Pasos

1. Conceda acceso a SP a únicamente las direcciones IP que especifique mediante el `system service-processor ssh add-allowed-addresses` con el `-allowed-addresses` parámetro.
 - El valor de `-allowed-addresses` el parámetro debe especificarse en el formato de `address/netmask`, y múltiple `address/netmask` los pares deben estar separados por comas; por ejemplo, `10.98.150.10/24, fd20:8b1e:b255:c09b::/64`.
 - Ajuste de `-allowed-addresses` parámetro a `0.0.0.0/0, ::/0` Habilita todas las direcciones IP para acceder al SP (predeterminado).
 - Cuando cambia el valor predeterminado limitando el acceso a SP a sólo las direcciones IP especificadas, ONTAP le solicita que confirme que desea que las direcciones IP especificadas sustituyan el valor predeterminado «allow all» (`0.0.0.0/0, ::/0`).
 - La `system service-processor ssh show` Command muestra las direcciones IP que permiten acceder al SP.
2. Si desea bloquear que una dirección IP concreta acceda al SP, utilice el `system service-processor ssh remove-allowed-addresses` con el `-allowed-addresses` parámetro.

Si bloquea todas las direcciones IP para acceder al SP, no se puede acceder al SP desde cualquier host de administración.

Ejemplos de gestionar las direcciones IP que pueden acceder al SP

Los siguientes ejemplos muestran el valor predeterminado para el acceso SSH al SP, cambian el valor predeterminado limitando el acceso de SP a únicamente las direcciones IP especificadas, quitan las direcciones IP especificadas de la lista de acceso y, a continuación, restaure el acceso a SP para todas las direcciones IP:

```
cluster1::> system service-processor ssh show
Allowed Addresses: 0.0.0.0/0, ::/0

cluster1::> system service-processor ssh add-allowed-addresses -allowed
-addresses 192.168.1.202/24, 192.168.10.201/24

Warning: The default "allow all" setting (0.0.0.0/0, ::/0) will be
replaced
        with your changes. Do you want to continue? {y|n}: y

cluster1::> system service-processor ssh show
Allowed Addresses: 192.168.1.202/24, 192.168.10.201/24

cluster1::> system service-processor ssh remove-allowed-addresses -allowed
-addresses 192.168.1.202/24, 192.168.10.201/24

Warning: If all IP addresses are removed from the allowed address list,
all IP
        addresses will be denied access. To restore the "allow all"
default,
        use the "system service-processor ssh add-allowed-addresses
        -allowed-addresses 0.0.0.0/0, ::/0" command. Do you want to
continue?
        {y|n}: y

cluster1::> system service-processor ssh show
Allowed Addresses: -

cluster1::> system service-processor ssh add-allowed-addresses -allowed
-addresses 0.0.0.0/0, ::/0

cluster1::> system service-processor ssh show
Allowed Addresses: 0.0.0.0/0, ::/0
```

Utilice la ayuda en línea de la CLI del SP/BMC

La ayuda en línea muestra los comandos y las opciones de la CLI del SP/BMC.

Acerca de esta tarea

Esta tarea se aplica tanto al SP como al BMC.

Pasos

1. Para mostrar información de ayuda de los comandos del SP/BMC, introduzca lo siguiente:

| Para acceder a la ayuda del SP... | Para acceder a la ayuda de BMC... |
|--|---|
| Tipo <code>help</code> En el aviso del SP. | Tipo <code>system</code> En el símbolo del sistema del BMC. |

En el ejemplo siguiente se muestra la ayuda en línea de la CLI del SP.

```
SP> help
date - print date and time
exit - exit from the SP command line interface
events - print system events and event information
help - print command help
priv - show and set user mode
sp - commands to control the SP
system - commands to control the system
version - print SP version
```

El ejemplo siguiente muestra la ayuda en línea de la CLI de BMC.

```
BMC> system
system acp - acp related commands
system battery - battery related commands
system console - connect to the system console
system core - dump the system core and reset
system cpld - cpld commands
system log - print system console logs
system power - commands controlling system power
system reset - reset the system using the selected firmware
system sensors - print environmental sensors status
system service-event - print service-event status
system fru - fru related commands
system watchdog - system watchdog commands

BMC>
```

2. Para mostrar información de ayuda para la opción de un comando del SP/BMC, introduzca `help` Antes o después del comando SP/BMC.

En el ejemplo siguiente se muestra la ayuda en línea de la CLI del SP para el `SP events` comando.

```

SP> help events
events all - print all system events
events info - print system event log information
events newest - print newest system events
events oldest - print oldest system events
events search - search for and print system events

```

En el ejemplo siguiente se muestra la ayuda en línea de la CLI de BMC para el BMC `system power` comando.

```

BMC> system power help
system power cycle - power the system off, then on
system power off - power the system off
system power on - power the system on
system power status - print system power status

BMC>

```

Comandos para gestionar un nodo de forma remota


Puede gestionar un nodo de forma remota accediendo a su SP y ejecutando comandos de la CLI de SP para realizar tareas de gestión de nodos. Para varias tareas de gestión remota de nodos de ejecución común, también puede utilizar comandos ONTAP de otro nodo en el clúster. Algunos comandos del SP son específicos de la plataforma y es posible que no estén disponibles en la plataforma.


| Si desea... | Usar este comando del SP... | Usar este comando de BMC... | O este comando de ONTAP ... |
|--|------------------------------|--|-----------------------------|
| Mostrar los comandos de SP disponibles o subcomandos de un comando de SP especificado | <code>help [command]</code> | | |
| Muestra el nivel actual de privilegio de la CLI del SP | <code>priv show</code> | | |
| Establezca el nivel de privilegio para acceder al modo especificado para la CLI del SP | <code>priv set {admin</code> | <code>advanced</code> | <code>diag}</code> |
| | | Muestra la fecha y la hora del sistema | <code>date</code> |

| Si desea... | Usar este comando del SP... | Usar este comando de BMC... | O este comando de ONTAP ... |
|--|--|---|-------------------------------|
| | date | Muestra los eventos que ha registrado el SP | events {all |
| info | newest number | oldest number | search keyword} |
| | | Mostrar el estado del SP y la información de configuración de red | sp status [-v |
| -d] La -v La opción muestra las estadísticas de SP en forma detallada. La -d La opción añade el registro de depuración del SP a la pantalla. | bmc status [-v | -d] La -v La opción muestra las estadísticas de SP en forma detallada. La -d La opción añade el registro de depuración del SP a la pantalla. | system service-processor show |
| Muestra la cantidad de tiempo que ha estado activo el SP y el número medio de trabajos de la cola de ejecución durante los últimos 1, 5 y 15 minutos | sp uptime | bmc uptime | |
| Mostrar los registros de la consola del sistema | system log | | |
| Mostrar los archivos de registro del SP o los archivos de un archivo | sp log history show [-archive {latest | {all | archive-name}} [-dump {all |
| file-name}} | bmc log history show [-archive {latest | {all | archive-name}} [-dump {all |
| file-name}} | | Muestra el estado de alimentación de la controladora de un nodo | system power status |
| | system node power show | Muestra información de la batería | system battery show |
| | | Muestre información de ACP o el estado de los sensores de ampliación | system acp [show |

| Si desea... | Usar este comando del SP... | Usar este comando de BMC... | O este comando de ONTAP ... |
|---|--|--------------------------------------|--|
| sensors show] | | | Enumerar todas las FRU del sistema y sus ID |
| system fru list | | | Muestra información de producto de la FRU especificada |
| system fru show fru_id | | | Mostrar el registro del historial de datos de FRU |
| system fru log show (nivel de privilegio avanzado) | | | Muestra el estado de los sensores medioambientales, incluidos sus estados y valores actuales |
| system sensors 0. system sensors show | | system node environment sensors show | Muestra el estado y los detalles del sensor especificado |
| system sensors get sensor_name Usted puede obtener sensor_name mediante el uso de system sensors 0 o la system sensors show comando. | | | Muestra la información de la versión del firmware del SP |
| version | | system service-processor image show | Muestra el historial de comandos del SP |
| sp log audit (nivel de privilegio avanzado) | bmc log audit | | Muestra la información de depuración del SP |
| sp log debug (nivel de privilegio avanzado) | bmc log debug (nivel de privilegio avanzado) | | Muestra el archivo de mensajes del SP |

| Si desea... | Usar este comando del SP... | Usar este comando de BMC... | O este comando de ONTAP ... |
|--|---|---|--|
| sp log messages (nivel de privilegio avanzado) | bmc log messages (nivel de privilegio avanzado) | | Mostrar la configuración para recopilar información forense del sistema en un evento de restablecimiento del guardián, mostrar la información forense del sistema recopilada durante un evento de restablecimiento del guardián o borrar la información forense del sistema recopilada |
| system forensics [show | log dump | log clear] | |
| | Inicie sesión en la consola del sistema | system console | |
| system node run-console | Debe pulsar Ctrl-D para salir de la sesión de la consola del sistema. | Encender o apagar el nodo, o realizar un ciclo de encendido y apagado (apagando la alimentación y volviendo a encender) | system power on |
| | system node power on (nivel de privilegio avanzado) | system power off | |
| | system power cycle | | |

| Si desea... | Usar este comando del SP... | Usar este comando de BMC... | O este comando de ONTAP ... |
|--|---|---|-----------------------------|
| <p>La alimentación en espera permanece encendida para mantener el SP en funcionamiento sin interrupciones. Durante el ciclo de encendido, se produce una breve pausa antes de volver a encender la alimentación.</p> <div>  <p>El uso de estos comandos para apagar o realizar un ciclo de apagado y encendido del nodo puede provocar un apagado incorrecto del nodo (también llamado <i>dirty shutdown</i>) y no es un sustituto para un apagado correcto usando la ONTAP <code>system node halt</code> comando.</p> </div> | <p>Cree un volcado de memoria y restablezca el nodo</p> | <p><code>system core [-f]</code></p> <p>La <code>-f</code> option fuerza la creación de un volcado de memoria y el restablecimiento del nodo.</p> | |

| Si desea... | Usar este comando del SP... | Usar este comando de BMC... | O este comando de ONTAP ... |
|---|--|--|--|
| <code>system node coredump trigger</code> (nivel de privilegio avanzado) | Estos comandos tienen el mismo efecto que presionar el botón de interrupción no enmascarable (NMI) en un nodo, lo que provoca un apagado con errores del nodo y obliga a un volcado de los archivos principales cuando se detenga el nodo. Estos comandos son útiles cuando ONTAP del nodo está colgado o no responde a comandos como <code>system node shutdown</code> . Los archivos de volcado de memoria generados se muestran en el resultado del <code>system node coredump show</code> comando. El SP sigue operativo siempre que no se interrumpa la alimentación de entrada del nodo. | Reinicie el nodo con una imagen de firmware de BIOS especificada opcionalmente (principal, de backup o actual) para recuperarse de problemas, como una imagen dañada del dispositivo de arranque del nodo | <code>system reset {primary</code> |
| <code>backup</code> | <code>current}</code> | | <code>system node reset con la -firmware {primary</code> |
| <code>backup</code> | <code>current`parámetro } (nivel de privilegio avanzado) `system node reset</code> | <div>  <p>Esta operación provoca un apagado con errores del nodo.</p> </div> <p>Si no se especifica ninguna imagen de firmware de BIOS, se utiliza la imagen actual para el reinicio. El SP sigue operativo siempre que no se interrumpa la alimentación de entrada del nodo.</p> | Muestra el estado de la actualización automática del firmware de la batería, o habilita o deshabilita la actualización automática del firmware de la batería tras el siguiente arranque del SP |

| Si desea... | Usar este comando del SP... | Usar este comando de BMC... | O este comando de ONTAP ... |
|--|---|--|---|
| system battery auto_update [status | enable | disable] (nivel de privilegio avanzado) | |
| | Compare la imagen del firmware de la batería actual con una imagen de firmware especificada | system battery verify [image_URL] (nivel de privilegio avanzado) Si image_URL no se especifica, se utiliza la imagen de firmware de la batería predeterminada para la comparación. | |
| | Actualice el firmware de la batería desde la imagen en la ubicación especificada | system battery flash image_URL (nivel de privilegio avanzado) Es posible utilizar este comando si no se pudo realizar el proceso de actualización automática del firmware de la batería por algún motivo. | |
| | Actualice el firmware del SP con la imagen en la ubicación especificada | sp update image_URL image_URL no debe superar los 200 caracteres. | bmc update image_URL image_URL no debe superar los 200 caracteres. |
| system service-processor image update | Reinicia el SP | sp reboot | |
| system service-processor reboot-sp | Borre el contenido flash de NVRAM | system nvram flash clear (nivel de privilegio avanzado) No es posible iniciar este comando cuando la controladora está apagada (system power off). | |

| Si desea... | Usar este comando del SP... | Usar este comando de BMC... | O este comando de ONTAP ... |
|-------------|-----------------------------|-----------------------------|-----------------------------|
| | Salga de la CLI del SP | <code>exit</code> | |

Acerca de las lecturas del sensor de SP basado en umbrales y los valores de estado del resultado de comandos de sensores del sistema

Los sensores basados en umbrales realizan lecturas periódicas de una variedad de componentes del sistema. El SP compara la lectura de un sensor basado en umbrales con sus límites de umbrales preestablecidos que definen las condiciones aceptables para el funcionamiento de un componente.

Según la lectura del sensor, el SP muestra el estado del sensor para ayudarle a supervisar la condición del componente.

Entre los ejemplos de sensores basados en umbrales se incluyen los sensores de temperatura del sistema, tensiones, corrientes y velocidad del ventilador. La lista específica de sensores basados en umbrales depende de la plataforma.

Los sensores basados en umbrales tienen los siguientes umbrales, que se muestran en el resultado del `SP system sensors` comando:

- Inferior crítico (LCR)
- Inferior no crítico (LNC)
- Superior no crítico (UNC)
- Superior crítico (UCR)

Una lectura de sensor entre LNC y LCR o entre UNC y UCR significa que el componente muestra signos de un problema y que se podría producir un fallo del sistema como resultado. Por lo tanto, debería planificar pronto la reparación del componente.

Una lectura de sensor por debajo de LCR o por encima de UCR significa que el componente no está funcionando correctamente y que está a punto de producirse un fallo del sistema. Por lo tanto, el componente requiere atención inmediata.

En el siguiente diagrama se muestran los rangos de gravedad que se especifican por los umbrales:



Puede encontrar la lectura de un sensor basado en umbrales en la `Current` en la `system sensors` resultado del comando. La `system sensors get sensor_name` el comando muestra detalles adicionales del sensor especificado. A medida que la lectura de un sensor basado en umbrales supera los rangos de umbrales no críticos, el sensor informa de un problema de gravedad creciente. Cuando la lectura supera un límite de umbral, el estado del sensor en la `system sensors` el resultado del comando cambia desde `ok` para `nc` (no crítico) o `cr` (Crítico) según el umbral superado y se registra un mensaje de evento en el registro

de eventos SEL.

Algunos sensores basados en umbrales no tienen los cuatros niveles de umbral. Para esos sensores, aparecen los umbrales que faltan na como sus límites en el `system sensors` Resultado del comando, lo que indica que el sensor concreto no tiene límite o gravedad que afecte al umbral dado y que el SP no supervisa el sensor para ese umbral.

Ejemplo del resultado de comandos de sensores del sistema

En el siguiente ejemplo se muestra parte de la información que muestra el `system sensors` Comando en la CLI del SP:

```
SP node1> system sensors

Sensor Name      | Current      | Unit         | Status| LCR          | LNC
| UNC          | UCR
-----+-----+-----+-----+-----+
-----+-----+-----+-----+
CPU0_Temp_Margin | -55.000     | degrees C   | ok    | na           | na
| -5.000       | 0.000
CPU1_Temp_Margin | -56.000     | degrees C   | ok    | na           | na
| -5.000       | 0.000
In_Flow_Temp     | 32.000      | degrees C   | ok    | 0.000        | 10.000
| 42.000       | 52.000
Out_Flow_Temp    | 38.000      | degrees C   | ok    | 0.000        | 10.000
| 59.000       | 68.000
CPU1_Error       | 0x0         | discrete    | 0x0180| na           | na
| na           | na
CPU1_Therm_Trip  | 0x0         | discrete    | 0x0180| na           | na
| na           | na
CPU1_Hot         | 0x0         | discrete    | 0x0180| na           | na
| na           | na
IO_Mid1_Temp     | 30.000      | degrees C   | ok    | 0.000        | 10.000
| 55.000       | 64.000
IO_Mid2_Temp     | 30.000      | degrees C   | ok    | 0.000        | 10.000
| 55.000       | 64.000
CPU_VTT          | 1.106       | Volts       | ok    | 1.028        | 1.048
| 1.154       | 1.174
CPU0_VCC         | 1.154       | Volts       | ok    | 0.834        | 0.844
| 1.348       | 1.368
3.3V             | 3.323       | Volts       | ok    | 3.053        | 3.116
| 3.466       | 3.546
5V               | 5.002       | Volts       | ok    | 4.368        | 4.465
| 5.490       | 5.636
STBY_1.8V        | 1.794       | Volts       | ok    | 1.678        | 1.707
| 1.892       | 1.911
...
```

Ejemplo del resultado del comando `sensor_name` de los sensores del sistema para un sensor basado en umbrales

El siguiente ejemplo muestra el resultado de introducir `system sensors get sensor_name` En la CLI de SP para el sensor basado en umbrales de 5 V:

```
SP node1> system sensors get 5V

Locating sensor record...
Sensor ID           : 5V (0x13)
Entity ID           : 7.97
Sensor Type (Analog) : Voltage
Sensor Reading       : 5.002 (+/- 0) Volts
Status               : ok
Lower Non-Recoverable : na
Lower Critical        : 4.246
Lower Non-Critical    : 4.490
Upper Non-Critical    : 5.490
Upper Critical        : 5.758
Upper Non-Recoverable : na
Assertion Events      :
Assertions Enabled    : lnc- lcr- ucr+
Deassertions Enabled : lnc- lcr- ucr+
```

Acerca de los valores discretos de estado del sensor del SP del resultado de comandos de sensores del sistema

Los sensores discretos no tienen umbrales. Sus lecturas se muestran bajo la `Current` En la CLI del SP `system sensors` Resultado del comando, no lleve el significado real y, por lo tanto, el SP lo ignora. La `Status` en la `system sensors` el resultado del comando muestra los valores de estado de los sensores discretos en formato hexadecimal.

Entre los ejemplos de sensores discretos se incluyen sensores para el fallo del ventilador, la unidad de suministro de alimentación (PSU) y errores del sistema. La lista específica de sensores discretos depende de la plataforma.

Puede utilizar la CLI del SP `system sensors get sensor_name` comando para obtener ayuda con la interpretación de los valores de estado de la mayoría de los sensores discretos. Los siguientes ejemplos muestran los resultados de la introducción de datos `system sensors get sensor_name` Para los sensores discretos `CPU0_error` y `IO_Slo1_Present`:

```

SP node1> system sensors get CPU0_Error
Locating sensor record...
Sensor ID           : CPU0_Error (0x67)
Entity ID           : 7.97
Sensor Type (Discrete): Temperature
States Asserted      : Digital State
                      [State Deasserted]

```

```

SP node1> system sensors get IO_Slot1_Present
Locating sensor record...
Sensor ID           : IO_Slot1_Present (0x74)
Entity ID           : 11.97
Sensor Type (Discrete): Add-in Card
States Asserted      : Availability State
                      [Device Present]

```

Aunque la `system sensors get sensor_name` El comando muestra la información de estado de la mayoría de los sensores discretos, no proporciona información de estado para los sensores discretos `System_FW_Status`, `System_Watchdog`, `PSU1_Input_Type` y `PSU2_Input_Type`. Puede utilizar la siguiente información para interpretar los valores de estado de estos sensores.

System_FW_Status

La condición del sensor `System_FW_Status` aparece en forma de `0xAABB`. Puede combinar la información de `AA` y `BB` para determinar el estado del sensor.

`AA` puede tener uno de los siguientes valores:

| Valores | Estado del sensor |
|---------|-----------------------------------|
| 01 | Error de firmware del sistema |
| 02 | Firmware del sistema colgado |
| 04 | Progreso del firmware del sistema |

`BB` puede tener uno de los siguientes valores:

| Valores | Estado del sensor |
|---------|---|
| 00 | El software del sistema se ha apagado correctamente |
| 01 | Inicialización de la memoria en curso |

| Valores | Estado del sensor |
|---------|---|
| 02 | Inicialización de NVMEM en curso (cuando NVMEM está presente) |
| 04 | Restaurando los valores del concentrador de memoria de la controladora (MCH) (cuando NVMEM está presente) |
| 05 | El usuario ha introducido configuración |
| 13 | Arrancar el sistema operativo o EL CARGADOR |
| 1F | BIOS se está iniciando |
| 20 | LOADER se está ejecutando |
| 21 | LOADER está programando el firmware de BIOS principal. No debe apagar el sistema. |
| 22 | LOADER está programando el firmware BIOS alternativo. No debe apagar el sistema. |
| 2F | ONTAP está ejecutando |
| 60 | SP ha apagado el sistema |
| 61 | SP ha encendido el sistema |
| 62 | SP ha restablecido el sistema |
| 63 | Ciclo de apagado y encendido del guardián de SP |
| 64 | Restablecimiento completo del guardián de SP |

Por ejemplo, el estado 0x042F del sensor System_FW_Status significa "curso del firmware del sistema (04), ONTAP se está ejecutando (2F)".

System_Watchdog

El sensor System_Watchdog puede tener una de las siguientes condiciones:

- **0x0080**

El estado de este sensor no ha cambiado

| Valores | Estado del sensor |
|---------|-------------------------------|
| 0x0081 | Interrupción del temporizador |
| 0x0180 | El temporizador ha caducado |
| 0x0280 | Restablecimiento completo |
| 0x0480 | Apagado |
| 0x0880 | Ciclo de apagado y encendido |

Por ejemplo, el estado 0x0880 del sensor System_Watchdog significa que se ha superado el tiempo de espera de un guardián y que ha provocado un ciclo de apagado y encendido del sistema.

PSU1_Input_Type y PSU2_Input_Type

Para suministros de alimentación de corriente continua (CC), los sensores PSU1_Input_Type y PSU2_Input_Type no se aplican. Para suministros de alimentación de corriente alterna (CA), el estado de los sensores puede tener uno de los valores siguientes:

| Valores | Estado del sensor |
|---------|-----------------------|
| 0x01 xx | Tipo de PSU de 220 V. |
| 0x02 xx | Tipo de PSU de 110 V. |

Por ejemplo, el estado 0x0280 del sensor PSU1_Input_Type significa que el sensor informa de que el tipo de PSU es 110 V.

Comandos para gestionar el SP desde ONTAP

ONTAP proporciona comandos para gestionar el SP, incluida la configuración de red del SP, la imagen del firmware del SP, el acceso SSH al SP y la administración general del SP.

Comandos para gestionar la configuración de red del SP


| Si desea... | Ejecute este comando ONTAP... |
|--|--|
| Habilite la configuración de red automática de SP para que el SP utilice la familia de direcciones IPv4 o IPv6 de la subred especificada | <code>system service-processor network auto-configuration enable</code> |
| Deshabilite la configuración de red automática del SP para la familia de direcciones IPv4 o IPv6 de la subred especificada para el SP | <code>system service-processor network auto-configuration disable</code> |

| Si desea... | Ejecute este comando ONTAP... |
|---|---|
| Muestra la configuración de red automática del SP | <code>system service-processor network auto-configuration show</code> |
| <p>Configure manualmente la red del SP para un nodo, incluidos los siguientes:</p> <ul style="list-style-type: none"> • La familia de direcciones IP (IPv4 o IPv6) • Si debe habilitarse la interfaz de red de la familia de direcciones IP especificada • Si se utiliza IPv4, ya sea para usar la configuración de red desde el servidor DHCP o la dirección de red que se especifique • La dirección IP pública del SP • La máscara de red del SP (si se utiliza IPv4) • La longitud del prefijo de red de la máscara de subred del SP (si se utiliza IPv6) • La dirección IP de la pasarela para el SP | <code>system service-processor network modify</code> |
| <p>Muestra la configuración de red del SP, incluidos los siguientes:</p> <ul style="list-style-type: none"> • La familia de direcciones configurada (IPv4 o IPv6) y si está habilitada • Tipo de dispositivo de administración remota • El estado actual de SP y el estado de enlace • Configuración de red, como la dirección IP, la dirección MAC, la máscara de red, la longitud del prefijo de la máscara de subred, la dirección IP asignada por el enrutador, la dirección IP local de enlace y la dirección IP de pasarela • La hora en la que se actualizó el SP por última vez • El nombre de la subred que se utiliza para la configuración automática de SP • Si la dirección IP asignada por el enrutador IPv6 está habilitada • Estado de configuración de la red del SP • Motivo del error de configuración de la red del SP | <p><code>system service-processor network show</code></p> <p>Para mostrar los detalles de red completos del SP es necesario <code>-instance</code> parámetro.</p> |

| Si desea... | Ejecute este comando ONTAP... |
|---|--|
| <p>Modifique la configuración del servicio API del SP, incluidos los siguientes:</p> <ul style="list-style-type: none"> • Cambiar el puerto que utiliza el servicio API del SP • Habilitar o deshabilitar el servicio API de SP | <pre>system service-processor api-service modify</pre> <p>(nivel de privilegio avanzado)</p> |
| <p>Muestra la configuración del servicio API del SP</p> | <pre>system service-processor api-service show</pre> <p>(nivel de privilegio avanzado)</p> |
| <p>Renueve los certificados SSL y SSH que utiliza el servicio API de SP para la comunicación interna</p> | <ul style="list-style-type: none"> • Para ONTAP 9.5 o posterior: <pre>system service-processor api-service renew-internal-certificates</pre> • Para ONTAP 9.4 o anterior: <pre>system service-processor api-service renew-certificates</pre> <p>(nivel de privilegio avanzado)</p> |

Comandos para gestionar la imagen del firmware del SP

| Si desea... | Ejecute este comando ONTAP... |
|--|--|
| <p>Muestre los detalles de la imagen del firmware del SP instalada actualmente, incluidos los siguientes:</p> <ul style="list-style-type: none"> • Tipo de dispositivo de administración remota • La imagen (principal o backup) desde la que se inicia el SP, su estado y versión de firmware • Si la actualización automática del firmware está habilitada y el estado de la última actualización | <pre>system service-processor image show</pre> <p>La <code>-is-current</code> Parámetro indica la imagen (principal o backup) desde la que se arranca actualmente el SP, no si la versión de firmware instalada es más reciente.</p> |
| <p>Habilitar o deshabilitar la actualización automática del firmware del SP</p> | <pre>system service-processor image modify</pre> <p>De forma predeterminada, el firmware del SP se actualiza automáticamente con la actualización de ONTAP o cuando se descarga manualmente una nueva versión del firmware del SP. No se recomienda deshabilitar la actualización automática porque, al hacerlo, puede dar lugar a combinaciones no óptimas o no cualificadas entre la imagen ONTAP y la imagen del firmware del SP.</p> |

| Si desea... | Ejecute este comando ONTAP... |
|---|--|
| <p>Descargar manualmente una imagen de firmware del SP en un nodo</p> | <pre>system node image get</pre> <div>  <p>Antes de ejecutar <code>system node image</code> comandos, debe configurar el nivel de privilegio en advanced (<code>set -privilege advanced</code>), introduzca y cuando se le solicite continuar.</p> </div> <p>La imagen del firmware del SP está empaquetada con ONTAP. No es necesario descargar el firmware del SP manualmente, a menos que desee utilizar una versión de firmware del SP diferente a la de los paquetes con ONTAP.</p> |
| <p>Muestre el estado de la última actualización del firmware del SP activada desde ONTAP, incluida la información siguiente:</p> <ul style="list-style-type: none"> • La hora de inicio y de finalización de la última actualización del firmware del SP • Si hay una actualización en curso y el porcentaje que se ha completado | <pre>system service-processor image update-progress show</pre> |

Comandos para gestionar el acceso SSH al SP

| Si desea... | Ejecute este comando ONTAP... |
|--|--|
| <p>Conceda acceso a SP únicamente a las direcciones IP especificadas</p> | <pre>system service-processor ssh add-allowed-addresses</pre> |
| <p>Bloquee las direcciones IP especificadas para que no puedan acceder al SP</p> | <pre>system service-processor ssh remove-allowed-addresses</pre> |
| <p>Muestre las direcciones IP que pueden acceder al SP</p> | <pre>system service-processor ssh show</pre> |

Comandos para la administración general de SP

| Si desea... | Ejecute este comando ONTAP... |
|---|--|
| <p>Muestra información general de SP, incluidos los siguientes:</p> <ul style="list-style-type: none"> • Tipo de dispositivo de administración remota • El estado actual de SP • Si la red del SP está configurada • Información de red, como la dirección IP pública y la dirección MAC • La versión del firmware del SP y la versión de la interfaz de gestión de la plataforma inteligente (IPMI) • Si la actualización automática del firmware del SP está habilitada | <p><code>system service-processor show</code> Para mostrar la información completa del SP es necesario <code>-instance</code> parámetro.</p> |
| Reinicie el SP en un nodo | <code>system service-processor reboot-sp</code> |
| Genere y envíe un mensaje de AutoSupport que incluya los archivos de registro de SP recopilados desde un nodo especificado | <code>system node autosupport invoke-splog</code> |
| Mostrar el mapa de asignación de los archivos de registro del SP recopilados en el clúster, incluidos los números de secuencia de los archivos de registro del SP que residen en cada nodo de recopilación | <code>system service-processor log show-allocations</code> |

Información relacionada

["Comandos de ONTAP 9"](#)

Comandos de ONTAP para la gestión de BMC

Estos comandos de la ONTAP son compatibles con la controladora de gestión de placa base (BMC).

El BMC utiliza algunos de los mismos comandos que el Service Processor (SP). Los siguientes comandos del SP son compatibles con el BMC.

| Si desea... | Utilice este comando |
|---|---|
| Muestre la información del BMC | <code>system service-processor show</code> |
| Mostrar/modificar la configuración de red del BMC | <code>system service-processor network show/modify</code> |
| Restablezca el BMC | <code>system service-processor reboot-sp</code> |

| Si desea... | Utilice este comando |
|---|--|
| Muestra/modifica los detalles de la imagen de firmware del BMC instalada actualmente | system service-processor image show/modify |
| Actualizar el firmware del BMC | system service-processor image update |
| Muestra el estado de la última actualización del firmware del BMC | system service-processor image update-progress show |
| Habilite la configuración de red automática para que el BMC utilice una dirección IPv4 o IPv6 en la subred especificada | system service-processor network auto-configuration enable |
| Deshabilite la configuración de red automática para una dirección IPv4 o IPv6 en la subred especificada para el BMC | system service-processor network auto-configuration disable |
| Mostrar la configuración de red automática del BMC | system service-processor network auto-configuration show |

Para los comandos que no son compatibles con el firmware del BMC, se devuelve el siguiente mensaje de error.

```
::> Error: Command not supported on this platform.
```

Comandos de la CLI de BMC

Puede iniciar sesión en el BMC mediante SSH. Los siguientes comandos se admiten desde la línea de comandos de BMC.

| Comando | Función |
|--|---|
| sistema | Mostrar una lista de todos los comandos. |
| consola del sistema | Conecta a la consola del sistema. Uso Ctrl+D para salir de la sesión. |
| núcleo del sistema | Vuelca la memoria del sistema y reinicia. |
| ciclo de apagado y encendido del sistema | Apaga el sistema y lo enciende después. |
| apagado del sistema | Apaga el sistema. |
| encendido del sistema | Enciende el sistema. |

| Comando | Función |
|-------------------------------|--|
| estado de energía del sistema | Imprimir estado de energía del sistema. |
| restablecimiento del sistema | Restablezca el sistema. |
| registro del sistema | Imprimir los registros de la consola del sistema |
| fru del sistema mostrar [id] | Volcar toda la información de la unidad reemplazable del campo (FRU)/seleccionada. |

Gestionar la hora del clúster (solo administradores de clúster)

Los problemas pueden surgir cuando la hora del clúster no es precisa. Aunque ONTAP le permite establecer manualmente la zona horaria, la fecha y la hora del clúster, debe configurar los servidores de protocolo de hora de red (NTP) para sincronizar la hora del clúster.

A partir de ONTAP 9.5, puede configurar el servidor NTP con autenticación simétrica.

NTP está siempre habilitado. Sin embargo, sigue siendo necesaria la configuración para que el clúster se sincronice con un origen de tiempo externo. ONTAP permite gestionar la configuración de NTP del clúster de las siguientes maneras:

- Es posible asociar un máximo de 10 servidores NTP externos al clúster (`cluster time-service ntp server create`).
 - Para la redundancia y la calidad del servicio de tiempo, debe asociar al menos tres servidores NTP externos al clúster.
 - Es posible especificar un servidor NTP con su dirección IPv4 o IPv6, o bien un nombre de host completo.
 - Puede especificar manualmente la versión de NTP (v3 o v4) que desee usar.

De forma predeterminada, ONTAP selecciona automáticamente la versión de NTP que se admite para un servidor NTP externo determinado.

Si la versión de NTP especificada no es compatible con el servidor NTP, no se puede realizar el intercambio de hora.

- En el nivel de privilegio avanzado, puede especificar un servidor NTP externo que esté asociado con el clúster para que sea el origen de hora principal para corregir y ajustar la hora del clúster.
- Puede mostrar los servidores NTP asociados con el clúster (`cluster time-service ntp server show`).
- Es posible modificar la configuración de NTP del clúster (`cluster time-service ntp server modify`).
- Es posible desasociar el clúster de un servidor NTP externo (`cluster time-service ntp server delete`).
- En el nivel de privilegio avanzado, puede restablecer la configuración borrando la asociación de todos los

servidores NTP externos con el clúster (`cluster time-service ntp server reset`).

Un nodo que se une a un clúster adopta automáticamente la configuración de NTP del clúster.

Además de usar NTP, ONTAP también le permite gestionar manualmente la hora del clúster. Esta funcionalidad resulta útil cuando es necesario corregir una hora incorrecta (por ejemplo, la hora de un nodo se ha vuelto significativamente incorrecta después de un reinicio). En ese caso, puede especificar una hora aproximada para el clúster hasta que NTP pueda sincronizar con un servidor de tiempo externo. El tiempo que establece manualmente surte efecto en todos los nodos del clúster.

Puede gestionar manualmente la hora del clúster de las siguientes maneras:

- Puede configurar o modificar la zona horaria, la fecha y la hora del clúster (`cluster date modify`).
- Puede mostrar la configuración actual de la zona horaria, la fecha y la hora del clúster (`cluster date show`).



Las programaciones de trabajos no se ajustan a los cambios de fecha y hora del clúster manuales. Estos trabajos se programan para que se ejecuten en función de la hora actual del clúster cuando se creó el trabajo o cuando se ejecutó el trabajo más recientemente. Por lo tanto, si cambia manualmente la fecha o la hora del clúster, debe usar el `job show` y `job history show` comandos para verificar que todos los trabajos programados se ponen en cola y se completan de acuerdo con los requisitos que haya.



Comandos para gestionar la hora del clúster

Utilice la `cluster time-service ntp server` Comandos para gestionar los servidores NTP para el clúster. Utilice la `cluster date` comandos para gestionar la hora del clúster de forma manual.

A partir de ONTAP 9.5, puede configurar el servidor NTP con autenticación simétrica.

Los siguientes comandos permiten gestionar los servidores NTP para el clúster:

| Si desea... | Se usa este comando... |
|--|--|
| Asocie el clúster con un servidor NTP externo sin autenticación simétrica | <code>cluster time-service ntp server create -server server_name</code> |
| Asocie el clúster con un servidor NTP externo con autenticación simétrica. Disponibilidad en ONTAP 9.5 o posterior | <div><div><code>cluster time-service ntp server create -server server_ip_address -key-id key_id</code></div><div> La <code>key_id</code> debe hacer referencia a una clave compartida existente configurada con "clave ntp de servicio de tiempo del clúster".</div></div> |

| Si desea... | Se usa este comando... |
|--|---|
| Habilitar autenticación simétrica para un servidor NTP existente se puede modificar el servidor NTP existente para habilitar la autenticación agregando el Id. De clave requerido Disponible en ONTAP 9.5 o posterior | <pre>cluster time-service ntp server modify -server server_name -key-id key_id</pre> |
| Deshabilitar la autenticación simétrica | <pre>cluster time-service ntp server modify -server server_name -is-authentication -enabled false</pre> |
| Configure una clave NTP compartida | <pre>cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value</pre> <div>  <p>Las claves compartidas se refieren a un ID. El ID, su tipo y el valor deben ser idénticos tanto en el nodo como en el servidor NTP</p> </div> |
| Muestra información sobre los servidores NTP asociados con el clúster | <pre>cluster time-service ntp server show</pre> |
| Modifique la configuración de un servidor NTP externo asociado con el clúster | <pre>cluster time-service ntp server modify</pre> |
| Disocie un servidor NTP del clúster | <pre>cluster time-service ntp server delete</pre> |
| Restablezca la configuración borrando la asociación de todos los servidores NTP externos con el clúster | <pre>cluster time-service ntp server reset</pre> <div>  <p>Este comando requiere el nivel de privilegio avanzado.</p> </div> |

Los siguientes comandos le permiten gestionar la hora del clúster de forma manual:

| Si desea... | Se usa este comando... |
|---|--------------------------------|
| Configure o modifique la zona horaria, la fecha y la hora | <pre>cluster date modify</pre> |
| Muestre la configuración de la zona horaria, la fecha y la hora del clúster | <pre>cluster date show</pre> |

Información relacionada

["Comandos de ONTAP 9"](#)

Administrar el banner y el MOTD

Gestione el banner y la visión general de MOTD

ONTAP permite configurar un banner de inicio de sesión o un mensaje del día (MOTD) para comunicar la información administrativa a los usuarios de la CLI del clúster o de la máquina virtual de almacenamiento (SVM).

Se muestra un banner en una sesión de consola (solo para el acceso al clúster) o una sesión SSH (para el acceso al clúster o a SVM) antes de que se solicite a un usuario que realice la autenticación, como una contraseña. Por ejemplo, puede utilizar el banner para mostrar un mensaje de advertencia como el siguiente a alguien que intenta iniciar sesión en el sistema:

```
$ ssh admin@cluster1-01
```

```
This system is for authorized users only. Your IP Address has been logged.
```

```
Password:
```

Un MDT se muestra en una sesión de consola (sólo para acceso a clústeres) o una sesión SSH (para acceso a clústeres o SVM) después de que un usuario se autentica pero antes de que aparezca el mensaje clustershell. Por ejemplo, puede utilizar el MOTD para mostrar un mensaje de bienvenida o informativo como el siguiente, que sólo verán los usuarios autenticados:

```
$ ssh admin@cluster1-01
```

```
Password:
```

```
Greetings. This system is running ONTAP 9.0.
```

```
Your user name is 'admin'. Your last login was Wed Apr 08 16:46:53 2015  
from 10.72.137.28.
```

Puede crear o modificar el contenido del banner o el MOTD mediante el `security login banner modify` o `security login motd modify` command, respectivamente, de las siguientes formas:

- Puede utilizar la CLI de forma interactiva o no interactiva para especificar el texto que se va a utilizar para el banner o el MOTD.

El modo interactivo, se inicia cuando el comando se utiliza sin el `-message` o `-uri` parámetro, permite utilizar nuevas líneas (también llamadas fin de líneas) en el mensaje.

El modo no interactivo, que utiliza `-message` parámetro para especificar la cadena de mensaje, no admite newlines.

- Puede cargar contenido desde una ubicación FTP o HTTP para utilizarlo en el banner o en el MOTD.
- Puede configurar el módulo MOTD para que muestre contenido dinámico.

Algunos ejemplos de lo que puede configurar el MOTD para que se muestre dinámicamente son los

siguientes:

- El nombre del clúster, el nombre del nodo o el nombre de SVM
- Fecha y hora del clúster
- Nombre del usuario que inicia sesión
- Último inicio de sesión para el usuario en cualquier nodo del clúster
- Nombre de dispositivo de inicio de sesión o dirección IP
- Nombre del sistema operativo
- Versión del software
- Cadena de versión efectiva del clúster

La `security login motd modify` La página man describe las secuencias de escape que puede utilizar para permitir que el MOTD muestre contenido generado dinámicamente.

El banner no admite contenido dinámico.

Puede gestionar el banner y el MOTD en el nivel de clúster o SVM:

- Los siguientes hechos se aplican al banner:
 - El banner configurado para el clúster también se usa para todas las SVM que no tienen un mensaje de banner definido.
 - Se puede configurar un banner a nivel de SVM para cada SVM.

Si se configuró un banner a nivel de clúster, este será anulado por el banner de SVM de la SVM indicada.

- Los siguientes hechos se aplican al MDD:
 - De forma predeterminada, el MOTD configurado para el clúster también está habilitado para todas las SVM.
 - Además, se puede configurar un MOTD a nivel de SVM para cada SVM.

En este caso, los usuarios que inicien sesión en la SVM verán dos MOTDs, uno definido a nivel de clúster y el otro a nivel de SVM.

- El administrador del clúster puede habilitar o deshabilitar el MOTD a nivel de clúster por SVM.

Si el administrador de clúster deshabilita el MOTD a nivel de clúster para una SVM, un usuario que inicia sesión en la SVM no ve el MOTD a nivel de clúster.

Cree un banner

Puede crear un banner para que muestre un mensaje a alguien que intente acceder al clúster o a una SVM. El banner se muestra en una sesión de consola (solo para el acceso al clúster) o una sesión SSH (para el acceso a clústeres o SVM) antes de que se pida al usuario que realice la autenticación.

Pasos

1. Utilice la `security login banner modify` Comando para crear un banner para el clúster o la SVM:

| Si desea... | Realice lo siguiente... |
|--|--|
| Especifique un mensaje que sea una sola línea | Utilice la <code>-message "text"</code> parámetro para especificar el texto. |
| Incluya nuevas líneas (también conocidas como fin de líneas) en el mensaje | Utilice el comando sin el <code>-message</code> o. <code>-uri</code> parámetro para iniciar el modo interactivo de edición del banner. |
| Cargue el contenido de una ubicación para usarlo como banner | Utilice la <code>-uri</code> Parámetro para especificar la ubicación FTP o HTTP del contenido. |

El tamaño máximo de un banner es de 2,048 bytes, incluidas las líneas nuevas.

Un banner creado mediante el `-uri` el parámetro es estático. No se actualiza automáticamente para reflejar los cambios posteriores del contenido de origen.

El banner creado para el clúster también se muestra para todas las SVM que no tienen un banner existente. Cualquier banner creado posteriormente para una SVM anula el banner a nivel de clúster de esa SVM. Especifique el `-message` parámetro con un guión entre comillas dobles ("`-`") Para que la SVM restablece la SVM para usar el banner a nivel de clúster.

2. Verifique que el banner se haya creado mostrándolo con el `security login banner show` comando.

Especifique el `-message` parámetro con una cadena vacía ("`''`") muestra banners que no tienen contenido.

Especifique el `-message` parámetro con "`-`" Muestra todas las SVM (administrador o datos) que no tienen un banner configurado.

Ejemplos de creación de banners

En el siguiente ejemplo se utiliza el modo no interactivo para crear un banner para el clúster "`cluster1`":

```
cluster1::> security login banner modify -message "Authorized users only!"

cluster1::>
```

En el siguiente ejemplo se utiliza el modo interactivo para crear un banner para la «SVM «`svm1`»:

```
cluster1::> security login banner modify -vserver svm1

Enter the message of the day for Vserver "svm1".
Max size: 2048. Enter a blank line to terminate input. Press Ctrl-C to
abort.
0          1          2          3          4          5          6          7
8
1234567890123456789012345678901234567890123456789012345678901234
567890
The svm1 SVM is reserved for authorized users only!

cluster1::>
```

El siguiente ejemplo muestra los banners que se han creado:

```
cluster1::> security login banner show
Vserver: cluster1
Message
-----
---
Authorized users only!

Vserver: svm1
Message
-----
---
The svm1 SVM is reserved for authorized users only!

2 entries were displayed.

cluster1::>
```

Información relacionada

[Gestión del banner](#)

Gestión del banner

Puede gestionar el banner en el nivel del clúster o de la SVM. El banner configurado para el clúster también se usa para todas las SVM que no tienen un mensaje de banner definido. Un banner creado posteriormente para una SVM anula el banner de clúster de esa SVM.

Opciones

- Gestione el banner en el nivel de clúster:

| Si desea... | Realice lo siguiente... |
|--|--|
| Cree un banner que aparezca para todas las sesiones de inicio de sesión de la CLI | Establezca un banner a nivel del clúster: `*security login banner modify -vserver <i>cluster_name</i> { [-message "text"] |
| <i>[-uri ftp_or_http_addr] }</i> *` | Quite el banner de todos los inicios de sesión (clúster y SVM) |
| Establezca el banner en una cadena vacía (""): security login banner modify -vserver * -message "" | Anule el banner creado por un administrador de SVM |
| Modifique el mensaje de banner de la SVM: `*security login banner modify -vserver <i>svm_name</i> { [-message "text"] | <i>[-uri ftp_or_http_addr] }</i> *` |

- Gestione el banner a nivel de SVM:

Especificando `-vserver svm_name` No es necesario en el contexto de SVM.

| Si desea... | Realice lo siguiente... |
|--|--|
| Anule el banner proporcionado por el administrador del clúster con un banner diferente para la SVM | Cree un banner para la SVM: `*security login banner modify -vserver <i>svm_name</i> { [-message "text"] |
| <i>[-uri ftp_or_http_addr] }</i> *` | Elimine el banner proporcionado por el administrador del clúster de modo que no se muestre ningún banner para la SVM |
| Establezca el banner de SVM en una cadena vacía para la SVM: security login banner modify -vserver <i>svm_name</i> -message "" | Use el banner a nivel de clúster cuando la SVM actualmente utiliza un banner de SVM |

Cree un MOTD

Puede crear un mensaje del día (MOTD) para comunicar información a usuarios CLI autenticados. El MOTD se muestra en una sesión de consola (sólo para acceso a clústeres) o en una sesión SSH (para acceso a clústeres o SVM) después de que un usuario se autentica pero antes de que aparezca el mensaje clustershell.

Pasos

1. Utilice la `security login motd modify` Comando para crear un MOTD para el clúster o SVM:

| Si desea... | Realice lo siguiente... |
|--|--|
| Especifique un mensaje que sea una sola línea | Utilice la <code>-message "text"</code> parámetro para especificar el texto. |
| Incluir nuevas líneas (también conocido como fin de líneas) | Utilice el comando sin el <code>-message</code> o. <code>-uri</code> Parámetro para iniciar el modo interactivo para editar el MOTD. |
| Cargue contenido desde una ubicación para utilizarlo en el dispositivo | Utilice la <code>-uri</code> Parámetro para especificar la ubicación FTP o HTTP del contenido. |

El tamaño máximo para un MDE es de 2,048 bytes, incluyendo líneas nuevas.

La `security login motd modify` La página man describe las secuencias de escape que puede utilizar para permitir que el MOTD muestre contenido generado dinámicamente.

Un MDT creado mediante el `-uri` el parámetro es estático. No se actualiza automáticamente para reflejar los cambios posteriores del contenido de origen.

De forma predeterminada, se muestra un MOTD creado para el clúster también para todos los inicios de sesión de SVM, junto con un MOTD de nivel de SVM que se puede crear por separado para un SVM determinado. Ajuste de `-is-cluster-message-enabled` parámetro a. `false` Para una SVM impide que se muestre el MOTD a nivel de clúster para esa SVM.

2. Compruebe que el MDD se ha creado mostrándolo con el `security login motd show` comando.

Especifique el `-message` parámetro con una cadena vacía (`" "`) Muestra los MODs que no están configurados o que no tienen contenido.

Consulte ["modificación de los motd de inicio de sesión de seguridad"](#) Página de comando manual para una lista de parámetros que se utilizarán para permitir que el MOTD muestre contenido generado dinámicamente. Asegúrese de consultar la página de manual específica de su versión de ONTAP.

Ejemplos de creación de MODs

En el siguiente ejemplo se utiliza el modo no interactivo para crear un MDE para el clúster `"cluster1"`:

```
cluster1::> security login motd modify -message "Greetings!"
```

En el siguiente ejemplo se utiliza el modo interactivo para crear un MDE para la `"VMs1"` que utiliza secuencias de escape para mostrar contenido generado dinámicamente:

```
cluster1::> security login motd modify -vserver svm1
```

```
Enter the message of the day for Vserver "svm1".
```

```
Max size: 2048. Enter a blank line to terminate input. Press Ctrl-C to abort.
```

```
0          1          2          3          4          5          6          7
8
```

```
1234567890123456789012345678901234567890123456789012345678901234
567890
```

```
Welcome to the \n SVM.  Your user ID is '\N'. Your last successful login
was \L.
```

El siguiente ejemplo muestra los MODs que se han creado:

```
cluster1::> security login motd show
```

```
Vserver: cluster1
```

```
Is the Cluster MOTD Displayed?: true
```

```
Message
```

```
-----
---
```

```
Greetings!
```

```
Vserver: svm1
```

```
Is the Cluster MOTD Displayed?: true
```

```
Message
```

```
-----
---
```

```
Welcome to the \n SVM.  Your user ID is '\N'. Your last successful login
was \L.
```

```
2 entries were displayed.
```

Administrar el MDT

Puede gestionar el mensaje del día (MOTD) a nivel de clúster o SVM. De forma predeterminada, el MOTD configurado para el clúster también está habilitado para todas las SVM. Además, se puede configurar un MOTD a nivel de SVM para cada SVM. El administrador del clúster puede habilitar o deshabilitar el MOTD a nivel de clúster para cada SVM.

Para obtener una lista de secuencias de escape que se pueden utilizar para generar contenido de forma dinámica para el MOTD, consulte la ["referencia de comandos"](#).

Opciones

- Gestione el MOTD a nivel de clúster:

| Si desea... | Realice lo siguiente... |
|--|--|
| Cree un MOTD para todos los inicios de sesión cuando no haya ningún MDE existente | Establecer un MOTD a nivel de clúster: `*security login motd modify -vserver <i>cluster_name</i> { [-message " <i>text</i> "] } |
| <code>[-uri <i>ftp_or_http_addr</i>] }*</code> | Cambie el MOTD para todos los inicios de sesión cuando no se haya configurado ningún MODs de nivel SVM |
| Modifique el módulo de MOTD a nivel de clúster: `*security login motd modify -vserver <i>cluster_name</i> { [-message " <i>text</i> "] } | <code>[-uri <i>ftp_or_http_addr</i>] }*</code> |
| Quite el MOTD para todos los inicios de sesión cuando no haya ningún MODs de nivel SVM configurado | Establezca el MODD a nivel de clúster en una cadena vacía (""): security login motd modify -vserver <i>cluster_name</i> -message "" |
| Haga que cada SVM muestre el MOTD a nivel de clúster en lugar de usar el MOTD a nivel de SVM | Establezca un MDE a nivel de clúster y, a continuación, establezca todos los MODs a nivel de SVM en una cadena vacía con el MODD a nivel de clúster activado: a. <code>*security login motd modify -vserver <i>cluster_name</i> { [-message "<i>text</i>"] }</code> |
| <code>[-uri <i>ftp_or_http_addr</i>] }*</code> .. security login motd modify { -vserver !"cluster_name" } -message "" -is -cluster-message-enabled true | Mostrar un MOTD sólo para los SVM seleccionados y no utilizar ningún MOTD a nivel de clúster |
| Establezca el MOTD a nivel de clúster en una cadena vacía y, a continuación, establezca MOTDs a nivel de SVM para las SVM seleccionadas: a. security login motd modify -vserver <i>cluster_name</i> -message "" b. <code>*security login motd modify -vserver <i>svm_name</i> { [-message "<i>text</i>"] }</code> | <code>[-uri <i>ftp_or_http_addr</i>] }*</code> + Puede repetir este paso con cada SVM según sea necesario. |
| Use el mismo MOTD a nivel de SVM para todas las SVM (datos y administrador) | Configure el clúster y todas las SVM para que utilicen el mismo MOTD: `*security login motd modify -vserver * { [-message " <i>text</i> "] } |

| Si desea... | Realice lo siguiente... |
|--|--|
| <pre>[-uri ftp_or_http_addr] }*</pre> <p>[NOTE] ====</p> <p>Si utiliza el modo interactivo, la CLI le pedirá que introduzca el MOTD individualmente para el clúster y cada SVM. Puede pegar el mismo MOTD en cada instancia cuando se le solicite.</p> <p>====</p> | <p>Tener un MOTD a nivel de clúster disponible opcionalmente para todas las SVM, pero no desea que se muestre el MOTD para los inicios de sesión de clúster</p> |
| <p>Establezca un MDE a nivel de clúster, pero desactive su visualización para el clúster:</p> <pre>*security login motd modify -vserver cluster_name { [-message "text"]</pre> | <pre>[-uri ftp_or_http_addr] } -is-cluster-message-enabled false*</pre> |
| <p>Quite todos los MOD de los niveles de clúster y SVM cuando solo algunas SVM tengan MOTDS a nivel de clúster y SVM</p> | <p>Establezca el clúster y todas las SVM para usar una cadena vacía para la fecha de MOTD:</p> <pre>security login motd modify -vserver * -message ""</pre> |
| <p>Modifique el MOTD sólo para las SVM que tengan una cadena no vacía, cuando otras SVM utilicen una cadena vacía y cuando se utilice un MOTD diferente a nivel de clúster</p> | <p>Utilice consultas extendidas para modificar el MOTD de forma selectiva:</p> <pre>*security login motd modify { -vserver !"cluster_name" -message !"" } { [-message "text"]</pre> |
| <pre>[-uri ftp_or_http_addr] }*</pre> | <p>Mostrar todos los MODs que contienen texto específico (por ejemplo, «'enero'» seguido de «'2015'») en cualquier lugar de un mensaje único o multilínea, incluso si el texto está dividido entre líneas diferentes</p> |
| <p>Utilice una consulta para mostrar los MODs:</p> <pre>security login motd show -message *"January"*"2015"*</pre> | <p>Crear interactivamente un MDE que incluya varias y consecutivas líneas nuevas (también conocidas como fin de línea o EOLs)</p> |

- Gestione el MOTD a nivel de SVM:

Especificando `-vserver svm_name` No es necesario en el contexto de SVM.

| Si desea... | Realice lo siguiente... |
|---|--|
| Use un MOTD de nivel SVM diferente, cuando la SVM ya tenga un MOTD de nivel SVM existente | Modifique el MOTD en el nivel SVM: `*security login motd modify -vserver <i>svm_name</i> { [-message " <i>text</i> "] |
| <code>[-uri <i>ftp_or_http_addr</i>] }*</code> | Utilice únicamente el MOTD a nivel de clúster para la SVM, cuando la SVM ya tenga un MOTD a nivel de SVM |
| <p>Establezca el MOTD a nivel de SVM en una cadena vacía y, a continuación, haga que el administrador del clúster habilite el MOTD a nivel de clúster para la SVM:</p> <ol style="list-style-type: none"> <code>security login motd modify -vserver <i>svm_name</i> -message ""</code> (Para el administrador de clúster) <code>security login motd modify -vserver <i>svm_name</i> -is-cluster-message-enabled true</code> | No es necesario que la SVM muestre ningún MOTD, cuando se muestran actualmente los MOTDs a nivel de clúster y de SVM para la SVM |

Gestionar trabajos y programar

Los trabajos se colocan en una cola de trabajos y se ejecutan en segundo plano cuando los recursos están disponibles. Si una tarea consume demasiados recursos del clúster, puede detenerla o pausar hasta que haya menos demanda en el clúster. También puede supervisar y reiniciar los trabajos.

Categorías de trabajo

Hay tres categorías de trabajos que puede administrar: Afiliados al servidor, afiliados al cluster y privados.

Un trabajo puede encontrarse en cualquiera de las siguientes categorías:

- **Trabajos afiliados al servidor**

El marco de gestión pone estos trabajos en cola en un nodo específico para su ejecución.

- **Trabajos afiliados al grupo**

Este trabajo se pone en cola en el marco de gestión de cualquier nodo del clúster que se ejecute.

- **Trabajos privados**

Estos trabajos son específicos de un nodo y no utilizan la base de datos replicada (RDB) ni ningún otro mecanismo del cluster. Los comandos que administran trabajos privados requieren el nivel de privilegio avanzado o superior.

Comandos para gestionar trabajos

Cuando se introduce un comando que invoca un trabajo, normalmente, el comando le informa de que el

trabajo se ha puesto en cola y, a continuación, vuelve al símbolo del sistema de la CLI. Sin embargo, algunos comandos, en su lugar, informan el progreso de los trabajos y no vuelven a símbolo del sistema de la CLI hasta que se completa el trabajo. En estos casos, puede pulsar Ctrl-C para mover el trabajo al fondo.

| Si desea... | Se usa este comando... |
|---|---|
| Muestra información sobre todos los trabajos | <code>job show</code> |
| Muestra información sobre los trabajos nodo a nodo | <code>job show bynode</code> |
| Muestra información acerca de los trabajos afiliados al clúster | <code>job show-cluster</code> |
| Muestra información sobre los trabajos completados | <code>job show-completed</code> |
| Muestra información sobre el historial de trabajos | <code>job history show</code> Se almacenan hasta 25,000 registros de trabajos para cada nodo del clúster. Por lo tanto, intentar mostrar el historial completo del trabajo puede tardar mucho tiempo. Para evitar tiempos de espera potencialmente largos, debe mostrar trabajos por nodo, máquina virtual de almacenamiento (SVM) o ID de registro. |
| Mostrar la lista de trabajos privados | <code>job private show</code> (nivel de privilegio avanzado) |
| Muestra información sobre los trabajos privados completados | <code>job private show-completed</code> (nivel de privilegio avanzado) |
| Muestra información sobre el estado de inicialización de los gestores de trabajos | <code>job initstate show</code> (nivel de privilegio avanzado) |
| Supervise el progreso de un trabajo | <code>job watch-progress</code> |
| Supervisar el progreso de un trabajo privado | <code>job private watch-progress</code> (nivel de privilegio avanzado) |
| Poner en pausa un trabajo | <code>job pause</code> |
| Poner en pausa un trabajo privado | <code>job private pause</code> (nivel de privilegio avanzado) |
| Reanudar un trabajo pausado | <code>job resume</code> |
| Reanudar un trabajo privado en pausa | <code>job private resume</code> (nivel de privilegio avanzado) |

| Si desea... | Se usa este comando... |
|---|--|
| Detener un trabajo | <code>job stop</code> |
| Detener un trabajo privado | <code>job private stop</code> (nivel de privilegio avanzado) |
| Eliminar un trabajo | <code>job delete</code> |
| Eliminar un trabajo privado | <code>job private delete</code> (nivel de privilegio avanzado) |
| Desasociar un trabajo afiliado al clúster con un nodo no disponible que lo posea, de forma que otro nodo pueda hacerse cargo de ese trabajo | <code>job unclaim</code> (nivel de privilegio avanzado) |



Puede utilizar el `event log show` comando para determinar el resultado de un trabajo completado.

Información relacionada

["Comandos de ONTAP 9"](#)

Comandos para gestionar programaciones de trabajos

Muchas tareas, por ejemplo, copias Snapshot de volumen, se pueden configurar para ejecutarse en programaciones específicas. Las programaciones que se ejecuten en momentos específicos se denominan programaciones *cron* (similares a UNIX) *cron* horarios). Los horarios que se ejecutan a intervalos se denominan programas *INTERVAL*. Utilice la `job schedule` comandos para gestionar programaciones de trabajos.

Las programaciones de trabajos no se ajustan a los cambios manuales en la fecha y la hora del clúster. Estos trabajos se programan para que se ejecuten en función de la hora actual del clúster cuando se creó el trabajo o cuando se ejecutó el trabajo más recientemente. Por lo tanto, si cambia manualmente la fecha o la hora del clúster, debe usar el `job show y.. job history show` comandos para verificar que todos los trabajos programados se ponen en cola y se completan de acuerdo con los requisitos que haya.

Si el clúster forma parte de una configuración de MetroCluster, las programaciones de trabajos en ambos clústeres deben ser idénticas. Por lo tanto, si crea, modifica o elimina una programación de trabajos, debe realizar la misma operación en el clúster remoto.

| Si desea... | Se usa este comando... |
|--|-------------------------------------|
| Muestra información sobre todos los programas | <code>job schedule show</code> |
| Mostrar la lista de trabajos según la programación | <code>job schedule show-jobs</code> |
| Mostrar información acerca de las programaciones de cron | <code>job schedule cron show</code> |

| Si desea... | Se usa este comando... |
|---|--|
| Muestra información acerca de los programas de intervalos | <code>job schedule interval show</code> |
| Crear una programación Cron | <code>job schedule cron create</code> A partir de ONTAP 9.10.1, puede incluir la máquina virtual de almacenamiento SVM en su programación de trabajos. |
| Cree una programación de intervalo | <code>job schedule interval create</code> Debe especificar al menos uno de los siguientes parámetros: <code>-days</code> , <code>-hours</code> , <code>-minutes</code> , <code>0</code> , <code>-seconds</code> . |
| Modificar una programación de cron | <code>job schedule cron modify</code> |
| Modificar una programación de intervalo | <code>job schedule interval modify</code> |
| Eliminar una programación | <code>job schedule delete</code> |
| Eliminar una programación cron | <code>job schedule cron delete</code> |
| Eliminar una programación de intervalo | <code>job schedule interval delete</code> |

Información relacionada

["Comandos de ONTAP 9"](#)

Realizar backups y restaurar configuraciones del clúster (solo administradores de clúster)

Que son los archivos de copia de seguridad de configuración

Los archivos de copia de seguridad de configuración son archivos de archivo (.7z) que contienen información sobre todas las opciones configurables que son necesarias para que el clúster y los nodos que contiene funcionen correctamente.

Estos archivos almacenan la configuración local de cada nodo, además de la configuración replicada en todo el clúster. Se utilizan archivos de backup de configuración para realizar una copia de seguridad y restaurar la configuración del clúster.

Existen dos tipos de archivos de copia de seguridad de configuración:

- **Archivo de copia de seguridad de configuración de nodos**

Cada nodo en buen estado del clúster incluye un archivo de backup de configuración de nodos, que

contiene toda la información de configuración y los metadatos necesarios para que el nodo funcione en buen estado del clúster.

- **Archivo de copia de seguridad de la configuración del clúster**

Estos archivos incluyen un archivo de todos los archivos de copia de seguridad de configuración del nodo en el clúster, además de la información de configuración del clúster replicado (la base de datos replicada o el archivo RDB). Los archivos de backup de configuración del clúster permiten restaurar la configuración de todo el clúster o de cualquier nodo del clúster. Las programaciones de backup de configuración del clúster crean estos archivos automáticamente y los almacenan en varios nodos del clúster.



Los archivos de copia de seguridad de configuración sólo contienen información de configuración. No incluyen datos de usuario. Para obtener más información sobre cómo restaurar datos de usuario, consulte ["Protección de datos"](#).

Cómo se realiza automáticamente la copia de seguridad de las configuraciones de nodos y clústeres

Tres programaciones independientes crean automáticamente archivos de backup de configuración de clúster y nodo y los replican entre los nodos del clúster.

Los archivos de copia de seguridad de configuración se crean automáticamente según las siguientes programaciones:



- Cada 8 horas
- Todos los días
- Semanal

En cada una de estas ocasiones, se crea un archivo de backup de configuración de nodo en cada nodo en buen estado del clúster. Todos estos archivos de backup de configuración de nodo se recopilan en un único archivo de backup de configuración de clúster junto con la configuración de clúster replicada y se guardan en uno o más nodos del clúster.

Comandos para gestionar las programaciones de backup de configuración

Puede utilizar el `system configuration backup settings` comandos para gestionar las programaciones de backup de configuración.

Estos comandos están disponibles en el nivel de privilegio avanzado.



| Si desea... | Se usa este comando... |
|---|--|
| <p>Cambie los ajustes de una programación de copia de seguridad de la configuración:</p> <ul style="list-style-type: none"> • Especifique una URL remota (HTTP, HTTPS, FTP, FTPS o TFTP) donde se cargarán los archivos de copia de seguridad de configuración además de las ubicaciones predeterminadas del clúster • Especifique un nombre de usuario que se utilizará para iniciar sesión en la URL remota • Establecer el número de copias de seguridad que se conservarán para cada programación de copia de seguridad de la configuración | <p><code>system configuration backup settings modify</code></p> <p>Cuando utilice HTTPS en la URL remota, utilice <code>-validate-certification</code> opción para habilitar o deshabilitar la validación de certificados digitales. De forma predeterminada, la validación de certificados está deshabilitada.</p> <div>  <p>El servidor web al cual se carga el archivo de backup de configuración debe tener habilitadas las operaciones HTTP y POSTERIORES habilitadas para HTTPS. Para obtener más información, consulte la documentación de su servidor web.</p> </div> |
| <p>Defina la contraseña que se utilizará para iniciar sesión en la URL remota</p> | <p><code>system configuration backup settings set-password</code></p> |
| <p>Vea la configuración de la programación de backup de configuración</p> | <p><code>system configuration backup settings show</code></p> <div>  <p>Establezca la <code>-instance</code> parámetro para ver el nombre de usuario y la cantidad de backups que se deben conservar para cada programación.</p> </div> |

Comandos para gestionar los archivos de copia de seguridad de configuración

Utilice la `system configuration backup` comandos para gestionar archivos de backup de configuración de clúster y nodo.

Estos comandos están disponibles en el nivel de privilegio avanzado.

| Si desea... | Se usa este comando... |
|--|--|
| <p>Cree un nuevo archivo de copia de seguridad de configuración de nodo o clúster</p> | <p><code>system configuration backup create</code></p> |
| <p>Copiar un archivo de backup de configuración de un nodo a otro nodo del clúster</p> | <p><code>system configuration backup copy</code></p> |

| Si desea... | Se usa este comando... |
|--|---|
| Cargar un archivo de copia de seguridad de configuración desde un nodo del clúster en una URL remota (FTP, HTTP, HTTPS, TFTP o FTPS) | <p><code>system configuration backup upload</code></p> <p>Cuando utilice HTTPS en la URL remota, utilice <code>-validate-certification</code> opción para habilitar o deshabilitar la validación de certificados digitales. De forma predeterminada, la validación de certificados está deshabilitada.</p> <div>  <p>El servidor web al cual se carga el archivo de backup de configuración debe tener habilitadas las operaciones HTTP y POSTERIORES habilitadas para HTTPS. Algunos servidores Web pueden requerir la instalación de un módulo adicional. Para obtener más información, consulte la documentación de su servidor web. Los formatos de URL admitidos varían según la versión de ONTAP. Consulte la ayuda de la línea de comandos para su versión de ONTAP.</p> </div> |
| Descargue un archivo de backup de configuración de una URL remota a un nodo del clúster y, si se especifica, valide el certificado digital | <p><code>system configuration backup download</code></p> <p>Cuando utilice HTTPS en la URL remota, utilice <code>-validate-certification</code> opción para habilitar o deshabilitar la validación de certificados digitales. De forma predeterminada, la validación de certificados está deshabilitada.</p> |
| Cambie el nombre de un archivo de backup de configuración en un nodo del clúster | <code>system configuration backup rename</code> |
| Vea los archivos de backup de configuración de nodo y clúster para uno o varios nodos en el clúster | <code>system configuration backup show</code> |
| Eliminar un archivo de copia de seguridad de configuración en un nodo | <p><code>system configuration backup delete</code></p> <div>  <p>Este comando elimina el archivo de backup de configuración únicamente en el nodo especificado. Si el archivo de backup de configuración también existe en otros nodos del clúster, permanece en esos nodos.</p> </div> |

Busque un archivo de backup de configuración que se utilizará para recuperar un nodo

Para recuperar una configuración de nodo, se utiliza un archivo de backup de

configuración ubicado en una URL remota o en un nodo del clúster.

Acerca de esta tarea

Puede usar un archivo de backup de configuración de clúster o nodo para restaurar una configuración de nodos.

Paso

1. Haga que el archivo de copia de seguridad de configuración esté disponible en el nodo para el que necesita restaurar la configuración.

| Si el archivo de copia de seguridad de configuración se encuentra... | Realice lo siguiente... |
|--|--|
| En una URL remota | Utilice la <code>system configuration backup download</code> en el nivel de privilegio avanzado para descargarlo en el nodo en recuperación. |
| En un nodo del clúster | <ol style="list-style-type: none">a. Utilice la <code>system configuration backup show</code> comando en el nivel de privilegio avanzado para ver la lista de archivos de backup de configuración disponibles en el clúster que contiene la configuración del nodo recuperado.b. Si el archivo de copia de seguridad de configuración que identifica no existe en el nodo de recuperación, utilice la <code>system configuration backup copy</code> para copiarla en el nodo en recuperación. |

Si anteriormente volvió a crear el clúster, debe elegir un archivo de backup de configuración que se creó después de la recreación del clúster. Si debe utilizar un archivo de backup de configuración que se creó antes de la recreación de clúster, después de recuperar el nodo, debe volver a crear el clúster.

Restaurar la configuración de nodo mediante un archivo de backup de configuración

Se restaura la configuración del nodo con el archivo de backup de configuración que se identificó y se puso a disposición del nodo en recuperación.

Acerca de esta tarea

Solo debe realizar esta tarea para recuperar el sistema tras un desastre que provocó la pérdida de los archivos de configuración local del nodo.

Pasos

1. Cambie al nivel de privilegio avanzado:

```
set -privilege advanced
```

2. Si el estado del nodo es correcto, utilice el para el nivel de privilegio avanzado de un nodo diferente `cluster modify` con el `-node` y.. `-eligibility` parámetros para marcarlo como no apto y aislarlo del clúster.

Si el nodo no está en buen estado, debe omitir este paso.

En este ejemplo, se modifica el nodo 2 para que no sea apto para participar en el clúster para poder restaurar su configuración:

```
cluster1::*> cluster modify -node node2 -eligibility false
```

3. Utilice la `system configuration recovery node restore` comando en el nivel de privilegio avanzado para restaurar la configuración del nodo desde un archivo de backup de configuración.

Si el nodo perdió su identidad, incluido su nombre, debe usar el `-nodename-in-backup` parámetro para especificar el nombre del nodo en el archivo de copia de seguridad de configuración.

En este ejemplo se restaura la configuración del nodo mediante uno de los archivos de backup de configuración almacenados en el nodo:

```
cluster1::*> system configuration recovery node restore -backup
cluster1.8hour.2011-02-22.18_15_00.7z

Warning: This command overwrites local configuration files with
files contained in the specified backup file. Use this
command only to recover from a disaster that resulted
in the loss of the local configuration files.
The node will reboot after restoring the local configuration.
Do you want to continue? {y|n}: y
```

Se restaura la configuración y el nodo se reinicia.

4. Si marcó el nodo no apto, utilice el `system configuration recovery cluster sync` comando para marcar el nodo como elegible y sincronizarlo con el clúster.
5. Si está trabajando en un entorno SAN, utilice el `system node reboot` Para reiniciar el nodo y restablecer el quórum DE SAN.

Después de terminar

Si anteriormente volvió a crear el clúster y si va a restaurar la configuración de nodo mediante un archivo de backup de configuración que se creó antes de volver a crear el clúster, debe volver a crear el clúster.

Busque una configuración que se usará para recuperar un clúster

Utiliza la configuración desde un nodo del clúster o un archivo de backup de configuración de clústeres para recuperar un clúster.

Pasos

1. Seleccione un tipo de configuración para recuperar el clúster.
 - Un nodo en el clúster

Si el clúster consta de más de un nodo y uno de los nodos tiene una configuración de clúster desde

cuando el clúster estaba en la configuración deseada, entonces puede recuperar el clúster mediante la configuración almacenada en ese nodo.

En la mayoría de los casos, el nodo que contiene el anillo de replicación con el identificador de transacción más reciente es el mejor nodo que se puede usar para restaurar la configuración de clúster. La `cluster ring show` el comando en el nivel de privilegio avanzado le permite ver una lista de los anillos replicados disponibles en cada nodo del clúster.

- Un archivo de copia de seguridad de configuración de clúster

Si no puede identificar un nodo con la configuración de clúster correcta o si el clúster consta de un único nodo, puede utilizar un archivo de backup de configuración de clúster para recuperar el clúster.

Si va a recuperar el clúster a partir de un archivo de copia de seguridad de configuración, se perderán todos los cambios de configuración realizados desde que se realizó la copia de seguridad. Debe resolver las discrepancias entre el archivo de copia de seguridad de la configuración y la actual después de la recuperación. Consulte el artículo de Knowledge base ["Guía de resolución de backups de configuración de ONTAP"](#) para obtener orientación sobre la solución de problemas.

2. Si decide utilizar un archivo de copia de seguridad de configuración de clúster, haga que el archivo esté disponible para el nodo que planea utilizar para recuperar el clúster.

| Si el archivo de copia de seguridad de configuración se encuentra... | Realice lo siguiente... |
|--|---|
| En una URL remota | Utilice la <code>system configuration backup download</code> en el nivel de privilegio avanzado para descargarlo en el nodo en recuperación. |
| En un nodo del clúster | <ol style="list-style-type: none">a. Utilice la <code>system configuration backup show</code> comando en el nivel de privilegio avanzado para encontrar un archivo de backup de configuración de clúster que se creó cuando el clúster estaba en la configuración deseada.b. Si el archivo de backup de configuración del clúster no se encuentra en el nodo que planea utilizar para recuperar el clúster, utilice el <code>system configuration backup copy</code> para copiarla en el nodo en recuperación. |

Restaurar una configuración de clúster a partir de una configuración existente

Para restaurar una configuración de clúster a partir de una configuración existente tras el fallo de un clúster, debe volver a crear el clúster con la configuración de clúster que seleccionó y poner a disposición del nodo a recuperar y, a continuación, volver a unir cada nodo adicional al nuevo clúster.

Acerca de esta tarea

Solo debe realizar esta tarea para recuperar el sistema tras un desastre que provocó la pérdida de la configuración del clúster.

Si va a volver a crear el clúster a partir de un archivo de backup de configuración, debe ponerse en contacto con el soporte técnico para resolver las discrepancias entre el archivo de backup de configuración y la configuración presente en el clúster.



Si va a recuperar el clúster a partir de un archivo de copia de seguridad de configuración, se perderán todos los cambios de configuración realizados desde que se realizó la copia de seguridad. Debe resolver las discrepancias entre el archivo de copia de seguridad de la configuración y la actual después de la recuperación. Consulte el artículo de la base de conocimientos ["Guía de resolución de backups de configuración de ONTAP para la solución de problemas"](#).

Pasos

1. Desactive la conmutación por error del almacenamiento para cada par de alta disponibilidad:

```
storage failover modify -node node_name -enabled false
```

Solo tiene que deshabilitar la conmutación por error del almacenamiento una vez para cada par de alta disponibilidad. Cuando deshabilita la conmutación al respaldo de almacenamiento para un nodo, la conmutación al respaldo de almacenamiento también se deshabilita en el compañero de nodo.

2. Detenga cada nodo excepto el nodo en recuperación:

```
system node halt -node node_name -reason "text"
```

```
cluster1::*> system node halt -node node0 -reason "recovering cluster"
```

```
Warning: Are you sure you want to halt the node? {y|n}: y
```

3. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

4. En el nodo de recuperación, utilice **system configuration recovery cluster recreate** comando para volver a crear el clúster.

En este ejemplo se vuelve a crear el clúster con la información de configuración almacenada en el nodo a recuperar:

```
cluster1::*> configuration recovery cluster recreate -from node
```

```
Warning: This command will destroy your existing cluster. It will
        rebuild a new single-node cluster consisting of this node
        and its current configuration. This feature should only be
        used to recover from a disaster. Do not perform any other
        recovery operations while this operation is in progress.
Do you want to continue? {y|n}: y
```

Se crea un nuevo clúster en el nodo a recuperar.

5. Si va a volver a crear el clúster desde un archivo de backup de configuración, compruebe que la recuperación del clúster aún esté en curso:

system configuration recovery cluster show

No es necesario comprobar el estado de recuperación del clúster si se vuelve a crear el clúster desde un nodo en buen estado.

```
cluster1::*> system configuration recovery cluster show
Recovery Status: in-progress
Is Recovery Status Persisted: false
```

6. Arranque cada nodo que se tiene que volver a unir al clúster creado nuevamente.

Debe reiniciar los nodos de uno en uno.

7. Para cada nodo que debe unirse al clúster de nuevo creado, haga lo siguiente:

- a. A partir de un nodo en buen estado del clúster recreado, vuelva a unir el nodo de destino:

system configuration recovery cluster rejoin -node *node_name*

En este ejemplo se vuelve a unir el nodo de destino «'2'» al clúster creado de nuevo:

```
cluster1::*> system configuration recovery cluster rejoin -node node2

Warning: This command will rejoin node "node2" into the local
cluster, potentially overwriting critical cluster
configuration files. This command should only be used
to recover from a disaster. Do not perform any other
recovery operations while this operation is in progress.
This command will cause node "node2" to reboot.
Do you want to continue? {y|n}: y
```

El nodo de destino se reinicia y, a continuación, se une al clúster.

- b. Compruebe que el nodo de destino esté en buen estado y que haya formado quórum con el resto de los nodos del clúster:

cluster show -eligibility true

El nodo de destino debe volver a unirse al clúster recreado antes de poder volver a unir otro nodo.

```
cluster1::*> cluster show -eligibility true
```

| Node | Health | Eligibility | Epsilon |
|-------|--------|-------------|---------|
| node0 | true | true | false |
| node1 | true | true | false |

2 entries were displayed.

- Si vuelve a crear el clúster a partir de un archivo de backup de configuración, establezca el estado de recuperación en Complete:

```
system configuration recovery cluster modify -recovery-status complete
```

- Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

- Si el clúster solo consta de dos nodos, use el **cluster ha modify** Comando para volver a habilitar el clúster ha.
- Utilice la **storage failover modify** Comando para volver a habilitar la recuperación tras fallos del almacenamiento para cada par de alta disponibilidad.

Después de terminar

Si el clúster tiene relaciones de SnapMirror entre iguales, también debe volver a crear esas relaciones. Para obtener más información, consulte ["Protección de datos"](#).

Sincronice un nodo con el clúster

Si existe quórum para todo el clúster, pero uno o varios nodos no están sincronizados con el clúster, debe sincronizar el nodo para restaurar la base de datos replicada (RDB) del nodo y quórum.

Paso

- Desde un nodo en buen estado, utilice `system configuration recovery cluster sync` comando en el nivel de privilegio avanzado para sincronizar el nodo que está fuera de sincronización con la configuración del clúster.

En este ejemplo, se sincroniza un nodo (2) con el resto del clúster:

```
cluster1::*> system configuration recovery cluster sync -node node2
```

Warning: This command will synchronize node "node2" with the cluster configuration, potentially overwriting critical cluster configuration files on the node. This feature should only be used to recover from a disaster. Do not perform any other recovery operations while this operation is in progress. This command will cause all the cluster applications on node "node2" to restart, interrupting administrative CLI and Web interface on that node.

Do you want to continue? {y|n}: y

All cluster applications on node "node2" will be restarted. Verify that the cluster applications go online.

Resultado

El RDB se replica en el nodo y el nodo puede participar en el clúster.

Gestionar volcados de memoria (solo administradores de clúster)

Cuando un nodo produce una alarma, se produce un volcado de memoria y el sistema crea un archivo de volcado de memoria que el soporte técnico puede utilizar para solucionar el problema. Es posible configurar o mostrar atributos de volcado de memoria. También puede guardar, mostrar, segmentar, cargar o eliminar un archivo de volcado de memoria.

Puede gestionar volcados de memoria de las siguientes maneras:

- Configurar volcados de memoria y mostrar las opciones de configuración
- Mostrar información básica, el estado y los atributos de los volcados principales

Los archivos de volcado principal y los informes se almacenan en la `/mroot/etc/crash/` directorio de un nodo. Puede mostrar el contenido del directorio mediante `system node coredump` o un navegador web.



- Se guarda el contenido de volcado principal y se carga el archivo guardado en una ubicación específica o al soporte técnico

ONTAP evita que se inicie el almacenamiento de un archivo de volcado principal durante la toma de control, la reubicación de agregados o una devolución del nodo principal.

- Eliminación de archivos de volcado de memoria que ya no son necesarios

Comandos para gestionar volcados de memoria

Utilice la `system node coredump config` comandos para gestionar la configuración de volcados principales, el `system node coredump` comandos para gestionar los archivos de volcado principales y el `system node coredump reports` comandos para gestionar informes principales de aplicaciones.

| Si desea... | Se usa este comando... |
|--|---|
| Configurar volcados de memoria | <code>system node coredump config modify</code> |
| Muestra las opciones de configuración de los volcados principales | <code>system node coredump config show</code> |
| Mostrar información básica sobre volcados de memoria | <code>system node coredump show</code> |
| Active manualmente un volcado de memoria cuando reinicie un nodo | <code>system node reboot con ambos -dump y.. -skip -lif-migration-before-reboot parámetros</code> <div>  <p>El enlace: <code>skip-lif-migration-before-reboot</code> Especifica que se omitirá la migración de LIF antes de un reinicio.</p> </div> |
| Active manualmente un volcado de memoria cuando apague un nodo | <code>system node halt con ambos -dump y.. -skip -lif-migration-before-shutdown parámetros</code> <div>  <p>El enlace: <code>skip-lif-migration-before-shutdown</code> El parámetro especifica que se omitirá la migración de LIF antes de un apagado.</p> </div> |
| Guarde un volcado de memoria especificado | <code>system node coredump save</code> |
| Guarde todos los volcados de memoria no guardados que estén en un nodo especificado | <code>system node coredump save-all</code> |
| Genere y envíe un mensaje de AutoSupport con un archivo de volcado principal que especifique | <code>system node autosupport invoke-core-upload</code> <div>  <p>La <code>-uri</code> El parámetro opcional especifica un destino alternativo para el mensaje AutoSupport.</p> </div> |
| Mostrar información de estado de volcados principales | <code>system node coredump status</code> |
| Elimine un volcado de memoria especificado | <code>system node coredump delete</code> |
| Elimine todos los volcados de memoria que no haya guardado o todos los archivos principales guardados de un nodo | <code>system node coredump delete-all</code> |

| Si desea... | Se usa este comando... |
|---|--|
| Mostrar informes de volcado de memoria de aplicaciones | <code>system node coredump reports show</code> |
| Elimine un informe de volcado de memoria de la aplicación | <code>system node coredump reports delete</code> |

Información relacionada

["Comandos de ONTAP 9"](#)

Gestión de discos y niveles (agregados)

Descripción general de discos y niveles locales (agregados)

Puede gestionar el almacenamiento físico de ONTAP mediante System Manager y la CLI. Puede crear, expandir y gestionar niveles locales (agregados), trabajar con niveles locales de Flash Pool (agregados), gestionar discos y gestionar políticas de RAID.

Qué son los niveles locales (agregados)

Local Tiers (también denominado *aggregates*) son contenedores para los discos gestionados por un nodo. Puede utilizar niveles locales para aislar cargas de trabajo con diferentes demandas de rendimiento, colocar en niveles los datos con diferentes patrones de acceso o segregar los datos con fines normativos.

- En el caso de aplicaciones vitales para el negocio que necesitan la menor latencia posible y el mayor rendimiento posible, puede crear un nivel local que conste únicamente de SSD.
- Para organizar los datos en niveles con distintos patrones de acceso, puede crear un *nivel local* híbrido, poniendo en marcha flash como caché de alto rendimiento para un conjunto de datos en funcionamiento, mientras utiliza HDD de menor coste o almacenamiento de objetos para los datos a los que se accede con menor frecuencia.
 - Un *Flash Pool* está compuesto tanto por SSD como HDD.
 - Un *FabricPool* consta de un nivel local completamente SSD con un almacén de objetos asociado.
- Si necesita segregar datos archivados de datos activos para fines normativos, puede utilizar un nivel local formado por HDD de capacidad o una combinación de HDD de rendimiento y capacidad.



Datacenter



Cloud

You can use a FabricPool to tier data with different access patterns, deploying SSDs for frequently accessed “hot” data and object storage for rarely accessed “cold” data.

Trabajar con niveles locales (agregados)

Es posible realizar las siguientes tareas:

- ["Gestión de niveles locales \(agregados\)"](#)
- ["Gestionar discos"](#)
- ["Gestione las configuraciones de RAID"](#)
- ["Gestione niveles de Flash Pool"](#)

Puede realizar estas tareas si se cumplen las siguientes condiciones:

- No desea usar una herramienta de secuencias de comandos automatizadas.
- Quiere utilizar las prácticas recomendadas, no explorar todas las opciones disponibles.
- Tiene una configuración MetroCluster y sigue los procedimientos que se describen en ["MetroCluster"](#) documentación para la configuración inicial y directrices para la gestión de discos y niveles locales (agregados).

Información relacionada

- ["Gestione los niveles de cloud de FabricPool"](#)

Gestión de niveles locales (agregados)

Gestión de niveles locales (agregados)

Es posible usar System Manager o la interfaz de línea de comandos de ONTAP para añadir niveles locales (agregados), gestionar su uso y añadir capacidad (discos) a ellos.

Es posible realizar las siguientes tareas:

- ["Añadir \(crear\) un nivel local \(agregado\)"](#)

Para agregar un nivel local, debe seguir un flujo de trabajo específico. Determine el número de discos o particiones de disco que necesita para el nivel local y decida qué método utilizar para crear el nivel local. Es posible añadir niveles locales de forma automática al permitir que ONTAP asigne la configuración, o bien especificar la configuración manualmente.

- ["Gestión del uso de niveles locales \(agregados\)"](#)

Para los niveles locales existentes, puede cambiarles el nombre, configurar costos de medios o determinar la información de sus unidades y grupos RAID. Es posible modificar la configuración de RAID de un nivel local y asignar niveles locales a las máquinas virtuales de almacenamiento (SVM).

Es posible modificar la configuración de RAID de un nivel local y asignar niveles locales a las máquinas virtuales de almacenamiento (SVM). Puede determinar qué volúmenes residen en un nivel local y cuánto espacio usan en un nivel local. Puede controlar la cantidad de espacio que pueden utilizar los volúmenes. Puede reubicar la propiedad del nivel local con un par de alta disponibilidad. También puede eliminar un nivel local.

- ["Añadir capacidad \(discos\) a un nivel local \(agregado\)"](#)

Utilice diferentes métodos para seguir un flujo de trabajo específico y añadir capacidad. Es posible añadir discos a un nivel local y añadir unidades a un nodo o a una bandeja. Si es necesario, puede corregir las particiones de repuesto mal alineadas.

Añadir (crear) un nivel local (agregado)

Añadir un nivel local (crear un agregado)

Para añadir un nivel local (crear un agregado), debe seguir un flujo de trabajo específico.

Determine el número de discos o particiones de disco que necesita para el nivel local y decida qué método utilizar para crear el nivel local. Es posible añadir niveles locales de forma automática al permitir que ONTAP asigne la configuración, o bien especificar la configuración manualmente.

- ["Flujo de trabajo para añadir un nivel local \(agregado\)"](#)
- ["Determinar la cantidad de discos o particiones de disco necesarias para un nivel local \(agregado\)"](#)
- ["Decida qué método de creación de nivel local \(agregado\) utilizar "](#)
- ["Añadir niveles locales \(agregados\) automáticamente"](#)
- ["Añadir niveles locales \(agregados\) manualmente"](#)

Flujo de trabajo para añadir un nivel local (agregado)

La creación de niveles locales (agregados) proporciona almacenamiento a los volúmenes del sistema.

El flujo de trabajo para crear niveles locales (agregados) es específico de la interfaz que usa: System Manager o la CLI:

Flujo de trabajo de System Manager

Utilice System Manager para agregar (crear) un nivel local

System Manager crea niveles locales basados en prácticas recomendadas para la configuración de niveles locales.

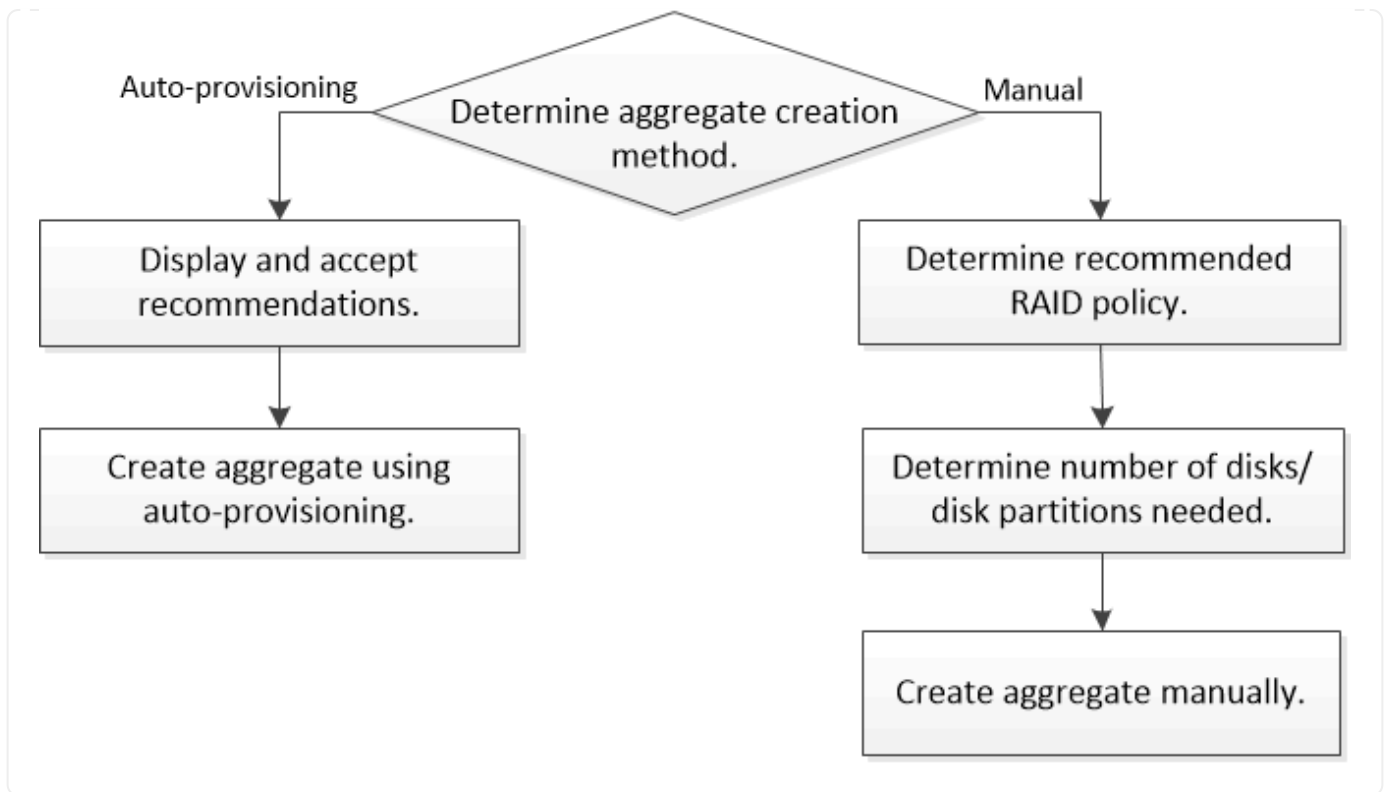
A partir de ONTAP 9.11.1, puede decidir configurar niveles locales manualmente si desea una configuración diferente de la recomendada durante el proceso automático para añadir un nivel local.



Flujo de trabajo de la CLI

Utilice la CLI para agregar (crear) un agregado

A partir de ONTAP 9.2, ONTAP puede proporcionar configuraciones recomendadas al crear agregados (aprovisionamiento automático). Si las configuraciones recomendadas, basadas en las prácticas recomendadas, son adecuadas en su entorno, puede aceptarlas para crear los agregados. De lo contrario, puede crear agregados manualmente.



Determinar la cantidad de discos o particiones de disco necesarias para un nivel local (agregado)

Debe tener suficientes discos o particiones de disco en su nivel local (agregado) para cumplir con los requisitos del sistema y del negocio. También debe tener la cantidad recomendada de discos de repuesto activo o particiones de discos de repuesto activo para minimizar el potencial de pérdida de datos.

La partición de datos raíz está habilitada de forma predeterminada en determinadas configuraciones. Los sistemas con particiones de datos raíz habilitadas utilizan particiones de disco para crear niveles locales. Los sistemas que no tienen habilitada la partición de datos raíz utilizan discos sin particiones.

Debe tener suficientes discos o particiones de disco para cumplir con el número mínimo necesario para su política de RAID y lo suficiente como para satisfacer sus requisitos de capacidad mínima.



En ONTAP, el espacio utilizable de la unidad es menor que la capacidad física de la unidad. Puede encontrar el espacio utilizable de una unidad específica y el número mínimo de discos o particiones de disco necesarios para cada política de RAID en el ["Hardware Universe"](#).

Determinar el espacio utilizable de un disco específico


El procedimiento que siga depende de la interfaz que utilice: System Manager o CLI:

System Manager

Use System Manager para determinar el espacio utilizable de los discos

Realice los pasos siguientes para ver el tamaño utilizable de un disco:

Pasos

1. Vaya a **almacenamiento > niveles**
2. Haga clic en  junto al nombre del nivel local.
3. Seleccione la ficha **Información de disco**.

CLI

Utilice la CLI para determinar el espacio útil de los discos

Realice el paso siguiente para ver el tamaño utilizable de un disco:

Paso

1. Mostrar información del disco de repuesto:

```
storage aggregate show-spare-disks
```

Además del número de discos o particiones de disco necesarios para crear el grupo RAID y satisfacer sus requisitos de capacidad, debe tener también la cantidad mínima de discos de repuesto activos o particiones de disco de repuesto en caliente recomendadas para su agregado:

- Para todos los agregados flash, debe tener como mínimo un disco de repuesto o partición de disco.



AFF C190 no tiene como valor predeterminado ninguna unidad de repuesto. Esta excepción es totalmente compatible.

- Para agregados homogéneos que no sean flash, debe tener un mínimo de dos discos de repuesto en caliente o particiones de disco.
- Para los pools de almacenamiento SSD, debe tener como mínimo un disco de repuesto en cada pareja de alta disponibilidad.
- Para los agregados de Flash Pool, debe tener un mínimo de dos discos de repuesto en cada pareja de alta disponibilidad. Puede encontrar más información sobre las políticas de RAID compatibles con los agregados de Flash Pool en la ["Hardware Universe"](#).
- Para admitir el uso del centro de mantenimiento y evitar problemas causados por varios fallos simultáneos de discos, debe contar con un mínimo de cuatro piezas de repuesto en portadores de varios discos.

Información relacionada

["Hardware Universe de NetApp"](#)

["Informe técnico de NetApp 3838: Guía de configuración del subsistema de almacenamiento"](#)

Decidir qué método se utilizará para crear niveles locales (agregados)

Aunque ONTAP ofrece recomendaciones de prácticas recomendadas para agregar automáticamente los niveles locales (crear agregados con aprovisionamiento

automático), debe determinar si las configuraciones recomendadas son compatibles con su entorno. Si no lo son, debe tomar decisiones acerca de la política de RAID y la configuración de discos y, a continuación, crear los niveles locales manualmente.

Cuando se crea automáticamente un nivel local, ONTAP analiza los discos de reserva disponibles en el clúster y genera una recomendación acerca de cómo se deben utilizar los discos de reserva para añadir niveles locales de acuerdo con las prácticas recomendadas. ONTAP muestra las configuraciones recomendadas. Puede aceptar las recomendaciones o agregar manualmente los niveles locales.

Antes de poder aceptar las recomendaciones de ONTAP

Si se produce alguna de las siguientes condiciones de disco, deben solucionarse antes de aceptar las recomendaciones del ONTAP:

- Faltan discos
- Fluctuación en los números de disco de repuesto
- Discos sin asignar
- Repuestos no puestos a cero
- Discos sometidos a pruebas de mantenimiento

La `storage aggregate auto-provision` la página de manual contiene más información sobre estos requisitos.

Cuando debe utilizar el método manual

En muchos casos, la distribución recomendada del nivel local será óptima para su entorno. Sin embargo, si el clúster ejecuta ONTAP 9.1 o una versión anterior, o bien el entorno incluye las siguientes configuraciones, debe crear el nivel local mediante el método manual.



A partir de ONTAP 9.11.1, es posible añadir manualmente niveles locales con System Manager.

- Agregados que utilizan LUN de cabina de terceros
- Discos virtuales con Cloud Volumes ONTAP o ONTAP Select
- Sistema MetroCluster
- SyncMirror
- Discos MSATA
- Niveles Flash Pool (agregados)
- Los diferentes tipos o tamaños de disco están conectados al nodo

Seleccione el método para crear niveles locales (agregados).

Elija el método que desea utilizar:

- ["Añada \(cree\) niveles locales \(agregados\) automáticamente"](#)
- ["Añada \(cree\) niveles locales \(agregados\) manualmente"](#)

Información relacionada

["Comandos de ONTAP 9"](#)

Añada niveles locales automáticamente (cree agregados con aprovisionamiento automático).

Si la práctica recomendada que proporciona ONTAP para agregar automáticamente un nivel local (creación de un agregado con aprovisionamiento automático)

Es adecuado para su entorno, puede aceptar la recomendación y dejar que ONTAP agregue el nivel local.

Antes de empezar

Un nodo debe pertenecer a los discos para poder utilizarlos en un nivel local (agregado). Si el clúster no está configurado para utilizar la asignación automática de propiedad de disco, debe ["asignar propiedad manualmente"](#).

System Manager

Pasos

1. En System Manager, haga clic en **almacenamiento > niveles**.
2. En la página **Tiers**, haga clic en [+ Add Local Tier](#) para crear un nuevo nivel local:

La página **Agregar nivel local** muestra el número recomendado de niveles locales que se pueden crear en los nodos y el almacenamiento utilizable disponible.

3. Haga clic en **Detalles recomendados** para ver la configuración recomendada por System Manager.

System Manager muestra la siguiente información a partir de ONTAP 9.8:

- **Nombre de nivel local** (puede editar el nombre de nivel local comenzando por ONTAP 9.10.1)
- **Nombre de nodo**
- **Tamaño útil**
- **Tipo de almacenamiento**

A partir de ONTAP 9.10.1, se muestra información adicional:

- **Discos:** Muestra el número, tamaño y tipo de los discos
- **Diseño:** Muestra la disposición del grupo RAID, incluyendo qué discos son de paridad o datos y qué ranuras no se utilizan.
- **Discos de repuesto:** Mostrando el nombre del nodo, el número y el tamaño de los discos de repuesto, y el tipo de almacenamiento.

4. Realice uno de los siguientes pasos:

| Si desea... | Haga esto... |
|---|---|
| Acepte las recomendaciones de System Manager. | Vaya a. El paso para configurar el gestor de claves incorporado para el cifrado . |
| Configurar manualmente los niveles locales y not utilizar las recomendaciones de System Manager. | <div>Vaya a. "Añada un nivel local (crear agregado) manualmente":</div> <ul style="list-style-type: none">• Para ONTAP 9.10.1 y versiones anteriores, siga los pasos para usar la CLI.• A partir de ONTAP 9.11.1, siga los pasos para usar System Manager. |

5. (Opcional): Si se ha instalado Onboard Key Manager, puede configurarlo para el cifrado. Active la casilla de verificación **Configurar el Administrador de claves incorporado para cifrado**.
 - a. Introduzca una frase de contraseña.
 - b. Introduzca una vez más la contraseña para confirmarla.
 - c. Guarde la frase de acceso para su uso futuro en caso de que el sistema necesite recuperarse.
 - d. Realice un backup de la base de datos clave para usarlo en el futuro.
6. Haga clic en **Guardar** para crear el nivel local y añadirlo a su solución de almacenamiento.

CLI

Usted ejecuta el `storage aggregate auto-provision` comando para generar recomendaciones de distribución de agregados. A continuación, se pueden crear agregados después de revisar y aprobar las recomendaciones de ONTAP.

Lo que necesitará

ONTAP 9.2 o una versión posterior debe estar en ejecución en el clúster.

Acerca de esta tarea

El resumen predeterminado generado con `storage aggregate auto-provision` comando enumera los agregados recomendados que se van a crear, incluidos los nombres y el tamaño útil. Puede ver la lista y determinar si desea crear los agregados recomendados cuando se le solicite.

También puede mostrar un resumen detallado utilizando la `-verbose` opción, que muestra los siguientes informes:

- Por nodo, un resumen de los nuevos agregados que se van a crear, se han detectado repuestos y demás discos y particiones de repuesto tras la creación del agregado
- Nuevos agregados de datos que se crearán con un número total de discos y particiones que se utilizarán
- Distribución de grupos RAID que muestra cómo se usarán los discos y las particiones de reserva en los nuevos agregados de datos para crear
- Detalles sobre los discos de repuesto y las particiones restantes tras la creación del agregado

Si está familiarizado con el método de aprovisionamiento automático y su entorno esté preparado correctamente, puede utilizar el `-skip-confirmation` opción para crear el agregado recomendado sin mostrar ni confirmar. La `storage aggregate auto-provision` El comando no se ve afectado por la sesión CLI `-confirmations` ajuste.

La[`storage aggregate auto-provision manual page`] contiene más información acerca de las recomendaciones de diseño de agregado.

Pasos

1. Ejecute el `storage aggregate auto-provision` comando con las opciones de visualización deseadas.
 - Sin opciones: Mostrar resumen estándar
 - `-verbose` Opción: Mostrar resumen detallado
 - `-skip-confirmation` Opción: Cree agregados recomendados sin mostrar ni confirmar
2. Realice uno de los siguientes pasos:

| | |
|-------------|--------------|
| Si desea... | Haga esto... |
|-------------|--------------|

Acepte las recomendaciones de ONTAP.

Revise la visualización de agregados recomendados y responda al símbolo del sistema para crear los agregados recomendados.

```
myA400-44556677::> storage aggregate auto-
provision
Node                               New Data Aggregate
Usable Size
-----
-----
myA400-364                         myA400_364_SSD_1
3.29TB
myA400-363                         myA400_363_SSD_1
1.46TB
-----
-----
Total:                             2      new data aggregates
4.75TB

Do you want to create recommended
aggregates? {y
```

n}): y

Info: Aggregate auto provision has started. Use the "storage aggregate show-auto-provision-progress" command to track the progress.

myA400-44556677::>

Configure manualmente los niveles locales y **not** use las recomendaciones de ONTAP.

Información relacionada

["Comandos de ONTAP 9"](#)

Añada niveles locales (cree agregados) manualmente

Si no desea añadir un nivel local (crear un agregado) con las recomendaciones de prácticas recomendadas de ONTAP, puede llevar a cabo el proceso de forma manual.

Antes de empezar

Un nodo debe pertenecer a los discos para poder utilizarlos en un nivel local (agregado). Si el clúster no está configurado para utilizar la asignación automática de propiedad de disco, debe ["asignar propiedad manualmente"](#).

System Manager

A partir de ONTAP 9.11.1, si no desea usar la configuración recomendada por System Manager para crear un nivel local, puede especificar la configuración que desea.

Pasos

1. En System Manager, haga clic en **almacenamiento > niveles**.
2. En la página **Tiers**, haga clic en **+ Add Local Tier** para crear un nuevo nivel local:

La página **Agregar nivel local** muestra el número recomendado de niveles locales que se pueden crear en los nodos y el almacenamiento utilizable disponible.

3. Cuando System Manager muestre la recomendación de almacenamiento para el nivel local, haga clic en **Cambiar a creación manual de nivel local** en la sección **discos de repuesto**.

La página **Agregar nivel local** muestra los campos que utiliza para configurar el nivel local.

4. En la primera sección de la página **Agregar nivel local**, complete lo siguiente:
 - a. Introduzca el nombre del nivel local.
 - b. (Opcional): Marque la casilla de verificación **reflejar este nivel local** si desea duplicar el nivel local.
 - c. Seleccione un tipo de disco.
 - d. Seleccione la cantidad de discos.
5. En la sección **Configuración RAID**, lleve a cabo lo siguiente:
 - a. Seleccione el tipo de RAID.
 - b. Seleccione el tamaño del grupo RAID.
 - c. Haga clic en asignación de RAID para ver cómo se asignan los discos en el grupo.
6. (Opcional): Si se ha instalado Onboard Key Manager, puede configurarlo para cifrado en la sección **Cifrado** de la página. Active la casilla de verificación **Configurar el Administrador de claves incorporado para cifrado**.
 - a. Introduzca una frase de contraseña.
 - b. Introduzca una vez más la contraseña para confirmarla.
 - c. Guarde la frase de acceso para su uso futuro en caso de que el sistema necesite recuperarse.
 - d. Realice un backup de la base de datos clave para usarlo en el futuro.
7. Haga clic en **Guardar** para crear el nivel local y añadirlo a su solución de almacenamiento.

CLI

Antes de crear agregados manualmente, debe revisar las opciones de configuración de discos y simular la creación.

Entonces puede emitir el `storage aggregate create` command y verifique los resultados.

Lo que necesitará

Debe haber determinado la cantidad de discos y la cantidad de discos de repuesto que necesita en el agregado.

Acerca de esta tarea

Si se habilita la partición de datos raíz y tiene 24 unidades de estado sólido (SSD) o menos en la configuración, se recomienda asignar sus particiones de datos a diferentes nodos.

El procedimiento para crear agregados en sistemas con partición de datos raíz y partición de datos raíz activada es el mismo que el procedimiento para crear agregados en sistemas que utilizan discos sin particiones. Si la partición de datos raíz está activada en el sistema, debe usar el número de particiones de disco para `-diskcount` opción. Para la partición de datos raíz, la `-diskcount` la opción especifica el número de discos que se van a utilizar.



Cuando se crean múltiples agregados para su uso con FlexGroups, los agregados deben tener el mayor tamaño posible.

La `storage aggregate create` la página de manual contiene más información sobre las opciones y requisitos de creación de agregados.

Pasos

1. Vea la lista de particiones de disco de repuesto para verificar que tiene suficiente para crear su agregado:

```
storage aggregate show-spare-disks -original-owner node_name
```

Las particiones de datos se muestran en `Local Data Usable`. No se puede utilizar una partición raíz como reserva.

2. Simule la creación del agregado:

```
storage aggregate create -aggregate aggregate_name -node node_name  
-raidtype raid_dp -diskcount number_of_disks_or_partitions -simulate true
```

3. Si se muestra alguna advertencia desde el comando simulado, ajuste el comando y repita la simulación.

4. Cree el agregado:

```
storage aggregate create -aggregate aggr_name -node node_name -raidtype  
raid_dp -diskcount number_of_disks_or_partitions
```

5. Mostrar el agregado para verificar que se ha creado:

```
storage aggregate show-status aggregate_name
```

Información relacionada

["Comandos de ONTAP 9"](#)

Gestión del uso de niveles locales (agregados)

Gestión del uso de niveles locales (agregados)

Una vez creados los niveles locales (agregados), puede gestionar cómo se usan.

Es posible realizar las siguientes tareas:

- "Cambiar el nombre de un nivel local (agregado)"
- "Establecer el coste de medios de un nivel local (agregado)"
- "Determinar la información de las unidades y los grupos RAID para un nivel local (agregado)"
- "Asignar niveles locales (agregados) a máquinas virtuales de almacenamiento (SVM)"
- "Determinar qué volúmenes residen en un nivel local (agregado)"
- "Determinar y controlar el uso de espacio de un volumen en un nivel local (agregado)"
- "Determinar el uso de espacio en un nivel local (agregado)"
- "Reubique la propiedad de nivel local (agregado) dentro de un par de alta disponibilidad"
- "Eliminar un nivel local (agregado)"

Cambiar el nombre de un nivel local (agregado)


Puede cambiar el nombre de un nivel local (agregado). El método siguiente depende de la interfaz que utilice: System Manager o CLI:

System Manager

Utilice System Manager para cambiar el nombre de un nivel local (agregado)

A partir de ONTAP 9.10.1, se puede modificar el nombre de un nivel local (agregado).

Pasos

1. En System Manager, haga clic en **almacenamiento > niveles**.
2. Haga clic en  junto al nombre del nivel local.
3. Seleccione **Cambiar nombre**.
4. Especifique un nuevo nombre para el nivel local.

CLI

Utilice la CLI para cambiar el nombre de un nivel local (agregado)

Paso

1. Con la CLI, cambie el nombre del nivel local (agregado):

```
storage aggregate rename -aggregate aggr-name -newname aggr-new-name
```

En el ejemplo siguiente se cambia el nombre de un agregado denominado «'aggr5'» por «sales-aggr»:

```
> storage aggregate rename -aggregate aggr5 -newname sales-aggr
```

Establecer coste de medios de un nivel local (agregado)

A partir de ONTAP 9.11.1, puede usar System Manager para configurar el coste de medios de un nivel local (agregado).

Pasos

1. En System Manager, haga clic en **almacenamiento > niveles** y, a continuación, haga clic en **establecer coste de medios** en los cuadros de nivel local (agregado) que desee.
2. Seleccione **niveles activos e inactivos** para activar la comparación.
3. Introduzca un tipo de moneda y un importe.

Al introducir o cambiar el coste del material, el cambio se realiza en todos los tipos de material.

Unidades de cero rápido manualmente

En los sistemas recién instalados con ONTAP 9.4 o posterior y los sistemas reinicializados con ONTAP 9.4 o posterior, se utiliza *fast Zero* para poner a cero unidades.

Con *FAST puesta a cero*, las unidades se ponen a cero en segundos. Esta acción se realiza automáticamente antes del aprovisionamiento y reduce en gran medida el tiempo necesario para inicializar el sistema, crear agregados o expandir los agregados cuando se añaden unidades de repuesto.

Fast puesta a cero es compatible tanto con SSD como con HDD.



La puesta a cero rápida no es compatible con los sistemas actualizados desde ONTAP 9.3 o versiones anteriores. ONTAP 9.4 o posterior debe estar recién instalado o el sistema debe ser reinicializado. En ONTAP 9.3 y versiones anteriores, ONTAP también pone a cero automáticamente las unidades, pero el proceso tarda más tiempo.

Si necesita poner a cero una unidad manualmente, puede usar uno de los siguientes métodos. En ONTAP 9.4 y versiones posteriores, la puesta a cero manual de una unidad también tarda solo segundos.

Comando CLI

Utilice un comando CLI para unidades FAST-Zero

Acerca de esta tarea

Se requieren privilegios de administrador para usar este comando.

Pasos

1. Introduzca el comando CLI:

```
storage disk zerospares
```

Opciones del menú de inicio

Seleccione las opciones del menú de inicio a unidades FAST-Zero

Acerca de esta tarea

- La mejora de puesta a cero rápida no admite sistemas actualizados desde una versión anterior a ONTAP 9.4.
- Si algún nodo del clúster contiene un nivel local (agregado) con unidades a cero rápido, no puede revertir el clúster a ONTAP 9.2 o una versión anterior.

Pasos

1. En el menú de inicio, seleccione una de las siguientes opciones:
 - (4) limpiar la configuración e inicializar todos los discos
 - (9a) desparticionar todos los discos y eliminar su información de propiedad
 - (9b) limpiar la configuración e inicializar el nodo con discos completos

Asignar manualmente la propiedad de disco

Un nodo debe pertenecer a los discos para poder utilizarlos en un nivel local (agregado).

Acerca de esta tarea

- Si va a asignar la propiedad manualmente a un par de alta disponibilidad que no se está inicializando y no tiene solo bandejas DS460C, use la opción 1.
- Si va a inicializar una pareja de HA que solo contiene DS460C bandejas, use la opción 2 para asignar manualmente la propiedad a las unidades raíz.

Opción 1: La mayoría de los pares de alta disponibilidad

Para un par de alta disponibilidad que no se está inicializando y no tiene solo DS460C bandejas, use este procedimiento para asignar la propiedad manualmente.

Acerca de esta tarea

- Los discos a los que asigna la propiedad deben estar en una bandeja que se conecte físicamente al nodo al que asigna la propiedad.
- Si va a utilizar discos en un nivel local (agregado):
 - Un nodo debe pertenecer a los discos para poder utilizarlos en un nivel local (agregado).
 - No es posible reasignar la propiedad de un disco que se está utilizando en un nivel local (agregado).

Pasos

1. Utilice la CLI para mostrar todos los discos sin propietario:

```
storage disk show -container-type unassigned
```

2. Asigne cada disco:

```
storage disk assign -disk disk_name -owner owner_name
```

Puede utilizar el carácter comodín para asignar más de un disco a la vez. Si va a reasignar un disco de repuesto que ya sea propiedad de un nodo diferente, deberá utilizar la opción « »-force».

Opción 2: Una pareja de alta disponibilidad con solo DS460C bandejas

Para una pareja de alta disponibilidad que va a inicializar y que solo tiene DS460C bandejas, utilice este procedimiento para asignar manualmente la propiedad a las unidades raíz.

Acerca de esta tarea

- Cuando se inicializa una pareja de alta disponibilidad que solo contiene DS460C bandejas, debe asignar manualmente las unidades raíz para cumplir con la política de medio cajón.

Después de la inicialización del par de alta disponibilidad (arranque), la asignación automática de propiedad de discos se habilita automáticamente y utiliza la política de medio cajón para asignar la propiedad a las unidades restantes (aparte de las unidades raíz) y a cualquier unidad añadida en el futuro, como reemplazar discos con fallos, responder a un mensaje de «repuestos bajos», o añadir capacidad.

Más información sobre la política de medio cajón en el tema ["Acerca de la asignación automática de propiedad de disco"](#).

- RAID necesita un mínimo de 10 unidades para cada par de alta disponibilidad (5 por cada nodo) para cualquiera de las 8TB unidades NL-SAS de una bandeja DS460C.

Pasos

1. Si las bandejas DS460C no están completamente llenas, complete los siguientes subpasos; de lo contrario, vaya al siguiente paso.

- a. En primer lugar, instale las unidades en la fila frontal (bahías de unidades 0, 3, 6 y 9) de cada cajón.

La instalación de unidades en la fila delantera de cada cajón permite un flujo de aire adecuado y evita el sobrecalentamiento.

- b. Para las unidades restantes, distribuir las de manera uniforme en cada cajón.

Llene las filas del cajón de adelante hacia atrás. Si no tiene suficientes unidades para llenar filas, instálelas en parejas para que las unidades ocupen el lado izquierdo y derecho de un cajón de manera uniforme.

En la siguiente ilustración, se muestra la numeración de las bahías de unidades y las ubicaciones de un cajón de DS460C.



2. Inicie sesión en el clustershell usando el LIF de gestión de nodos o la LIF de gestión de clústeres.
3. Asigne manualmente las unidades raíz en cada cajón para satisfacer la política de medio cajón mediante los siguientes subpasos:

La política de medio cajón hace que se asigne la mitad izquierda de las unidades de un cajón (bahías de 0 a 5) al nodo A y la mitad derecha de las unidades de un cajón (bahías de 6 a 11) al nodo B.

- a. Muestre todos los discos sin propietario:

```
storage disk show -container-type unassigned`
```

- b. Asigne los discos raíz:

```
storage disk assign -disk disk_name -owner owner_name
```

Puede utilizar el carácter comodín para asignar más de un disco a la vez.

Determinar la información de las unidades y los grupos RAID para un nivel local (agregado)

Algunas tareas de administración de nivel local (agregado) requieren conocer qué tipos de unidades componen el nivel local, su tamaño, suma de comprobación y estado, si se comparten con otros niveles locales, y el tamaño y la composición de los grupos RAID.

Paso

1. Muestre las unidades del agregado, por grupo RAID:

```
storage aggregate show-status aggr_name
```

Las unidades se muestran para cada grupo RAID en el agregado.

Puede ver el tipo de RAID de la unidad (datos, paridad, dparidad) en el `Position` columna. Si la `Position` la columna muestra `shared`, Entonces la unidad es compartida: Si es una unidad de disco duro, es un disco particionado; si es una unidad SSD, forma parte de un pool de almacenamiento.

```
cluster1::> storage aggregate show-status nodeA_fp_1
```

Owner Node: cluster1-a

Aggregate: nodeA_fp_1 (online, mixed_raid_type, hybrid) (block checksums)

Plex: /nodeA_fp_1/plex0 (online, normal, active, pool0)

RAID Group /nodeA_fp_1/plex0/rg0 (normal, block checksums, raid_dp)

| Position | Disk | Pool | Type | RPM | Usable Size | Physical Size | Status |
|----------|--------|------|------|-------|-------------|---------------|----------|
| shared | 2.0.1 | 0 | SAS | 10000 | 472.9GB | 547.1GB | (normal) |
| shared | 2.0.3 | 0 | SAS | 10000 | 472.9GB | 547.1GB | (normal) |
| shared | 2.0.5 | 0 | SAS | 10000 | 472.9GB | 547.1GB | (normal) |
| shared | 2.0.7 | 0 | SAS | 10000 | 472.9GB | 547.1GB | (normal) |
| shared | 2.0.9 | 0 | SAS | 10000 | 472.9GB | 547.1GB | (normal) |
| shared | 2.0.11 | 0 | SAS | 10000 | 472.9GB | 547.1GB | (normal) |

RAID Group /nodeA_flashpool_1/plex0/rg1

(normal, block checksums, raid4) (Storage Pool: SmallSP)

| Position | Disk | Pool | Type | RPM | Usable Size | Physical Size | Status |
|----------|--------|------|------|-----|-------------|---------------|----------|
| shared | 2.0.13 | 0 | SSD | - | 186.2GB | 745.2GB | (normal) |
| shared | 2.0.12 | 0 | SSD | - | 186.2GB | 745.2GB | (normal) |

8 entries were displayed.

Asignar niveles locales (agregados) a máquinas virtuales de almacenamiento (SVM)

Si asigna uno o más niveles locales (agregados) a una máquina virtual de almacenamiento (máquina virtual de almacenamiento o SVM, antes conocida como Vserver), entonces solo podrá utilizar esos niveles locales para contener volúmenes para esa máquina virtual de almacenamiento (SVM).

Lo que necesitará

La máquina virtual de almacenamiento y los niveles locales que desea asignar a esa máquina virtual de almacenamiento ya deben existir.

Acerca de esta tarea

La asignación de niveles locales a sus máquinas virtuales de almacenamiento le ayuda a mantener sus máquinas virtuales de almacenamiento aisladas entre sí; esto es especialmente importante en un entorno multi-tenancy.

Pasos

1. Compruebe la lista de niveles locales (agregados) que ya están asignados a la SVM:

```
vserver show -fields aggr-list
```

Se muestran los agregados actualmente asignados a la SVM. Si no hay agregados asignados, se mostrará «»-».

2. Añada o elimine agregados asignados, en función de sus requisitos:

| Si desea... | Se usa este comando... |
|--------------------------------|--|
| Asigne agregados adicionales | <code>vserver add-aggregates</code> |
| Anular asignación de agregados | <code>vserver remove-aggregates</code> |

Los agregados enumerados se asignan o se quitan de la SVM. Si la SVM ya tiene volúmenes que utilizan un agregado que no está asignado a la SVM, se muestra un mensaje de advertencia pero el comando se ha completado correctamente. Todos los agregados que ya se asignaron a la SVM y que no se nombraron en el comando no se ven afectados.

Ejemplo

En el ejemplo siguiente, los agregados `aggr1` y `aggr2` se asignan a SVM `svm1`:

```
vserver add-aggregates -vserver svm1 -aggregates aggr1,aggr2
```

Determinar qué volúmenes residen en un nivel local (agregado)

Es posible que deba determinar qué volúmenes residen en un nivel local (agregado) antes de realizar operaciones en el nivel local, como reubicarlos o desconectarlos.

Pasos

1. Para mostrar los volúmenes que residen en un agregado, introduzca

```
volume show -aggregate aggregate_name
```

Se muestran todos los volúmenes que residen en el agregado especificado.

Determinar y controlar el uso de espacio de un volumen en un nivel local (agregado)

Puede determinar qué volúmenes de FlexVol utilizan más espacio en un nivel local (agregado) y específicamente qué funciones dentro del volumen.

La `volume show-footprint` el comando proporciona información sobre el espacio físico de un volumen o el uso que ocupa el espacio dentro del agregado que lo contiene.

La `volume show-footprint` el comando muestra detalles sobre el uso de espacio de cada volumen en un agregado, incluidos los volúmenes sin conexión. Este comando suple la separación entre la salida del `volume show-space` y `aggregate show-space` comandos. Todos los porcentajes se calculan como un porcentaje del tamaño del agregado.

En el siguiente ejemplo se muestra el `volume show-footprint` resultado de comando para un volumen denominado `testvol`:

```
cluster1::> volume show-footprint testvol
```

```
Vserver : thevs
Volume  : testvol
```

| Feature | Used | Used% |
|--------------------------|---------|-------|
| ----- | ----- | ----- |
| Volume Data Footprint | 120.6MB | 4% |
| Volume Guarantee | 1.88GB | 71% |
| Flexible Volume Metadata | 11.38MB | 0% |
| Delayed Frees | 1.36MB | 0% |
| Total Footprint | 2.01GB | 76% |

En la siguiente tabla se explican algunas de las filas clave de la salida del `volume show-footprint` comando y lo que puede hacer para intentar reducir el uso de espacio con esa función:

| Nombre de fila/operación | Descripción/contenido de la fila | Algunas maneras de disminuir |
|--------------------------|---|--|
| Volume Data Footprint | Cantidad total de espacio usado en el agregado contenedor por los datos de un volumen en el sistema de archivos activo y el espacio usado por las copias de Snapshot del volumen. Esta fila no incluye espacio reservado. | <ul style="list-style-type: none"> • Eliminación de datos del volumen. • Eliminar copias Snapshot del volumen. |
| Volume Guarantee | La cantidad de espacio reservado por el volumen en el agregado para futuras escrituras. La cantidad de espacio reservado depende del tipo de garantía del volumen. | Cambie el tipo de garantía para el volumen a. none. |
| Flexible Volume Metadata | La cantidad total de espacio usado en el agregado por los archivos de metadatos del volumen. | No hay un método directo para controlar. |
| Delayed Frees | Los bloques que ONTAP utilizó para el rendimiento y no se pueden liberar inmediatamente. Para destinos de SnapMirror, esta fila tiene el valor de 0 y no se muestra. | No hay un método directo para controlar. |
| File Operation Metadata | La cantidad total de espacio reservado para los metadatos de las operaciones de archivos. | No hay un método directo para controlar. |

| | | |
|-----------------|--|--|
| Total Footprint | La cantidad total de espacio que el volumen utiliza en el agregado. Es la suma de todas las filas. | Cualquiera de los métodos utilizados para reducir el espacio utilizado por un volumen. |
|-----------------|--|--|

Información relacionada

["Informe técnico de NetApp 3483: Thin Provisioning en un entorno empresarial SAN o SAN IP DE NetApp"](#)

Determinar el uso de espacio en un nivel local (agregado)

Puede ver la cantidad de espacio que utilizan todos los volúmenes en uno o más niveles locales (agregados) para poder realizar acciones para liberar más espacio.

WAFL reserva el 10% del espacio total en disco para el rendimiento y los metadatos a nivel de agregado. El espacio utilizado para mantener los volúmenes del agregado sale de la reserva de WAFL y no se puede cambiar.



A partir de la versión 9.12.1 de ONTAP, la reserva de WAFL para agregados superiores a 30TB TB se ha reducido del 10 % al 5 % para las plataformas AFF y para las plataformas FAS500f. A partir de ONTAP 9.14.1, esta misma reducción se aplica a los agregados en todas las plataformas de FAS, lo que da como resultado un 5 % más de espacio utilizable en los agregados.

Puede ver el uso de espacio por parte de todos los volúmenes de uno o varios agregados con el `aggregate show-space` comando. De este modo, puede ver qué volúmenes consumen más espacio en los agregados que los contienen, de modo que puede llevar a cabo acciones para liberar más espacio.

El espacio utilizado de un agregado se ve directamente afectado por el espacio utilizado en los volúmenes de FlexVol que contiene. Las medidas que se toman para aumentar el espacio de un volumen también afectan al espacio del agregado.

Las siguientes filas se incluyen en la `aggregate show-space` resultado del comando:

- **Calzado por volumen**

El total de espacios de volumen dentro del agregado. Incluye todo el espacio que usa o se reserva para todos los datos y metadatos de todos los volúmenes del agregado que contiene.

- **Metadatos agregados**

Los metadatos del sistema de archivos totales necesarios para el agregado, como los mapas de bits de asignación y los archivos de nodos de información.

- **Reserva Snapshot**

La cantidad de espacio reservado para las copias de Snapshot del agregado, en función del tamaño del volumen. Se considera espacio usado y no está disponible para los datos o metadatos de volúmenes o agregados.

- **Reserva instantánea no utilizable**

La cantidad de espacio asignado originalmente para la reserva de Snapshot agregado que no está disponible para las copias Snapshot del agregado, ya que está siendo utilizada por los volúmenes

asociados con el agregado. Solo se puede producir para agregados con una reserva de Snapshot sin agregados.

- **Total usado**

La suma de todo el espacio usado o reservado en el agregado por volúmenes, metadatos o copias de Snapshot.

- **Total físico utilizado**

La cantidad de espacio que se utiliza para los datos ahora (en lugar de reservarse para uso futuro). Incluye el espacio utilizado por las copias de Snapshot agregadas.

En el siguiente ejemplo se muestra el `aggregate show-space` Resultado del comando para un agregado cuya reserva Snapshot es del 5%. Si la reserva de instantánea era 0, no se mostraría la fila.

```
cluster1::> storage aggregate show-space
```

Aggregate : wqa_gx106_aggr1

| Feature | Used | Used% |
|---------------------|------------|--------|
| ----- | ----- | ----- |
| Volume Footprints | 101.0MB | 0% |
| Aggregate Metadata | 300KB | 0% |
| Snapshot Reserve | 5.98GB | 5% |
| Total Used | 6.07GB | 5% |
| Total Physical Used | 34.82KB | 0% |

Información relacionada

- ["Artículo de la base de conocimientos: Uso del espacio"](#)
- ["Libere hasta un 5 % de su capacidad de almacenamiento actualizando a ONTAP 9.12.1"](#)

La propiedad de reubicación de un nivel local (agregado) dentro de un par de alta disponibilidad

Puede cambiar la propiedad de los niveles locales (agregados) entre los nodos de un par de alta disponibilidad sin interrumpir el servicio desde los niveles locales.

Ambos nodos de una pareja de alta disponibilidad están conectados físicamente entre sí a los discos o LUN de cabina. Cada LUN de disco o cabina es propiedad de uno de los nodos.

La propiedad de todos los discos o LUN de cabina dentro de un nivel local (agregado) cambia temporalmente de un nodo a otro cuando se produce una toma de control. Sin embargo, las operaciones de reubicación de niveles locales también pueden cambiar permanentemente la propiedad (por ejemplo, si se realiza para el equilibrio de carga). La propiedad cambia sin ningún proceso de copia de datos ni movimiento físico de los discos o los LUN de cabina.

Acerca de esta tarea

- Dado que los límites de recuento de volúmenes se validan mediante programación durante las operaciones de reubicación de nivel local, no es necesario comprobar este valor manualmente.

Si el número de volúmenes supera el límite admitido, la operación de reubicación de nivel local produce un error indicando un mensaje de error relevante.

- No se debe iniciar la reubicación de nivel local cuando existen operaciones a nivel del sistema en curso en el nodo de origen o en el de destino; del mismo modo, no se deben iniciar estas operaciones durante la reubicación de nivel local.

Estas operaciones pueden incluir las siguientes:

- Respaldo
 - Devolución
 - Apagado
 - Otra operación de reubicación de nivel local
 - Cambia la propiedad del disco
 - Operaciones de configuración de nivel local o volumen
 - Reemplazo de la controladora de almacenamiento
 - Actualización de ONTAP
 - Reversión de ONTAP
- Si dispone de una configuración MetroCluster, no debe iniciar la reubicación de niveles local mientras las operaciones de recuperación ante desastres (*switchover*, *curing* o *Switched*) están en curso.
 - Si tiene una configuración de MetroCluster e inicia la reubicación de nivel local en un nivel local de conmutación, es posible que se produzca un error en la operación porque supera el número de límite de volúmenes del partner de DR.
 - No se debe iniciar la reubicación de nivel local en agregados dañados o sometidos a mantenimiento.
 - Antes de iniciar la reubicación de nivel local, debe guardar cualquier volcado principal en los nodos de origen y destino.

Pasos

1. Visualice los agregados en el nodo para confirmar qué agregados se moverán y asegúrese de que estén en línea y en buenas condiciones:

```
storage aggregate show -node source-node
```

El siguiente comando muestra seis agregados en los cuatro nodos del clúster. Todos los agregados están en línea. Los nodos 1 y Node3 forman un par de alta disponibilidad y Node2 y Node4 forman un par de alta disponibilidad.

```
cluster::> storage aggregate show
```

| Aggregate | Size | Available | Used% | State | #Vols | Nodes | RAID | Status |
|-----------|---------|-----------|-------|--------|-------|-------|----------|--------|
| aggr_0 | 239.0GB | 11.13GB | 95% | online | 1 | node1 | raid_dp, | normal |
| aggr_1 | 239.0GB | 11.13GB | 95% | online | 1 | node1 | raid_dp, | normal |
| aggr_2 | 239.0GB | 11.13GB | 95% | online | 1 | node2 | raid_dp, | normal |
| aggr_3 | 239.0GB | 11.13GB | 95% | online | 1 | node2 | raid_dp, | normal |
| aggr_4 | 239.0GB | 238.9GB | 0% | online | 5 | node3 | raid_dp, | normal |
| aggr_5 | 239.0GB | 239.0GB | 0% | online | 4 | node4 | raid_dp, | normal |

6 entries were displayed.

2. Ejecute el comando para iniciar la reubicación de agregados:

```
storage aggregate relocation start -aggregate-list aggregate-1, aggregate-2...
-node source-node -destination destination-node
```

El siguiente comando mueve los agregados aggr_1 y aggr_2 de Node1 a Node3. El nodo 3 es el partner de alta disponibilidad de Node1. Los agregados solo se pueden mover dentro del par de alta disponibilidad.

```
cluster::> storage aggregate relocation start -aggregate-list aggr_1,
aggr_2 -node node1 -destination node3
Run the storage aggregate relocation show command to check relocation
status.
node1::storage aggregate>
```

3. Supervise el progreso de la reubicación de agregados con la storage aggregate relocation show comando:

```
storage aggregate relocation show -node source-node
```

El siguiente comando muestra el progreso de los agregados que se están moviendo a Node3:

```
cluster::> storage aggregate relocation show -node node1
Source Aggregate      Destination      Relocation Status
-----
node1
      aggr_1          node3            In progress, module: waf1
      aggr_2          node3            Not attempted yet
2 entries were displayed.
node1::storage aggregate>
```

Una vez finalizada la reubicación, el resultado de este comando muestra cada agregado con el estado de reubicación de "Done".

Eliminar un nivel local (agregado)

Puede eliminar un nivel local (agregado) si no hay volúmenes en el nivel local.

La `storage aggregate delete` comando elimina un agregado de almacenamiento. Error del comando si hay volúmenes presentes en el agregado. Si el agregado tiene un almacén de objetos asociado, además de eliminar el agregado, el comando elimina también los objetos del almacén de objetos. No se realizan cambios en la configuración del almacén de objetos como parte de este comando.

En el siguiente ejemplo se elimina un agregado denominado «'aggr1'»:

```
> storage aggregate delete -aggregate aggr1
```

Comandos para reubicación de agregados

Hay comandos ONTAP específicos para reubicar la propiedad del agregado en una pareja de ha.

| | |
|---|---|
| Si desea... | Se usa este comando... |
| Inicie el proceso de reubicación del agregado | <code>storage aggregate relocation start</code> |
| Supervisar el proceso de reubicación de agregados | <code>storage aggregate relocation show</code> |

Información relacionada

["Comandos de ONTAP 9"](#)

Comandos para gestionar agregados

Utilice la `storage aggregate` comando para gestionar los agregados.

| Si desea... | Se usa este comando... |
|--|--|
| Muestra el tamaño de la caché de todos los agregados de Flash Pool | <code>storage aggregate show -fields hybrid-cache-size-total -hybrid-cache-size-total >0</code> |
| Mostrar la información y el estado de los discos de un agregado | <code>storage aggregate show-status</code> |
| Muestre los discos de repuesto por nodo | <code>storage aggregate show-spare-disks</code> |
| Muestre los agregados raíz en el clúster | <code>storage aggregate show -has-mroot true</code> |
| Mostrar información básica y estado de los agregados | <code>storage aggregate show</code> |
| Muestra el tipo de almacenamiento utilizado en un agregado | <code>storage aggregate show -fields storage-type</code> |
| Poner un agregado en línea | <code>storage aggregate online</code> |
| Eliminar un agregado | <code>storage aggregate delete</code> |
| Ponga un agregado en estado restringido | <code>storage aggregate restrict</code> |
| Cambiar el nombre de un agregado | <code>storage aggregate rename</code> |
| Desconectar un agregado | <code>storage aggregate offline</code> |
| Cambie el tipo de RAID de un agregado | <code>storage aggregate modify -raidtype</code> |

Información relacionada

["Comandos de ONTAP 9"](#)

Añada capacidad (discos) a un nivel local (agregado)

Añada capacidad (discos) a un nivel local (agregado)

Utilice diferentes métodos para seguir un flujo de trabajo específico y añadir capacidad.

- ["Flujo de trabajo para añadir capacidad a un nivel local \(agregado\)"](#)
- ["Métodos para crear espacio en un nivel local \(agregado\)"](#)

Es posible añadir discos a un nivel local y añadir unidades a un nodo o a una bandeja.

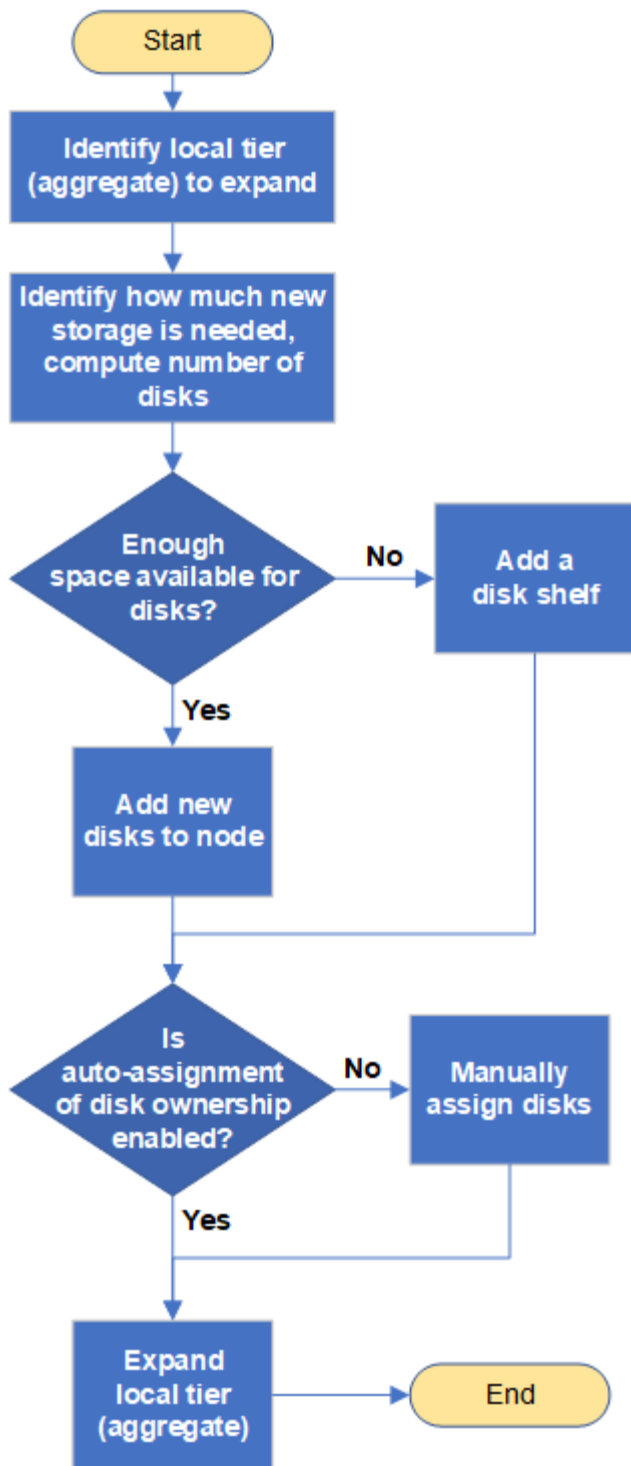
Si es necesario, puede corregir las particiones de repuesto mal alineadas.

- "Añadir discos a un nivel local (agregado)"
- "Añadir unidades a un nodo o bandeja"
- "Corrija las particiones de repuesto mal alineadas"

Flujo de trabajo para añadir capacidad a un nivel local (expandir un agregado)

Para añadir capacidad a un nivel local (expandir un agregado) primero debe identificar al nivel local al que desea añadir, determinar cuánto almacenamiento nuevo necesita, instalar nuevos discos, asignar propiedad de discos y crear un nuevo grupo RAID, si es necesario.

Puede usar System Manager o la CLI para añadir capacidad.



Métodos para crear espacio en un nivel local (agregado)

Si un nivel local (agregado) se queda sin espacio libre, se pueden producir varios problemas que van desde la pérdida de datos hasta la garantía de un volumen. Hay varias maneras de crear más espacio en un nivel local.

Todos los métodos tienen diversas consecuencias. Antes de llevar a cabo cualquier acción, debe leer la sección pertinente de la documentación.

Las siguientes son algunas maneras comunes de hacer espacio en el nivel local, con el orden de lo menos a

la mayoría de las consecuencias:

- Añada discos al nivel local.
- Mueva algunos volúmenes a otro nivel local con espacio disponible.
- Reduzca el tamaño de los volúmenes con garantía de volumen en el nivel local.
- Elimine las copias snapshot de volumen innecesarias si el tipo de garantía del volumen es "none".
- Elimine volúmenes innecesarios.
- Active funciones que ahorran espacio como la deduplicación o la compresión.
- (Temporalmente) deshabilite las funciones que utilizan una gran cantidad de metadatos .

Añada capacidad a un nivel local (añada discos a un agregado)

Puede añadir discos a un nivel local (agregado) para que pueda proporcionar más almacenamiento a sus volúmenes asociados.

System Manager (ONTAP 9.8 y posterior)

Utilice el Administrador del sistema para agregar capacidad (ONTAP 9.8 y posterior)

Puede añadir capacidad a un nivel local con la adición de discos de capacidad.



A partir de ONTAP 9.12.1, se puede usar System Manager para ver la capacidad comprometida de un nivel local con el fin de determinar si se requiere capacidad adicional para el nivel local. Consulte "[Supervise la capacidad en System Manager](#)".

Acerca de esta tarea

Realice esta tarea solo si ha instalado ONTAP 9.8 o una versión posterior. Si ha instalado una versión anterior de ONTAP, consulte la ficha (o sección) con la etiqueta «System Manager (ONTAP 9,7 y versiones anteriores).

".

Pasos

1. Haga clic en **almacenamiento > niveles**.
2. Haga clic en junto al nombre del nivel local al que se desea añadir capacidad.
3. Haga clic en **Añadir capacidad**.



Si no hay discos de repuesto que pueda agregar, no se muestra la opción **Añadir capacidad** y no puede aumentar la capacidad del nivel local.

4. Realice los pasos siguientes, según la versión de ONTAP que esté instalada:

| Si esta versión de ONTAP está instalada... | Realice estos pasos... |
|--|--|
| ONTAP 9.8, 9.9 o 9.10.1 | <ol style="list-style-type: none">a. Si el nodo contiene varios niveles de almacenamiento, seleccione el número de discos que desea añadir al nivel local. De lo contrario, si el nodo contiene solo un nivel de almacenamiento único, la capacidad añadida se estima automáticamente.b. Haga clic en Agregar. |
| A partir de ONTAP 9.11.1 | <ol style="list-style-type: none">a. Seleccione el tipo de disco y el número de discos.b. Si desea añadir discos a un nuevo grupo RAID, active la casilla de comprobación. Aparece la asignación de RAID.c. Haga clic en Guardar. |

5. (Opcional) el proceso tarda un poco en completarse. Si desea ejecutar el proceso en segundo plano, seleccione **Ejecutar en fondo**.
6. Una vez completado el proceso, puede ver la cantidad de capacidad aumentada en la información de nivel local en **almacenamiento > niveles**.

System Manager (ONTAP 9.7 y versiones anteriores)

Utilice el Administrador del sistema para agregar capacidad (ONTAP 9.7 y versiones anteriores)

Puede añadir capacidad a un nivel local (agregado) mediante la adición de discos de capacidad.

Acerca de esta tarea

Esta tarea debe realizarse solo si ha instalado ONTAP 9.7 o una versión anterior. Si ha instalado ONTAP 9.8 o posterior, consulte [Use System Manager para añadir capacidad \(ONTAP 9.8 o posterior\)](#).

Pasos

1. (Sólo para ONTAP 9.7) haga clic en **(Volver a la versión clásica)**.
2. Haga clic en **hardware y diagnósticos > agregados**.
3. Seleccione el agregado al que desea agregar discos de capacidad y, a continuación, haga clic en **acciones > Añadir capacidad**.



Debe añadir discos con el mismo tamaño que los demás discos del agregado.

4. (Sólo para ONTAP 9.7) haga clic en **Cambiar a la nueva experiencia**.
5. Haga clic en **almacenamiento > niveles** para comprobar el tamaño del nuevo agregado.

CLI

Utilice la CLI para agregar capacidad

El procedimiento para añadir discos con particiones a un agregado es similar al procedimiento para añadir discos sin particiones.

Lo que necesitará

Debe saber a qué tamaño del grupo RAID corresponde el agregado al que va a añadir el almacenamiento.

Acerca de esta tarea

Al expandir un agregado, debe saber si va a agregar partición o discos sin particiones al agregado. Cuando se añaden unidades sin particiones a un agregado existente, el tamaño de los grupos RAID existentes se hereda por el nuevo grupo RAID, que puede afectar al número de discos de paridad requeridos. Si se agrega un disco sin particiones a un grupo RAID compuesto por discos con particiones, se crea una partición del nuevo disco, dejando una partición de repuesto sin utilizar.

Cuando aprovisiona particiones, debe asegurarse de no dejar el nodo sin una unidad con ambas particiones como repuesto. Si lo hace y el nodo experimenta una interrupción en la controladora, es posible que no haya disponible información valiosa sobre el problema (el archivo de núcleo) para proporcionarla al soporte técnico.



No utilice la `disklist` comando para expandir los agregados. Esto puede provocar una alineación incorrecta de las particiones.

Pasos

1. Muestre el almacenamiento de reserva disponible en el sistema que posee el agregado:

```
storage aggregate show-spare-disks -original-owner node_name
```

Puede utilizar el `-is-disk-shared` parámetro para mostrar solo unidades con particiones o solo unidades sin particiones.

```
cl1-s2::> storage aggregate show-spare-disks -original-owner cl1-s2
-is-disk-shared true
```

Original Owner: cl1-s2

Pool0

Shared HDD Spares

| | | | | Local | |
|---------------------------|---------|--------|------|-------|-----------------|
| Local | | | | Data | |
| Root Physical | | | | | |
| Disk | | | Type | RPM | Checksum Usable |
| Usable | Size | Status | | | |
| ----- | | | | | |
| 1.0.1 | | | BSAS | 7200 | block 753.8GB |
| 73.89GB | 828.0GB | zeroed | | | |
| 1.0.2 | | | BSAS | 7200 | block 753.8GB |
| 0B | 828.0GB | zeroed | | | |
| 1.0.3 | | | BSAS | 7200 | block 753.8GB |
| 0B | 828.0GB | zeroed | | | |
| 1.0.4 | | | BSAS | 7200 | block 753.8GB |
| 0B | 828.0GB | zeroed | | | |
| 1.0.8 | | | BSAS | 7200 | block 753.8GB |
| 0B | 828.0GB | zeroed | | | |
| 1.0.9 | | | BSAS | 7200 | block 753.8GB |
| 0B | 828.0GB | zeroed | | | |
| 1.0.10 | | | BSAS | 7200 | block 0B |
| 73.89GB | 828.0GB | zeroed | | | |
| 2 entries were displayed. | | | | | |

2. Muestra los grupos RAID actuales del agregado:

```
storage aggregate show-status aggr_name
```

```
cl1-s2::> storage aggregate show-status -aggregate data_1
```

Owner Node: cl1-s2

Aggregate: data_1 (online, raid_dp) (block checksums)

Plex: /data_1/plex0 (online, normal, active, pool0)

RAID Group /data_1/plex0/rg0 (normal, block checksums)

| | Position | Disk | Pool | Type | RPM | Usable Size | Physical Size | Status |
|----------|----------|-------|------|------|---------|-------------|---------------|--------|
| | ----- | ----- | ---- | ---- | ----- | ----- | ----- | |
| ----- | | | | | | | | |
| shared | 1.0.10 | 0 | BSAS | 7200 | 753.8GB | 828.0GB | | |
| (normal) | | | | | | | | |
| shared | 1.0.5 | 0 | BSAS | 7200 | 753.8GB | 828.0GB | | |
| (normal) | | | | | | | | |
| shared | 1.0.6 | 0 | BSAS | 7200 | 753.8GB | 828.0GB | | |
| (normal) | | | | | | | | |
| shared | 1.0.11 | 0 | BSAS | 7200 | 753.8GB | 828.0GB | | |
| (normal) | | | | | | | | |
| shared | 1.0.0 | 0 | BSAS | 7200 | 753.8GB | 828.0GB | | |
| (normal) | | | | | | | | |

5 entries were displayed.

3. Simule la adición del almacenamiento al agregado:

```
storage aggregate add-disks -aggregate aggr_name -diskcount  
number_of_disks_or_partitions -simulate true
```

Puede ver el resultado de la adición del almacenamiento sin realmente aprovisionar ningún almacenamiento. Si se muestra alguna advertencia desde el comando simulado, puede ajustar el comando y repetir la simulación.

```
cl1-s2::> storage aggregate add-disks -aggregate aggr_test
-diskcount 5 -simulate true
```

Disks would be added to aggregate "aggr_test" on node "cl1-s2" in the following manner:

First Plex

```
RAID Group rg0, 5 disks (block checksum, raid_dp)

Physical                               Usable
Position  Disk                        Type      Size
Size
-----
shared    1.11.4                      SSD       415.8GB
415.8GB
shared    1.11.18                     SSD       415.8GB
415.8GB
shared    1.11.19                     SSD       415.8GB
415.8GB
shared    1.11.20                     SSD       415.8GB
415.8GB
shared    1.11.21                     SSD       415.8GB
415.8GB
```

Aggregate capacity available for volume use would be increased by 1.83TB.

4. Añada el almacenamiento al agregado:

```
storage aggregate add-disks -aggregate aggr_name -raidgroup new -diskcount
number_of_disks_or_partitions
```

Cuando se crea un agregado de Flash Pool, debe utilizar la si se añaden discos con una suma de comprobación diferente a la del agregado, o si se añaden discos a un agregado de suma de comprobación mixto `-checksumstyle` parámetro.

Si va a añadir discos a un agregado de Flash Pool, debe usar el `-disktype` parámetro para especificar el tipo de disco.

Puede utilizar el `-disksize` parámetro para especificar el tamaño de los discos que se van a añadir. Solo se seleccionan discos con el tamaño aproximadamente especificado para agregarlos.

```
cl1-s2::> storage aggregate add-disks -aggregate data_1 -raidgroup
new -diskcount 5
```

5. Compruebe que el almacenamiento se ha añadido correctamente:

```
storage aggregate show-status -aggregate aggr_name
```

```
cl1-s2::> storage aggregate show-status -aggregate data_1

Owner Node: cl1-s2
Aggregate: data_1 (online, raid_dp) (block checksums)
Plex: /data_1/plex0 (online, normal, active, pool0)
RAID Group /data_1/plex0/rg0 (normal, block checksums)

Physical                                                                 Usable
Position Disk                                Pool Type      RPM      Size
Size Status
-----
shared 1.0.10                                0    BSAS      7200    753.8GB
828.0GB (normal)
shared 1.0.5                                  0    BSAS      7200    753.8GB
828.0GB (normal)
shared 1.0.6                                  0    BSAS      7200    753.8GB
828.0GB (normal)
shared 1.0.11                                 0    BSAS      7200    753.8GB
828.0GB (normal)
shared 1.0.0                                  0    BSAS      7200    753.8GB
828.0GB (normal)
shared 1.0.2                                  0    BSAS      7200    753.8GB
828.0GB (normal)
shared 1.0.3                                  0    BSAS      7200    753.8GB
828.0GB (normal)
shared 1.0.4                                  0    BSAS      7200    753.8GB
828.0GB (normal)
shared 1.0.8                                  0    BSAS      7200    753.8GB
828.0GB (normal)
shared 1.0.9                                  0    BSAS      7200    753.8GB
828.0GB (normal)
10 entries were displayed.
```

6. Compruebe que el nodo sigue teniendo al menos una unidad con la partición raíz y la partición de datos como repuesto:

```
storage aggregate show-spare-disks -original-owner node_name
```

```
cl1-s2::> storage aggregate show-spare-disks -original-owner cl1-s2
-is-disk-shared true
```

Original Owner: cl1-s2

Pool0

Shared HDD Spares

| | | | | Local |
|---------------------------|---------|--------|----------|---------|
| | | | | Data |
| Root Physical | | | | |
| Disk | Type | RPM | Checksum | Usable |
| Usable | Size | Status | | |
| 1.0.1 | BSAS | 7200 | block | 753.8GB |
| 73.89GB | 828.0GB | zeroed | | |
| 1.0.10 | BSAS | 7200 | block | 0B |
| 73.89GB | 828.0GB | zeroed | | |
| 2 entries were displayed. | | | | |

Añada unidades a un nodo o bandeja

Se añaden unidades a un nodo o una bandeja para aumentar la cantidad de piezas de repuesto o añadir espacio al nivel local (agregado).

Antes de empezar

La unidad que desea agregar debe ser compatible con su plataforma. Puede confirmar con el ["Hardware Universe de NetApp"](#).

La cantidad mínima de unidades que debe añadir en un solo procedimiento es de seis. Al añadir una sola unidad, se puede reducir el rendimiento.

Pasos para el NetApp Hardware Universe

1. En el menú desplegable **Productos**, seleccione su configuración de hardware
2. Seleccione la plataforma.
3. Selecciona la versión de ONTAP que estás ejecutando y luego **Mostrar resultados**.
4. Debajo del gráfico, selecciona **Haga clic aquí para ver vistas alternativas**. Elija la vista que coincida con su configuración.



Pasos para instalar las unidades

1. Compruebe la ["Sitio de soporte de NetApp"](#) Para más reciente firmware de unidad y bandeja y archivos de paquetes de cualificación de disco.

Si su nodo o bandeja no tienen las versiones más recientes, actualice antes de instalar la unidad nueva.

El firmware de la unidad se actualiza automáticamente (sin interrupciones) en las unidades nuevas que no tienen versiones de firmware actuales.

2. Puesta a tierra apropiadamente usted mismo.
3. Retire con cuidado el bisel de la parte delantera de la plataforma.
4. Identifique la ranura correcta para la unidad nueva.



Las ranuras correctas para añadir unidades varían según el modelo de plataforma y la versión de ONTAP. En algunos casos, es necesario añadir unidades a ranuras específicas en secuencia. Por ejemplo, en un AFF A800 se añaden las unidades a intervalos específicos, lo que deja los clústeres de ranuras vacías. Mientras que, en un AFF A220, se añaden nuevas unidades a las próximas ranuras vacías que van desde el exterior hacia el medio de la bandeja.

Consulte los pasos descritos en **Antes de comenzar** para identificar las ranuras correctas para su configuración en el ["Hardware Universe de NetApp"](#).

5. Inserte la nueva unidad:
 - a. Con la palanca de leva en posición abierta, utilice ambas manos para insertar la nueva transmisión.
 - b. Presione hasta que la unidad se detenga.
 - c. Cierre el asa de leva de forma que la unidad esté completamente asentada en el plano medio y el asa encaje en su lugar. Asegúrese de cerrar el mango de leva lentamente para que quede alineado correctamente con la cara de la transmisión.
6. Verifique que el LED de actividad de la unidad (verde) esté iluminado.

Cuando el LED de actividad de la unidad está sólido, significa que la unidad tiene alimentación. Cuando el LED de actividad de la unidad parpadea, significa que la unidad tiene alimentación y I/O está en curso. Si el firmware de la unidad se actualiza automáticamente, el LED parpadea.

7. Para añadir otra unidad, repita los pasos 4 a 6.

Las unidades nuevas no se reconocen hasta que se asignan a un nodo. Es posible asignar las unidades nuevas de forma manual, o bien se puede esperar a que ONTAP asigne automáticamente las unidades nuevas si el nodo sigue las reglas de la asignación automática de unidades.

8. Una vez reconocidas las unidades nuevas, compruebe que se hayan añadido y que su propiedad se haya especificado correctamente.

Pasos para confirmar la instalación

1. Mostrar la lista de discos:

```
storage aggregate show-spare-disks
```

Debe ver las unidades nuevas, que son propiedad del nodo correcto.

2. **Opcionalmente (solo para ONTAP 9,3 y versiones anteriores)**, pone a cero las unidades recién añadidas:

```
storage disk zerospares
```

Las unidades que se hayan usado previamente en un nivel local de ONTAP (agregado) deben ponerse a cero para poder añadirse a otro agregado. En ONTAP 9.3 y versiones anteriores, la puesta a cero puede tardar horas en completarse, según el tamaño de las unidades no ceros del nodo. La puesta a cero de las unidades ahora puede evitar retrasos en caso de que necesite aumentar rápidamente el tamaño de un nivel local. Esto no supone un problema en ONTAP 9.4 o versiones posteriores en las que las unidades se ponen a cero con *fast puesta a cero*, lo que solo tarda unos segundos.

Resultados

Ya están listas las nuevas unidades. Puede añadirlos a un nivel local (agregado), colocarlos en la lista de piezas de repuesto o añadirlas al crear un nuevo nivel local.

Corrija las particiones de repuesto mal alineadas

Cuando se agregan discos con particiones a un nivel local (agregado), se debe dejar un disco con la partición raíz y de datos disponibles como reserva para cada nodo. Si no lo hace y el nodo experimenta una interrupción, ONTAP no puede volcar la memoria en la partición de datos de reserva.

Antes de empezar

Debe tener una partición de datos de reserva y una partición raíz de repuesto en el mismo tipo de disco que pertenece al mismo nodo.

Pasos

1. Con la CLI, muestre las particiones de repuesto del nodo:

```
storage aggregate show-spare-disks -original-owner node_name
```

Observe qué disco tiene una partición de datos de reserva (*spare_data*) y qué disco tiene una partición raíz de reserva (*spare_root*). La partición de reserva mostrará un valor distinto de cero en la *Local Data Usable* o *Local Root Usable* columna.

2. Sustituya el disco por una partición de datos de repuesto con el disco por la partición raíz de repuesto:

```
storage disk replace -disk spare_data -replacement spare_root -action start
```

Puede copiar los datos en cualquier dirección; sin embargo, copiar la partición raíz tarda menos tiempo en completarse.

3. Supervise el progreso de la sustitución de discos:

```
storage aggregate show-status -aggregate aggr_name
```

4. Una vez completada la operación de sustitución, vuelva a mostrar las piezas de repuesto para confirmar que dispone de un disco de repuesto completo:

```
storage aggregate show-spare-disks -original-owner node_name
```

Debería ver un disco de repuesto con espacio útil bajo los términos «'datos locales útiles» y Local Root Usable.

Ejemplo

Muestra las particiones de repuesto del nodo c1-01 y comprueba que las particiones de repuesto no están alineadas:

```
c1::> storage aggregate show-spare-disks -original-owner c1-01
```

Original Owner: c1-01

Pool0

Shared HDD Spares

| Disk | Type | RPM | Checksum | Local Data Usable | Local Root Usable | Physical Size |
|--------|------|------|----------|-------------------------|-------------------------|------------------|
| 1.0.1 | BSAS | 7200 | block | 753.8GB | 0B | 828.0GB |
| 1.0.10 | BSAS | 7200 | block | 0B | 73.89GB | 828.0GB |

El trabajo de sustitución de discos se inicia:

```
c1::> storage disk replace -disk 1.0.1 -replacement 1.0.10 -action start
```

Mientras espera a que finalice la operación de sustitución, muestra el progreso de la operación:

```
c1::> storage aggregate show-status -aggregate aggr0_1
```

Owner Node: c1-01

Aggregate: aggr0_1 (online, raid_dp) (block checksums)

Plex: /aggr0_1/plex0 (online, normal, active, pool0)

RAID Group /aggr0_1/plex0/rg0 (normal, block checksums)

| Position | Disk | Pool | Type | RPM | Usable Size | Physical Size | Status |
|----------|--------|------|------|------|----------------|------------------|-------------------------------|
| shared | 1.0.1 | 0 | BSAS | 7200 | 73.89GB | 828.0GB | (replacing, copy in progress) |
| shared | 1.0.10 | 0 | BSAS | 7200 | 73.89GB | 828.0GB | (copy 63% completed) |
| shared | 1.0.0 | 0 | BSAS | 7200 | 73.89GB | 828.0GB | (normal) |
| shared | 1.0.11 | 0 | BSAS | 7200 | 73.89GB | 828.0GB | (normal) |
| shared | 1.0.6 | 0 | BSAS | 7200 | 73.89GB | 828.0GB | (normal) |
| shared | 1.0.5 | 0 | BSAS | 7200 | 73.89GB | 828.0GB | (normal) |

Una vez finalizada la operación de sustitución, confirme que dispone de un disco de repuesto completo:

```
ie2220::> storage aggregate show-spare-disks -original-owner c1-01
```

Original Owner: c1-01

Pool0

Shared HDD Spares

| | | | | Local Data Usable | Local Root Usable | Physical Size |
|-------|-------|------|----------|-------------------------|-------------------------|------------------|
| Disk | Type | RPM | Checksum | | | |
| ----- | ----- | ---- | ----- | ----- | ----- | ----- |
| 1.0.1 | BSAS | 7200 | block | 753.8GB | 73.89GB | 828.0GB |

Gestionar discos

Información general sobre la gestión de discos

Puede realizar varios procedimientos para gestionar los discos del sistema.

- **Aspectos de la administración de discos**
 - ["Cuando necesite actualizar el paquete de cualificación de disco"](#)
 - ["Cómo funcionan los discos de repuesto"](#)
 - ["La poca advertencia de repuestos puede ayudarle a gestionar sus discos de repuesto"](#)
 - ["Opciones adicionales de gestión de la partición de datos raíz"](#)
- **Propiedad de disco y partición**
 - ["Propiedad de disco y partición"](#)
- **Error en la eliminación del disco**
 - ["Quitar un disco con errores"](#)
- **Saneamiento de disco**
 - ["El saneamiento de disco"](#)

Cómo funcionan los discos de repuesto

Un disco de repuesto activo es un disco que está asignado a un sistema de almacenamiento y está listo para su uso, pero no lo está utilizando un grupo RAID y no contiene ningún dato.

Si se produce un fallo de disco dentro de un grupo RAID, el disco de repuesto activo se asigna automáticamente al grupo RAID para sustituir los discos que han fallado. Los datos del disco con error se reconstruyen en el disco de repuesto en segundo plano desde el disco de paridad RAID. La actividad de reconstrucción se registra en la `/etc/message`. Se envía un archivo y un mensaje AutoSupport.

Si el disco de repuesto activo disponible no tiene el mismo tamaño que el disco que ha fallado, se elige un disco del siguiente tamaño mayor y, a continuación, se reducirá para que coincida con el tamaño del disco que va a sustituir.

Requisitos de repuesto para el disco portador de varios discos

Mantener el número correcto de repuestos para los discos en portadores de discos es fundamental para optimizar la redundancia de almacenamiento y minimizar el tiempo que ONTAP debe dedicar a copiar discos para lograr una distribución óptima de los discos.

Debe mantener un mínimo de dos piezas de repuesto para los discos portadores de varios discos en todo momento. Para admitir el uso del centro de mantenimiento y evitar problemas causados por varios fallos de disco simultáneos, debe mantener al menos cuatro repuestos en caliente para que el funcionamiento siempre sea estable y sustituir los discos con fallos con prontitud.

Si dos discos fallan al mismo tiempo con solo dos piezas de repuesto disponibles, es posible que ONTAP no pueda cambiar el contenido del disco con fallo y la relación de posición del portador con los discos de repuesto. Este escenario se denomina un punto muerto. Si esto sucede, se le notificarán mediante mensajes de EMS y AutoSupport. Cuando los operadores de sustitución estén disponibles, debe seguir las instrucciones proporcionadas por los mensajes EMS.

Para obtener información acerca de mí, consulte el artículo de la base de conocimientos ["El diseño RAID no se puede autoCorregir - mensaje AutoSupport"](#)

La poca advertencia de repuestos puede ayudarle a gestionar sus discos de repuesto

De forma predeterminada, se emiten advertencias a la consola y los registros si tiene menos de una unidad de repuesto que coincide con los atributos de cada unidad del sistema de almacenamiento.

Puede cambiar el valor de umbral para estos mensajes de advertencia para garantizar que el sistema cumple las prácticas recomendadas.

Acerca de esta tarea

Debería establecer la opción «main_spare_count» en RAID «2» para asegurarse de que siempre dispone del número mínimo recomendado de discos de repuesto.

Paso

1. Establezca la opción en «'2'»:

```
storage raid-options modify -node nodename -name min_spare_count -value 2
```

Opciones adicionales de gestión de la partición de datos raíz

A partir de ONTAP 9.2, hay disponible una nueva opción de partición de datos raíz en el menú de inicio que proporciona funciones de administración adicionales para los discos configurados para la partición de datos raíz.

Las siguientes funciones de administración están disponibles en la opción Boot Menu 9.

- **Desparticionar todos los discos y eliminar su información de propiedad**

Esta opción es útil si el sistema está configurado para la partición de datos raíz y debe reiniciarla con una configuración diferente.

- **Limpie la configuración e inicialice el nodo con discos particionados**

Esta opción es útil para lo siguiente:

- El sistema no está configurado para la partición de datos raíz y desea configurarlo para la partición de datos raíz
- El sistema está configurado incorrectamente para la partición de datos raíz y debe corregirlo
- Tiene una plataforma AFF o una plataforma FAS solo con SSD conectados que está configurada para la versión anterior de la partición de datos raíz y desea actualizarla a la versión más reciente de la partición de datos raíz para obtener una mayor eficiencia de almacenamiento

- **Limpiar la configuración e inicializar nodo con discos completos**

Esta opción es útil si necesita:

- Desparticionar particiones existentes
- Quitar la propiedad de disco local
- Reinicie el sistema con discos completos utilizando RAID-DP

Cuando necesite actualizar el paquete de cualificación de disco

El paquete de cualificación de disco (DQP) añade compatibilidad total con las unidades recién cualificadas. Antes de actualizar el firmware de la unidad o añadir nuevos tipos o tamaños de unidad a un clúster, debe actualizar el DQP. Una práctica recomendada es actualizar también el DQP regularmente; por ejemplo, cada trimestre o semestral.

Debe descargar e instalar el DQP en las siguientes situaciones:

- Cuando se añade un tamaño o un tipo de unidad nuevo al nodo

Por ejemplo, si ya tiene unidades de 1 TB y añade unidades de 2 TB, debe comprobar la actualización más reciente del DQP.

- Cada vez que se actualiza el firmware de disco
- Siempre que estén disponibles los archivos DQP o firmware de disco más nuevos
- Siempre que actualice a una versión nueva de ONTAP.

El DQP no se actualiza como parte de una actualización de ONTAP.

Información relacionada

["Descargas de NetApp: Paquete de cualificación de disco"](#)

["Descargas de NetApp: Firmware de la unidad de disco"](#)

Propiedad de disco y partición

Propiedad de disco y partición

Puede gestionar la propiedad de discos y particiones.

Es posible realizar las siguientes tareas:

- **"Mostrar propiedad de disco y partición"**

Es posible ver la propiedad de un disco para determinar qué nodo controla el almacenamiento. También

puede ver la propiedad de la partición en sistemas que utilizan discos compartidos.

- **"Cambie la configuración de la asignación automática de propiedad de disco"**

Puede seleccionar una política no predeterminada para asignar automáticamente propiedad de disco o deshabilitar la asignación automática de propiedad de disco.

- **"Asigne manualmente la propiedad de discos sin particiones"**

Si el clúster no está configurado para utilizar la asignación de propiedad de disco automática, debe asignar la propiedad de forma manual.

- **"Asigne manualmente la propiedad de discos con particiones"**

Puede establecer la propiedad del disco de contenedor o de las particiones manualmente o mediante la asignación automática, igual que en los discos sin particiones.

- **"Quitar un disco con errores"**

Un disco que ha fallado completamente ya no es considerado por ONTAP como un disco utilizable y el disco se puede desconectar inmediatamente de la bandeja.

- **"Quitar la propiedad de un disco"**

ONTAP escribe la información de propiedad del disco en el disco. Antes de quitar un disco de repuesto o su bandeja de un nodo, se debe eliminar la información de propiedad para que se pueda integrar correctamente en otro nodo.

Acerca de la asignación automática de propiedad de disco

La asignación automática de discos sin propiedad está habilitada de forma predeterminada. La asignación automática de propiedad de discos se produce 10 minutos después de la inicialización del par de alta disponibilidad y cada cinco minutos durante el funcionamiento normal del sistema.

Cuando agrega un nuevo disco a un par de alta disponibilidad, por ejemplo, al reemplazar un disco con errores, responder a un mensaje de «piezas de repuesto bajas» o agregar capacidad, la política de asignación automática predeterminada asigna la propiedad del disco a un nodo como reserva.

La política de asignación automática predeterminada se basa en las características específicas de la plataforma, o la bandeja DS460C si el par de alta disponibilidad solo tiene estas bandejas y utiliza uno de los siguientes métodos (políticas) para asignar la propiedad de disco:

| Método de asignación | Efecto en las asignaciones de nodos | Configuraciones de plataforma que se establecen por defecto en el método de asignación |
|----------------------|--|--|
| bahía | Las bahías pares están asignadas al nodo A y las bahías impares al nodo B. | Sistemas de gama básica en una configuración de par de alta disponibilidad con una única bandeja compartida. |

| | | |
|---|--|--|
| bandeja | Todos los discos de la bandeja están asignados al nodo A. | Sistemas de gama básica en una configuración de par de alta disponibilidad con una pila de dos o más bandejas, y configuraciones de MetroCluster con una pila por nodo, dos o más bandejas. |
| bandeja dividida Esta política se encuentra bajo el valor de “defecto” para el <code>-autoassign-policy</code> parámetro de <code>storage disk option</code> comando para las configuraciones de plataforma y bandejas aplicables. | Los discos del lado izquierdo de la bandeja se asignan al nodo A y, en el lado derecho, al nodo B. Las bandejas parciales de parejas de alta disponibilidad salen de fábrica con los discos que ocupan desde el borde de la bandeja al centro. | La mayoría de las plataformas AFF y algunas configuraciones MetroCluster. |
| pila | Todos los discos de la pila se asignan al nodo A. | Sistemas de gama básica independientes y todas las demás configuraciones. |
| medio cajón Esta política se encuentra bajo el valor de “defecto” para el <code>-autoassign-policy</code> parámetro de <code>storage disk option</code> comando para las configuraciones de plataforma y bandejas aplicables. | <p>Todas las unidades de la mitad izquierda de un cajón de DS460C (bahías de unidades de 0 a 5) se asignan al nodo A; todas las unidades de la mitad derecha de un cajón (bahías de unidades de 6 a 11) se asignan al nodo B.</p> <p>Al inicializar un par de alta disponibilidad con solo DS460C bandejas, no se admite la asignación automática de propiedad de disco. Debe asignar manualmente la propiedad a las unidades que contienen unidades raíz/contenedor que tengan la partición raíz conforme a la política de medio cajón.</p> | <p>Pares DE ALTA disponibilidad con solo DS460C bandejas, después de la inicialización del par de alta disponibilidad (arranque).</p> <p>Después de arrancar una pareja de alta disponibilidad, se habilita automáticamente la asignación automática de propiedad de disco y utiliza la política de medio cajón para asignar la propiedad a las unidades restantes (aparte de las unidades raíz/contenedores que poseen la partición raíz) y cualquier unidad que se añada en el futuro.</p> <p>Si la pareja de alta disponibilidad tiene DS460C bandejas además de otros modelos de bandeja, no se usa la política de medio cajón. La política por defecto utilizada está dictada por características específicas de la plataforma.</p> |

Ajustes y modificaciones de asignación automática:

- Puede visualizar la configuración de asignación automática actual (ON/OFF) con el `storage disk option show` comando.
- Puede desactivar la asignación automática mediante el `storage disk option modify` comando.
- Si la política de asignación automática predeterminada no es deseable en el entorno, puede especificar

(cambiar) el método de asignación de bahía, bandeja o pila mediante el `-autoassign-policy` en la `storage disk option modify` comando.

Aprenda cómo ["Cambie la configuración de la asignación automática de propiedad de disco"](#).



Las políticas de asignación automática predeterminadas de medio cajón y bandeja dividida son únicas porque los usuarios como las políticas de bahía, bandeja y pila no pueden definir las.

En los sistemas de partición avanzada de unidades (ADP), para poder asignar automáticamente el trabajo en bandejas semiocupadas, las unidades deben instalarse en las bahías de bandeja correctas según el tipo de bandeja que tenga:

- Si su bandeja no es una bandeja DS460C, instale las unidades igualmente en el extremo izquierdo y el extremo derecho que se mueven hacia el centro. Por ejemplo, seis unidades en bahías 0-5 y seis unidades en bahías 18-23 de una bandeja DS224C.
- Si la bandeja es una bandeja DS460C, instale las unidades en la fila frontal (bahías de las unidades 0, 3, 6 y 9) de cada cajón. Para las unidades restantes, distribuya de manera uniforme en cada cajón llenando filas de cajones de la parte delantera hacia atrás. Si no tiene suficientes unidades para llenar filas, instálelas en parejas para que las unidades ocupen el lado izquierdo y derecho de un cajón de manera uniforme.

La instalación de unidades en la fila delantera de cada cajón permite un flujo de aire adecuado y evita el sobrecalentamiento.



Si no se instalan unidades en las bahías de bandeja correctas en bandejas medio llenas, cuando se produce un error y se reemplaza la unidad de contenedor, ONTAP no asigna automáticamente la propiedad. En este caso, la asignación de la nueva unidad de contenedor debe realizarse manualmente. Una vez que haya asignado la propiedad a la unidad de contenedor, ONTAP gestiona automáticamente todas las asignaciones de particiones y particiones de unidades que sean necesarias.

En algunas situaciones en las que la asignación automática no funciona, es necesario asignar manualmente la propiedad del disco mediante el `storage disk assign` comando:

- Si deshabilita la asignación automática, los nuevos discos no se encontrarán disponibles como repuestos hasta que se asignen manualmente a un nodo.
- Si desea que los discos se asignen automáticamente y tiene varias pilas o bandejas que deben tener una propiedad diferente, debe haber asignado manualmente un disco en cada pila o bandeja, de modo que la asignación de propiedad automática funcione en cada pila o bandeja.
- Si la asignación automática está habilitada y asigna manualmente una sola unidad a un nodo que no está especificado en la directiva activa, la asignación automática deja de funcionar y se muestra un mensaje EMS.

Aprenda cómo ["Asigne manualmente la propiedad del disco de los discos sin particionar"](#).

Aprenda cómo ["Asigne manualmente la propiedad del disco de los discos particionados"](#).

Mostrar propiedad de disco y partición

Es posible ver la propiedad de un disco para determinar qué nodo controla el

almacenamiento. También puede ver la propiedad de la partición en sistemas que utilizan discos compartidos.

Pasos

- 1. Mostrar la propiedad de los discos físicos:

```
storage disk show -ownership
```

```
cluster::> storage disk show -ownership
```

| Disk | Aggregate | Home | Owner | DR | Home | Home ID | Owner ID | DR |
|------------|-----------|-------|-------|----|------|------------|------------|----|
| Home ID | Reserver | Pool | | | | | | |
| 1.0.0 | aggr0_2 | node2 | node2 | - | | 2014941509 | 2014941509 | - |
| 2014941509 | Pool0 | | | | | | | |
| 1.0.1 | aggr0_2 | node2 | node2 | - | | 2014941509 | 2014941509 | - |
| 2014941509 | Pool0 | | | | | | | |
| 1.0.2 | aggr0_1 | node1 | node1 | - | | 2014941219 | 2014941219 | - |
| 2014941219 | Pool0 | | | | | | | |
| 1.0.3 | - | node1 | node1 | - | | 2014941219 | 2014941219 | - |
| 2014941219 | Pool0 | | | | | | | |

- 2. Si tiene un sistema que utiliza discos compartidos, puede mostrar la propiedad de la partición:

```
storage disk show -partition-ownership
```

```
cluster::> storage disk show -partition-ownership
```

| Container | Container | Root | Data | | | |
|------------|-----------|------------|------------|------------|------------|-------|
| Disk | Aggregate | Root Owner | Owner ID | Data Owner | Owner ID | Owner |
| Owner ID | | | | | | |
| 1.0.0 | - | node1 | 1886742616 | node1 | 1886742616 | node1 |
| 1886742616 | | | | | | |
| 1.0.1 | - | node1 | 1886742616 | node1 | 1886742616 | node1 |
| 1886742616 | | | | | | |
| 1.0.2 | - | node2 | 1886742657 | node2 | 1886742657 | node2 |
| 1886742657 | | | | | | |
| 1.0.3 | - | node2 | 1886742657 | node2 | 1886742657 | node2 |
| 1886742657 | | | | | | |

Cambie la configuración de la asignación automática de propiedad de disco

Puede utilizar el `storage disk option modify` comando para seleccionar una

política no predeterminada para la asignación automática de propiedad de disco o para deshabilitar la asignación automática de propiedad de disco.

Descubra "[asignación automática de propiedad de disco](#)".

Acerca de esta tarea

Si tiene una pareja de alta disponibilidad con solo DS460C bandejas, la política de asignación automática predeterminada es de medio cajón. No es posible cambiar a una política no predeterminada (bahía, bandeja, pila).

Pasos

- 1. Modificar la asignación automática de discos:
 - a. Si desea seleccionar una política no predeterminada, introduzca:

```
storage disk option modify -autoassign-policy autoassign_policy -node node_name
```

- Uso *stack* como la *autoassign_policy* para configurar la propiedad automática a nivel de pila o bucle.
- Uso *shelf* como la *autoassign_policy* para configurar la propiedad automática en el nivel de bandeja.
- Uso *bay* como la *autoassign_policy* para configurar la propiedad automática a nivel de bahía.

- b. Si desea deshabilitar la asignación automática de propiedad de disco, introduzca:

```
storage disk option modify -autoassign off -node node_name
```

- 2. Compruebe la configuración de asignación automática de los discos:

```
storage disk option show
```

```
cluster1::> storage disk option show
```

| Node | BKg. FW. Upd. | Auto Copy | Auto Assign | Auto Assign Policy |
|------------|---------------|-----------|-------------|--------------------|
| ----- | ----- | ----- | ----- | ----- |
| cluster1-1 | on | on | on | default |
| cluster1-2 | on | on | on | default |

Asigne manualmente la propiedad del disco de los discos sin particionar

Si el par de alta disponibilidad no está configurado para utilizar la asignación automática de propiedad de disco, debe asignar la propiedad manualmente. Si va a inicializar una pareja de alta disponibilidad que solo contiene DS460C bandejas, debe asignar manualmente la propiedad a las unidades raíz.

Acerca de esta tarea

- Si va a asignar la propiedad manualmente a un par de alta disponibilidad que no se está inicializando y no

tiene solo bandejas DS460C, use la opción 1.

- Si va a inicializar una pareja de HA que solo contiene DS460C bandejas, use la opción 2 para asignar manualmente la propiedad a las unidades raíz.

Opción 1: La mayoría de los pares de alta disponibilidad

Para un par de alta disponibilidad que no se está inicializando y no tiene solo DS460C bandejas, use este procedimiento para asignar la propiedad manualmente.

Acerca de esta tarea

- Los discos a los que asigna la propiedad deben estar en una bandeja que se conecte físicamente al nodo al que asigna la propiedad.
- Si va a utilizar discos en un nivel local (agregado):
 - Un nodo debe pertenecer a los discos para poder utilizarlos en un nivel local (agregado).
 - No es posible reasignar la propiedad de un disco que se está utilizando en un nivel local (agregado).

Pasos

1. Utilice la CLI para mostrar todos los discos sin propietario:

```
storage disk show -container-type unassigned
```

2. Asigne cada disco:

```
storage disk assign -disk disk_name -owner owner_name
```

Puede utilizar el carácter comodín para asignar más de un disco a la vez. Si va a reasignar un disco de repuesto que ya sea propiedad de un nodo diferente, deberá utilizar la opción « »-force».

Opción 2: Una pareja de alta disponibilidad con solo DS460C bandejas

Para una pareja de alta disponibilidad que va a inicializar y que solo tiene DS460C bandejas, utilice este procedimiento para asignar manualmente la propiedad a las unidades raíz.

Acerca de esta tarea

- Cuando se inicializa una pareja de alta disponibilidad que solo contiene DS460C bandejas, debe asignar manualmente las unidades raíz para cumplir con la política de medio cajón.

Después de la inicialización del par de alta disponibilidad (arranque), la asignación automática de propiedad de discos se habilita automáticamente y utiliza la política de medio cajón para asignar la propiedad a las unidades restantes (aparte de las unidades raíz) y a cualquier unidad añadida en el futuro, como reemplazar discos con fallos, responder a un mensaje de «repuestos bajos», o añadir capacidad.

Más información sobre la política de medio cajón en el tema ["Acerca de la asignación automática de propiedad de disco"](#).

- RAID necesita un mínimo de 10 unidades para cada par de alta disponibilidad (5 por cada nodo) para cualquiera de las 8TB unidades NL-SAS de una bandeja DS460C.

Pasos

1. Si las bandejas DS460C no están completamente llenas, complete los siguientes subpasos; de lo contrario, vaya al siguiente paso.

- a. En primer lugar, instale las unidades en la fila frontal (bahías de unidades 0, 3, 6 y 9) de cada cajón.

La instalación de unidades en la fila delantera de cada cajón permite un flujo de aire adecuado y evita el sobrecalentamiento.

- b. Para las unidades restantes, distribuir las de manera uniforme en cada cajón.

Llene las filas del cajón de adelante hacia atrás. Si no tiene suficientes unidades para llenar filas, instálelas en parejas para que las unidades ocupen el lado izquierdo y derecho de un cajón de manera uniforme.

En la siguiente ilustración, se muestra la numeración de las bahías de unidades y las ubicaciones de un cajón de DS460C.



2. Inicie sesión en el clustershell usando el LIF de gestión de nodos o la LIF de gestión de clústeres.
3. Asigne manualmente las unidades raíz en cada cajón para satisfacer la política de medio cajón mediante los siguientes subpasos:

La política de medio cajón hace que se asigne la mitad izquierda de las unidades de un cajón (bahías de 0 a 5) al nodo A y la mitad derecha de las unidades de un cajón (bahías de 6 a 11) al nodo B.

- a. Mostrar todos los discos sin propietario:

```
storage disk show -container-type unassigned`
```

- b. Asigne los discos raíz:

```
storage disk assign -disk disk_name -owner owner_name
```

Puede utilizar el carácter comodín para asignar más de un disco a la vez.

Asigne manualmente la propiedad de discos con particiones

Puede asignar manualmente la propiedad del disco contenedor o las particiones en los sistemas de partición avanzada de unidades (ADP). Si va a inicializar una pareja de alta disponibilidad que solo contiene bandejas DS460C, debe asignar manualmente la propiedad a las unidades de contenedor que incluyen particiones raíz.

Acerca de esta tarea

- El tipo de sistema de almacenamiento que tiene determina qué método de ADP es compatible, datos raíz (RD) o datos raíz (RD2).

Los sistemas de almacenamiento de FAS utilizan los sistemas de almacenamiento RD y AFF utilizan RD2.

- Si va a asignar la propiedad manualmente en un par de alta disponibilidad que no se está inicializando y que no tiene solo DS460C bandejas, use la opción 1 para asignar discos manualmente con particiones de datos raíz (RD) o utilice la opción 2 para asignar manualmente discos con particiones raíz-datos-(RD2).
- Si va a inicializar una pareja de HA que solo contiene DS460C bandejas, use la opción 3 para asignar manualmente la propiedad para las unidades de contenedor que tienen la partición raíz.

Opción 1: Asignar manualmente discos con partición de datos raíz (RD)

Para la partición de datos raíz, existen tres entidades propiedad (el disco contenedor y las dos particiones) que pertenecen colectivamente al par de alta disponibilidad.

Acerca de esta tarea

- El disco de contenedor y las dos particiones no necesitan ser propiedad del mismo nodo en el par de alta disponibilidad siempre y cuando sean propiedad de uno de los nodos del par de alta disponibilidad. Sin embargo, cuando se utiliza una partición en un nivel local (agregado), debe ser propiedad del mismo nodo que posee el nivel local.
- Si un disco de contenedor falla en una bandeja medio llena y se reemplaza, es posible que deba asignar manualmente la propiedad del disco porque ONTAP no siempre asigna automáticamente la propiedad en este caso.
- Una vez asignado el disco contenedor, el software de ONTAP gestiona automáticamente cualquier asignación de partición y partición que sea necesaria.

Pasos

1. Use la interfaz de línea de comandos para mostrar la propiedad actual del disco con particiones:

```
storage disk show -disk disk_name -partition-ownership
```

2. Configure el nivel de privilegio de la CLI en Advanced:

```
set -privilege advanced
```

3. Escriba el comando apropiado, en función de la entidad de propiedad a la que desee asignar la propiedad:

Si alguna de las entidades de propiedad ya está en propiedad, deberá incluir la opción « »-force».

| Si desea asignar la propiedad para... | Se usa este comando... |
|---------------------------------------|---|
| Disco de contenedor | <code>storage disk assign -disk <i>disk_name</i> -owner <i>owner_name</i></code> |
| Partición de datos | <code>storage disk assign -disk <i>disk_name</i> -owner <i>owner_name</i> -data true</code> |
| Partición raíz | <code>storage disk assign -disk <i>disk_name</i> -owner <i>owner_name</i> -root true</code> |

Opción 2: Asignar manualmente discos con particiones root-data-data (RD2)

Para la partición raíz-datos, hay cuatro entidades propiedad (el disco contenedor y las tres particiones) que pertenecen colectivamente al par de alta disponibilidad. La partición raíz-datos-datos crea una partición pequeña como la partición raíz y dos particiones de datos de tamaño similar para los datos.

Acerca de esta tarea

- Los parámetros deben utilizarse con `disk assign` comando para asignar la partición correcta de un disco particionado raíz-datos-datos. Estos parámetros no se pueden usar con discos que forman parte de un pool de almacenamiento. El valor predeterminado es «'false'».
 - La `-data1 true` el parámetro asigna la partición "data1" de un disco particionado root-data1-data2.
 - La `-data2 true` el parámetro asigna la partición "data2" de un disco particionado root-data1-data2.
- Si un disco de contenedor falla en una bandeja medio llena y se reemplaza, es posible que deba asignar manualmente la propiedad del disco porque ONTAP no siempre asigna automáticamente la propiedad en este caso.
- Una vez asignado el disco contenedor, el software de ONTAP gestiona automáticamente cualquier asignación de partición y partición que sea necesaria.

Pasos

1. Use la interfaz de línea de comandos para mostrar la propiedad actual del disco con particiones:

```
storage disk show -disk disk_name -partition-ownership
```

2. Configure el nivel de privilegio de la CLI en Advanced:

```
set -privilege advanced
```

3. Escriba el comando apropiado, en función de la entidad de propiedad a la que desee asignar la propiedad:

Si alguna de las entidades de propiedad ya está en propiedad, deberá incluir la opción «`-force`».

| Si desea asignar la propiedad para... | Se usa este comando... |
|---------------------------------------|--|
| Disco de contenedor | <code>storage disk assign -disk <i>disk_name</i> -owner <i>owner_name</i></code> |
| Partición Data1 | <code>storage disk assign -disk <i>disk_name</i> -owner <i>owner_name</i> -data1 true</code> |
| Data2 partición | <code>storage disk assign -disk <i>disk_name</i> -owner <i>owner_name</i> -data2 true</code> |
| Partición raíz | <code>storage disk assign -disk <i>disk_name</i> -owner <i>owner_name</i> -root true</code> |

Opción 3: Asigne manualmente DS460C unidades de contenedor que tengan la partición raíz

Si va a inicializar una pareja de alta disponibilidad que solo contiene DS460C bandejas, debe asignar manualmente la propiedad a las unidades de contenedor que tienen la partición raíz conforme a la política de medio cajón.

Acerca de esta tarea

- Cuando se inicializa una pareja de alta disponibilidad que solo contiene DS460C bandejas, el menú de arranque ADP (disponible con ONTAP 9.2 y versiones posteriores) las opciones 9a y 9b no admiten la asignación automática de propiedad de unidad. Debe asignar manualmente las unidades de contenedor que poseen la partición raíz mediante el cumplimiento de la política de medio cajón.

Después de la inicialización del par de alta disponibilidad (arranque), la asignación automática de propiedad de discos se habilita automáticamente y utiliza la política de medio cajón para asignar la propiedad a las unidades restantes (excepto las unidades de contenedores que tienen la partición raíz) y cualquier unidad que se añada en el futuro, como reemplazar unidades con errores. responder a un mensaje de «piezas de repuesto bajas» o añadir capacidad.

- Más información sobre la política de medio cajón en el tema ["Acerca de la asignación automática de propiedad de disco"](#).

Pasos

1. Si las bandejas DS460C no están completamente llenas, complete los siguientes subpasos; de lo contrario, vaya al siguiente paso.

- a. En primer lugar, instale las unidades en la fila frontal (bahías de unidades 0, 3, 6 y 9) de cada cajón.

La instalación de unidades en la fila delantera de cada cajón permite un flujo de aire adecuado y evita el sobrecalentamiento.

- b. Para las unidades restantes, distribuir las de manera uniforme en cada cajón.

Llene las filas del cajón de adelante hacia atrás. Si no tiene suficientes unidades para llenar filas, instálelas en parejas para que las unidades ocupen el lado izquierdo y derecho de un cajón de manera uniforme.

En la siguiente ilustración, se muestra la numeración de las bahías de unidades y las ubicaciones de un cajón de DS460C.



2. Inicie sesión en el clustershell usando el LIF de gestión de nodos o la LIF de gestión de clústeres.
3. Para cada cajón, asigne manualmente las unidades de contenedor que poseen la partición raíz mediante el cumplimiento de la política de medio cajón, mediante los siguientes subpasos:

La política de medio cajón hace que se asigne la mitad izquierda de las unidades de un cajón (bahías de 0 a 5) al nodo A y la mitad derecha de las unidades de un cajón (bahías de 6 a 11) al nodo B.

- a. Mostrar todos los discos sin propietario:


```
storage disk show -container-type unassigned
```
- b. Asigne las unidades de contenedor que tienen la partición raíz:


```
storage disk assign -disk disk_name -owner owner_name
```

Es posible usar el carácter comodín para asignar más de una unidad a la vez.

Establezca una configuración activo-pasivo en los nodos mediante la partición de datos raíz

Cuando un par de alta disponibilidad se configura para usar la partición de datos raíz por fábrica, la propiedad de las particiones de datos se divide entre ambos nodos de la pareja para su uso en una configuración activo-activo. Si desea utilizar el par ha en una configuración activo-pasivo, debe actualizar la propiedad de la partición antes de crear el nivel local de datos (agregado).

Lo que necesitará

- Debió haber decidido qué nodo será el activo y qué nodo será el pasivo.
- La conmutación por error del almacenamiento debe configurarse en el par de alta disponibilidad.

Acerca de esta tarea

Esta tarea se realiza en dos nodos: Nodo A y nodo B.

Este procedimiento está diseñado para nodos para los que no se ha creado ningún nivel local de datos (agregado) a partir de los discos con particiones.

Descubra "creación avanzada de particiones de disco".

Pasos

Todos los comandos se introducen en el shell del clúster.

- 1. Ver la propiedad actual de las particiones de datos:

```
storage aggregate show-spare-disks
```

El resultado muestra que la mitad de las particiones de datos son propiedad de un nodo y la mitad son propiedad del otro. Todas las particiones de datos deben ser de repuesto.

```
cluster1::> storage aggregate show-spare-disks

Original Owner: cluster1-01
Pool0
Partitioned Spares

Local
Local
Root Physical
Disk
Usable      Size
-----
1.0.0
0B 828.0GB
1.0.1
73.89GB 828.0GB
1.0.5
0B 828.0GB
1.0.6
0B 828.0GB
1.0.10
0B 828.0GB
1.0.11
0B 828.0GB
Type      RPM Checksum      Usable
-----
BSAS      7200 block      753.8GB
BSAS      7200 block      753.8GB
BSAS      7200 block      753.8GB
BSAS      7200 block      753.8GB
BSAS      7200 block      753.8GB
BSAS      7200 block      753.8GB
BSAS      7200 block      753.8GB

Original Owner: cluster1-02
Pool0
Partitioned Spares

Local
Local
Root Physical
Disk
Usable      Size
-----
Type      RPM Checksum      Usable
```

```

-----
1.0.2          BSAS      7200 block      753.8GB
0B  828.0GB
1.0.3          BSAS      7200 block      753.8GB
0B  828.0GB
1.0.4          BSAS      7200 block      753.8GB
0B  828.0GB
1.0.7          BSAS      7200 block      753.8GB
0B  828.0GB
1.0.8          BSAS      7200 block      753.8GB
73.89GB  828.0GB
1.0.9          BSAS      7200 block      753.8GB
0B  828.0GB
12 entries were displayed.

```

2. Introduzca el nivel de privilegio avanzado:

```
set advanced
```

3. Para cada partición de datos que pertenezca al nodo que será el nodo pasivo, asígnelo al nodo activo:

```
storage disk assign -force -data true -owner active_node_name -disk disk_name
```

No es necesario incluir la partición como parte del nombre del disco.

Debe introducir un comando similar al siguiente ejemplo para cada partición de datos que necesita reasignar:

```
storage disk assign -force -data true -owner cluster1-01 -disk 1.0.3
```

4. Confirme que todas las particiones están asignadas al nodo activo.

```

cluster1::*> storage aggregate show-spare-disks

Original Owner: cluster1-01
Pool0
  Partitioned Spares
                                Local
Local
                                Data
Root Physical
Disk          Type      RPM Checksum      Usable
Usable      Size
-----
1.0.0          BSAS      7200 block      753.8GB
0B  828.0GB

```

```

1.0.1          BSAS      7200 block      753.8GB
73.89GB  828.0GB
1.0.2          BSAS      7200 block      753.8GB
0B  828.0GB
1.0.3          BSAS      7200 block      753.8GB
0B  828.0GB
1.0.4          BSAS      7200 block      753.8GB
0B  828.0GB
1.0.5          BSAS      7200 block      753.8GB
0B  828.0GB
1.0.6          BSAS      7200 block      753.8GB
0B  828.0GB
1.0.7          BSAS      7200 block      753.8GB
0B  828.0GB
1.0.8          BSAS      7200 block      753.8GB
0B  828.0GB
1.0.9          BSAS      7200 block      753.8GB
0B  828.0GB
1.0.10         BSAS      7200 block      753.8GB
0B  828.0GB
1.0.11         BSAS      7200 block      753.8GB
0B  828.0GB

```

Original Owner: cluster1-02

Pool0

Partitioned Spares

Local

Local

Data

Root Physical

Disk

Type

RPM Checksum

Usable

Usable Size

```

-----
-----
1.0.8          BSAS      7200 block      0B

```

73.89GB 828.0GB

13 entries were displayed.

Tenga en cuenta que cluster1-02 sigue teniendo una partición raíz de repuesto.

5. Devolver al privilegio administrativo:

```
set admin
```

6. Cree su agregado de datos, dejando al menos una partición de datos como reserva:

```
storage aggregate create new_aggr_name -diskcount number_of_partitions -node
```

active_node_name

El agregado de datos se crea y pertenece al nodo activo.

Establezca una configuración activa-pasiva en los nodos mediante la partición de datos raíz

Cuando un par de alta disponibilidad se configura de fábrica para usar la partición de datos raíz, la propiedad de las particiones de datos se divide entre ambos nodos de la pareja para su uso en una configuración activo-activo. Si desea utilizar el par ha en una configuración activo-pasivo, debe actualizar la propiedad de la partición antes de crear el nivel local de datos (agregado).

Lo que necesitará

- Debió haber decidido qué nodo será el activo y qué nodo será el pasivo.
- La conmutación por error del almacenamiento debe configurarse en el par de alta disponibilidad.

Acerca de esta tarea

Esta tarea se realiza en dos nodos: Nodo A y nodo B.

Este procedimiento está diseñado para nodos para los que no se ha creado ningún nivel local de datos (agregado) a partir de los discos con particiones.

Descubra "[creación avanzada de particiones de disco](#)".

Pasos

Todos los comandos se introducen en el shell del clúster.

1. Ver la propiedad actual de las particiones de datos:

```
storage aggregate show-spare-disks -original-owner passive_node_name -fields  
local-usable-data1-size, local-usable-data2-size
```

El resultado muestra que la mitad de las particiones de datos son propiedad de un nodo y la mitad son propiedad del otro. Todas las particiones de datos deben ser de repuesto.

2. Introduzca el nivel de privilegio avanzado:

```
set advanced
```

3. Para cada partición data1 propiedad del nodo que será el nodo pasivo, asígnelo al nodo activo:

```
storage disk assign -force -data1 -owner active_node_name -disk disk_name
```

No es necesario incluir la partición como parte del nombre del disco

4. Para cada partición data2 del nodo que será el nodo pasivo, asígnelo al nodo activo:

```
storage disk assign -force -data2 -owner active_node_name -disk disk_name
```

No es necesario incluir la partición como parte del nombre del disco

5. Confirme que todas las particiones están asignadas al nodo activo:

```
cluster1::*> storage aggregate show-spare-disks

Original Owner: cluster1-01
Pool0
Partitioned Spares

Local
Local
Data
Root Physical
Disk          Type      RPM Checksum  Usable
Usable      Size
-----
-----
1.0.0        BSAS      7200 block    753.8GB
0B  828.0GB
1.0.1        BSAS      7200 block    753.8GB
73.89GB  828.0GB
1.0.2        BSAS      7200 block    753.8GB
0B  828.0GB
1.0.3        BSAS      7200 block    753.8GB
0B  828.0GB
1.0.4        BSAS      7200 block    753.8GB
0B  828.0GB
1.0.5        BSAS      7200 block    753.8GB
0B  828.0GB
1.0.6        BSAS      7200 block    753.8GB
0B  828.0GB
1.0.7        BSAS      7200 block    753.8GB
0B  828.0GB
1.0.8        BSAS      7200 block    753.8GB
0B  828.0GB
1.0.9        BSAS      7200 block    753.8GB
0B  828.0GB
1.0.10       BSAS      7200 block    753.8GB
0B  828.0GB
1.0.11       BSAS      7200 block    753.8GB
0B  828.0GB

Original Owner: cluster1-02
Pool0
Partitioned Spares

Local
Local
Data
```

```

Root Physical
Disk                               Type      RPM  Checksum      Usable
Usable      Size
-----
1.0.8                               BSAS     7200  block          0B
73.89GB    828.0GB
13 entries were displayed.

```

Tenga en cuenta que cluster1-02 sigue teniendo una partición raíz de repuesto.

6. Devolver al privilegio administrativo:

```
set admin
```

7. Cree su agregado de datos, dejando al menos una partición de datos como reserva:

```
storage aggregate create new_aggr_name -diskcount number_of_partitions -node
active_node_name
```

El agregado de datos se crea y pertenece al nodo activo.

8. Como alternativa, puede utilizar la distribución de agregados recomendada de ONTAP, que incluye prácticas recomendadas para la distribución de grupos RAID y el número de repuestos:

```
storage aggregate auto-provision
```

Quitar la propiedad de un disco

ONTAP escribe la información de propiedad del disco en el disco. Antes de quitar un disco de repuesto o su bandeja de un nodo, se debe eliminar la información de propiedad para que se pueda integrar correctamente en otro nodo.



Si el disco está particionado para crear particiones de datos raíz y ejecuta ONTAP 9.10.1 o una versión posterior, comuníquese con el soporte técnico de NetApp para obtener ayuda para eliminar propiedad. Para obtener más información, consulte ["Artículo de la base de conocimientos: Error al eliminar el propietario del disco"](#).

Lo que necesitará

El disco del que desea eliminar la propiedad debe cumplir los siguientes requisitos:

- Debe ser un disco de repuesto.

No se puede eliminar la propiedad de un disco que se esté utilizando en un nivel local (agregado).

- No puede estar en el centro de mantenimiento.
- No se puede estar sometiendo a un saneamiento.
- No puede haber fallado.

No es necesario eliminar la propiedad de un disco con errores.

Acerca de esta tarea

Si la asignación automática de discos está habilitada, ONTAP podría reasignar automáticamente la propiedad antes de quitar el disco del nodo. Por este motivo, se deshabilita la asignación de propiedad automática hasta que se quita el disco y, a continuación, se vuelve a habilitar.

Pasos

1. Si la asignación automática de propiedad de disco está activada, utilice la CLI para desactivarla:

```
storage disk option modify -node node_name -autoassign off
```

2. Si es necesario, repita el paso anterior para el partner de alta disponibilidad del nodo.
3. Elimine la información de propiedad del software del disco:

```
storage disk removeowner disk_name
```

Para eliminar la información de propiedad de varios discos, use una lista separada por comas.

Ejemplo:

```
storage disk removeowner sys1:0a.23,sys1:0a.24,sys1:0a.25
```

4. Si el disco está particionado para la partición de datos raíz y está ejecutando ONTAP 9.9.1 o una versión anterior, elimine la propiedad de las particiones:

```
storage disk removeowner -disk disk_name -root true
```

```
storage disk removeowner -disk disk_name -data true
```

Ambas particiones ya no son propiedad de ningún nodo.

5. Si anteriormente ha desactivado la asignación automática de propiedad de disco, actívela después de que el disco se haya eliminado o reasignado:

```
storage disk option modify -node node_name -autoassign on
```

6. Si es necesario, repita el paso anterior para el partner de alta disponibilidad del nodo.

Quitar un disco con errores

Un disco que ha fallado completamente ya no tiene en cuenta ONTAP como un disco utilizable y puede desconectar inmediatamente el disco de la bandeja de discos. Sin embargo, debería dejar un disco parcialmente fallido conectado lo suficiente como para que finalice el proceso de recuperación de RAID rápida.

Acerca de esta tarea

Si va a quitar un disco porque ha fallado o porque está produciendo mensajes de error excesivos, no debe volver a utilizar el disco en este o cualquier otro sistema de almacenamiento.

Pasos

1. Utilice la interfaz de línea de comandos para encontrar el ID del disco con errores:

```
storage disk show -broken
```

Si el disco no aparece en la lista de discos con errores, puede que haya fallado parcialmente, con una recuperación de RAID rápida en proceso. En este caso, debe esperar hasta que el disco esté presente en la lista de discos defectuosos (lo que significa que el proceso de recuperación rápida de RAID está completo) antes de quitar el disco.

2. Determine la ubicación física del disco que desea quitar:

```
storage disk set-led -action on -disk disk_name 2
```

El LED de fallo de la parte frontal del disco se ilumina.

3. Quite el disco de la bandeja de discos siguiendo las instrucciones de la guía de hardware para su modelo de bandeja de discos.

El saneamiento de disco

Descripción general del saneamiento de disco

El saneamiento de disco es el proceso de destrucción física de datos mediante la sobrescritura de discos o SSD con patrones de bytes especificados o datos aleatorios, de modo que la recuperación de los datos originales se convierta en imposible. El uso del proceso de saneamiento garantiza que nadie pueda recuperar los datos en los discos.

Esta funcionalidad está disponible en todas las versiones de ONTAP 9 e empezando por ONTAP 9.6 en modo de mantenimiento.

El proceso de saneamiento de disco utiliza tres patrones de sobrescritura de bytes predeterminados sucesivos o especificados por el usuario para hasta siete ciclos por operación. El patrón de sobrescritura aleatorio se repite para cada ciclo.

Según la capacidad del disco, los patrones y la cantidad de ciclos, el proceso puede llevar varias horas. El saneamiento se ejecuta en segundo plano. Puede iniciar, detener y mostrar el estado del proceso de saneamiento. El proceso de saneamiento contiene dos fases: La "fase de formato" y la "fase de sobrescritura de patrón".

Fase de formato

La operación realizada para la fase de formato depende de la clase de disco que se está saneando, como se muestra en la siguiente tabla:

| Clase de disco | Operación de fase de formateo |
|--------------------|-------------------------------|
| HDD de capacidad | Omitida |
| HDD de rendimiento | Operación de formato SCSI |
| SSD | Operación de higienizar SCSI |

Fase de sobrescritura de patrones

Los patrones de sobrescritura especificados se repiten para el número de ciclos especificado.

Cuando el proceso de saneamiento se completa, los discos especificados están en estado sanitizado. No se

devuelven al estado de reserva automáticamente. Debe devolver los discos sanitizados al pool de repuesto antes de que los discos recién sanitizados estén disponibles para poder añadir a otro agregado.

Cuando no se puede realizar el saneamiento de disco

El saneamiento de disco no es compatible con todos los tipos de disco. Además, hay circunstancias en las que no se puede realizar el saneamiento de disco.

- No es compatible con todos los números de pieza de SSD.

Para obtener más información sobre qué números de pieza de SSD admiten el saneamiento de disco, consulte ["Hardware Universe"](#).

- No es compatible con el modo de toma de control para sistemas de un par de alta disponibilidad.
- No se puede realizar en discos que hayan fallado debido a problemas de legibilidad o de escritura.
- No realiza su fase de formato en unidades ATA.
- Si está utilizando el patrón aleatorio, no se puede realizar en más de 100 discos a la vez.
- No es compatible con los LUN de cabina.
- Si desinfecte ambos discos SES en la misma bandeja ESH al mismo tiempo, verá errores en la consola sobre el acceso a esa bandeja y no se producirán advertencias durante el saneamiento.

Sin embargo, el acceso a los datos a esa bandeja no se interrumpe.

Qué ocurre si se interrumpe el saneamiento de disco

Si el saneamiento de disco se interrumpe mediante la intervención del usuario o un evento inesperado, como una interrupción del suministro eléctrico, ONTAP realiza acciones para devolver los discos que se estaban saneando a un estado conocido, pero también debe realizar acciones antes de que finalice el proceso de saneamiento.

El saneamiento de disco es una operación de ejecución prolongada. Si el proceso de saneamiento se interrumpe por un fallo de alimentación, pánico del sistema o intervención manual, el proceso de saneamiento se debe repetir desde el principio. El disco no está designado como sanitizado.

Si se interrumpe la fase de formato del saneamiento de disco, ONTAP debe recuperar todos los discos dañados por la interrupción. Tras el reinicio del sistema y una vez cada hora, ONTAP comprueba si hay un disco de saneamiento de destino que no haya completado la fase de formato de su saneamiento. Si se encuentra algún disco de este tipo, ONTAP los recupera. El método de recuperación depende del tipo de disco. Tras recuperar un disco, puede volver a ejecutar el proceso de saneamiento en ese disco; para los HDD, puede utilizar el `-s` opción para especificar que la fase de formato no se repita de nuevo.

Consejos para crear y realizar copias de seguridad de niveles locales (agregados) que contienen datos que se van a sanitizar

Si crea o realiza backups de niveles locales (agregados) para contener datos que deban sanarse, siguiendo algunas directrices simples reducirá el tiempo que lleva desinfectar los datos.

- Asegúrese de que los niveles locales que contienen datos confidenciales no sean mayores de lo que necesitan.

Si son más grandes de lo necesario, el saneamiento requiere más tiempo, espacio en disco y ancho de banda.

- Al realizar un backup de niveles locales que contengan datos confidenciales, se debe evitar realizar un backup del nivel local que también contenga grandes cantidades de datos no confidenciales.

De este modo se reducen los recursos necesarios para mover datos no confidenciales antes de sanitizar datos confidenciales.

Desinfecte un disco

El saneamiento de un disco le permite eliminar datos de un disco o un conjunto de discos en sistemas retirados del servicio o inoperables para que los datos nunca puedan recuperarse.

Existen dos métodos para desinfectar discos utilizando la CLI:

Desinfecte un disco con `storage encryption disk sanitize` comando (ONTAP 9.6 y versiones posteriores)

A partir de ONTAP 9.6, puede realizar un saneamiento de disco en modo de mantenimiento.

Antes de empezar

- Los discos no pueden ser discos de autocifrado (SED).

Debe utilizar el `storage encryption disk sanitize` Comando para desinfectar un SED.

["Cifrado de datos en reposo"](#)

Pasos

1. Arranque en modo de mantenimiento.

- a. Para salir del shell actual, introduzca `halt`.

Aparece el aviso del CARGADOR.

- b. Para entrar en el modo de mantenimiento, introduzca `boot_ontap maint`.

Después de ver alguna información, se muestra el símbolo del sistema del modo de mantenimiento.

2. Si los discos que desea desinfectar se crean particiones, desparticionar cada disco:



El comando para anular la partición de un disco solo está disponible a nivel de diagnóstico y solo se debe realizar bajo la supervisión del soporte de NetApp. Es muy recomendable que se ponga en contacto con el soporte de NetApp antes de continuar. También puede consultar el artículo de la base de conocimientos ["Cómo desparticionar una unidad de reserva en ONTAP"](#)

```
disk unpartition disk_name
```

3. Desinfecte los discos especificados:

```
disk sanitize start [-p pattern1|-r [-p pattern2|-r [-p pattern3|-r]]] [-c cycle_count] disk_list
```



No apague el nodo, interrumpa la conectividad de almacenamiento ni elimine los discos de destino mientras se está saneando. Si se interrumpe la operación durante la fase de formateo, se debe reiniciar la fase de formateo y se debe permitir que finalice antes de que los discos se saneen y estén listos para ser devueltos al pool de reserva. Si necesita anular el proceso de saneamiento, puede hacerlo utilizando el `disk sanitize abort` comando. Si los discos especificados se están sometiendo a la fase de formateo del saneamiento, la interrupción no se producirá hasta que se complete la fase.

``-p` `_pattern1_` `-p` `_pattern2_` `-p` `_pattern3_`` especifica un ciclo de uno a tres patrones de sobrescritura de bytes hex definidos por el usuario que se pueden aplicar sucesivamente a los discos que se están saneando. El patrón predeterminado son tres pasadas, usando 0x55 para la primera pasada, 0xaa para la segunda pasada y 0x3c para la tercera pasada.

`-r` reemplaza una sobrescritura con patrón por una sobrescritura aleatoria para cualquiera de las pasadas o para todas ellas.

`-c cycle_count` especifica el número de veces que se aplican los patrones de sobrescritura especificados. El valor predeterminado es un ciclo. El valor máximo es siete ciclos.

`disk_list` Especifica una lista separada por espacio de los ID de los discos de repuesto que se van a desinfectar.

4. Si lo desea, compruebe el estado del proceso de saneamiento de disco:

```
disk sanitize status [disk_list]
```

5. Una vez completado el proceso de saneamiento, devuelva los discos al estado de reserva de cada disco:

```
disk sanitize release disk_name
```

6. Salga del modo de mantenimiento.

Desinfecte un disco con `y#8220;nodeshell` comandos (todas las versiones de ONTAP 9)

Para todas las versiones de ONTAP 9, cuando se habilita el saneamiento de disco mediante comandos `nodeshell`, se deshabilitan algunos comandos ONTAP de bajo nivel. Cuando el saneamiento de disco está habilitado en un nodo, no se puede deshabilitar.

Antes de empezar

- Los discos deben ser discos de repuesto; deben ser propiedad de un nodo, pero no se usan en un nivel local (agregado).

Si los discos están particionados, ninguna partición puede estar en uso en un nivel local (agregado).

- Los discos no pueden ser discos de autocifrado (SED).

Debe utilizar el `storage encryption disk sanitize` Comando para desinfectar un SED.

["Cifrado de datos en reposo"](#)

- Los discos no pueden formar parte de una agrupación de almacenamiento.

Pasos

1. Si los discos que desea desinfectar se crean particiones, desparticionar cada disco:



El comando para anular la partición de un disco solo está disponible a nivel de diagnóstico y solo se debe realizar bajo la supervisión del soporte de NetApp. **Es muy recomendable que se ponga en contacto con el servicio de asistencia de NetApp antes de continuar.** También puede consultar el artículo de la base de conocimientos ["Cómo desparticionar una unidad de reserva en ONTAP"](#).

```
disk unpartition disk_name
```

2. Introduzca el nodo que posee los discos que desea desinfectar:

```
system node run -node node_name
```

3. Habilitar el saneamiento de disco:

```
options licensed_feature.disk_sanitization.enable on
```

Se le pide que confirme el comando porque es irreversible.

4. Cambie al nivel de privilegio avanzado de Nodeseinferno:

```
priv set advanced
```

5. Desinfecte los discos especificados:

```
disk sanitize start [-p pattern1|-r [-p pattern2|-r [-p pattern3|-r]]] [-c cycle_count] disk_list
```



No apague el nodo, interrumpa la conectividad de almacenamiento ni elimine el destino discos mientras se sanean. Si el saneamiento se interrumpe durante la fase de formateo, el formateo la fase debe reiniciarse y dejarse terminar antes de que los discos estén higienizados y listos para ser devuelto al pool de reserva. Si necesita cancelar el proceso de saneamiento, puede hacerlo mediante el saneamiento del disco comando abort. Si los discos especificados están pasando por la fase de formateo de saneamiento, el la interrupción no se produce hasta que se completa la fase.

`-p pattern1 -p pattern2 -p pattern3` especifica un ciclo de uno a tres bytes hexadecimales definidos por el usuario patrones de sobrescritura que se pueden aplicar sucesivamente a los discos que se están saneando. El valor predeterminado el patrón es de tres pasadas, usando 0x55 para la primera pasada, 0xaa para la segunda pasada, y 0x3c para la tercera pasada.

`-r` reemplaza una sobrescritura con patrón por una sobrescritura aleatoria para cualquiera de las pasadas o para todas ellas.

`-c cycle_count` especifica el número de veces que se aplican los patrones de sobrescritura especificados.

El valor predeterminado es un ciclo. El valor máximo es siete ciclos.

`disk_list` Especifica una lista separada por espacio de los ID de los discos de repuesto que se van a desinfectar.

6. Si desea comprobar el estado del proceso de saneamiento de disco:

```
disk sanitize status [disk_list]
```

7. Una vez finalizado el proceso de saneamiento, devuelva los discos a estado de repuesto:

```
disk sanitize release disk_name
```

8. Volver al nivel de privilegios de administración nodesinferno:

```
priv set admin
```

9. Volver a la CLI de ONTAP:

```
exit
```

10. Determine si todos los discos se han devuelto al estado de repuesto:

```
storage aggregate show-spare-disks
```

| | |
|-------|-------------------------|
| Si... | Realice lo siguiente... |
|-------|-------------------------|

| | |
|--|---|
| Todos los discos sanitizados se enumeran como repuestos | Ha terminado. Los discos se sanean y están en estado de repuesto. |
| Algunos de los discos sanitizados no aparecen como repuestos | <p>Complete los siguientes pasos:</p> <p>a. Entre en el modo de privilegio avanzado:</p> <pre>set -privilege advanced</pre> <p>b. Asigne los discos sanitizados sin asignar al nodo adecuado para cada disco:</p> <pre>storage disk assign -disk <i>disk_name</i> -owner <i>node_name</i></pre> <p>c. Devuelva los discos al estado de repuesto de cada disco:</p> <pre>storage disk unfail -disk <i>disk_name</i> -s -q</pre> <p>d. Volver al modo administrativo:</p> <pre>set -privilege admin</pre> |

Resultado

Los discos especificados están sancionados y designados como piezas de repuesto. Los números de serie de los discos sanitizados se escriben en `/etc/log/sanitized_disks`.

Los registros de saneamiento de los discos especificados, que muestran lo que se completó en cada disco, se escriben en `/mroot/etc/log/sanitization.log`.

Comandos para gestionar discos

Puede utilizar el `storage disk` y.. `storage aggregate` comandos para gestionar los discos.

| Si desea... | Se usa este comando... |
|---|---|
| Muestra una lista de los discos de repuesto, incluidos los discos con particiones, por propietario | <code>storage aggregate show-spare-disks</code> |
| Mostrar el tipo de RAID de disco, el uso actual y el grupo RAID por agregado | <code>storage aggregate show-status</code> |
| Mostrar el tipo de RAID, el uso actual, el agregado y el grupo RAID, incluidos los repuestos, para discos físicos | <code>storage disk show -raid</code> |
| Muestre una lista de discos con errores | <code>storage disk show -broken</code> |

| | |
|--|--|
| Muestre el nombre de la unidad de clúster previo (nodescope) para un disco | <code>storage disk show -primary-paths (avanzado)</code> |
| Ilumina el LED de un disco o una bandeja en particular | <code>storage disk set-led</code> |
| Mostrar el tipo de suma de comprobación para un disco específico | <code>storage disk show -fields checksum-compatibility</code> |
| Muestre el tipo de suma de comprobación para todos los discos de repuesto | <code>storage disk show -fields checksum-compatibility -container-type spare</code> |
| Muestra información de ubicación y conectividad de los discos | <code>storage disk show -fields disk,primary-port,secondary-name,secondary-port,shelf,bay</code> |
| Mostrar los nombres de discos previos a los clústeres para discos específicos | <code>storage disk show -disk diskname -fields diskpathnames</code> |
| Muestre la lista de discos en el centro de mantenimiento | <code>storage disk show -maintenance</code> |
| Muestra la vida útil de los SSD | <code>storage disk show -ssd-wear</code> |
| Desparticionar un disco compartido | <code>storage disk unpartition (disponible a nivel de diagnóstico)</code> |
| Ponga a cero todos los discos que no estén a cero | <code>storage disk zerospares</code> |
| Detenga un proceso de saneamiento en curso en uno o más discos especificados | <code>system node run -node nodename -command disk sanitize</code> |
| Mostrar información del disco de cifrado de almacenamiento | <code>storage encryption disk show</code> |
| Recupere las claves de autenticación de todos los servidores de gestión de claves vinculados | <code>security key-manager restore</code> |

Información relacionada

["Comandos de ONTAP 9"](#)

Comandos para mostrar información de uso de espacio

Utilice la `storage aggregate y.. volume` Comandos para ver cómo se utiliza el espacio en los agregados y volúmenes y en sus copias snapshot.

| Para mostrar información acerca de... | Se usa este comando... |
|--|--|
| Agregados, incluidos detalles sobre los porcentajes de espacio utilizados y disponibles, el tamaño de reserva de Snapshot y otra información de uso de espacio | <code>storage aggregate show</code> <code>storage aggregate show-space -fields snap-size-total,used-including-snapshot-reserve</code> |
| Cómo se usan los discos y los grupos RAID en un agregado y el estado de RAID | <code>storage aggregate show-status</code> |
| La cantidad de espacio en disco que se reclamaría si eliminó una copia de Snapshot específica | <code>volume snapshot compute-reclaimable</code> |
| La cantidad de espacio utilizada por un volumen | <code>volume show -fields size,used,available,percent-used</code> <code>volume show-space</code> |
| La cantidad de espacio utilizada por un volumen en el agregado que contiene | <code>volume show-footprint</code> |

Información relacionada

["Comandos de ONTAP 9"](#)

Comandos para mostrar información acerca de las bandejas de almacenamiento

Utilice la `storage shelf show` comando para mostrar información de configuración y errores de las bandejas de discos.

| Si desea mostrar... | Se usa este comando... |
|---|---|
| Información general sobre la configuración de bandejas y el estado del hardware | <code>storage shelf show</code> |
| Información detallada de una bandeja específica, incluido el ID de pila | <code>storage shelf show -shelf</code> |
| Sin resolver, el cliente puede actuar, errores por bandeja | <code>storage shelf show -errors</code> |
| Información sobre la bahía | <code>storage shelf show -bay</code> |
| Información sobre la conectividad | <code>storage shelf show -connectivity</code> |
| Información de refrigeración, incluidos los sensores de temperatura y los ventiladores de refrigeración | <code>storage shelf show -cooling</code> |
| Información sobre los módulos de E/S. | <code>storage shelf show -module</code> |

| Si desea mostrar... | Se usa este comando... |
|--|--|
| Información del puerto | <code>storage shelf show -port</code> |
| Información de alimentación, incluidas las fuentes de alimentación (unidades de alimentación), los sensores de corriente y los sensores de tensión | <code>storage shelf show -power</code> |

Información relacionada

["Comandos de ONTAP 9"](#)

Gestione las configuraciones de RAID

Información general sobre la gestión de configuraciones de RAID

Puede realizar varios procedimientos para administrar las configuraciones de RAID en su sistema.

- **Aspectos de la administración de configuraciones RAID:**
 - ["Políticas de RAID predeterminadas para niveles locales \(agregados\)"](#)
 - ["Niveles de protección RAID para discos"](#)
- **Información de unidad y grupo RAID para un nivel local (agregado)**
 - ["Determinar la información de las unidades y los grupos RAID para un nivel local \(agregado\)"](#)
- **Conversiones de configuración RAID**
 - ["Convierta de RAID-DP a RAID-TEC"](#)
 - ["Conversión de RAID-TEC a RAID-DP"](#)
- **Tamaño del grupo RAID**
 - ["Consideraciones que tener en cuenta para configurar grupos RAID"](#)
 - ["Personalice el tamaño de su grupo RAID"](#)

Políticas de RAID predeterminadas para niveles locales (agregados)

RAID-DP o RAID-TEC es la política de RAID predeterminada para todos los nuevos niveles locales (agregados). La política de RAID determina la protección de paridad que tiene en caso de un error en el disco.

RAID-DP proporciona protección de doble paridad en caso de un fallo de uno o dos discos. RAID-DP es la política de RAID predeterminada para los siguientes tipos de nivel local (agregado):

- Niveles locales all-flash
- Niveles locales de Flash Pool
- Niveles locales de las unidades de disco duro de alto rendimiento (HDD)

RAID-TEC es compatible con todos los tipos de disco y todas las plataformas, incluido AFF. Los niveles locales que contienen discos de mayor tamaño tienen una mayor posibilidad de que se produzcan fallos de disco simultáneos. RAID-TEC ayuda a mitigar este riesgo ofreciendo protección de triple paridad para que sus

datos puedan sobrevivir a tres fallos simultáneos del disco. RAID-TEC es la política RAID predeterminada para los niveles locales de las unidades de disco duro de capacidad con discos de 6 TB o mayores.

Cada tipo de política de RAID requiere un número mínimo de discos:

- RAID-DP: Mínimo de 5 discos
- RAID-TEC: Mínimo de 7 discos

Niveles de protección RAID para discos

ONTAP admite tres niveles de protección RAID para niveles locales (agregados). El nivel de protección RAID determina el número de discos de paridad disponibles para la recuperación de datos en caso de fallos de disco.

Con la protección RAID, si se produce un error en el disco de datos en un grupo RAID, ONTAP puede reemplazar el disco con error por un disco de repuesto y utilizar los datos de paridad para reconstruir los datos del disco con error.

- **RAID4**

Con la protección RAID4, ONTAP puede utilizar un disco de reserva para reemplazar y reconstruir los datos de un disco con fallo en el grupo RAID.

- **RAID-DP**

Con la protección RAID-DP, ONTAP puede usar hasta dos discos de repuesto para reemplazar y reconstruir los datos desde hasta dos discos con fallos simultáneos en el grupo RAID.

- **RAID-TEC**

Con la protección RAID-TEC, ONTAP puede usar hasta tres discos de repuesto para reemplazar y reconstruir los datos de hasta tres discos con fallos simultáneos en el grupo RAID.

Información de unidades y grupos RAID para un nivel local (agregado)

Algunas tareas de administración de nivel local (agregado) requieren conocer qué tipos de unidades componen el nivel local, su tamaño, suma de comprobación y estado, si se comparten con otros niveles locales, y el tamaño y la composición de los grupos RAID.

Paso

1. Muestre las unidades del agregado, por grupo RAID:

```
storage aggregate show-status aggr_name
```

Las unidades se muestran para cada grupo RAID en el agregado.

Puede ver el tipo de RAID de la unidad (datos, paridad, dparidad) en el `Position` columna. Si la `Position` la columna muestra `shared`, Entonces la unidad es compartida: Si es una unidad de disco duro, es un disco particionado; si es una unidad SSD, forma parte de un pool de almacenamiento.

```
cluster1::> storage aggregate show-status nodeA_fp_1
```

Owner Node: cluster1-a

Aggregate: nodeA_fp_1 (online, mixed_raid_type, hybrid) (block checksums)

Plex: /nodeA_fp_1/plex0 (online, normal, active, pool0)

RAID Group /nodeA_fp_1/plex0/rg0 (normal, block checksums, raid_dp)

| Position | Disk | Pool | Type | RPM | Usable Size | Physical Size | Status |
|----------|--------|------|------|-------|-------------|---------------|----------|
| shared | 2.0.1 | 0 | SAS | 10000 | 472.9GB | 547.1GB | (normal) |
| shared | 2.0.3 | 0 | SAS | 10000 | 472.9GB | 547.1GB | (normal) |
| shared | 2.0.5 | 0 | SAS | 10000 | 472.9GB | 547.1GB | (normal) |
| shared | 2.0.7 | 0 | SAS | 10000 | 472.9GB | 547.1GB | (normal) |
| shared | 2.0.9 | 0 | SAS | 10000 | 472.9GB | 547.1GB | (normal) |
| shared | 2.0.11 | 0 | SAS | 10000 | 472.9GB | 547.1GB | (normal) |

RAID Group /nodeA_flashpool_1/plex0/rg1

(normal, block checksums, raid4) (Storage Pool: SmallSP)

| Position | Disk | Pool | Type | RPM | Usable Size | Physical Size | Status |
|----------|--------|------|------|-----|-------------|---------------|----------|
| shared | 2.0.13 | 0 | SSD | - | 186.2GB | 745.2GB | (normal) |
| shared | 2.0.12 | 0 | SSD | - | 186.2GB | 745.2GB | (normal) |

8 entries were displayed.

Convierta de RAID-DP a RAID-TEC

Si desea disfrutar de la protección añadida de la triple paridad, puede convertir de RAID-DP a RAID-TEC. Se recomienda a RAID-TEC si el tamaño de los discos utilizados en el nivel local (agregado) es mayor que 4 TIB.

Lo que necesitará

El nivel local (agregado) que se va a convertir debe tener un mínimo de siete discos.

Acerca de esta tarea

Los niveles locales de la unidad de disco duro (HDD) pueden convertirse de RAID-DP a RAID-TEC. Esto incluye niveles de HDD en niveles locales de Flash Pool.

Pasos

1. Compruebe que el agregado está en línea y que tiene un mínimo de seis discos:

```
storage aggregate show-status -aggregate aggregate_name
```

2. Convierta el agregado de RAID-DP a RAID-TEC:

```
storage aggregate modify -aggregate aggregate_name -raidtype raid_tec
```

3. Compruebe que la política RAID del agregado es RAID-TEC:

```
storage aggregate show aggregate_name
```

Conversión de RAID-TEC a RAID-DP

Si reduce el tamaño de su nivel local (agregado) y ya no necesita la triple paridad, puede convertir su política de RAID de RAID-TEC a RAID-DP y reducir el número de discos que necesita para la paridad de RAID.

Lo que necesitará

El tamaño máximo del grupo RAID para RAID-TEC es más grande que el tamaño máximo de grupo de RAID para RAID-DP. Si el tamaño del grupo RAID-TEC más grande no se encuentra dentro de los límites de RAID-DP, no se puede convertir a RAID-DP.

Pasos

1. Compruebe que el agregado está en línea y que tiene un mínimo de seis discos:

```
storage aggregate show-status -aggregate aggregate_name
```

2. Convierta el agregado de RAID-TEC a RAID-DP:

```
storage aggregate modify -aggregate aggregate_name -raidtype raid_dp
```

3. Compruebe que la política de RAID del agregado es RAID-DP:

```
storage aggregate show aggregate_name
```

Consideraciones que tener en cuenta para configurar grupos RAID

Para configurar un tamaño de grupo RAID óptimo, se deben sacrificar factores. Debe decidir qué factores (la velocidad de la recompilación de RAID, la garantía de riesgo de pérdida de datos debido al fallo de la unidad, la optimización del rendimiento de I/O y la maximización del espacio de almacenamiento de datos) son los más importantes para el agregado (nivel local) que se está configurando.

Cuando se crean grupos RAID de mayor tamaño, se maximiza el espacio disponible para el almacenamiento de datos para la misma cantidad de almacenamiento utilizado para la paridad (también conocido como « impuesto de paridad»). Por otro lado, cuando un disco falla en un grupo RAID mayor, el tiempo de reconstrucción aumenta, lo que afecta al rendimiento durante un período de tiempo más prolongado. Además, al tener más discos en un grupo RAID, aumenta la probabilidad de que se produzca un fallo de varios discos en el mismo grupo RAID.

Grupos RAID de HDD o LUN de cabina

Debe seguir estas directrices al configurar sus grupos RAID compuestos por HDD o LUN de cabina:

- Todos los grupos RAID de un nivel local (agregado) deben tener la misma cantidad de discos.

Aunque se puede tener hasta un 50 % menos o más que el número de discos de diferentes grupos RAID en un nivel local, esto puede producir cuellos de botella en el rendimiento en algunos casos, por lo que es mejor evitar.

- El intervalo recomendado de números de disco de grupos RAID está entre 12 y 20.

La fiabilidad de los discos de rendimiento puede admitir un tamaño de grupo RAID de hasta 28, si fuera necesario.

- Si puede satisfacer las dos primeras directrices con varios números de disco de grupos RAID, debe elegir un mayor número de discos.

Grupos RAID de SSD en niveles locales de Flash Pool (agregados)

El tamaño del grupo de RAID de SSD puede ser diferente del tamaño del grupo de RAID para los grupos de RAID de HDD en un nivel local de Flash Pool (agregado). Por lo general, debe asegurarse de tener solo un grupo RAID de SSD para un nivel local de Flash Pool a fin de minimizar el número de SSD necesarios para la paridad.

Grupos RAID de SSD en niveles locales de SSD (agregados)

Debe seguir estas directrices para configurar los grupos RAID compuestos por SSD:

- Todos los grupos RAID de un nivel local (agregado) deben tener una cantidad similar de unidades.

No es necesario que los grupos de RAID tengan exactamente el mismo tamaño, pero debe evitar que haya grupos RAID con menos de la mitad del tamaño de otros grupos RAID en el mismo nivel local cuando sea posible.

- Para RAID-DP, el rango recomendado de tamaño de grupo de RAID está entre 20 y 28.

Personalice el tamaño de sus grupos RAID

Puede personalizar el tamaño de sus grupos RAID para garantizar que los tamaños de grupos RAID sean apropiados para la cantidad de almacenamiento que piensa incluir en un nivel local (agregado).

Acerca de esta tarea

Para los niveles locales estándar (agregados), debe cambiar el tamaño de los grupos RAID para cada nivel local por separado. En el caso de los niveles locales de Flash Pool, es posible cambiar el tamaño del grupo RAID de los grupos RAID de SSD y de los grupos RAID de HDD de forma independiente.

En la siguiente lista, se describen algunos hechos para cambiar el tamaño del grupo RAID:

- De forma predeterminada, si el número de discos o LUN de cabina en el grupo RAID más reciente es inferior al tamaño del nuevo grupo RAID, se añadirán discos o LUN de cabina al grupo RAID más reciente creado hasta que alcance el nuevo tamaño.
- El resto de los grupos RAID existentes en ese nivel local siguen teniendo el mismo tamaño, a menos que se añadan explícitamente discos a ellos.
- Nunca es posible que un grupo de RAID sea mayor que el tamaño máximo actual del grupo de RAID para el nivel local.

- No es posible reducir el tamaño de los grupos RAID ya creados.
- El nuevo tamaño se aplica a todos los grupos RAID de ese nivel local (o, en el caso de un nivel local Flash Pool, a todos los grupos RAID del tipo de grupo RAID afectado: SSD o HDD).

Pasos

1. Utilice el comando correspondiente:

| Si desea... | Introduzca el siguiente comando... |
|--|--|
| Cambiar el tamaño máximo del grupo RAID para los grupos RAID de SSD de un agregado de Flash Pool | <code>storage aggregate modify -aggregate aggr_name -cache-raid-group-size size</code> |
| Cambie el tamaño máximo de otros grupos RAID | <code>storage aggregate modify -aggregate aggr_name -maxraidsz size</code> |

Ejemplos

El siguiente comando cambia el tamaño máximo del grupo RAID del agregado n1_a4 a 20 discos o LUN de cabina:

```
storage aggregate modify -aggregate n1_a4 -maxraidsz 20
```

El siguiente comando cambia el tamaño máximo del grupo RAID de los grupos RAID de la caché SSD del agregado de Flash Pool n1_cache_a2 a 24:

```
storage aggregate modify -aggregate n1_cache_a2 -cache-raid-group-size 24
```

Gestión de niveles locales de Flash Pool (agregados)

Gestión de niveles de Flash Pool (agregados)

Puede realizar diversos procedimientos para gestionar los niveles de Flash Pool (agregados) en el sistema.

- **Políticas de almacenamiento en caché**
 - ["Políticas de almacenamiento en caché de nivel local \(agregado\) de Flash Pool"](#)
 - ["Gestione políticas de almacenamiento en caché de Flash Pool"](#)
- **Partición SSD**
 - ["Creación de particiones SSD de Flash Pool para niveles locales de Flash Pool \(agregados\) mediante pools de almacenamiento"](#)
- **Tamaño de la candidatura y de la caché**
 - ["Determine la candidatura de Flash Pool y el tamaño óptimo de la caché"](#)
- **Creación de Flash Pool**
 - ["Cree un nivel local de Flash Pool \(agregado\) mediante SSD físicos"](#)
 - ["Cree un nivel local de Flash Pool \(agregado\) mediante los pools de almacenamiento SSD"](#)

Políticas de almacenamiento en caché de nivel local (agregado) de Flash Pool

Las políticas de almacenamiento en caché para los volúmenes en un nivel local de Flash Pool (agregado) le permiten poner en marcha Flash como una caché de alto rendimiento para su conjunto de datos de trabajo utilizando HDD de menor coste para los datos a los que se accede con menor frecuencia. Si va a proporcionar caché a dos o más niveles locales de Flash Pool, debe usar la partición de SSD de Flash Pool para compartir SSD en los niveles locales de Flash Pool.

Las políticas de almacenamiento en caché se aplican a volúmenes que residen en niveles locales de Flash Pool. Debe comprender el funcionamiento de las políticas de almacenamiento en caché antes de cambiarlas.

En la mayoría de los casos, la política predeterminada de almacenamiento en caché de «'auto» es la mejor política de almacenamiento en caché que se debe utilizar. La política de almacenamiento en caché solo se debe cambiar si otra política proporciona un mejor rendimiento para su carga de trabajo. La configuración de una normativa de almacenamiento en caché errónea puede degradar de manera considerable el rendimiento del volumen; la degradación del rendimiento puede aumentar de forma gradual con el tiempo.

Las políticas de almacenamiento en caché combinan una política de almacenamiento en caché de lectura y una política de almacenamiento en caché de escritura. El nombre de la política concatena los nombres de la política de almacenamiento en caché de lectura y la política de almacenamiento en caché de escritura, separados por un guión. Si no hay guión en el nombre de la política, la política de almacenamiento en caché de escritura es «'none'», excepto la política «'auto'».

Las políticas de almacenamiento en caché de lectura optimizan para el rendimiento de lectura futuro al colocar una copia de los datos en la caché además de los datos almacenados en HDD. Para las políticas de almacenamiento en caché de lectura que insertan datos en la caché para operaciones de escritura, la caché funciona como una caché *write-through*.

Los datos insertados en la caché utilizando la política de almacenamiento en caché de escritura solo existen en la caché; no se copian en las HDD. La caché de Flash Pool está protegida por RAID. Al habilitar el almacenamiento en caché de escritura, los datos de las operaciones de escritura están disponibles para las lecturas desde la caché inmediatamente, mientras se posponen la escritura de los datos en las unidades de disco duro hasta que envejecen en la caché.

Si mueve un volumen de un nivel local de Flash Pool a un nivel local de un único nivel, pierde su política de almacenamiento en caché; si posteriormente lo mueve de nuevo a un nivel local de Flash Pool, se le asigna la política de almacenamiento en caché predeterminada de «'auto'». Si mueve un volumen entre dos nivel local de Flash Pool, se conserva la política de almacenamiento en caché.

Cambiar una política de almacenamiento en caché

Puede usar la interfaz de línea de comandos para cambiar la política de almacenamiento en caché de un volumen que reside en un nivel local de Flash Pool mediante el uso del `-caching-policy` con el `volume create` comando.

Cuando se crea un volumen en un nivel local de Flash Pool, de forma predeterminada, se asigna al volumen la política de almacenamiento en caché «'auto'».

Gestione políticas de almacenamiento en caché de Flash Pool

Mediante la CLI, puede realizar varios procedimientos para gestionar las políticas de almacenamiento en caché de Flash Pool en el sistema.

- **Preparación**

- "Determinar si se modifica la política de almacenamiento en caché de los niveles locales de Flash Pool (agregados)"

- **Modificación de directivas de almacenamiento en caché**

- "Modificar las políticas de almacenamiento en caché de niveles locales de Flash Pool (agregados)"
- "Establecer la política de retención de caché para niveles locales de Flash Pool (agregados)"

Determinar si se modifica la política de almacenamiento en caché de los niveles locales de Flash Pool (agregados)

Se pueden asignar políticas de retención de caché a volúmenes en niveles locales (agregados) de Flash Pool para determinar cuánto tiempo permanecen los datos de un volumen en la caché Flash Pool. Sin embargo, en algunos casos, cambiar la política de retención de caché puede no afectar la cantidad de tiempo que permanecen los datos del volumen en la caché.

Acerca de esta tarea

Si los datos cumplen alguna de las siguientes condiciones, es posible que el cambio de la política de retención de caché no afecte:

- La carga de trabajo es secuencial.
- Su carga de trabajo no releer los bloques aleatorios almacenados en caché en las unidades de estado sólido (SSD).
- El tamaño de la caché del volumen es demasiado pequeño.

Pasos

Los siguientes pasos comprueban las condiciones que deben cumplir los datos. La tarea debe realizarse mediante la interfaz de línea de comandos en modo de privilegios avanzado.

1. Use la interfaz de línea de comandos para ver el volumen de carga de trabajo:

```
statistics start -object workload_volume
```

2. Determine el patrón de carga de trabajo del volumen:

```
statistics show -object workload_volume -instance volume-workload -counter sequential_reads
```

3. Determine la tasa de aciertos del volumen:

```
statistics show -object waf1_hya_vvol -instance volume -counter read_ops_replaced_ppercent|wc_write_blks_overwritten_percent
```

4. Determine el Cacheable Ready.. Project Cache Alloc del volumen:

```
system node run -node node_name waf1 awa start aggr_name
```

5. Mostrar el resumen de AWA:

```
system node run -node node_name waf1 awa print aggr_name
```

6. Compare la tasa de aciertos del volumen con la `Cacheable Read`.

Si la tasa de aciertos del volumen es mayor que la `Cacheable Read`, Entonces su carga de trabajo no releer bloques aleatorios almacenados en caché en los SSD.

7. Compare el tamaño actual de la caché del volumen con el `Project Cache Alloc`.

Si el tamaño actual de la caché del volumen es mayor que el `Project Cache Alloc`, entonces el tamaño de la caché de volumen es demasiado pequeño.

Modificar las políticas de almacenamiento en caché de niveles locales de Flash Pool (agregados)

Debe modificar la política de almacenamiento en caché de un volumen solo si se espera que otra política de almacenamiento en caché proporcione un mejor rendimiento. Puede modificar la política de almacenamiento en caché de un volumen en un nivel local de Flash Pool (agregado).

Lo que necesitará

Debe determinar si desea modificar la política de almacenamiento en caché.

Acerca de esta tarea

En la mayoría de los casos, la política de almacenamiento en caché predeterminada de «'auto'» es la mejor política de almacenamiento en caché que puede utilizar. La política de almacenamiento en caché solo se debe cambiar si otra política proporciona un mejor rendimiento para su carga de trabajo. La configuración de una normativa de almacenamiento en caché errónea puede degradar de manera considerable el rendimiento del volumen; la degradación del rendimiento puede aumentar de forma gradual con el tiempo. Debe ser cauteloso al modificar las políticas de almacenamiento en caché. Si experimenta problemas de rendimiento con un volumen para el que se ha cambiado la política de almacenamiento en caché, debería devolver la política de almacenamiento en caché a "auto".

Paso

1. Use la interfaz de línea de comandos para modificar la política de almacenamiento en caché del volumen:

```
volume modify -volume volume_name -caching-policy policy_name
```

Ejemplo

En el siguiente ejemplo se modifica la política de almacenamiento en caché de un volumen denominado «'vol2'» a la política «'none'»:

```
volume modify -volume vol2 -caching-policy none
```

Establecer la política de retención de caché para niveles locales de Flash Pool (agregados)

Se pueden asignar políticas de retención de caché a volúmenes en niveles locales (agregados) de Flash Pool. Los datos de los volúmenes que tienen una política de retención de caché alta permanecen durante más tiempo en la caché y los datos de los volúmenes que tienen una política de retención de caché baja se eliminan antes. Esto

aumenta el rendimiento de las cargas de trabajo cruciales al permitir acceder a información de alta prioridad a un ritmo más rápido durante más tiempo.

Lo que necesitará

Debe saber si el sistema tiene condiciones que pueden evitar que la política de retención de caché afecte al período de tiempo que permanecen los datos en la caché.

Pasos

Utilice la CLI en modo de privilegios avanzado para realizar los siguientes pasos:

- 1. Cambie la configuración del privilegio a avanzado:

```
set -privilege advanced
```

- 2. Verifique la política de retención de caché del volumen:

De forma predeterminada, la política de retención de la memoria caché es «normal».

- 3. Configure la política de retención de caché:

| Versión de ONTAP | Comando |
|-----------------------|--|
| ONTAP 9.0, 9.1 | <pre>priority hybrid-cache set volume_name read-cache=read_cache_value write- cache=write_cache_value cache- retention- priority=cache_retention_policy</pre> <p>Configurado <code>cache_retention_policy</code> para <code>high</code> para los datos que se desean permanecer en la caché durante más tiempo. Configurado <code>cache_retention_policy</code> para <code>low</code> para los datos que se desean quitar de la caché antes.</p> |
| ONTAP 9,2 o posterior | <pre>volume modify -volume volume_name -vserver vservers_name -caching-policy policy_name.</pre> |

- 4. Compruebe que la política de retención de caché del volumen se modifique a la opción seleccionada.
- 5. Devuelva la configuración de privilegio a admin:

```
set -privilege admin
```

Creación de particiones SSD de Flash Pool para niveles locales de Flash Pool (agregados) mediante pools de almacenamiento

Si va a proporcionar caché en dos o más niveles locales de Flash Pool (agregados), debe usar la partición de la unidad de estado sólido (SSD) de Flash Pool. La creación de particiones de SSD con Flash Pool permite compartir los SSD con todos los niveles locales que usan Flash Pool. Esto permite distribuir el coste de la paridad frente a varios

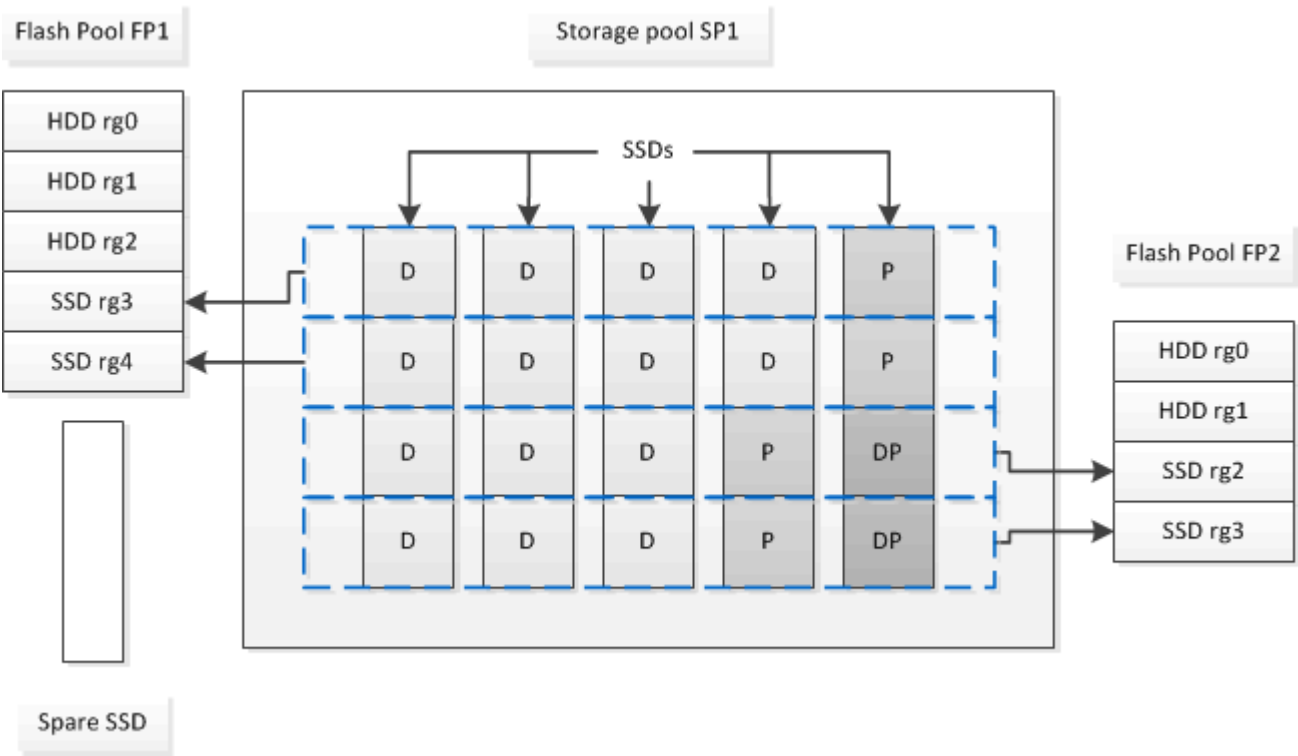
niveles locales, aumenta la flexibilidad de asignación de caché SSD y maximiza el rendimiento de SSD.

Para poder utilizar un SSD en un nivel local de Flash Pool, el SSD se debe colocar en un pool de almacenamiento. No se pueden usar SSD que se particionaran para la partición de datos raíz en un pool de almacenamiento. Después de colocar el SSD en el pool de almacenamiento, el SSD ya no se puede gestionar como un disco independiente y no se puede eliminar del pool de almacenamiento a menos que se destruyan los niveles locales asociados con Flash Pool y se destruya el pool de almacenamiento.

Los pools de almacenamiento SSD se dividen en cuatro unidades de asignación iguales. Las SSD añadidas al pool de almacenamiento se dividen en cuatro particiones y una partición está asignada a cada una de las cuatro unidades de asignación. La misma pareja de ha debe ser la propietaria de los SSD del pool de almacenamiento. De manera predeterminada, se asignan dos unidades de asignación a cada nodo en el par de alta disponibilidad. Las unidades de asignación deben ser propiedad del nodo al que pertenece el nivel local que está sirviendo. Si se necesita más Flash Cache para los niveles locales en uno de los nodos, el número predeterminado de unidades de asignación se puede mover para reducir el número en un nodo y aumentar el número en el nodo asociado.

Se utilizan SSD de repuesto para añadir a un pool de almacenamiento SSD. Si el pool de almacenamiento proporciona unidades de asignación a niveles locales de Flash Pool propiedad de ambos nodos del par de alta disponibilidad, cualquiera de los nodos puede tener la propiedad de los SSD de repuesto. Sin embargo, si el pool de almacenamiento proporciona unidades de asignación solo a niveles locales de Flash Pool propiedad de uno de los nodos del par de alta disponibilidad, los repuestos de SSD deben ser propiedad de ese mismo nodo.

En la siguiente ilustración se muestra un ejemplo de creación de particiones SSD de Flash Pool. El pool de almacenamiento de SSD proporciona caché a dos niveles locales de Flash Pool:



El SP1 del pool de almacenamiento está compuesto por cinco SSD y un SSD de pieza de repuesto. Dos de las unidades de asignación del pool de almacenamiento se asignan a Flash Pool FP1 y dos se asignan a Flash Pool FP2. FP1 tiene un tipo de RAID de caché de RAID4. Por lo tanto, las unidades de asignación proporcionadas a FP1 sólo contienen una partición designada para la paridad. FP2 tiene un tipo de RAID de

caché de RAID-DP. Por lo tanto, las unidades de asignación proporcionadas a FP2 incluyen una partición de paridad y una partición de doble paridad.

En este ejemplo, se asignan dos unidades de asignación a cada nivel local de Flash Pool. Sin embargo, si un nivel local de Flash Pool requería una mayor memoria caché, podría asignar tres de las unidades de asignación a ese nivel local de Flash Pool y solo una a la otra.

Determine la candidatura de Flash Pool y el tamaño óptimo de la caché

Antes de convertir un nivel local (agregado) existente en un nivel local de Flash Pool, se puede determinar si el nivel local está ligado a I/O y el mejor tamaño de la caché Flash Pool para su carga de trabajo y presupuesto. También puede comprobar si la caché de un nivel local de Flash Pool existente tiene el tamaño correcto.

Lo que necesitará

Debe saber aproximadamente cuándo el nivel local que está analizando experimenta su carga máxima.

Pasos

1. Entrar al modo avanzado:

```
set advanced
```

2. Si necesita determinar si un nivel local (agregado) existente sería un buen candidato para la conversión a un agregado de Flash Pool, determine el nivel de actividad de los discos del agregado durante un periodo de carga pico y cómo esto afecta a la latencia:

```
statistics show-periodic -object disk:raid_group -instance raid_group_name
-counter disk_busy|user_read_latency -interval 1 -iterations 60
```

Puede decidir si tiene sentido reducir la latencia añadiendo la caché de Flash Pool para este agregado.

El siguiente comando muestra las estadísticas del primer grupo RAID del agregado «'aggr1'»:

```
statistics show-periodic -object disk:raid_group -instance /aggr1/plex0/rg0
-counter disk_busy|user_read_latency -interval 1 -iterations 60
```

3. Iniciar analizador de carga de trabajo automática (AWA):

```
storage automated-working-set-analyzer start -node node_name -aggregate
aggr_name
```

AWA comienza a recoger datos de cargas de trabajo de los volúmenes asociados con el agregado especificado.

4. Salir del modo avanzado:

```
set admin
```

Permitir que AWA funcione hasta que se hayan producido uno o más intervalos de carga máxima. AWA recopila estadísticas de carga de trabajo de los volúmenes asociados con el agregado especificado y analiza los datos de hasta una semana de duración. La ejecución de AWA durante más de una semana sólo informará sobre los datos recopilados de la semana más reciente. Las estimaciones de tamaño de caché se basan en las cargas más altas observadas durante el período de recopilación de datos; la carga

no necesita ser alta durante todo el período de recopilación de datos.

5. Entrar al modo avanzado:

```
set advanced
```

6. Mostrar el análisis de la carga de trabajo:

```
storage automated-working-set-analyzer show -node node_name -instance
```

7. Detener AWA:

```
storage automated-working-set-analyzer stop node_name
```

Todos los datos de las cargas de trabajo se vacían y ya no están disponibles para el análisis.

8. Salir del modo avanzado:

```
set admin
```

Cree un nivel local de Flash Pool (agregado) mediante SSD físicos

Puede crear un nivel local de Flash Pool (agregado) al habilitar la función en un nivel local existente compuesto por grupos RAID de HDD y, a continuación, añadir uno o varios grupos RAID de SSD a ese nivel local. Esto da como resultado dos conjuntos de grupos RAID para ese nivel local: Grupos RAID de SSD (la caché SSD) y grupos RAID de HDD.

Acerca de esta tarea

Después de añadir una caché SSD a un nivel local para crear un nivel local de Flash Pool, no se puede quitar la caché SSD para convertir el nivel local de nuevo a su configuración original.

De forma predeterminada, el nivel de RAID de la caché SSD es el mismo que el nivel de RAID de los grupos de RAID de HDD. Puede anular esta selección predeterminada especificando la opción "raidtype" al agregar los primeros grupos de SSD RAID.

Antes de empezar

- Debe haber identificado un nivel local válido compuesto por HDD para convertir a un nivel local de Flash Pool.
- Debe haber determinado la elegibilidad del almacenamiento en caché de escritura de los volúmenes asociados con el nivel local y completar los pasos necesarios para resolver los problemas de elegibilidad.
- Debe haber determinado los SSD que añadirá y estos SSD deben ser propiedad del nodo en el que se creará el nivel local de Flash Pool.
- Debe haber determinado los tipos de suma de comprobación de los SSD que va a añadir y los HDD ya están en el nivel local.
- Debe haber determinado la cantidad de SSD que va a añadir y el tamaño de grupo RAID óptimo para los grupos RAID de SSD.

Al utilizar menos grupos RAID en la caché SSD, se reduce el número de discos de paridad necesarios, pero los grupos RAID de mayor tamaño requieren RAID-DP.

- Debe haber determinado el nivel de RAID que desea usar para la caché SSD.
- Se debe haber determinado el tamaño máximo de caché para el sistema y determinar que añadir caché SSD al nivel local no hará que lo supere.
- Debe haberse familiarizado con los requisitos de configuración de los niveles locales de Flash Pool.



Pasos

Puede crear un agregado de Flash Pool mediante System Manager o la interfaz de línea de comandos de ONTAP.

System Manager

A partir de ONTAP 9.12.1, se puede usar System Manager para crear un nivel local de Flash Pool con SSD físicos.

Pasos

1. Seleccione **Almacenamiento > Niveles** y, a continuación, seleccione un nivel de almacenamiento de disco duro local existente.
2. Seleccione  A continuación, **Añadir Flash Pool Cache**.
3. Seleccione **Usar SSD dedicados como caché**.
4. Seleccione un tipo de disco y la cantidad de discos.
5. Seleccione un tipo de RAID.
6. Seleccione **Guardar**.
7. Busque el nivel de almacenamiento y seleccione .
8. Seleccione **Más detalles**. Verifique que Flash Pool se muestre como **enabled**.

CLI

Pasos

1. Marcar el nivel local (agregado) como apto para convertirse en un agregado de Flash Pool:

```
storage aggregate modify -aggregate aggr_name -hybrid-enabled true
```

Si este paso no tiene éxito, determine la idoneidad del almacenamiento en caché de escritura para el agregado objetivo.

2. Añada los SSD al agregado mediante el `storage aggregate add` comando.
 - Puede especificar los SSD por ID o mediante el `diskcount` y.. `disktype` parámetros.
 - Si los HDD y los SSD no tienen el mismo tipo de suma de comprobación, o si el agregado es un agregado con suma de comprobación mixta, debe utilizar el `checksumstyle` parámetro para especificar el tipo de suma de comprobación de los discos que se van a añadir al agregado.
 - Es posible especificar un tipo de RAID diferente para la caché SSD mediante el `raidtype` parámetro.
 - Si desea que el tamaño del grupo de RAID de la caché sea diferente del predeterminado para el tipo de RAID que utiliza, debe cambiarlo ahora, mediante la `-cache-raid-group-size` parámetro.

Cree un nivel local de Flash Pool (agregado) mediante los pools de almacenamiento SSD

Información general sobre la creación de un nivel local de Flash Pool (agregado) mediante pools de almacenamiento SSD

Puede realizar varios procedimientos para crear un nivel local de Flash Pool (agregado) mediante pools de almacenamiento SSD:

- **Preparación**
 - ["Determine si un nivel local de Flash Pool \(agregado\) utiliza un pool de almacenamiento SSD"](#)
- **Creación de pool de almacenamiento SSD**
 - ["Cree un pool de almacenamiento SSD"](#)
 - ["Añadir SSD a un pool de almacenamiento de SSD"](#)
- **Creación de Flash Pool mediante agrupaciones de almacenamiento SSD**
 - ["Cree un nivel local de Flash Pool \(agregado\) mediante las unidades de asignación de pool de almacenamiento de SSD"](#)
 - ["Determine el impacto en el tamaño de la caché de añadir SSD a un pool de almacenamiento SSD"](#)

Determine si un nivel local de Flash Pool (agregado) utiliza un pool de almacenamiento SSD

Puede configurar un agregado de Flash Pool (nivel local) añadiendo una o varias unidades de asignación desde un pool de almacenamiento de SSD a un nivel local de HDD existente.

Los niveles locales de Flash Pool se gestionan de manera diferente cuando utilizan pools de almacenamiento SSD para proporcionar su caché que cuando utilizan SSD independientes.

Paso

1. Mostrar las unidades del agregado por grupo RAID:

```
storage aggregate show-status aggr_name
```

Si el agregado utiliza uno o varios pools de almacenamiento SSD, el valor de `Position` La columna de los grupos RAID SSD se muestra como `Shared`, Y el nombre del grupo de almacenamiento se muestra junto al nombre del grupo RAID.

Añada la caché a un nivel local (agregado) mediante la creación de un pool de almacenamiento SSD

Se puede aprovisionar la caché mediante la conversión de un nivel local (agregado) existente en un nivel local de Flash Pool (agregado) mediante la adición de unidades de estado sólido (SSD).

Puede crear pools de almacenamiento de unidades de estado sólido (SSD) para proporcionar caché SSD para dos a cuatro niveles locales de Flash Pool (agregados). Los agregados Flash Pool le permiten poner en marcha flash como memoria caché de alto rendimiento para sus datos de trabajo utilizando HDD de menor coste para datos a los que se accede con menor frecuencia.

Acerca de esta tarea

- Debe proporcionar una lista de discos al crear o añadir discos a un pool de almacenamiento.

Los pools de almacenamiento no admiten un `diskcount` parámetro.

- Los SSD utilizados en el pool de almacenamiento deben tener el mismo tamaño.

System Manager

Use System Manager para añadir una caché SSD (ONTAP 9.12.1 y versiones posteriores)

A partir de ONTAP 9.12.1, es posible usar System Manager para añadir una caché SSD.



Las opciones de pool de almacenamiento no están disponibles en los sistemas AFF.

Pasos

1. Haga clic en **Cluster > Disks** y a continuación, haga clic en **Mostrar/Ocultar**.
2. Seleccione **Tipo** y compruebe que existen SSD de repuesto en el clúster.
3. Haga clic en **almacenamiento > niveles** y haga clic en **Agregar grupo de almacenamiento**.
4. Seleccione el tipo de disco.
5. Introduzca un tamaño de disco.
6. Seleccione la cantidad de discos que desea añadir al pool de almacenamiento.
7. Revise el tamaño estimado de la caché.

Use System Manager para añadir una caché SSD (solo ONTAP 9.7)



Utilice el procedimiento de la CLI si utiliza una versión de ONTAP posterior a ONTAP 9.7 o anterior a ONTAP 9.12.1.

Pasos

1. Haga clic en **(Volver a la versión clásica)**.
2. Haga clic en **almacenamiento > agregados y discos > agregados**.
3. Seleccione el nivel local (agregado) y, a continuación, haga clic en **acciones > Agregar caché**.
4. Seleccione el origen de caché como "pools de almacenamiento" o "SSD dedicados".
5. Haga clic en **(Cambiar a la nueva experiencia)**.
6. Haga clic en **almacenamiento > niveles** para comprobar el tamaño del nuevo agregado.

CLI

Utilice la CLI para crear un pool de almacenamiento SSD

Pasos

1. Determine los nombres de los SSD de repuesto disponibles:

```
storage aggregate show-spare-disks -disk-type SSD
```

Los SSD que se utilizan en un pool de almacenamiento pueden ser la propiedad de cualquiera de los nodos de una pareja de ha.

2. Cree el pool de almacenamiento:

```
storage pool create -storage-pool sp_name -disk-list disk1,disk2,...
```

3. **Opcional:** Compruebe el grupo de almacenamiento recién creado:

```
storage pool show -storage-pool sp_name
```

Resultados

Una vez que los SSD se colocan en el pool de almacenamiento, dejan de aparecer como repuestos en el clúster, a pesar de que el almacenamiento proporcionado por el pool de almacenamiento aún no se haya asignado a ninguna caché Flash Pool. No es posible añadir SSD a un grupo RAID como unidades discretas; su almacenamiento solo se puede aprovisionar mediante las unidades de asignación del pool de almacenamiento al que pertenecen.

Cree un nivel local de Flash Pool (agregado) mediante las unidades de asignación de pool de almacenamiento de SSD

Puede configurar un nivel local de Flash Pool (agregado) añadiendo una o varias unidades de asignación desde un pool de almacenamiento de SSD a un nivel local de HDD existente.

A partir de ONTAP 9.12.1, se puede usar System Manager rediseñado para crear un nivel local de Flash Pool con las unidades de asignación de pools de almacenamiento.

Lo que necesitará

- Debe haber identificado un nivel local válido compuesto por HDD para convertir a un nivel local de Flash Pool.
- Debe haber determinado la elegibilidad del almacenamiento en caché de escritura de los volúmenes asociados con el nivel local y completar los pasos necesarios para resolver los problemas de elegibilidad.
- Debe haber creado un pool de almacenamiento SSD para proporcionar la caché SSD a este nivel local de Flash Pool.

Cualquier unidad de asignación del pool de almacenamiento que desee usar debe ser propiedad del mismo nodo al que pertenece el nivel local de Flash Pool.

- Debe haber determinado la cantidad de caché que desea añadir al nivel local.

Se agrega caché al nivel local por unidades de asignación. Puede aumentar el tamaño de las unidades de asignación más adelante añadiendo SSD al pool de almacenamiento, si hay espacio.

- Debe haber determinado el tipo de RAID que desea usar para la caché SSD.

Después de añadir una caché al nivel local de los pools de almacenamiento SSD, no es posible cambiar el tipo de RAID de los grupos RAID de caché.

- Se debe haber determinado el tamaño máximo de caché para el sistema y determinar que añadir caché SSD al nivel local no hará que lo supere.

Puede ver la cantidad de caché que se añadirá al tamaño total de la caché usando el `storage pool show` comando.

- Debe haberse familiarizado con los requisitos de configuración del nivel local de Flash Pool.

Acerca de esta tarea

Si desea que el tipo de RAID de la caché sea diferente del de los grupos RAID de las HDD, debe especificar



el tipo de RAID de caché al añadir la capacidad SSD. Después de añadir la capacidad SSD al nivel local, no es posible cambiar el tipo de RAID de la caché.

Después de añadir una caché SSD a un nivel local para crear un nivel local de Flash Pool, no se puede quitar la caché SSD para convertir el nivel local de nuevo a su configuración original.

System Manager

A partir de ONTAP 9.12.1, se puede usar System Manager para añadir SSD a un pool de almacenamiento de SSD.

Pasos

1. Haga clic en **almacenamiento > niveles** y seleccione un nivel de almacenamiento de disco duro local existente.
2. Haga clic en  Y seleccione **Agregar Flash Pool Cache**.
3. Seleccione **utilizar agrupaciones de almacenamiento**.
4. Seleccione un pool de almacenamiento.
5. Seleccione un tamaño de caché y una configuración de RAID.
6. Haga clic en **Guardar**.
7. Vuelva a encontrar el nivel de almacenamiento y haga clic en .
8. Seleccione **más detalles** y compruebe que Flash Pool se muestra como **habilitado**.

CLI

Pasos

1. Marcar el agregado como apto para convertirse en un agregado de Flash Pool:

```
storage aggregate modify -aggregate aggr_name -hybrid-enabled true
```

Si este paso no tiene éxito, determine la idoneidad del almacenamiento en caché de escritura para el agregado objetivo.

2. Mostrar las unidades de asignación de pool de almacenamiento SSD disponibles:

```
storage pool show-available-capacity
```

3. Añada la capacidad de SSD al agregado:

```
storage aggregate add aggr_name -storage-pool sp_name -allocation-units  
number_of_units
```

Si desea que el tipo de RAID de la caché sea diferente del de los grupos RAID de las HDD, se debe cambiar cuando se introduce este comando mediante el `raidtype` parámetro.

No es necesario especificar un nuevo grupo RAID; ONTAP coloca automáticamente la caché SSD en grupos RAID separados de los grupos RAID de HDD.

No se puede configurar el tamaño del grupo RAID de la caché; sí se determina por la cantidad de SSD del pool de almacenamiento.

La caché se añade al agregado; el agregado ahora es un agregado de Flash Pool. Cada unidad de asignación añadida al agregado se convierte en su propio grupo RAID.

4. Confirme la presencia y el tamaño de la caché SSD:

```
storage aggregate show aggregate_name
```

El tamaño de la caché aparece en Total Hybrid Cache Size.

Información relacionada

["Informe técnico de NetApp 4070: Guía de diseño e implementación de Flash Pool"](#)

Determine el impacto en el tamaño de la caché de añadir SSD a un pool de almacenamiento SSD

Si se añaden SSD a un pool de almacenamiento, se superará el límite de caché del modelo de la plataforma, ONTAP no asigna la capacidad recién añadida a ningún nivel local de Flash Pool (agregados). Esto puede hacer que parte o la totalidad de la capacidad recién añadida no estén disponibles para su uso.

Acerca de esta tarea

Cuando se añaden SSD a un pool de almacenamiento SSD con unidades de asignación ya asignadas a los niveles locales de Flash Pool (agregados), se aumenta el tamaño de la caché de cada uno de esos niveles locales y la caché total del sistema. Si ninguna de las unidades de asignación del pool de almacenamiento se asignó, la adición de SSD a ese pool de almacenamiento no afecta al tamaño de la caché SSD hasta que una o más unidades de asignación se asignan a una caché.

Pasos

1. Determine el tamaño utilizable de los SSD que va a añadir al pool de almacenamiento:

```
storage disk show disk_name -fields usable-size
```

2. Determine cuántas unidades de asignación quedan sin asignar para el pool de almacenamiento:

```
storage pool show-available-capacity sp_name
```

Se muestran todas las unidades de asignación no asignados del grupo de almacenamiento.

3. Calcule la cantidad de caché que se agregará aplicando la siguiente fórmula:

$(4 - \text{número de unidades de asignación sin asignar}) \times 25\% \times \text{tamaño utilizable} \times \text{número de SSD}$

Añadir SSD a un pool de almacenamiento de SSD

Cuando se añaden unidades de estado sólido (SSD) a un pool de almacenamiento de SSD, se deben aumentar los tamaños físicos y utilizables del pool de almacenamiento y el tamaño de la unidad de asignación. El tamaño de la unidad de asignación más grande también afecta a las unidades de asignación que ya se han asignado a los niveles locales (agregados).

Lo que necesitará

Debe haber determinado que esta operación no hará que supere el límite de caché de su par de alta disponibilidad. ONTAP no impide que se supere el límite de caché cuando se añaden SSD a un pool de almacenamiento SSD y se puede hacer que la capacidad de almacenamiento recién añadida no esté disponible para su uso.

Acerca de esta tarea

Cuando se añaden SSD a un pool de almacenamiento SSD existente, los SSD deben ser propiedad de un


nodo o de la otra pareja de alta disponibilidad que ya poseía los SSD existentes en el pool de almacenamiento. Puede añadir los SSD que pertenecen a cualquier nodo de la pareja de ha.

El SSD que se añade al pool de almacenamiento debe tener el mismo tamaño que el disco utilizado actualmente en el pool de almacenamiento.

System Manager

A partir de ONTAP 9.12.1, se puede usar System Manager para añadir SSD a un pool de almacenamiento de SSD.

Pasos

- 1. Haga clic en **almacenamiento > niveles** y busque la sección **agrupaciones de almacenamiento**.
- 2. Busque el pool de almacenamiento. Haga clic en  Y seleccione **Agregar discos**.
- 3. Elija el tipo de disco y seleccione la cantidad de discos.
- 4. Revise el tamaño de la caché estimado.

CLI

Pasos

- 1. **Opcional:** Vea el tamaño actual de la unidad de asignación y el almacenamiento disponible para la agrupación de almacenamiento:

```
storage pool show -instance sp_name
```

- 2. Buscar SSD disponibles:

```
storage disk show -container-type spare -type SSD
```

- 3. Añada los SSD al pool de almacenamiento:

```
storage pool add -storage-pool sp_name -disk-list disk1,disk2...
```

El sistema muestra los agregados de Flash Pool a su tamaño aumentado mediante esta operación y con el número de agregados, y le solicita que confirme la operación.

Comandos para gestionar pools de almacenamiento SSD

ONTAP proporciona la `storage pool` Comando para gestionar pools de almacenamiento SSD.

| Si desea... | Se usa este comando... |
|--|--|
| Mostrar la cantidad de almacenamiento que un pool de almacenamiento proporciona a qué agregados | <code>storage pool show-aggregate</code> |
| Mostrar cuánta caché se añadiría a la capacidad total de la caché para los dos tipos de RAID (tamaño de datos de unidad de asignación) | <code>storage pool show -instance</code> |

| | |
|---|---|
| Visualice los discos en una pool de almacenamiento | <code>storage pool show-disks</code> |
| Muestre las unidades de asignación no asignados de una agrupación de almacenamiento | <code>storage pool show-available-capacity</code> |
| Cambie la propiedad de una o varias unidades de asignación de un pool de almacenamiento de un partner de alta disponibilidad a otro | <code>storage pool reassign</code> |

Información relacionada

["Comandos de ONTAP 9"](#)

Gestión de niveles FabricPool

Información general sobre la gestión de niveles de FabricPool

Puede usar FabricPool para organizar los datos en niveles automáticamente en función de la frecuencia de acceso a estos.

FabricPool es una solución de almacenamiento híbrido que utiliza un agregado all-flash (SSD) como nivel de rendimiento y un almacén de objetos como nivel cloud. El uso de FabricPool le ayuda a reducir los costes de almacenamiento sin que se vea afectado el rendimiento, la eficiencia o la protección.

El nivel de cloud se puede encontrar en StorageGRID o ONTAP S3 de NetApp (empezando por ONTAP 9.8), o en uno de los siguientes proveedores de servicios:

- Cloud de Alibaba
- Amazon S3
- Servicios de cloud comercial de Amazon
- Google Cloud
- Cloud de IBM
- Almacenamiento BLOB de Microsoft Azure



A partir de ONTAP 9.7, se pueden utilizar proveedores de almacenes de objetos adicionales que admiten API S3 genéricas seleccionando el proveedor de almacenes de objetos S3_COMPATIBLE.

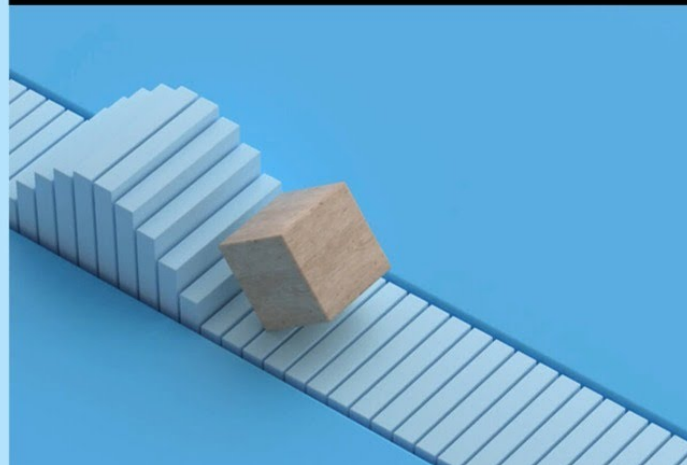
Vídeo de caso de uso de datos por niveles y menores costes

ONTAP FabricPool

Tier Data and Lower Costs

Use Case

© 2020 NetApp, Inc. All rights reserved.



Información relacionada

Consulte también la ["Organización en niveles del cloud de NetApp"](#) documentación.

Ventajas de los niveles de almacenamiento mediante FabricPool

La configuración de un agregado para utilizar FabricPool permite usar niveles de almacenamiento. Puede equilibrar de manera eficiente el rendimiento y los costos del sistema de almacenamiento, supervisar y optimizar el uso del espacio, y realizar movimientos de datos basados en políticas entre niveles de almacenamiento.

- Puede optimizar el rendimiento del almacenamiento y reducir los costes de almacenamiento almacenando los datos en un nivel en función de si se accede a ellos con frecuencia.

- Los datos a los que se accede con frecuencia ("hot") se almacenan en el *nivel de rendimiento*.

El nivel de rendimiento usa almacenamiento primario de alto rendimiento, como un agregado all-flash (todos SSD) del sistema de almacenamiento.

- Los datos a los que se accede con poca frecuencia ("frío") se almacenan en el *cloud Tier*, también conocido como *Capacity Tier*.

El nivel de cloud utiliza un almacén de objetos menos costoso y no requiere alto rendimiento.

- Puede especificar el nivel en el que deben almacenarse los datos.

Puede especificar una de las opciones de política de organización en niveles compatibles a nivel de volumen. Las opciones le permiten mover datos de forma eficiente entre niveles a medida que estos se activan o inactivan.

["Tipos de políticas de organización en niveles de FabricPool"](#)

- Puede elegir uno de los almacenes de objetos admitidos para usarlos como nivel de cloud para FabricPool.
- Puede supervisar el uso de espacio en un agregado habilitado para FabricPool.
- Puede ver cuántos datos de un volumen están inactivos utilizando los informes de datos inactivos.
- Puede reducir el espacio físico que ocupa el sistema de almacenamiento en las instalaciones.

Ahorra espacio físico cuando se utiliza un almacén de objetos basado en cloud para el nivel de cloud.

Consideraciones y requisitos para usar FabricPool

Debe familiarizarse con algunas consideraciones y requisitos sobre el uso de FabricPool.

Consideraciones y requisitos generales

- Debe ejecutar ONTAP 9.2 como mínimo para usar FabricPool.
- Debe ejecutar ONTAP 9.4 o versiones posteriores para la siguiente funcionalidad de FabricPool:
 - La auto ["política de organización en niveles"](#)
 - Especificación del período de enfriamiento mínimo de organización en niveles
 - Generación de informes de datos inactivos (IDR)
 - Uso del almacenamiento de Microsoft Azure Blob para el cloud como nivel de cloud para FabricPool
 - Uso de FabricPool con ONTAP Select
- Debe ejecutar ONTAP 9,5 o versiones posteriores para establecer la siguiente funcionalidad de FabricPool:
 - Especificar el umbral de ocupación de la organización en niveles
 - Uso del almacenamiento de objetos en el cloud de IBM como nivel de cloud para FabricPool
 - NetApp Volume Encryption (NVE) del nivel de cloud, habilitado de forma predeterminada.
- Debe ejecutar ONTAP 9,6 o versiones posteriores para establecer la siguiente funcionalidad de FabricPool:
 - La `all` política de organización en niveles
 - Generación de informes de datos inactivos habilitada manualmente en agregados de HDD
 - La generación de informes de datos inactivos se habilita automáticamente para los agregados de SSD cuando actualiza a ONTAP 9.6 y en el momento en que se crea el agregado, a excepción de los sistemas de gama baja con menos de 4 CPU, menos de 6 GB de RAM o cuando el tamaño de la caché de búfer de WAFL es inferior a 3 GB.

ONTAP supervisa la carga del sistema y si la carga permanece alta durante 4 minutos continuos, el IDR se desactiva y no se activa automáticamente. Puede volver a habilitar IDR manualmente, sin embargo, IDR habilitado manualmente no se desactiva automáticamente.

 - Uso de Alibaba Cloud Object Storage como nivel cloud para FabricPool
 - Uso de Google Cloud Platform como nivel de cloud para FabricPool
 - Movimiento de volúmenes sin copia de datos de nivel en el cloud
- Debe ejecutar ONTAP 9,7 o versiones posteriores para establecer la siguiente funcionalidad de FabricPool:

- Proxy HTTP y HTTPS no transparente para proporcionar acceso sólo a puntos de acceso en lista blanca y para proporcionar funciones de auditoría e informes.
- Mirroring de FabricPool para organizar los datos inactivos en niveles en dos almacenes de datos de forma simultánea
- Reflejos FabricPool en configuraciones MetroCluster
- El volcado y la restauración de NDMP están habilitados de manera predeterminada en los agregados conectados a FabricPool.



Si la aplicación de backup utiliza un protocolo distinto a NDMP, como NFS o SMB, el backup de todos los datos del nivel de rendimiento se activa y puede afectar a la organización en niveles de dichos datos en el nivel de cloud. Las lecturas que no sean de NDMP pueden provocar la migración de datos desde el nivel de cloud hasta el nivel de rendimiento.

"Compatibilidad con backup y restauración NDMP para FabricPool"

- Debe ejecutar ONTAP 9.8 o una versión posterior para obtener la siguiente funcionalidad de FabricPool:
 - El control de migración al cloud le permite anular la política de organización en niveles predeterminada
 - Promoción de los datos al nivel de rendimiento
 - FabricPool con SnapLock Enterprise. FabricPool con SnapLock Enterprise requiere una solicitud de variación de productos (FPVR) destacada. Para crear un FPVR, póngase en contacto con su equipo de ventas.
 - Período mínimo de enfriamiento máximo de 183 días
 - Etiquetado de objetos mediante etiquetas personalizadas creadas por el usuario
 - FabricPool en plataformas y agregados de unidades de disco duro

HDD FabricPools es compatible con discos SAS, FSAS, BSAS y MSATA solo en sistemas con 6 o más núcleos de CPU, incluidos los siguientes modelos:

- FAS9000
- FAS8700
- FAS8300
- FAS8200
- FAS8080
- FAS8060
- FAS8040
- FAS2750
- FAS2720
- FAS2650
- FAS2620

Comprobar "[Hardware Universe](#)" para obtener los últimos modelos admitidos.

- FabricPool es compatible con todas las plataformas compatibles con ONTAP 9.2 excepto con las siguientes:

- FAS8020
- FAS2554
- FAS2552
- FAS2520

- FabricPool admite los siguientes tipos de agregados:
 - En los sistemas AFF, solo puede utilizar agregados all-flash (todos SSD) para FabricPool.
 - En los sistemas FAS, puede usar agregados all-flash (todos SSD) o de HDD para FabricPool.

No se pueden usar agregados de Flash Pool, que contienen tanto SSD como HDD.

- En Cloud Volumes ONTAP y ONTAP Select, se pueden usar agregados de SSD o HDD para FabricPool.

Sin embargo, se recomienda usar agregados de SSD.

- FabricPool admite el uso de los siguientes almacenes de objetos como nivel de cloud:
 - NetApp StorageGRID 10.3 o posterior
 - NetApp ONTAP S3 (ONTAP 9.8 y posterior)
 - Almacenamiento de objetos en cloud de Alibaba
 - Simple Storage Service (AWS S3) de Amazon Web Services
 - Google Cloud Storage
 - Almacenamiento de objetos en cloud de IBM
 - Almacenamiento de Microsoft Azure Blob para el cloud
- El almacén de objetos «'bucket» (contenedor) que vaya a utilizar debe estar ya configurado, tener al menos 10 GB de espacio de almacenamiento y no debe cambiarse de nombre.
- Las parejas de ALTA DISPONIBILIDAD que usan FabricPool requieren una LIF de interconexión de clústeres para comunicarse con el almacén de objetos.
- No es posible desvincular un nivel de cloud de un nivel local una vez asociado; sin embargo, puede utilizar ["Espejo de FabricPool"](#) para adjuntar un nivel local a un nivel de nube diferente.
- Si utiliza pisos de rendimiento (calidad de servicio mínima), la política de organización en niveles de los volúmenes se debe establecer en `none` Antes de que el agregado pueda adjuntarse a FabricPool.

Otras políticas de organización en niveles impiden que el agregado se anexe a FabricPool. Una política de calidad de servicio no impondrá pisos de rendimiento cuando FabricPool está habilitado.

- Debe seguir las directrices de prácticas recomendadas para usar FabricPool en situaciones específicas.

["Informe técnico de NetApp 4598: Prácticas recomendadas de FabricPool en ONTAP 9"](#)

Consideraciones adicionales al utilizar Cloud Volumes ONTAP

Cloud Volumes ONTAP no requiere una licencia de FabricPool, independientemente del proveedor de almacenamiento de objetos que utilice.

Consideraciones adicionales sobre la organización en niveles de los datos a los que se accede mediante los protocolos SAN

En el caso de la organización en niveles de los datos a los que se accede mediante protocolos SAN, NetApp recomienda utilizar clouds privados, como StorageGRID, debido a consideraciones de conectividad.

Importante

Debe tener en cuenta que, al usar FabricPool en un entorno SAN con un host Windows, si el almacenamiento de objetos deja de estar disponible durante un periodo prolongado a la hora de organizar en niveles los datos en el cloud, es posible que no se pueda acceder o desaparezcan los archivos del LUN de NetApp en el host de Windows. Consulte el artículo de la base de conocimientos ["Durante el almacén de objetos de FabricPool S3 no disponible, un host SAN de Windows informó de daños en el sistema de archivos"](#).

Funcionalidad o funciones no compatibles con FabricPool

- Almacenes de objetos con WORM habilitado y versionado de objetos activado.
- Políticas de gestión de la vida útil de la información (ILM) que se aplican a los bloques de almacenamiento de objetos

FabricPool es compatible con las políticas de gestión del ciclo de vida de la información de StorageGRID solo para la replicación y el código de borrado de datos y proteger los datos del nivel de cloud ante fallos. Sin embargo, FabricPool no admite reglas avanzadas de ILM, como filtrado basado en metadatos o etiquetas de usuario. ILM suele incluir diversas políticas de movimiento y eliminación. Estas políticas pueden provocar interrupciones en los datos del nivel de cloud de FabricPool. El uso de FabricPool con políticas de ILM que están configuradas en almacenes de objetos puede ocasionar la pérdida de datos.

- Transición de datos de 7-Mode mediante comandos de la CLI de ONTAP o la herramienta de transición de 7-Mode
- Virtualización FlexArray
- RAID SyncMirror, excepto en una configuración MetroCluster
- Volúmenes de SnapLock al utilizar ONTAP 9.7 y versiones anteriores
- Backup a cinta mediante SMTape para agregados habilitados para FabricPool
- La función de equilibrio automático
- Volúmenes que usan una garantía de espacio distinta de `none`

Con la excepción de los volúmenes raíz de SVM y los volúmenes de configuración de auditoría CIFS, FabricPool no admite la asociación de un nivel de cloud a un agregado que contenga volúmenes que utilicen una garantía de espacio distinta de `none`. Por ejemplo, un volumen con una garantía de espacio de `volume` (`-space-guarantee volume`) no es compatible.

- Clústeres con ["Licencia DP_Optimized"](#)
- Agregados de Flash Pool

Acerca de las políticas de organización en niveles de FabricPool

Las políticas de organización en niveles de FabricPool le permiten mover los datos de forma eficiente entre niveles a medida que estos se activan o inactivan. Comprender las políticas de organización en niveles le ayuda a seleccionar la política adecuada que se adapte a sus necesidades de gestión del almacenamiento.

Tipos de políticas de organización en niveles de FabricPool

Las políticas de organización en niveles de FabricPool determinan cuándo y si los bloques de datos de usuario de un volumen en FabricPool se mueven al nivel cloud en función del volumen «temperatura» de los activos (activos) o inactivos (inactivos). El volumen «temperatura» aumenta cuando se accede frecuentemente y disminuye cuando no lo es. Algunas políticas de organización en niveles tienen un período de refrigeración mínimo asociado, que establece el tiempo en el que los datos de un volumen de FabricPool deben permanecer inactivos para que los datos se consideren «inactivos» y se trasladen al nivel de cloud.

Una vez identificado un bloque como frío, se marca como apto para la organización en niveles. Un análisis diario de organización en niveles en segundo plano busca los bloques inactivos. Cuando se han recogido suficientes bloques de 4KB KB del mismo volumen, se concatenan en un objeto de 4MB KB y se mueven al nivel de cloud en función de la política de organización en niveles del volumen.



Datos de volúmenes que usan el `all` la política de organización en niveles se marca de inmediato como inactiva y comienza la organización en niveles en el nivel de cloud lo antes posible. No tiene que esperar a que se ejecute el análisis de organización en niveles diario.

Puede utilizar el `volume object-store tiering show` Comando para ver el estado de organización en niveles de un volumen de FabricPool. Para obtener más información, consulte ["Referencia de comandos"](#).

La política de organización en niveles de FabricPool se especifica a nivel de volumen. Hay cuatro opciones disponibles:

- La `snapshot-only` La política de organización en niveles (predeterminada) mueve los bloques de datos de usuario de las copias Snapshot de volumen que no están asociadas con el sistema de archivos activo al nivel de cloud.

El período de refrigeración mínimo de organización en niveles es de 2 días. Puede modificar la configuración predeterminada para el período de refrigeración mínima de organización en niveles con el `-tiering-minimum-cooling-days` parámetro en el nivel de privilegio avanzado del `volume create` y `volume modify` comandos. Los valores válidos abarcan de 2 a 183 días usando ONTAP 9.8 y posterior. Si utiliza una versión de ONTAP anterior a 9.8, los valores válidos abarcan de 2 a 63 días.

- La `auto` La política de organización en niveles, que solo se admite en ONTAP 9.4 y versiones posteriores, mueve bloques de datos de usuario inactivos de las copias Snapshot y el sistema de archivos activo al nivel de cloud.

El período de refrigeración mínimo por niveles predeterminado es de 31 días y se aplica a todo el volumen, tanto en el sistema de archivos activo como en las copias Snapshot.

Puede modificar la configuración predeterminada para el período de refrigeración mínima de organización en niveles con el `-tiering-minimum-cooling-days` parámetro en el nivel de privilegio avanzado del `volume create` y `volume modify` comandos. Los valores válidos abarcan de 2 a 183 días.

- La `all` La política de organización en niveles, compatible solo con ONTAP 9,6 y versiones posteriores, mueve todos los bloques de datos de usuario del sistema de archivos activos y las copias Snapshot al nivel de cloud. Sustituye a la `backup` política de organización en niveles.

La `all` no se debe utilizar la política de organización en niveles de volúmenes de lectura/escritura que tengan tráfico de clientes normal.

El período mínimo de enfriamiento de la organización en niveles no se aplica porque los datos se mueven al nivel de cloud en cuanto se ejecuta el análisis de la organización en niveles y no se puede modificar la

configuración.

- La `none` la política de organización en niveles mantiene los datos de un volumen en el nivel de rendimiento y no se mueven fríos al nivel de cloud.

Configuración de la política de organización en niveles en `none` evita una nueva organización en niveles. Los datos del volumen que anteriormente se han movido al nivel de cloud permanecen en el nivel de cloud hasta que se activan y se trasladan de forma automática al nivel local.

El período de refrigeración mínimo de organización en niveles no se aplica porque los datos nunca se mueven al nivel de cloud y no se puede modificar el ajuste.

Cuando se bloquean bloques de datos inactivos en un volumen con una política de organización en niveles establecida en `none` se leen, se activan y se escriben en el nivel local.

La `volume show` el resultado del comando muestra la política de organización en niveles de un volumen. Un volumen que nunca se utilizó con FabricPool muestra el `none` política de organización en niveles del resultado.

Qué sucede cuando se modifica la política de organización en niveles de un volumen en FabricPool

Puede modificar la política de organización en niveles de un volumen ejecutando un `volume modify` funcionamiento. Debe comprender cómo el cambio de la política de organización en niveles puede afectar el tiempo que tardan los datos en dejar de estar activos y moverse al nivel de cloud.

- Cambiando la política de organización en niveles desde `snapshot-only` o `none` para `auto` Hace que ONTAP envíe bloques de datos de usuario en el sistema de archivos activo que ya están fríos en el nivel cloud, aunque esos bloques de datos de usuario no se hayan elegido anteriormente para el nivel de cloud.
- Cambiando la política de organización en niveles a `all` Desde otra directiva, ONTAP mueve todos los bloques de usuario del sistema de archivos activo y en las copias snapshot al cloud lo antes posible. Antes de ONTAP 9,8, los bloques tenían que esperar hasta que se ejecutara el siguiente análisis de organización en niveles.

No se permite volver a mover los bloques al nivel de rendimiento.

- Cambiando la política de organización en niveles desde `auto` para `snapshot-only` o `none` no hace que los bloques del sistema de archivos activos que ya se hayan movido al nivel de cloud se vuelvan a mover al nivel de rendimiento.

Las lecturas de volumen son necesarias para que los datos se muevan de nuevo al nivel de rendimiento.

- Cada vez que cambie la política de organización en niveles de un volumen, el período de refrigeración mínimo de organización en niveles se restablece al valor predeterminado para la política.

Qué sucede con la política de organización en niveles al mover un volumen

- A menos que se especifique explícitamente una política de organización en niveles diferente, un volumen conserva su política de organización en niveles original cuando este se mueve dentro y fuera de un agregado habilitado para FabricPool.

Sin embargo, la política de organización en niveles solo se aplica cuando el volumen se encuentra en un agregado habilitado para FabricPool.

- El valor existente de `-tiering-minimum-cooling-days` el parámetro de un volumen se mueve con el volumen a menos que se especifique otra política de organización en niveles para el destino.

Si especifica una política de organización en niveles diferente, el volumen utiliza el período de refrigeración mínimo de organización en niveles predeterminado para esa política. Este es el caso si el destino es FabricPool o no.

- Puede mover un volumen entre agregados y, al mismo tiempo, modificar la política de organización en niveles.
- Debe prestar especial atención cuando un `volume move` la operación implica el `auto` política de organización en niveles.

Suponiendo que el origen y el destino sean agregados habilitados para FabricPool, la siguiente tabla resume el resultado de un `volume move` operación que implica cambios de directiva relacionados con `auto`:

| Cuando se mueve un volumen con una política de organización en niveles de... | Y la política de organización en niveles se cambia a... | Después de mover el volumen... |
|--|---|--|
| <code>all</code> | <code>auto</code> | Todos los datos se mueven al nivel de rendimiento. |
| <code>snapshot-only, none, 0. auto</code> | <code>auto</code> | Los bloques de datos se mueven al mismo nivel del destino que anteriormente se encontraban en el origen. |
| <code>auto 0. all</code> | <code>snapshot-only</code> | Todos los datos se mueven al nivel de rendimiento. |
| <code>auto</code> | <code>all</code> | Todos los datos de usuario se mueven al nivel de cloud. |
| <code>snapshot-only, auto 0. all</code> | <code>none</code> | Todos los datos se conservan en el nivel de rendimiento. |

Qué sucede en la política de organización en niveles al clonar un volumen

- A partir de ONTAP 9.8, un volumen clonado siempre hereda la política de organización en niveles y la política de recuperación de cloud del volumen principal.

En las versiones anteriores a ONTAP 9.8, un clon hereda la política de organización en niveles del elemento principal, excepto cuando el elemento principal tiene el `all` política de organización en niveles.

- Si el volumen principal tiene el `never` política de recuperación de cloud, su volumen clonado debe tener el `never` política de recuperación en cloud o el `all` política de organización en niveles y una política de recuperación en el cloud correspondiente `default`.
- La política de recuperación de cloud del volumen principal no se puede cambiar a `never` a menos que todos los volúmenes clonados tengan una política de recuperación en el cloud `never`.

Al clonar volúmenes, tenga en cuenta las siguientes prácticas recomendadas:

- La `-tiering-policy` opción y `tiering-minimum-cooling-days` la opción del clon solo controla el comportamiento de organización en niveles de los bloques únicos para el clon. Por lo tanto, se recomienda utilizar la configuración de organización en niveles en la FlexVol principal que mueva la misma cantidad de datos o mueva menos datos que ninguno de los clones
- La política de recuperación de cloud del FlexVol principal debería mover la misma cantidad de datos o debería mover más datos que la política de recuperación de cualquiera de los clones

Funcionamiento de las políticas de organización en niveles con la migración al cloud

La recuperación de datos en el cloud de FabricPool se controla mediante políticas de niveles que determinan la recuperación de datos del nivel de cloud al nivel de rendimiento según el patrón de lectura. Los patrones de lectura pueden ser secuenciales o aleatorios.

En la siguiente tabla, se enumeran las políticas de organización en niveles y las reglas de recuperación de datos en el cloud para cada política.

| Política de organización en niveles | Comportamiento de la recuperación |
|-------------------------------------|------------------------------------|
| ninguno | Lecturas secuenciales y aleatorias |
| solo snapshot | Lecturas secuenciales y aleatorias |
| automático | Lecturas aleatorias |
| todo | Sin recuperación de datos |

A partir de ONTAP 9.8, el control de la migración al cloud `cloud-retrieval-policy` esta opción anula el comportamiento de migración o recuperación de cloud predeterminado controlado por la política de organización en niveles.

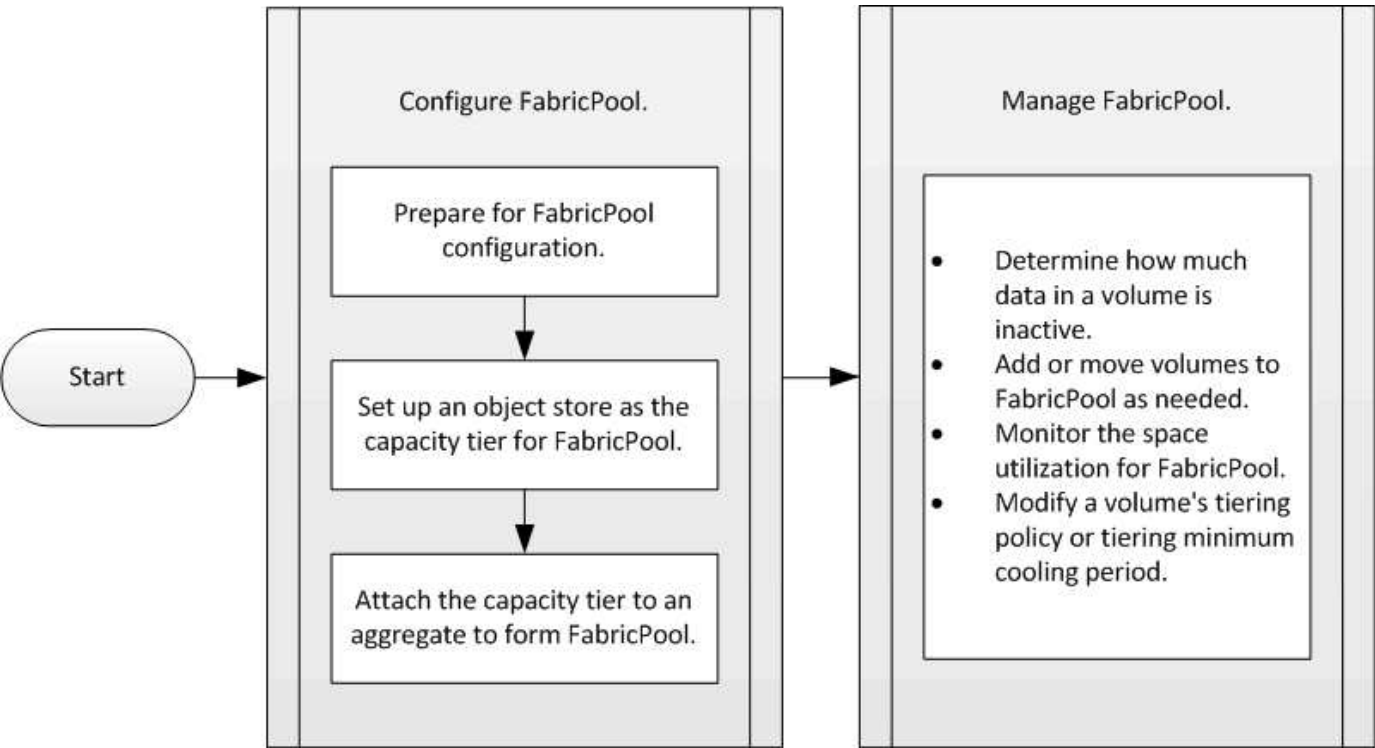
En la siguiente tabla se enumeran las políticas de recuperación de cloud admitidas y su comportamiento de recuperación.

| Política de recuperación de cloud | Comportamiento de la recuperación |
|-----------------------------------|---|
| predeterminado | La política de organización en niveles decide qué datos deben extraerse, de modo que no hay ningún cambio en la recuperación de datos en el cloud con "valor predeterminado," <code>`cloud-retrieval-policy</code> . Esta política es el valor predeterminado para cualquier volumen independientemente del tipo de agregado alojado. |
| lectura | Todas las lecturas de datos condicionadas por el cliente se realiza desde el nivel de cloud al nivel de rendimiento. |

| | |
|-------------|---|
| nunca | No se datos controlados por el cliente que pase del nivel de cloud al nivel de rendimiento |
| promocionar | <ul style="list-style-type: none">• En lo que respecta a la política de organización en niveles «'none'», todos los datos del cloud se envían del nivel de cloud al nivel de rendimiento• En cuanto a la política de organización en niveles, se obtienen los datos de AFS «solo sinapshot». |

Flujo de trabajo de gestión de FabricPool

Puede usar el diagrama de flujo de trabajo de FabricPool como ayuda para planificar las tareas de configuración y gestión.



Configure FabricPool

Prepárese para la configuración de FabricPool

Preparación para la información general de la configuración de FabricPool

La configuración de FabricPool le ayuda a gestionar qué nivel de almacenamiento (el nivel de rendimiento local o el nivel cloud) se deben almacenar en función de si se accede frecuentemente a los datos.

La preparación necesaria para la configuración de FabricPool depende del almacén de objetos que se use como nivel de cloud.

A partir de ONTAP 9.9.0, se puede usar System Manager para añadir una conexión al cloud.

Para comenzar, debe utilizar Cloud Insights de NetApp para configurar un recopilador. Durante el proceso de configuración, copia un código de emparejamiento que genera Cloud Insights y, a continuación, inicia sesión en un clúster mediante System Manager. Allí, se agrega una conexión de nube mediante ese código de emparejamiento. El resto del proceso se completa en Cloud Insights.



Si elige la opción de utilizar un servidor proxy al agregar una conexión de Cloud Volumes ONTAP al servicio Cloud Insights, debe asegurarse de que la URL <https://example.com> es accesible desde el servidor proxy. El mensaje "la configuración del proxy HTTP no es válida" se muestra cuando <https://example.com> no es accesible.

Pasos

1. En Cloud Insights, durante el proceso de configuración de un recopilador, copie el código de emparejamiento generado.
2. Utilice System Manager con ONTAP 9.9.0 o una versión posterior, inicie sesión en el clúster.
3. Vaya a **Cluster > Settings**.
4. En la sección conexiones en la nube, seleccione **Agregar** para agregar una conexión.
5. Introduzca un nombre para la conexión y pegue el código de emparejamiento en el espacio proporcionado.
6. Seleccione **Agregar**.
7. Vuelva a Cloud Insights para completar la configuración del recopilador.

Para obtener más información sobre Cloud Insights, consulte ["Documentación de Cloud Insights"](#).

Instalar una licencia de FabricPool

La licencia de FabricPool que podría haber utilizado en el pasado está cambiando y se mantiene sólo para configuraciones que no son compatibles con BlueXP. A partir del 21 de agosto de 2021, se incorporaron las licencias de BYOL de Cloud Tiering para las configuraciones de organización en niveles que son compatibles con BlueXP mediante el servicio Cloud Tiering.

["Obtenga más información sobre las nuevas licencias BYOL de Cloud Tiering"](#).

Las configuraciones compatibles con BlueXP deben utilizar la página de cartera digital de BlueXP para la organización en niveles de licencias para clústeres de ONTAP. Esto requiere que configure una cuenta de BlueXP y configure la organización en niveles para el proveedor de almacenamiento de objetos concreto que desee utilizar. Actualmente, BlueXP admite la organización en niveles en el siguiente almacenamiento de objetos: Amazon S3, almacenamiento blob de Azure, Google Cloud Storage, almacenamiento de objetos compatible con S3 y StorageGRID.

["Más información acerca del servicio de organización en niveles del cloud"](#).

Puede descargar y activar una licencia de FabricPool mediante System Manager si tiene una de las configuraciones que no es compatible con BlueXP:

- Instalaciones de ONTAP en sitios oscuros
- Clústeres de ONTAP que organizarán en niveles los datos en el almacenamiento de objetos en IBM Cloud o en el almacenamiento de objetos en Alibaba Cloud

La licencia FabricPool es una licencia para todo el clúster. Incluye un límite de uso autorizado que ha adquirido para el almacenamiento de objetos asociado con FabricPool en el clúster. El uso en todo el clúster no debe superar la capacidad del límite de uso autorizado. Si necesita aumentar el límite de uso de la licencia, debe ponerse en contacto con su representante de ventas.

Las licencias de FabricPool están disponibles en formatos perpetuas o basados en períodos de 1 o 3 años.

Existe una licencia de FabricPool basada en términos de términos con 10 TB de capacidad libre disponible por primera vez para pedidos de FabricPool para configuraciones de clusters existentes no compatibles con BlueXP. La capacidad libre no está disponible con licencias perpetuas.

La licencia no es necesaria si se usa StorageGRID de NetApp o ONTAP S3 para el nivel de cloud. Cloud Volumes ONTAP no requiere una licencia de FabricPool, independientemente del proveedor que utilice.

Esta tarea solo se admite cargando el archivo de licencia al clúster mediante System Manager.

Pasos

1. Descargue el archivo de licencia de NetApp (NLF) para obtener la licencia de FabricPool de ["Sitio de soporte de NetApp"](#).
2. Realice las siguientes acciones mediante System Manager para cargar la licencia de FabricPool en el clúster:
 - a. En el panel **Cluster > Settings**, en la tarjeta **Licenses**, haga clic en ➔.
 - b. En la página **Licencia**, haga clic en **+ Add**.
 - c. En el cuadro de diálogo **Agregar licencia**, haga clic en **examinar** para seleccionar el NLF que descargó y, a continuación, haga clic en **Agregar** para cargar el archivo en el clúster.

Información relacionada

["Descripción general de las licencias de ONTAP FabricPool \(FP\)"](#)

["Búsqueda de licencias de software de NetApp"](#)

["NetApp TechComm TV: Lista de reproducción de FabricPool"](#)

Instale un certificado de CA si utiliza StorageGRID

A menos que planifique deshabilitar la comprobación de certificados para StorageGRID, debe instalar un certificado de CA de StorageGRID en el clúster para que ONTAP pueda autenticarse con StorageGRID como almacén de objetos para FabricPool.

Acerca de esta tarea

ONTAP 9.4 y versiones posteriores permiten deshabilitar la comprobación de certificados para StorageGRID.

Pasos

1. Póngase en contacto con el administrador de StorageGRID para obtener el certificado de CA del sistema StorageGRID.
2. Utilice la `security certificate install` con el `-type server-ca` Parámetro para instalar el certificado de CA de StorageGRID en el clúster.

El nombre de dominio completo (FQDN) que introduzca debe coincidir con el nombre común personalizado del certificado de CA de StorageGRID.

Actualice un certificado caducado

Para actualizar un certificado caducado, la práctica recomendada es usar una CA de confianza para generar el nuevo certificado de servidor. Además, debe asegurarse de que el certificado se actualice en el servidor StorageGRID y en el clúster de ONTAP al mismo tiempo para mantener el tiempo de inactividad al mínimo.

Información relacionada

["Recursos de StorageGRID"](#)

Instale un certificado de CA si usa ONTAP S3

A menos que planifique deshabilitar la comprobación de certificados para ONTAP S3, debe instalar un certificado de CA de ONTAP S3 en el clúster para que ONTAP pueda autenticarse con ONTAP S3 como almacén de objetos para FabricPool.

Pasos

1. Obtenga el certificado de CA del sistema ONTAP S3.
2. Utilice la `security certificate install` con el `-type server-ca` Parámetro para instalar el certificado de CA de ONTAP S3 en el clúster.

El nombre de dominio completo (FQDN) que introduzca debe coincidir con el nombre común personalizado en el certificado de CA de ONTAP S3.

Actualice un certificado caducado

Para actualizar un certificado caducado, la práctica recomendada es usar una CA de confianza para generar el nuevo certificado de servidor. Además, debe asegurarse de que el certificado se actualice en el servidor ONTAP S3 y en el clúster ONTAP al mismo tiempo para mantener el tiempo de inactividad al mínimo.

Información relacionada

["Configuración de S3"](#)

Configure un almacén de objetos como nivel cloud para FabricPool

Configure un almacén de objetos como nivel del cloud para la información general de FabricPool

La configuración de FabricPool implica especificar la información de configuración del almacén de objetos (StorageGRID, ONTAP S3, Alibaba Cloud Object Storage, Amazon S3, Google Cloud Storage, IBM Cloud Object Storage o Microsoft Azure Blob Storage para el cloud) que planea utilizar como nivel de cloud para FabricPool.

Configure StorageGRID como nivel de cloud

Si utiliza ONTAP 9.2 o una versión posterior, puede configurar StorageGRID como nivel de cloud para FabricPool. En el caso de la organización en niveles de los datos a los que se accede mediante protocolos SAN, NetApp recomienda utilizar clouds privados, como StorageGRID, debido a consideraciones de conectividad.

Consideraciones para usar StorageGRID con FabricPool

- Debe instalar un certificado de CA para StorageGRID, a menos que deshabilite explícitamente la comprobación de certificados.
- No debe habilitar el control de versiones de objetos StorageGRID en el bloque de almacenamiento de objetos.
- No se necesita una licencia de FabricPool.
- Si un nodo StorageGRID se pone en marcha en una máquina virtual con almacenamiento asignado de un sistema AFF de NetApp, confirme que el volumen no tiene habilitada una política de organización en niveles de FabricPool.

Al deshabilitar el almacenamiento en niveles de FabricPool para los volúmenes que se usan con los nodos StorageGRID, se simplifica la solución de problemas y las operaciones de almacenamiento.



No utilice nunca FabricPool para colocar en niveles datos relacionados con StorageGRID en el propio StorageGRID. La organización en niveles de los datos de StorageGRID en StorageGRID aumenta la solución de problemas y la complejidad operativa.

Acerca de esta tarea

El equilibrio de carga se habilita para StorageGRID en ONTAP 9.8 y versiones posteriores. Cuando el nombre de host del servidor se resuelve en más de una dirección IP, ONTAP establece conexiones de cliente con todas las direcciones IP devueltas (hasta un máximo de 16 direcciones IP). Las direcciones IP se recogen en un método round-robin cuando se establecen conexiones.

Procedimientos

Puede configurar StorageGRID como nivel de cloud para FabricPool con ONTAP System Manager o la CLI de ONTAP.

System Manager

1. Haga clic en **almacenamiento > niveles > Agregar nivel de cloud** y seleccione StorageGRID como proveedor de almacén de objetos.
2. Complete la información solicitada.
3. Si desea crear una réplica en la nube, haga clic en **Agregar como réplica de FabricPool**.

El duplicado de FabricPool proporciona un método para sustituir sin problemas un almacén de datos y contribuye a garantizar que sus datos estén disponibles en caso de desastre.

CLI

1. Especifique la información de configuración de la StorageGRID mediante el `storage aggregate object-store config create` con el `-provider-type SGWS` parámetro.
 - La `storage aggregate object-store config create` Error del comando si ONTAP no puede acceder a StorageGRID con la información proporcionada.
 - Utilice la `-access-key` Parámetro para especificar la clave de acceso para autorizar solicitudes al almacén de objetos StorageGRID.
 - Utilice la `-secret-password` Parámetro para especificar la contraseña (clave de acceso secreta) para autenticar solicitudes en el almacén de objetos StorageGRID.
 - Si se cambia la contraseña de StorageGRID, debe actualizar inmediatamente la contraseña correspondiente almacenada en ONTAP.

De esta manera, ONTAP puede acceder a los datos en StorageGRID sin interrupciones.

- Ajuste de `-is-certificate-validation-enabled` parámetro a. `false` Deshabilita la comprobación de certificados para StorageGRID.

```
cluster1::> storage aggregate object-store config create
-object-store-name mySGWS -provider-type SGWS -server mySGWSserver
-container-name mySGWScontainer -access-key mySGWSkey
-secret-password mySGWSpass
```

2. Muestre y verifique la información de configuración de la StorageGRID mediante el `storage aggregate object-store config show` comando.

La `storage aggregate object-store config modify` Command le permite modificar la información de configuración de StorageGRID para FabricPool.

Configure ONTAP S3 como nivel del cloud

Si utiliza ONTAP 9.8 o una versión posterior, puede configurar ONTAP S3 como nivel de cloud para FabricPool.

Lo que necesitará

Debe tener el nombre del servidor ONTAP S3 y la dirección IP de sus LIF asociadas en el clúster remoto.

Deben haber LIF de interconexión de clústeres en el clúster local.

["Creación de LIF de interconexión de clústeres para la organización en niveles de FabricPool remota"](#)

Acerca de esta tarea

El equilibrio de carga se habilita para los servidores ONTAP S3 en ONTAP 9.8 y versiones posteriores. Cuando el nombre de host del servidor se resuelve en más de una dirección IP, ONTAP establece conexiones de cliente con todas las direcciones IP devueltas (hasta un máximo de 16 direcciones IP). Las direcciones IP se recogen en un método round-robin cuando se establecen conexiones.

Procedimientos

Puede configurar ONTAP S3 como nivel de cloud para FabricPool con ONTAP System Manager o la interfaz de línea de comandos de ONTAP.

System Manager

1. Haga clic en **almacenamiento > niveles > Agregar nivel de cloud** y seleccione ONTAP S3 como proveedor de almacén de objetos.
2. Complete la información solicitada.
3. Si desea crear una réplica en la nube, haga clic en **Agregar como réplica de FabricPool**.

El duplicado de FabricPool proporciona un método para sustituir sin problemas un almacén de datos y contribuye a garantizar que sus datos estén disponibles en caso de desastre.

CLI

1. Añada entradas para el servidor S3 y las LIF al servidor DNS.

| Opción | Descripción |
|---|---|
| Si utiliza un servidor DNS externo | Proporcione el nombre y las direcciones IP del servidor S3 al administrador del servidor DNS. |
| Si utiliza la tabla de hosts DNS del sistema local | Introduzca el siguiente comando: <pre>dns host create -vserver svm_name -address ip_address -hostname s3_server_name</pre> |

2. Especifique la información de configuración de ONTAP S3 mediante el `storage aggregate object-store config create` con el `-provider-type ONTAP_S3` parámetro.
 - La `storage aggregate object-store config create` Error de comando si el sistema ONTAP local no puede acceder al servidor ONTAP S3 con la información proporcionada.
 - Utilice la `-access-key` Parámetro para especificar la clave de acceso a fin de autorizar solicitudes al servidor ONTAP S3.
 - Utilice la `-secret-password` Parámetro para especificar la contraseña (clave de acceso secreta) para autenticar solicitudes en el servidor ONTAP S3.
 - Si se cambia la contraseña del servidor ONTAP S3, debe actualizar de inmediato la contraseña correspondiente almacenada en el sistema ONTAP local.

Así, es posible acceder a los datos del almacén de objetos ONTAP S3 sin interrumpir el proceso.

- Ajuste de `-is-certificate-validation-enabled` parámetro a. `false` Deshabilita la comprobación de certificados para ONTAP S3.

```
cluster1::> storage aggregate object-store config create  
-object-store-name myS3 -provider-type ONTAP_S3 -server myS3server  
-container-name myS3container -access-key myS3key  
-secret-password myS3pass
```

3. Muestre y verifique la información de configuración de ONTAP_S3 mediante el `storage aggregate object-store config show` comando.

La `storage aggregate object-store config modify` el comando le permite modificar la `ONTAP_S3` Información de configuración de FabricPool.

Configure Alibaba Cloud Object Storage como nivel de cloud

Si utiliza ONTAP 9.6 o una versión posterior, puede configurar Alibaba Cloud Object Storage como nivel cloud para FabricPool.

Consideraciones sobre el uso del almacenamiento de objetos en cloud de Alibaba con FabricPool

- Puede que necesite una licencia de FabricPool.

Los sistemas AFF recientemente solicitados incluyen 10 TB de capacidad libre para usar FabricPool. Si necesita capacidad adicional en un sistema AFF, si utiliza Alibaba Cloud Object Storage en un sistema distinto a AFF o si actualiza desde un clúster existente, necesita uno "[Licencia de FabricPool](#)".

- En los sistemas AFF y FAS y ONTAP Select, FabricPool es compatible con las siguientes clases de servicio de almacenamiento de objetos Alibaba:
 - Estándar de servicio de almacenamiento de objetos de Alibaba
 - Acceso poco frecuente al servicio de almacenamiento de objetos de Alibaba

["Alibaba Cloud: Introducción a clases de almacenamiento"](#)

Póngase en contacto con el representante de ventas de NetApp para obtener información sobre las clases de almacenamiento que no figuran en esta lista.

Pasos

1. Especifique la información de configuración del almacenamiento de objetos Alibaba Cloud mediante la `storage aggregate object-store config create` con el `-provider-type AliCloud` parámetro.
 - La `storage aggregate object-store config create` El comando genera un error si ONTAP no puede acceder al almacenamiento de objetos en cloud de Alibaba con la información proporcionada.
 - Utilice la `-access-key` Parámetro para especificar la clave de acceso para autorizar solicitudes al almacén de objetos Alibaba Cloud Object Storage.
 - Si se cambia la contraseña de almacenamiento de objetos Alibaba Cloud, debe actualizar la contraseña correspondiente almacenada en ONTAP inmediatamente.

Con ello, ONTAP puede acceder a los datos en el almacenamiento de objetos en cloud de Alibaba sin interrupciones.

```
storage aggregate object-store config create my_ali_oss_store_1
-provider-type AliCloud -server oss-us-east-1.aliyuncs.com
-container-name my-ali-oss-bucket -access-key DXJRXHPXHYXA9X31X3JX
```

2. Muestre y verifique la información de configuración del almacenamiento de objetos Alibaba Cloud mediante la `storage aggregate object-store config show` comando.

La `storage aggregate object-store config modify` Command permite modificar la información de configuración del almacenamiento de objetos Alibaba Cloud para FabricPool.

Configure Amazon S3 como nivel de cloud

Si ejecuta ONTAP 9,2 o una versión posterior, puede configurar Amazon S3 como nivel de cloud para FabricPool. Si ejecuta ONTAP 9,5 o una versión posterior, puede configurar Amazon Commercial Cloud Services (C2S) para FabricPool.

Consideraciones para usar Amazon S3 con FabricPool

- Puede que necesite una licencia de FabricPool.
 - Los sistemas AFF recientemente solicitados incluyen 10 TB de capacidad libre para usar FabricPool.
- Si necesita capacidad adicional en un sistema AFF, si usa Amazon S3 en un sistema que no es AFF o si actualiza desde un clúster existente, necesita uno "[Licencia de FabricPool](#)".

Si solicita FabricPool por primera vez para un clúster existente, existe una licencia FabricPool con 10 TB de capacidad libre.

- Se recomienda que la LIF que ONTAP utiliza para conectarse con el servidor de objetos Amazon S3 esté en un puerto de 10 Gbps.
- En los sistemas AFF y FAS y en ONTAP Select, FabricPool admite las siguientes clases de almacenamiento Amazon S3:
 - Amazon S3 Standard
 - Amazon S3 Estándar - acceso poco frecuente (Estándar - IA)
 - Amazon S3 One Zone - acceso poco frecuente (una zona - IA)
 - Segmentación inteligente de Amazon S3
 - Servicios de cloud comercial de Amazon
 - A partir de ONTAP 9.11.1, Amazon S3 Glacier Instant Retrieval (FabricPool no es compatible con Glacier Flexible Retrieval o Glacier Deep Archive)

["Documentación de Amazon Web Services: Clases de almacenamiento de Amazon S3"](#)

Póngase en contacto con su representante de ventas para obtener información sobre las clases de almacenamiento que no aparecen en esta lista.

- En Cloud Volumes ONTAP, FabricPool admite la organización en niveles desde SSD de uso general (gp2) y volúmenes de HDD optimizados para el rendimiento (st1) de Amazon Elastic Block Store (EBS).

Pasos

1. Especifique la información de configuración de Amazon S3 mediante el `storage aggregate object-store config create` con el `-provider-type AWS_S3` parámetro.
 - Utilice la `-auth-type CAP` Parámetro para obtener credenciales de acceso al C2S.

Cuando utilice la `-auth-type CAP` debe usar el `-cap-url` Parámetro para especificar la URL completa para solicitar credenciales temporales para el acceso C2S.

- La `storage aggregate object-store config create` El comando falla si ONTAP no puede acceder a Amazon S3 con la información proporcionada.
- Utilice la `-access-key` Parámetro para especificar la clave de acceso para autorizar solicitudes al almacén de objetos de Amazon S3.
- Utilice la `-secret-password` Parámetro para especificar la contraseña (clave de acceso secreta) para autenticar solicitudes al almacén de objetos Amazon S3.
- Si se cambia la contraseña de Amazon S3, debe actualizar inmediatamente la contraseña correspondiente almacenada en ONTAP.

Al hacerlo, ONTAP puede acceder a los datos de Amazon S3 sin interrupciones.

```
cluster1::> storage aggregate object-store config create
-object-store-name my_aws_store -provider-type AWS_S3
-server s3.amazonaws.com -container-name my-aws-bucket
-access-key DXJRXHPXHYXA9X31X3JX
```

+

```
cluster1::> storage aggregate object-store config create -object-store
-name my_c2s_store -provider-type AWS_S3 -auth-type CAP -cap-url
https://123.45.67.89/api/v1/credentials?agency=XYZ&mission=TESTACCT&role
=S3FULLACCESS -server my-c2s-s3server-fqdn -container my-c2s-s3-bucket
```

2. Muestre y verifique la información de configuración de Amazon S3 mediante el `storage aggregate object-store config show` comando.

La `storage aggregate object-store config modify` El comando le permite modificar la información de configuración de Amazon S3 para FabricPool.

Configure Google Cloud Storage como nivel del cloud

Si utiliza ONTAP 9.6 o una versión posterior, puede configurar Google Cloud Storage como nivel de cloud para FabricPool.

Consideraciones adicionales para usar Google Cloud Storage con FabricPool

- Puede que necesite una licencia de FabricPool.

Los sistemas AFF recientemente solicitados incluyen 10 TB de capacidad libre para usar FabricPool. Si necesita capacidad adicional en un sistema AFF, si usa Google Cloud Storage en un sistema distinto a AFF o si actualiza desde un clúster existente, necesita uno [xref:./fabricpool/"Licencia de FabricPool"](#).

- Se recomienda que el LIF que utiliza ONTAP para conectarse con el servidor de objetos Google Cloud Storage esté en un puerto de 10 Gbps.
- En los sistemas AFF y FAS y ONTAP Select, FabricPool admite las siguientes clases de almacenamiento de objetos Google Cloud:

- Google Cloud Multi-Regional
- Google Cloud Regional
- Google Cloud Nearline
- Google Cloud Coldline

["Google Cloud: Clases de almacenamiento"](#)

Pasos

1. Especifique la información de configuración de Google Cloud Storage mediante el `storage aggregate object-store config create` con el `-provider-type GoogleCloud` parámetro.
 - La `storage aggregate object-store config create` Error del comando si ONTAP no puede acceder a Google Cloud Storage con la información proporcionada.
 - Utilice la `-access-key` Parámetro para especificar la clave de acceso para autorizar solicitudes al almacén de objetos de Google Cloud Storage.
 - Si se cambia la contraseña de Google Cloud Storage, debe actualizar la contraseña correspondiente almacenada en ONTAP inmediatamente.

Al hacerlo, ONTAP puede acceder a los datos de Google Cloud Storage sin interrupciones.

```
storage aggregate object-store config create my_gcp_store_1 -provider
-type GoogleCloud -container-name my-gcp-bucket1 -access-key
GOOGAUZZUV2USCFGHGQ511I8
```

2. Muestre y verifique la información de configuración de Google Cloud Storage mediante la `storage aggregate object-store config show` comando.

La `storage aggregate object-store config modify` Command permite modificar la información de configuración de Google Cloud Storage para FabricPool.

Configure IBM Cloud Object Storage como nivel del cloud

Si utiliza ONTAP 9.5 o una versión posterior, puede configurar IBM Cloud Object Storage como nivel de cloud para FabricPool.

Consideraciones para usar el almacenamiento de objetos en cloud de IBM con FabricPool

- Puede que necesite una licencia de FabricPool.

Los sistemas AFF recientemente solicitados incluyen 10 TB de capacidad libre para usar FabricPool. Si necesita capacidad adicional en un sistema AFF, si usa IBM Cloud Object Storage en un sistema distinto a AFF o si actualiza desde un clúster existente, necesita uno ["Licencia de FabricPool"](#).

Si solicita FabricPool por primera vez para un clúster existente, existe una licencia FabricPool con 10 TB de capacidad libre.

- Se recomienda que el LIF que ONTAP utiliza para conectarse con el servidor de objetos IBM Cloud se encuentre en un puerto de 10 Gbps.

Pasos

1. Especifique la información de configuración del almacenamiento de objetos en el cloud de IBM mediante el `storage aggregate object-store config create` con el `-provider-type IBM_COS` parámetro.
 - La `storage aggregate object-store config create` Error del comando si ONTAP no puede acceder al almacenamiento de objetos en cloud de IBM con la información proporcionada.
 - Utilice la `-access-key` Parámetro para especificar la clave de acceso para autorizar solicitudes al almacén de objetos IBM Cloud Object Storage.
 - Utilice la `-secret-password` Parámetro para especificar la contraseña (clave de acceso secreta) para autenticar solicitudes en el almacén de objetos IBM Cloud Object Storage.
 - Si se cambia la contraseña IBM Cloud Object Storage, debe actualizar la contraseña correspondiente almacenada en ONTAP inmediatamente.

Esto permite que ONTAP acceda a los datos en el almacenamiento de objetos en cloud de IBM sin interrupciones.

```
storage aggregate object-store config create
-object-store-name MyIBM -provider-type IBM_COS
-server s3.us-east.objectstorage.softlayer.net
-container-name my-ibm-cos-bucket -access-key DXJRXHPXHYXA9X31X3JX
```

2. Para mostrar y verificar la información de configuración de IBM Cloud Object Storage, utilice la `storage aggregate object-store config show` comando.

La `storage aggregate object-store config modify` Comando permite modificar la información de configuración del almacenamiento de objetos en cloud de IBM para FabricPool.

Configure Azure Blob Storage para el cloud como nivel de cloud

Si utiliza ONTAP 9.4 o una versión posterior, puede configurar Azure Blob Storage para el cloud como nivel de cloud para FabricPool.

Consideraciones para usar el almacenamiento BLOB de Microsoft Azure con FabricPool

- Puede que necesite una licencia de FabricPool.

Los sistemas AFF recientemente solicitados incluyen 10 TB de capacidad libre para usar FabricPool. Si necesita capacidad adicional en un sistema AFF, si utiliza Azure Blob Storage en un sistema distinto a AFF o si actualiza desde un clúster existente, necesita un `xref:./fabricpool/"Licencia de FabricPool"`.

Si solicita FabricPool por primera vez para un clúster existente, existe una licencia FabricPool con 10 TB de capacidad libre.

- No es necesaria una licencia de FabricPool si utiliza Azure Blob Storage con Cloud Volumes ONTAP.
- Se recomienda que la LIF que ONTAP utiliza para conectar con el servidor de objetos de almacenamiento BLOB de Azure esté en un puerto de 10 Gbps.
- FabricPool actualmente no es compatible con la pila de Azure, que se trata de servicios de Azure en las instalaciones.

- En el nivel de cuenta de Microsoft Azure Blob Storage, FabricPool solo admite los niveles de almacenamiento caliente y frío.

FabricPool no admite la organización en niveles a nivel BLOB. Tampoco admite la segmentación en niveles para el nivel de almacenamiento de archivado de Azure.

Acerca de esta tarea

FabricPool actualmente no es compatible con la pila de Azure, que se trata de servicios de Azure en las instalaciones.

Pasos

1. Especifique la información de configuración de Azure Blob Storage mediante el `storage aggregate object-store config create` con el `-provider-type Azure_Cloud` parámetro.
 - La `storage aggregate object-store config create` El comando falla si ONTAP no puede acceder al almacenamiento BLOB de Azure con la información proporcionada.
 - Utilice la `-azure-account` Parámetro para especificar la cuenta de Azure Blob Storage.
 - Utilice la `-azure-private-key` Parámetro para especificar la clave de acceso para autenticar solicitudes a Azure Blob Storage.
 - Si se cambia la contraseña de almacenamiento blob de Azure, debe actualizar la contraseña correspondiente almacenada en ONTAP de forma inmediata.

Al hacerlo, ONTAP puede acceder a los datos de Azure Blob Storage sin interrupciones.

```
cluster1::> storage aggregate object-store config create
-object-store-name MyAzure -provider-type Azure_Cloud
-server blob.core.windows.net -container-name myAzureContainer
-azure-account myAzureAcct -azure-private-key myAzureKey
```

2. Muestre y verifique la información de configuración de Azure Blob Storage mediante el `storage aggregate object-store config show` comando.

La `storage aggregate object-store config modify` Command le permite modificar la información de configuración de Azure Blob Storage para FabricPool.

Configure almacenes de objetos para FabricPool en una configuración de MetroCluster

Si ejecuta ONTAP 9.7 o una versión posterior, puede configurar un FabricPool reflejado en una configuración MetroCluster con el fin de organizar los datos inactivos en almacenes de objetos en dos zonas de fallo diferentes.

Acerca de esta tarea

- FabricPool en MetroCluster requiere que el agregado reflejado subyacente y la configuración del almacén de objetos asociados deban ser propiedad de la misma configuración de MetroCluster.
- No puede adjuntar un agregado a un almacén de objetos que se cree en el sitio MetroCluster remoto.
- Debe crear configuraciones del almacén de objetos en la configuración de MetroCluster que posea el agregado.

Antes de empezar

- La configuración de MetroCluster está configurada y correctamente configurada.
- Se configuran dos almacenes de objetos en los sitios MetroCluster correspondientes.
- Los contenedores se configuran en cada almacén de objetos.
- Los espacios IP se crean o identifican en las dos configuraciones de MetroCluster y sus nombres coinciden.

Paso

1. Especifique la información de configuración del almacén de objetos en cada sitio MetroCluster mediante el `storage object-store config create` comando.

En este ejemplo, FabricPool solo es necesario en un clúster de la configuración de MetroCluster. Se crean dos configuraciones de almacén de objetos para ese clúster, una para cada bloque de almacenamiento de objetos.

```
storage aggregate
  object-store config create -object-store-name mcc1-ostore-config-s1
  -provider-type SGWS -server
    <SGWS-server-1> -container-name <SGWS-bucket-1> -access-key <key>
  -secret-password <password> -encrypt
    <true|false> -provider <provider-type> -is-ssl-enabled <true|false>
  ipspace
    <IPSpace>
```

```
storage aggregate object-store config create -object-store-name mcc1-
ostore-config-s2
  -provider-type SGWS -server <SGWS-server-2> -container-name <SGWS-
bucket-2> -access-key <key> -secret-password <password> -encrypt
  <true|false> -provider <provider-type>
  -is-ssl-enabled <true|false> ipspace <IPSpace>
```

En este ejemplo, se configura FabricPool en el segundo clúster de la configuración de MetroCluster.

```
storage aggregate
  object-store config create -object-store-name mcc2-ostore-config-s1
  -provider-type SGWS -server
    <SGWS-server-1> -container-name <SGWS-bucket-3> -access-key <key>
  -secret-password <password> -encrypt
    <true|false> -provider <provider-type> -is-ssl-enabled <true|false>
  ipspace
    <IPSpace>
```

```
storage aggregate
  object-store config create -object-store-name mcc2-ostore-config-s2
  -provider-type SGWS -server
    <SGWS-server-2> -container-name <SGWS-bucket-4> -access-key <key>
  -secret-password <password> -encrypt
    <true|false> -provider <provider-type> -is-ssl-enabled <true|false>
  ipspace
    <IPSpace>
```

Pruebe el rendimiento del almacén de objetos antes de vincularlo a un nivel local

Antes de conectar un almacén de objetos a un nivel local, puede probar la latencia y el rendimiento del almacén de objetos mediante el generador de perfiles de almacenes de objetos.

Antes de ser

- Debe agregar el nivel de cloud a ONTAP antes de poder usarlo con el analizador de perfiles del almacén de objetos.
- Debe estar en el modo de privilegios avanzado de la CLI de ONTAP.

Pasos

1. Inicie el analizador de perfiles del almacén de objetos:

```
storage aggregate object-store profiler start -object-store-name <name> -node
<name>
```

2. Vea los resultados:

```
storage aggregate object-store profiler show
```

Adjuntar el nivel de cloud a un nivel local (agregado)

Después de configurar un almacén de objetos como nivel de cloud, debe especificar el nivel local (agregado) que usará adjunto a FabricPool. En ONTAP 9.5 y versiones posteriores, también puede conectar niveles locales (agregados) que contengan componentes de volumen FlexGroup cualificados.

Acerca de esta tarea

Asociar un nivel de cloud a un nivel local es una acción permanente. No se puede desconectar un nivel de cloud de un nivel local después de conectarlo. Sin embargo, puede utilizar ["Espejo de FabricPool"](#) para adjuntar un nivel local a un nivel de nube diferente.

Antes de empezar

Cuando utilice la interfaz de línea de comandos de ONTAP para configurar un agregado para FabricPool, este ya debe existir.



Cuando se usa System Manager para configurar un nivel local para FabricPool, es posible crear el nivel local y configurarlo para que lo use para FabricPool al mismo tiempo.

Pasos

Puede asociar un nivel local (agregado) a un almacén de objetos FabricPool con System Manager de ONTAP o la CLI de ONTAP.

System Manager

1. Vaya a **almacenamiento > niveles**, seleccione un nivel en la nube y, a continuación, haga clic en
2. Seleccione **Adjuntar niveles locales**.
3. En **Agregar como primario**, compruebe que los volúmenes pueden adjuntar.
4. Si es necesario, seleccione **convertir volúmenes a Thin Provisioning**.
5. Haga clic en **Guardar**.

CLI

Para asociar un almacén de objetos a un agregado con la CLI:

1. **Opcional:** Para ver cuántos datos de un volumen están inactivos, siga los pasos de la "[Determinar cuántos datos de un volumen están inactivos mediante la generación de informes de datos inactivos](#)".

Ver la cantidad de datos de un volumen inactivos puede ayudarle a decidir qué agregado utilizar para FabricPool.

2. Para adjuntar el almacén de objetos a un agregado mediante el `storage aggregate object-store attach` comando.

Si el agregado no se ha usado nunca con FabricPool y contiene volúmenes existentes, se asignan los volúmenes de forma predeterminada `snapshot-only` política de organización en niveles.

```
cluster1::> storage aggregate object-store attach -aggregate myaggr
-object-store-name Amazon01B1
```

Puede utilizar el `allow-flexgroup true` Opción para conectar agregados que contienen componentes de volumen FlexGroup.

3. Muestre la información del almacén de objetos y compruebe que el almacén de objetos asociado esté disponible mediante el `storage aggregate object-store show` comando.

```
cluster1::> storage aggregate object-store show
```

| Aggregate | Object Store Name | Availability State |
|-----------|-------------------|--------------------|
| ----- | ----- | ----- |
| myaggr | Amazon01B1 | available |

Organizar los datos en niveles en el bloque local


A partir de ONTAP 9.8, puede organizar los datos en niveles en el almacenamiento de objetos local con ONTAP S3.

La organización en niveles de los datos en un bloque local ofrece una sencilla alternativa a mover los datos a otro nivel local. Este procedimiento usa un bloque existente en el clúster local o puede dejar que ONTAP cree automáticamente una nueva máquina virtual de almacenamiento y un nuevo bloque.

Tenga en cuenta que, una vez asociado a un nivel local (agregado), el nivel de cloud no podrá desadjuntarse.

Se necesita una licencia de S3 para este flujo de trabajo, que crea un servidor S3 nuevo y un bloque nuevo, o bien usa los existentes. Esta licencia se incluye en ["ONTAP One"](#). No se necesita una licencia de FabricPool para este flujo de trabajo.

Paso

1. Organizar los datos en un bloque local: Haga clic en **niveles**, seleccione un nivel y, a continuación, haga clic en .
2. Si es necesario, habilite el aprovisionamiento ligero.
3. Elija un nivel existente o cree uno nuevo.
4. Si es necesario, edite la política de organización en niveles existente.

Gestione FabricPool

Información general sobre Manage FabricPool

Para ayudarle con sus necesidades de almacenamiento por niveles, ONTAP le permite mostrar cuántos datos de un volumen están inactivos, agregar o mover volúmenes a FabricPool, supervisar el uso de espacio para FabricPool o modificar la política de organización en niveles o el período de enfriamiento mínimo de un volumen.

Determine cuántos datos de un volumen están inactivos usando los informes de datos inactivos

Ver la cantidad de datos de un volumen inactivos le permite utilizar correctamente los niveles de almacenamiento. La información de la generación de informes de datos inactivos le ayuda a decidir qué agregado utiliza para FabricPool, si va a mover un volumen dentro o fuera de FabricPool, o si desea modificar la política de organización en niveles de un volumen.

Lo que necesitará

Debe ejecutar ONTAP 9.4 o posterior para utilizar la funcionalidad de generación de informes de datos inactivos.

Acerca de esta tarea

- La generación de informes de datos inactivos no se admite en algunos agregados.

No se pueden habilitar los informes de datos inactivos cuando FabricPool no se puede habilitar, incluidas las siguientes instancias:

- Agregados raíz


- Agregados de MetroCluster que ejecutan versiones de ONTAP anteriores a 9.7
- Flash Pool (agregados híbridos o agregados de SnapLock)
- La generación de informes de datos inactivos está habilitada de forma predeterminada en agregados donde cualquier volumen tiene la compresión adaptativa habilitada.
- La generación de informes de datos inactivos está habilitada de forma predeterminada en todos los agregados de SSD de ONTAP 9.6.
- La generación de informes de datos inactivos está habilitada de forma predeterminada en el agregado de FabricPool en ONTAP 9.4 y ONTAP 9.5.
- Puede habilitar la generación de informes de datos inactivos en agregados que no son de FabricPool mediante la interfaz de línea de comandos de ONTAP, incluidos los agregados de HDD, empezando por ONTAP 9.6.

Procedimiento

Puede determinar cuántos datos están inactivos con System Manager de ONTAP o la CLI de ONTAP.

System Manager

1. Seleccione una de las siguientes opciones:

- Cuando tenga agregados de disco duro existentes, vaya a **almacenamiento > niveles** y haga clic en  para el agregado en el que desea habilitar la generación de informes de datos inactivos.
- Si no se ha configurado ningún nivel de nube, vaya a **Dashboard** y haga clic en el enlace **Activar informe de datos inactivos en capacidad**.

CLI

Para habilitar la generación de informes de datos inactivos con la CLI:

1. Si el agregado para el cual desea ver la generación de informes de datos inactivos no se utiliza en FabricPool, habilite la generación de informes de datos inactivos para el agregado mediante el `storage aggregate modify` con el `-is-inactive-data-reporting-enabled true` parámetro.

```
cluster1::> storage aggregate modify -aggregate aggr1 -is-inactive
-data-reporting-enabled true
```

Debe habilitar de forma explícita la funcionalidad de generación de informes de datos inactivos en un agregado que no se utiliza para FabricPool.

No puede ni necesita habilitar la generación de informes de datos inactivos en un agregado habilitado para FabricPool porque el agregado ya incluye la generación de informes de datos inactivos. La `-is-inactive-data-reporting-enabled` El parámetro no funciona en los agregados que admiten FabricPool.

La `-fields is-inactive-data-reporting-enabled` parámetro de `storage aggregate show` el comando muestra si la generación de informes de datos inactivos está habilitada en un agregado.

2. Para mostrar la cantidad de datos inactivos en un volumen, use la `volume show` con el `-fields performance-tier-inactive-user-data,performance-tier-inactive-user-data-percent` parámetro.

```
cluster1::> volume show -fields performance-tier-inactive-user-
data,performance-tier-inactive-user-data-percent

vserver volume performance-tier-inactive-user-data performance-tier-
inactive-user-data-percent
-----
vsim1    vol0    0B                                0%
vs1      vs1rv1  0B                                0%
vs1      vv1     10.34MB                             0%
vs1      vv2     10.38MB                             0%
4 entries were displayed.
```

- La `performance-tier-inactive-user-data` campo muestra la cantidad de datos de usuario almacenados en el agregado inactivos.
- La `performance-tier-inactive-user-data-percent` Field muestra el porcentaje de los datos que están inactivos en el sistema de archivos activos y las copias snapshot.
- Para un agregado que no se usa para FabricPool, la generación de informes inactivos usa la política de organización en niveles para decidir cuántos datos deben generar informes tan fríos.

- Para la `none` la política de organización en niveles se utiliza durante 31 días.
- Para la `snapshot-only` y `auto`, utiliza la generación de informes de datos inactivos `tiering-minimum-cooling-days`.
- Para la `ALL` política, los informes de datos inactivos asumen que los datos se organizan en niveles en el plazo de un día.

Hasta que se alcance el período, el resultado indica «» para el importe de los datos inactivos en lugar de un valor.

- En un volumen que forma parte de FabricPool, lo que ONTAP informa como inactivo depende de la política de organización en niveles que se establezca en un volumen.
 - Para la `none` Política de organización en niveles, ONTAP informa de la cantidad de volumen completo que está inactivo durante al menos 31 días. No puede utilizar el `-tiering-minimum-cooling-days` con el `none` política de organización en niveles.
 - Para la `ALL`, `snapshot-only`, y `auto` políticas de organización en niveles, no se admiten la generación de informes de datos inactivos.

Gestionar volúmenes para FabricPool

Cree un volumen para FabricPool

Puede añadir volúmenes a FabricPool creando volúmenes nuevos directamente en el agregado habilitado para FabricPool o moviendo los volúmenes existentes de otro agregado al agregado habilitado para FabricPool.

Al crear un volumen para FabricPool, tiene la opción de especificar una política de organización en niveles. Si no se especifica ninguna política de organización en niveles, el volumen creado utiliza el valor predeterminado `snapshot-only` política de organización en niveles. Para un volumen con `snapshot-only` o `auto` la política de organización en niveles, también puede especificar el período de enfriamiento mínimo de organización en niveles.

Lo que necesitará

- Configurar un volumen para usar el `auto` La política de organización en niveles o especificar el período de enfriamiento mínimo de organización en niveles requiere ONTAP 9.4 o posterior.
- El uso de volúmenes de FlexGroup requiere ONTAP 9.5 o posterior.
- Configurar un volumen para usar el `all` La política de organización en niveles requiere ONTAP 9.6 o posterior.
- Configurar un volumen para usar el `-cloud-retrieval-policy` El parámetro requiere ONTAP 9.8 o posterior.

Pasos

1. Cree un nuevo volumen para FabricPool mediante el `volume create` comando.

- La `-tiering-policy` el parámetro opcional permite especificar la política de organización en niveles del volumen.

Se puede especificar una de las siguientes políticas de organización en niveles:

- `snapshot-only` (predeterminado)
- `auto`
- `all`
- `backup` (en desuso)
- `none`

"Tipos de políticas de organización en niveles de FabricPool"

- La `-cloud-retrieval-policy` el parámetro opcional permite que los administradores de clústeres con el nivel de privilegios avanzado anulen el comportamiento de migración o recuperación de cloud predeterminado controlado por la política de organización en niveles.

Puede especificar una de las siguientes políticas de recuperación en el cloud:

- `default`

La política de organización en niveles determina con qué datos se devuelven, de modo que no hay cambio en la recuperación de datos en el cloud `default` política de recuperación de cloud. Esto significa que el comportamiento es el mismo que en las versiones anteriores a ONTAP 9.8:

- Si la política de organización en niveles es `none` o `snapshot-only`, por lo tanto, «predeterminado» significa que toda lectura de datos condicionada por el cliente se extrae del nivel de cloud al nivel de rendimiento.
- Si la política de organización en niveles es `auto`, entonces cualquier lectura aleatoria conducida por el cliente se tira pero no lecturas secuenciales.
- Si la política de organización en niveles es `all` entonces, ningún dato dirigido por el cliente se extrae del nivel de cloud.

- `on-read`

Todas las lecturas de datos condicionadas por el cliente se envían del nivel de cloud al nivel de rendimiento.

- `never`

No se datos controlados por el cliente que pase del nivel de cloud al nivel de rendimiento

- `promote`

- Para la política de organización en niveles `none`, todos los datos de la nube se obtienen del nivel de la nube al nivel de rendimiento
- Para la política de organización en niveles `snapshot-only`, todos los datos activos del sistema de archivos se envían del nivel de la nube al nivel de rendimiento.

- La `-tiering-minimum-cooling-days` el parámetro opcional del nivel de privilegio avanzado

permite especificar el período de refrigeración mínimo de organización en niveles para un volumen que utiliza la `snapshot-only` o `auto` política de organización en niveles.

A partir de ONTAP 9.8, puede especificar un valor entre 2 y 183 para los días de refrigeración mínima de organización en niveles. Si utiliza una versión de ONTAP anterior a 9.8, puede especificar un valor entre 2 y 63 para los días de refrigeración mínima de organización en niveles.

Ejemplo de creación de un volumen para FabricPool

En el siguiente ejemplo se crea un volumen denominado «myvol1» en el agregado «myFabricPool» habilitado para FabricPool. La política de organización en niveles se establece en `auto` además, el período de enfriamiento mínimo de organización en niveles se establece en 45 días:

```
cluster1::*> volume create -vserver myVS -aggregate myFabricPool  
-volume myvol1 -tiering-policy auto -tiering-minimum-cooling-days 45
```

Información relacionada

["Gestión de volúmenes de FlexGroup"](#)

Mueva un volumen a FabricPool

Cuando mueve un volumen a FabricPool, tiene la opción de especificar o cambiar la política de organización en niveles del volumen con el movimiento. A partir de ONTAP 9.8, cuando se mueve un volumen que no es de FabricPool con la función de generación de informes de datos inactivos habilitada, FabricPool utiliza una asignación de calor para leer bloques que pueden organizar los niveles de datos fríos en el nivel de capacidad del destino de FabricPool.

Lo que necesitará

Debe comprender cómo el cambio de la política de organización en niveles puede afectar el tiempo que tardan los datos en dejar de estar activos y moverse al nivel de cloud.

["Qué sucede con la política de organización en niveles al mover un volumen"](#)

Acerca de esta tarea

Si un volumen que no pertenece a FabricPool tiene habilitada la generación de informes de datos inactivos, al mover un volumen con política de organización en niveles `auto` o `snapshot-only` Para un FabricPool, FabricPool lee los bloques que pueden aumentar la temperatura desde un archivo de mapa de calor y utiliza esa temperatura para mover los datos inactivos directamente al nivel de capacidad del destino de FabricPool.

No debe utilizar el `-tiering-policy` La opción para mover el volumen si se usa ONTAP 9.8 y desea que FabricPool use la información de generación de informes de datos inactivos para mover datos directamente al nivel de capacidad. Al usar esta opción, los FabricPool ignoran los datos de temperatura y siguen el comportamiento de movimiento de las versiones antes de ONTAP 9.8.

Paso

1. Utilice la `volume move start` Comando para mover un volumen a FabricPool.

La `-tiering-policy` el parámetro opcional permite especificar la política de organización en niveles del volumen.

Se puede especificar una de las siguientes políticas de organización en niveles:

- snapshot-only (predeterminado)
- auto
- all
- none

"Tipos de políticas de organización en niveles de FabricPool"

Ejemplo de traslado de un volumen a FabricPool

En el siguiente ejemplo, se mueve un volumen denominado «myvol2» de la SVM «vs1» al agregado «dest_FabricPool» habilitado para FabricPool. El volumen se establece explícitamente para usar el none política de organización en niveles:

```
cluster1::> volume move start -vserver vs1 -volume myvol2  
-destination-aggregate dest_FabricPool -tiering-policy none
```

Habilite y deshabilite los volúmenes para escribir directamente en el cloud

A partir de ONTAP 9.14.1, puede habilitar y deshabilitar la escritura directamente en la nube en un volumen nuevo o existente en una FabricPool para permitir que los clientes de NFS escriban datos directamente en la nube sin esperar a los análisis de organización en niveles. Los clientes SMB siguen escribiendo en el nivel de rendimiento de un volumen con capacidad de escritura en la nube. El modo de escritura en cloud está deshabilitado de forma predeterminada.

Contar con la capacidad de escribir directamente en cloud es útil en casos como migraciones; por ejemplo, donde se transfieren grandes cantidades de datos a un clúster que las que admite el clúster en el nivel local. Sin el modo de escritura en el cloud, durante una migración, se transfieren las cantidades más pequeñas de datos, después se organizan en niveles, después se transfieren y se organizan de nuevo en niveles hasta que se completa la migración. Al utilizar el modo de escritura en el cloud, este tipo de gestión ya no se requiere porque los datos nunca se transfieren al nivel local.

Antes de empezar

- Debe ser un administrador de clústeres o de SVM.
- Debe estar en el nivel de privilegio avanzado.
- El volumen debe ser un volumen de tipo de lectura/escritura.
- El volumen debe tener la política ALL Tiering.

Habilite la escritura directamente en el cloud durante la creación del volumen

Pasos

1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Cree un volumen y habilite el modo de escritura en el cloud:

```
volume create -volume <volume name> -is-cloud-write-enabled <true|false>
-aggregate <local tier name>
```

En el ejemplo siguiente se crea un volumen llamado vol1 con la escritura de cloud habilitada en el nivel local de FabricPool (aggr1):

```
volume create -volume vol1 -is-cloud-write-enabled true -aggregate aggr1
```

Habilite la escritura directamente en el cloud en un volumen existente

Pasos

1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Modificar un volumen para habilitar el modo de escritura en cloud:

```
volume modify -volume <volume name> -is-cloud-write-enabled <true|false>
-aggregate <local tier name>
```

En el ejemplo siguiente se modifica un volumen llamado vol1 con la escritura de cloud habilitada en el nivel local de FabricPool (aggr1):

```
volume modify -volume vol1 -is-cloud-write-enabled true -aggregate aggr1
```

Deshabilita la escritura directamente en la nube de un volumen

Pasos

1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Deshabilite el modo de escritura en cloud:

```
volume modify -volume <volume name> -is-cloud-write-enabled <true|false>
-aggregate <aggregate name>
```

En el ejemplo siguiente se crea un volumen llamado vol1 con la función de escritura de cloud habilitada:

```
volume modify -volume voll -is-cloud-write-enabled false -aggregate  
aggr1
```

Activa y desactiva el modo agresivo de lectura anticipada

A partir de ONTAP 9.14.1, puede habilitar y deshabilitar el modo agresivo de lectura anticipada en volúmenes de FabricPool que ofrezcan soporte para medios y entretenimiento, como las cargas de trabajo de transmisión de películas. El modo agresivo y de lectura anticipada está disponible en ONTAP 9.14.1 en todas las plataformas en las instalaciones compatibles con FabricPool. La función está desactivada de forma predeterminada.

Acerca de esta tarea

La `aggressive-readahead-mode` el comando tiene dos opciones:

- `none`: la lectura anticipada está desactivada.
- `file_prefetch`: el sistema lee todo el archivo en la memoria delante de la aplicación cliente.

Antes de empezar

- Debe ser un administrador de clústeres o de SVM.
- Debe estar en el nivel de privilegio avanzado.

Habilite el modo agresivo de lectura anticipada durante la creación del volumen

Pasos

1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Cree un volumen y habilite el modo agresivo de lectura anticipada:

```
volume create -volume <volume name> -aggressive-readahead-mode  
<none|file_prefetch>
```

En el siguiente ejemplo, se crea un volumen llamado `vol1` con lectura anticipada agresiva habilitada con la opción `file_prefetch`:

```
volume create -volume voll -aggressive-readahead-mode file_prefetch
```

Desactiva el modo de lectura anticipada agresivo

Pasos

1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Deshabilite el modo de lectura anticipada agresivo:

```
volume modify -volume <volume name> -aggressive-readahead-mode none
```

En el ejemplo siguiente se modifica un volumen llamado vol1 para deshabilitar el modo de lectura anticipada agresivo:

```
volume modify -volume vol1 -aggressive-readahead-mode none
```

Vea el modo agresivo de lectura anticipada en un volumen

Pasos

1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Vea el modo agresivo de lectura anticipada:

```
volume show -fields aggressive-readahead-mode
```

Etiquetado de objetos mediante etiquetas personalizadas creadas por el usuario

Información general sobre el etiquetado de objetos mediante etiquetas personalizadas creadas por el usuario

A partir de ONTAP 9.8, FabricPool admite el etiquetado de objetos mediante etiquetas personalizadas creadas por el usuario para que pueda clasificar y ordenar objetos para facilitar la gestión. Si es un usuario con el nivel de privilegio admin, puede crear nuevas etiquetas de objetos y modificar, eliminar y ver las etiquetas existentes.

Asigne una nueva etiqueta durante la creación del volumen

Puede crear una nueva etiqueta de objeto cuando desee asignar una o varias etiquetas a los objetos nuevos organizados en niveles a partir de un nuevo volumen que cree. Puede utilizar etiquetas para ayudarle a clasificar y ordenar objetos de organización en niveles para simplificar la gestión de los datos. A partir de ONTAP 9.8, puede usar System Manager para crear etiquetas de objetos.

Acerca de esta tarea

Solo puede establecer etiquetas en volúmenes de FabricPool conectados a StorageGRID. Estas etiquetas se conservan durante un movimiento de volumen.

- Se permite un máximo de 4 etiquetas por volumen
- En la CLI, cada etiqueta de objeto debe ser una pareja de clave-valor separada por un signo igual ("")
- En la CLI, se deben separar varias etiquetas con una coma (",")
- Cada valor de etiqueta puede contener un máximo de 127 caracteres
- Cada clave de etiqueta debe comenzar con un carácter alfabético o un guión bajo.

Las claves deben contener sólo caracteres alfanuméricos y guiones bajos, y el número máximo de caracteres permitido es 127.

Procedimiento

Puede asignar etiquetas de objetos con ONTAP System Manager o la interfaz de línea de comandos de ONTAP.

System Manager

1. Vaya a **almacenamiento > niveles**.
2. Busque un nivel de almacenamiento con los volúmenes que desee etiquetar.
3. Haga clic en la ficha **Volumes**.
4. Localice el volumen que desea etiquetar y en la columna **Etiquetas de objeto** seleccione **haga clic para introducir etiquetas**.
5. Introduzca una clave y un valor.
6. Haga clic en **aplicar**.

CLI

1. Utilice la `volume create` con el `-tiering-object-tags` opción para crear un nuevo volumen con las etiquetas especificadas. Puede especificar varias etiquetas en pares separados por comas:

```
volume create [ -vserver <vserver name> ] -volume <volume_name>
-tiering-object-tags <key1=value1> [
    ,<key2=value2>,<key3=value3>,<key4=value4> ]
```

En el siguiente ejemplo, se crea un volumen llamado `fp_volume1` con tres etiquetas de objetos.

```
vol create -volume fp_volume1 -vserver vs0 -tiering-object-tags
project=fabricpool,type=abc,content=data
```

Modifique una etiqueta existente

Puede cambiar el nombre de una etiqueta, reemplazar etiquetas de objetos existentes en

el almacén de objetos o agregar una etiqueta diferente a objetos nuevos que desee agregar más adelante.

Acerca de esta tarea

Con el `volume modify` con el `-tiering-object-tags` la opción sustituye las etiquetas existentes por el nuevo valor que proporciona.

Procedimiento

System Manager

1. Vaya a **almacenamiento > niveles**.
2. Busque un nivel de almacenamiento con volúmenes que contengan etiquetas que desee modificar.
3. Haga clic en la ficha **Volumes**.
4. Localice el volumen con etiquetas que desee modificar y, en la columna **Etiquetas de objeto**, haga clic en el nombre de la etiqueta.
5. Modifique la etiqueta.
6. Haga clic en **aplicar**.

CLI

1. Utilice la `volume modify` con el `-tiering-object-tags` opción para modificar una etiqueta existente.

```
volume modify [ -vserver <vserver name> ] -volume <volume_name>  
-tiering-object-tags <key1=value1> [ ,<key2=value2>,  
<key3=value3>,<key4=value4> ]
```

En el ejemplo siguiente se cambia el nombre del tipo de etiqueta existente=abc por type=xyz.

```
vol create -volume fp_volumel -vserver vs0 -tiering-object-tags  
project=fabricpool,type=xyz,content=data
```

Eliminar una etiqueta

Puede eliminar etiquetas de objetos cuando ya no desee que estén establecidas en un volumen o en objetos del almacén de objetos.

Procedimiento

Puede eliminar etiquetas de objetos con ONTAP System Manager o la interfaz de línea de comandos de ONTAP.

System Manager

1. Vaya a **almacenamiento > niveles**.
2. Busque un nivel de almacenamiento con volúmenes que contengan etiquetas que desee eliminar.
3. Haga clic en la ficha **Volumes**.
4. Localice el volumen con etiquetas que desee eliminar y, en la columna **Etiquetas de objeto**, haga clic en el nombre de la etiqueta.
5. Para eliminar la etiqueta, haga clic en el icono de papelera.
6. Haga clic en **aplicar**.

CLI

1. Utilice la `volume modify` con el `-tiering-object-tags` opción seguida de un valor vacío ("") para eliminar una etiqueta existente.

En el siguiente ejemplo, se eliminan las etiquetas existentes en `fp_volume1`.

```
vol modify -volume fp_volume1 -vserver vs0 -tiering-object-tags ""
```

Ver las etiquetas existentes en un volumen

Puede ver las etiquetas existentes en un volumen para ver qué etiquetas están disponibles antes de anexar nuevas etiquetas a la lista.

Paso

1. Utilice la `volume show` con el `-tiering-object-tags` opción para ver las etiquetas existentes en un volumen.

```
volume show [ -vserver <vserver name> ] -volume <volume_name> -fields  
-tiering-object-tags
```

Compruebe el estado de etiquetado de objetos en FabricPool Volumes

Compruebe si el etiquetado se ha completado en uno o varios volúmenes de FabricPool.

Paso

1. Utilice la `vol show` con el `-fieldsneeds-object-retagging` opción para ver si el etiquetado está en curso, si ha finalizado o si no se ha configurado el etiquetado.

```
vol show -fields needs-object-retagging [ -instance | -volume <volume  
name>]
```

Se muestra uno de los siguientes valores:

- `true` — el escáner de marcado de objetos aún no se ha ejecutado o necesita ejecutarse de nuevo para este volumen
- `false` — el escáner de marcado de objetos ha completado el etiquetado de este volumen
- `<->` — el escáner de marcado de objetos no se aplica a este volumen. Esto sucede en volúmenes que no residen en FabricPool.

Supervise el uso de espacio para FabricPool

Necesita saber cuántos datos se almacenan en el rendimiento y los niveles cloud para FabricPool. Esa información le ayuda a determinar si necesita cambiar la política de organización en niveles de un volumen, aumentar el límite de uso de licencias de FabricPool o aumentar el espacio de almacenamiento del nivel de cloud.

Pasos

1. Supervise el uso del espacio de los agregados habilitados para FabricPool utilizando uno de los siguientes comandos para mostrar la información:

| Si desea mostrar... | Después, utilice este comando: |
|---|---|
| El tamaño usado del nivel de cloud en un agregado | <code>storage aggregate show</code> con la <code>-instance</code> parámetro |
| Detalles del uso de espacio dentro de un agregado, incluida la capacidad de referencia del almacén de objetos | <code>storage aggregate show-space</code> con la <code>-instance</code> parámetro |
| Aprovechamiento de espacio de los almacenes de objetos adjuntos a los agregados, incluido la cantidad de espacio de licencia que se está utilizando | <code>storage aggregate object-store show-space</code> |
| Una lista de volúmenes de un agregado y los espacios utilizados por sus datos y metadatos | <code>volume show-footprint</code> |

Además de usar comandos de la CLI, puede usar Active IQ Unified Manager (anteriormente Unified Manager de OnCommand), junto con FabricPool Advisor, que está compatible con ONTAP 9.4 y clústeres posteriores, o System Manager para supervisar el uso de espacio.

El ejemplo siguiente muestra maneras de mostrar la utilización del espacio y la información relacionada para FabricPool:

```
cluster1::> storage aggregate show-space -instance
```

```

Aggregate: MyFabricPool
...
Aggregate Display Name:
MyFabricPool
...
Total Object Store Logical Referenced
Capacity: -
Object Store Logical Referenced Capacity
Percentage: -
...
Object Store
Size: -
Object Store Space Saved by Storage
Efficiency: -
Object Store Space Saved by Storage Efficiency
Percentage: -
Total Logical Used
Size: -
Logical Used
Percentage: -
Logical Unreferenced
Capacity: -
Logical Unreferenced
Percentage: -
```

```
cluster1::> storage aggregate show -instance
```

```

Aggregate: MyFabricPool
...
Composite: true
Capacity Tier Used Size:
...
```

```
cluster1::> volume show-footprint
```

```
Vserver : vs1
```

```
Volume : rootvol
```

| Feature | Used | Used% |
|--------------------------|------|-------|
| Volume Footprint | KB | % |
| Volume Guarantee | MB | % |
| Flexible Volume Metadata | KB | % |
| Delayed Frees | KB | % |
| Total Footprint | MB | % |

```
Vserver : vs1
```

```
Volume : vol
```

| Feature | Used | Used% |
|-------------------------------|------|-------|
| Volume Footprint | KB | % |
| Footprint in Performance Tier | KB | % |
| Footprint in Amazon01 | KB | % |
| Flexible Volume Metadata | MB | % |
| Delayed Frees | KB | % |
| Total Footprint | MB | % |
| ... | | |

2. Realice una de las siguientes acciones según sea necesario:

| Si desea... | Realice lo siguiente... |
|--|---|
| Cambiar la política de organización en niveles de un volumen | Siga el procedimiento descrito en "Gestionar el almacenamiento por niveles mediante la modificación de la política de organización en niveles de un volumen o la organización en niveles del período de refrigeración mínimo" . |
| Aumente el límite de uso de licencias de FabricPool | Comuníquese con su representante de ventas para socios o con el representante de NetApp. "Soporte de NetApp" |
| Aumente el espacio de almacenamiento del nivel de cloud | Póngase en contacto con el proveedor del almacén de objetos que usa para el nivel de cloud. |

Gestione el almacenamiento por niveles modificando la política de organización en niveles de un volumen o organizando por niveles el período mínimo de enfriamiento

Puede cambiar la política de organización en niveles de un volumen para controlar si los datos se mueven al nivel de cloud cuando quedan inactivos (*Cold*). Para un volumen con `snapshot-only` o `auto` la política de organización en niveles, también puede especificar el período de refrigeración mínimo que los datos de usuario deben permanecer inactivos antes de moverlos al nivel de cloud.

Lo que necesitará

Cambiar un volumen a `auto` La política de organización en niveles o la modificación del período de enfriamiento mínimo de organización en niveles requiere ONTAP 9.4 o posterior.

Acerca de esta tarea

Al cambiar la política de organización en niveles de un volumen, solo se cambia el comportamiento posterior de la organización en niveles del volumen. No mueve datos retroactivamente al nivel de cloud.

El cambio en la política de organización en niveles puede afectar el tiempo que lleva dejar de usar los datos y moverlos al nivel de cloud.

["Qué sucede cuando se modifica la política de organización en niveles de un volumen en FabricPool"](#)

Pasos

1. Modifique la política de organización en niveles de un volumen existente mediante la `volume modify` con el `-tiering-policy` parámetro:

Se puede especificar una de las siguientes políticas de organización en niveles:

- `snapshot-only` (predeterminado)
- `auto`
- `all`
- `none`

["Tipos de políticas de organización en niveles de FabricPool"](#)

2. Si el volumen utiliza el `snapshot-only` o `auto` la política de organización en niveles y si desea modificar el período de enfriamiento mínimo de organización en niveles, utilice la `volume modify` con el `-tiering-minimum-cooling-days` parámetro opcional en el nivel de privilegio avanzado.

Puede especificar un valor entre 2 y 183 para los días de refrigeración mínima de organización en niveles. Si utiliza una versión de ONTAP anterior a 9.8, puede especificar un valor entre 2 y 63 para los días de refrigeración mínima de organización en niveles.

Ejemplo de modificación de la política de organización en niveles y el período de refrigeración mínimo de un volumen

En el siguiente ejemplo, se cambia la política de organización en niveles del volumen «mayvol» de la SVM «vs1» a `auto` y el período de enfriamiento mínimo de organización en niveles a 45 días:

```
cluster1::> volume modify -vserver vs1 -volume myvol  
-tiering-policy auto -tiering-minimum-cooling-days 45
```

Archive Volumes con FabricPool (vídeo)

En este vídeo se muestra una descripción general rápida de cómo usar System Manager para archivar un volumen en un nivel de cloud con FabricPool.

["Vídeo de NetApp: Archivado de volúmenes con FabricPool \(backup + movimiento de volumen\)"](#)

Información relacionada

["NetApp TechComm TV: Lista de reproducción de FabricPool"](#)

Utilice los controles de migración en la nube para anular la política de organización en niveles predeterminada de un volumen

Es posible cambiar la política de organización en niveles predeterminada de un volumen para controlar la recuperación de datos de usuario desde el nivel de cloud al nivel de rendimiento mediante el `-cloud-retrieval-policy` Opción introducida en ONTAP 9.8.

Lo que necesitará

- Modificar un volumen mediante `-cloud-retrieval-policy` Opción requiere ONTAP 9.8 o posterior.
- Debe tener el nivel de privilegio avanzado para realizar esta operación.
- Debe comprender el comportamiento de las políticas de organización en niveles con `-cloud-retrieval-policy`.

["Funcionamiento de las políticas de organización en niveles con la migración al cloud"](#)

Paso

1. Modifique el comportamiento de la política de organización en niveles para un volumen existente mediante la `volume modify` con el `-cloud-retrieval-policy` opción:

```
volume create -volume <volume_name> -vserver <vserver_name> - tiering-  
policy <policy_name> -cloud-retrieval-policy
```

```
vol modify -volume fp_volume4 -vserver vs0 -cloud-retrieval-policy  
promote
```

Promocione los datos al nivel de rendimiento

Promocione los datos a la información general sobre el nivel de rendimiento

A partir de ONTAP 9.8, si es un administrador de clúster en el nivel de privilegio

avanzado, puede promocionar datos de manera proactiva en el nivel de rendimiento desde el nivel de cloud con una combinación de `tiering-policy` y la `cloud-retrieval-policy` ajuste.

Acerca de esta tarea

Puede hacer esto si desea detener el uso de FabricPool en un volumen o si tiene un `snapshot-only` La política de organización en niveles y desea devolver los datos de copias Snapshot restaurados al nivel de rendimiento.

Promocione todos los datos de un volumen de FabricPool al nivel de rendimiento

Puede recuperar proactivamente todos los datos de un volumen de FabricPool en el cloud y promoverlos al nivel de rendimiento.

Paso

1. Utilice la `volume modify` comando que se va a definir `tiering-policy` para `none` y.. `cloud-retrieval-policy` para `promote`.

```
volume modify -vserver <vserver-name> -volume <volume-name> -tiering-policy none -cloud-retrieval-policy promote
```

Promocione los datos del sistema de archivos al nivel de rendimiento

Puede recuperar datos del sistema de archivos activos de forma proactiva desde una copia Snapshot restaurada en el nivel de cloud y promoverla al nivel de rendimiento.

Paso

1. Utilice la `volume modify` comando que se va a definir `tiering-policy` para `snapshot-only` y.. `cloud-retrieval-policy` para `promote`.

```
volume modify -vserver <vserver-name> -volume <volume-name> -tiering-policy snapshot-only cloud-retrieval-policy promote
```

Comprobar el estado de una promoción de nivel de rendimiento

Puede comprobar el estado de la promoción del nivel de rendimiento para determinar cuándo se completó la operación.

Paso

1. Utilice el volumen `object-store` con el `tiering` opción para comprobar el estado de la promoción de nivel de rendimiento.

```

volume object-store tiering show [ -instance | -fields <fieldname>, ...
] [ -vserver <vserver name> ] *Vserver
[[-volume] <volume name>] *Volume [ -node <nodename> ] *Node Name [ -vol
-dsid <integer> ] *Volume DSID
[ -aggregate <aggregate name> ] *Aggregate Name

```

```

volume object-store tiering show v1 -instance

Vserver: vs1
Volume: v1
Node Name: node1
Volume DSID: 1023
Aggregate Name: a1
State: ready
Previous Run Status: completed
Aborted Exception Status: -
Time Scanner Last Finished: Mon Jan 13 20:27:30 2020
Scanner Percent Complete: -
Scanner Current VBN: -
Scanner Max VBNs: -
Time Waiting Scan will be scheduled: -
Tiering Policy: snapshot-only
Estimated Space Needed for Promotion: -
Time Scan Started: -
Estimated Time Remaining for scan to complete: -
Cloud Retrieve Policy: promote

```

Ejecución de la migración y la organización en niveles programadas

A partir de ONTAP 9.8, puede activar una solicitud de análisis por niveles en cualquier momento si prefiere no esperar al análisis por niveles predeterminado.

Paso

1. Utilice la `volume object-store` con el `trigger` opción para solicitar migración y organización en niveles.

```

volume object-store tiering trigger [ -vserver <vserver name> ] *VServer
Name [-volume] <volume name> *Volume Name

```

Gestionar reflejos FabricPool

Información general sobre la gestión de reflejos FabricPool

Para garantizar que los datos están accesibles en los almacenes de datos en caso de desastre y para permitirle reemplazar un almacén de datos, puede configurar una réplica de FabricPool agregando un segundo almacén de datos para que los datos se establezcan en niveles de forma síncrona en dos almacenes de datos. Puede añadir un segundo almacén de datos a configuraciones de FabricPool nuevas o existentes, supervisar el estado de mirroring, mostrar detalles de reflejos de FabricPool, promocionar un reflejo y eliminar un reflejo. Debe ejecutar ONTAP 9,7 o una versión posterior.

Cree un reflejo de FabricPool

Para crear un reflejo de FabricPool, debe asociar dos almacenes de objetos a una sola FabricPool. Puede crear un reflejo de FabricPool asociando un segundo almacén de objetos a una configuración FabricPool existente de un único almacén de objetos o bien puede crear una nueva configuración de FabricPool del almacén de objetos únicos y, a continuación, asociar un segundo almacén de objetos a él. También puede crear reflejos FabricPool en configuraciones MetroCluster.

Lo que necesitará

- Debe haber creado ya los dos almacenes de objetos mediante el `storage aggregate object-store config` comando.
- Si va a crear reflejos FabricPool en las configuraciones MetroCluster:
 - Debe haber configurado y configurado MetroCluster
 - Debe haber creado las configuraciones del almacén de objetos en el clúster seleccionado.

Si va a crear reflejos de FabricPool en ambos clústeres de una configuración MetroCluster, debe haber creado configuraciones de almacén de objetos en ambos clústeres.

- Si no está usando en almacenes de objetos locales para configuraciones MetroCluster, debe asegurarse de que existe una de las siguientes situaciones:
 - Los almacenes de objetos se encuentran en zonas de disponibilidad diferentes
 - Los almacenes de objetos están configurados para mantener copias de objetos en varias zonas de disponibilidad

["Configuración de almacenes de objetos para FabricPool en una configuración de MetroCluster"](#)

Acerca de esta tarea

El almacén de objetos que se usa para el reflejo de FabricPool debe ser diferente del almacén de objetos primario.

El procedimiento para crear un reflejo de FabricPool es el mismo para las configuraciones de MetroCluster y que no son de MetroCluster.

Pasos

1. Si no está usando una configuración FabricPool existente, cree una nueva adjuntando un almacén de objetos a un agregado con el `storage aggregate object-store attach` comando.

En este ejemplo, se crea una nueva FabricPool agregando un almacén de objetos a un agregado.

```
cluster1::> storage aggregate object-store attach -aggregate aggr1 -name my-store-1
```

2. Asocie un segundo almacén de objetos al agregado con el `storage aggregate object-store mirror` comando.

En este ejemplo, se asocia un segundo almacén de objetos a un agregado para crear un reflejo de FabricPool.

```
cluster1::> storage aggregate object-store mirror -aggregate aggr1 -name my-store-2
```

Supervisar el estado de resincronización de mirroring FabricPool

Cuando reemplaza un almacén de objetos primario con un reflejo, puede que tenga que esperar a que el reflejo vuelva a realizar la sincronización con el almacén de datos primario.

Acerca de esta tarea

Si el reflejo de FabricPool está sincronizado, no se muestran entradas.

Paso

1. Supervise el estado de resincronización de los reflejos mediante `storage aggregate object-store show-resync-status` comando.

```
aggregate1::> storage aggregate object-store show-resync-status -aggregate aggr1
```

| Aggregate | Primary | Mirror | Complete Percentage |
|-----------|------------|------------|---------------------|
| ----- | ----- | ----- | ----- |
| aggr1 | my-store-1 | my-store-2 | 40% |

Muestra los detalles del reflejo de FabricPool

Puede ver detalles sobre un reflejo de FabricPool para ver los almacenes de objetos que hay en la configuración y si el reflejo del almacén de objetos está sincronizado con el almacén de objetos principal.

Paso

1. Muestra información sobre un reflejo de FabricPool mediante el `storage aggregate object-store`

show comando.

En este ejemplo, se muestran los detalles acerca de los almacenes de objetos primarios y de reflejo en un reflejo de FabricPool.

```
cluster1::> storage aggregate object-store show
```

| Aggregate | Object Store Name | Availability | Mirror Type |
|-----------|-------------------|--------------|-------------|
| aggr1 | my-store-1 | available | primary |
| | my-store-2 | available | mirror |

Este ejemplo muestra detalles acerca del reflejo FabricPool, incluido si el reflejo está degradado debido a una operación de resincronización.

```
cluster1::> storage aggregate object-store show -fields mirror-type,is-mirror-degraded
```

| aggregate | object-store-name | mirror-type | is-mirror-degraded |
|-----------|-------------------|-------------|--------------------|
| aggr1 | my-store-1 | primary | - |
| | my-store-2 | mirror | false |

Promocione un reflejo de FabricPool

Puede reasignar el espejo del almacén de objetos como almacén de objetos primario ascendiendo. Cuando el reflejo del almacén de objetos se convierte en el primario, el primario original se convierte automáticamente en el reflejo.

Lo que necesitará

- El reflejo de FabricPool debe estar sincronizado
- El almacén de objetos debe estar operativo

Acerca de esta tarea

Puede reemplazar el almacén de objetos original por un almacén de objetos de un proveedor de cloud diferente. Por ejemplo, su reflejo original puede ser un almacén de objetos AWS, pero puede reemplazarlo por un almacén de objetos de Azure.

Paso

1. Promocione un reflejo del almacén de objetos mediante el `storage aggregate object-store modify -aggregate` comando.

```
cluster1::> storage aggregate object-store modify -aggregate aggr1 -name  
my-store-2 -mirror-type primary
```

Quite un reflejo FabricPool

Es posible quitar un reflejo de FabricPool si ya no se necesita replicar un almacén de objetos.

Lo que necesitará

El almacén de objetos primario debe estar operativo; de lo contrario, el comando fallará.

Paso

1. Quite un reflejo de almacén de objetos en una FabricPool mediante el `storage aggregate object-store unmirror -aggregate comando`.

```
cluster1::> storage aggregate object-store unmirror -aggregate aggr1
```

Reemplace un almacén de objetos existente por medio de un reflejo FabricPool

Es posible usar la tecnología de duplicación FabricPool para reemplazar un almacén de objetos por otro. No es necesario que el nuevo almacén de objetos utilice el mismo proveedor de cloud que el almacén de objetos original.

Acerca de esta tarea

Puede reemplazar el almacén de objetos original por un almacén de objetos que utilice un proveedor de cloud diferente. Por ejemplo, su almacén de objetos original podría usar AWS como proveedor de cloud, pero puede reemplazarlo por un almacén de objetos que usa Azure como proveedor de cloud y viceversa. Sin embargo, el nuevo almacén de objetos debe conservar el mismo tamaño de objeto que el original.

Pasos

1. Cree un reflejo de FabricPool añadiendo un almacén de objetos nuevo a una FabricPool existente mediante el `storage aggregate object-store mirror comando`.

```
cluster1::> storage aggregate object-store mirror -aggregate aggr1 -name  
my-AZURE-store
```

2. Supervise el estado de resincronización de mirroring mediante el `storage aggregate object-store show-resync-status comando`.

```
cluster1::> storage aggregate object-store show-resync-status -aggregate  
aggr1
```

| Aggregate | Primary | Mirror | Complete Percentage |
|-----------|--------------|----------------|------------------------|
| ----- | ----- | ----- | ----- |
| aggr1 | my-AWS-store | my-AZURE-store | 40% |

3. Compruebe que el reflejo esté sincronizado mediante el `storage aggregate object-store> show -fields mirror-type,is-mirror-degraded` comando.

```
cluster1::> storage aggregate object-store show -fields mirror-type,is-
mirror-degraded
```

| aggregate | object-store-name | mirror-type | is-mirror-degraded |
|-----------|-------------------|-------------|--------------------|
| ----- | ----- | ----- | ----- |
| aggr1 | my-AWS-store | primary | - |
| | my-AZURE-store | mirror | false |

4. Cambie el almacén de objetos principal por el almacén de objetos mirror mediante `storage aggregate object-store modify` comando.

```
cluster1::> storage aggregate object-store modify -aggregate aggr1 -name
my-AZURE-store -mirror-type primary
```

5. Muestra detalles sobre el reflejo de FabricPool mediante el `storage aggregate object-store show -fields mirror-type,is-mirror-degraded` comando.

Este ejemplo muestra la información sobre el reflejo FabricPool, que incluye si el reflejo está degradado (no está sincronizado).

```
cluster1::> storage aggregate object-store show -fields mirror-type, is-
mirror-degraded
```

| aggregate | object-store-name | mirror-type | is-mirror-degraded |
|-----------|-------------------|-------------|--------------------|
| ----- | ----- | ----- | ----- |
| aggr1 | my-AZURE-store | primary | - |
| | my-AWS-store | mirror | false |

6. Quite el espejo FabricPool con el `storage aggregate object-store unmirror` comando.

```
cluster1::> storage aggregate object-store unmirror -aggregate aggr1
```

7. Compruebe que la FabricPool vuelve a estar en una configuración de almacén de objetos individual mediante el `storage aggregate object-store show -fields mirror-type,is-mirror-degraded` comando.

```
cluster1::> storage aggregate object-store show -fields mirror-type,is-mirror-degraded
```

| aggregate | object-store-name | mirror-type | is-mirror-degraded |
|-----------|-------------------|-------------|--------------------|
| aggr1 | my-AZURE-store | primary | - |

Reemplazar un reflejo de FabricPool en una configuración MetroCluster

Si uno de los almacenes de objetos de un reflejo de FabricPool se destruye o deja de estar disponible en una configuración de MetroCluster, puede hacer que el almacén de objetos del reflejo no sea el reflejo, si ya no se encuentra dañado, retirar el almacén de objetos del reflejo de FabricPool, Y, a continuación, añada un nuevo reflejo de almacén de objetos a la FabricPool.

Pasos

1. Si el almacén de objetos dañados no es el espejo, haga que el objeto almacene el espejo con el `storage aggregate object-store modify` comando.

```
storage aggregate object-store modify -aggregate -aggregate fp_aggr1_A01 -name mccl_ostore1 -mirror-type mirror
```

2. Quite el reflejo del almacén de objetos de la FabricPool mediante el `storage aggregate object-store unmirror` comando.

```
storage aggregate object-store unmirror -aggregate <aggregate name> -name mccl_ostore1
```

3. Puede forzar la reanudación de la organización en niveles en el almacén de datos principal después de eliminar el almacén de datos de mirroring mediante el `storage aggregate object-store modify` con la `-force-tiering-on-metrocluster true` opción.

La ausencia de un reflejo interfiere con los requisitos de replicación de la configuración de MetroCluster.

```
storage aggregate object-store modify -aggregate <aggregate name> -name mccl_ostore1 -force-tiering-on-metrocluster true
```

4. Cree un almacén de objetos de reemplazo mediante `storage aggregate object-store config`

create comando.

```
storage aggregate object-store config create -object-store-name
mccl_ostore3 -cluster clusterA -provider-type SGWS -server <SGWS-server-
1> -container-name <SGWS-bucket-1> -access-key <key> -secret-password
<password> -encrypt <true|false> -provider <provider-type> -is-ssl
-enabled <true|false> ipspace <IPSpace>
```

5. Añada el reflejo del almacén de objetos al reflejo FabricPool mediante el storage aggregate object-store mirror comando.

```
storage aggregate object-store mirror -aggregate aggr1 -name
mccl_ostore3-mc
```

6. Se muestra la información del almacén de objetos con el storage aggregate object-store show comando.

```
storage aggregate object-store show -fields mirror-type,is-mirror-
degraded
```

| aggregate | object-store-name | mirror-type | is-mirror-degraded |
|-----------|-------------------|-------------|--------------------|
| ----- | ----- | ----- | ----- |
| aggr1 | mccl_ostore1-mc | primary | - |
| | mccl_ostore3-mc | mirror | true |

7. Supervise el estado de resincronización de mirroring mediante el storage aggregate object-store show-resync-status comando.

```
storage aggregate object-store show-resync-status -aggregate aggr1
```

| Aggregate | Primary | Mirror | Complete Percentage |
|-----------|-----------------|-----------------|------------------------|
| ----- | ----- | ----- | ----- |
| aggr1 | mccl_ostore1-mc | mccl_ostore3-mc | 40% |

Comandos para gestionar agregados con FabricPool

Utilice la storage aggregate object-store Comandos para gestionar almacenes de objetos para FabricPool. Utilice la storage aggregate Comandos para gestionar

agregados para FabricPool. Utilice la `volume` Comandos para gestionar volúmenes para FabricPool.

| Si desea... | Utilizar este comando: |
|--|---|
| Defina la configuración de un almacén de objetos para que ONTAP pueda acceder a él | <code>storage aggregate object-store config create</code> |
| Modifique los atributos de configuración del almacén de objetos | <code>storage aggregate object-store config modify</code> |
| Cambie el nombre de una configuración de almacén de objetos existente | <code>storage aggregate object-store config rename</code> |
| Eliminar la configuración de un almacén de objetos | <code>storage aggregate object-store config delete</code> |
| Mostrar una lista de configuraciones del almacén de objetos | <code>storage aggregate object-store config show</code> |
| Asocie un segundo almacén de objetos a una FabricPool nueva o existente como reflejo | <code>storage aggregate object-store mirror</code> con la <code>-aggregate y.. -name</code> parámetro en el nivel de privilegios de administrador |
| Quite un reflejo de almacén de objetos de un reflejo de FabricPool existente | <code>storage aggregate object-store unmirror</code> con la <code>-aggregate y.. -name</code> parámetro en el nivel de privilegios de administrador |
| Supervisar el estado de resincronización de mirroring FabricPool | <code>storage aggregate object-store show-resync-status</code> |
| Muestra los detalles del reflejo de FabricPool | <code>storage aggregate object-store show</code> |
| Promocione un reflejo de almacén de objetos para reemplazar un almacén de objetos principal en una configuración de mirroring FabricPool | <code>storage aggregate object-store modify</code> con la <code>-aggregate</code> parámetro en el nivel de privilegios de administrador |
| Probar la latencia y el rendimiento de un almacén de objetos sin adjuntar el almacén de objetos a un agregado | <code>storage aggregate object-store profiler start</code> con la <code>-object-store-name y.. -node</code> parámetro en el nivel de privilegio avanzado |
| Supervise el estado del perfilador del almacén de objetos | <code>storage aggregate object-store profiler show</code> con la <code>-object-store-name y.. -node</code> parámetro en el nivel de privilegio avanzado |

| | |
|--|--|
| Aborte el perfilador del almacén de objetos cuando se está ejecutando | <code>storage aggregate object-store profiler abort</code> con la <code>-object-store-name</code> y.. <code>-node</code> parámetro en el nivel de privilegio avanzado |
| Asocie un almacén de objetos a un agregado para usar FabricPool | <code>storage aggregate object-store attach</code> |
| Asocie un almacén de objetos a un agregado que contiene un volumen de FlexGroup para usar FabricPool | <code>storage aggregate object-store attach</code> con la <code>allow-flexgroup true</code> |
| Muestra detalles de los almacenes de objetos adjuntos a agregados habilitados para FabricPool | <code>storage aggregate object-store show</code> |
| Muestre el umbral de ocupación del agregado utilizado por el análisis de organización en niveles | <code>storage aggregate object-store show</code> con la <code>-fields tiering-fullness-threshold</code> parámetro en el nivel de privilegio avanzado |
| Muestra el uso de espacio de los almacenes de objetos adjuntos a agregados habilitados para FabricPool | <code>storage aggregate object-store show-space</code> |
| Habilite la generación de informes de datos inactivos en un agregado que no se use para FabricPool | <code>storage aggregate modify</code> con la <code>-is -inactive-data-reporting-enabled true</code> parámetro |
| Mostrar si la generación de informes de datos inactivos está habilitada en un agregado | <code>storage aggregate show</code> con la <code>-fields is-inactive-data-reporting-enabled</code> parámetro |
| Muestra información sobre la cantidad de datos de usuario que están inactivos en un agregado | <code>storage aggregate show-space</code> con la <code>-fields performance-tier-inactive-user-data,performance-tier-inactive-user-data-percent</code> parámetro |
| <p>Cree un volumen para FabricPool, incluidos los siguientes elementos:</p> <ul style="list-style-type: none"> • La política de organización en niveles • El período de enfriamiento mínimo de organización en niveles (para la <code>snapshot-only</code> o. <code>auto</code> política de organización en niveles) | <p><code>volume create</code></p> <ul style="list-style-type: none"> • Utilice la <code>-tiering-policy</code> parámetro para especificar la política de organización en niveles. • Utilice la <code>-tiering-minimum-cooling-days</code> parámetro en el nivel de privilegio avanzado para especificar el período de refrigeración mínimo de organización en niveles. |

| | |
|--|--|
| <p>Modifique un volumen para FabricPool, incluidos los siguientes elementos:</p> <ul style="list-style-type: none"> • La política de organización en niveles • El período de enfriamiento mínimo de organización en niveles (para la <code>snapshot-only</code> o. auto política de organización en niveles) | <p><code>volume modify</code></p> <ul style="list-style-type: none"> • Utilice la <code>-tiering-policy</code> parámetro para especificar la política de organización en niveles. • Utilice la <code>-tiering-minimum-cooling-days</code> parámetro en el nivel de privilegio avanzado para especificar el período de refrigeración mínimo de organización en niveles. |
| <p>Muestra información de FabricPool relacionada con un volumen, incluidos los siguientes:</p> <ul style="list-style-type: none"> • El período de enfriamiento mínimo de organización en niveles • ¿Qué cantidad de datos de usuario no están activos | <p><code>volume show</code></p> <ul style="list-style-type: none"> • Utilice la <code>-fields tiering-minimum-cooling-days</code> parámetro en el nivel de privilegio avanzado para mostrar el período de refrigeración mínimo de organización en niveles. • Utilice la <code>-fields performance-tier-inactive-user-data,performance-tier-inactive-user-data-percent</code> parámetro para mostrar la cantidad de datos de usuario inactivos. |
| <p>Mover un volumen dentro o fuera de FabricPool</p> | <p><code>volume move start</code> Utilice la <code>-tiering-policy</code> parámetro opcional para especificar la política de organización en niveles del volumen.</p> |
| <p>Modifique el umbral para recuperar espacio no referenciado (el umbral de desfragmentación) para FabricPool</p> | <p><code>storage aggregate object-store modify</code> con la <code>-unreclaimed-space-threshold</code> parámetro en el nivel de privilegio avanzado</p> |
| <p>Modifique el umbral del porcentaje de completado del agregado antes de que el análisis por niveles comience a organizar los datos en niveles para FabricPool</p> <p>FabricPool sigue organizando datos fríos en niveles en un nivel de cloud hasta que el nivel local alcanza un 98 % de la capacidad.</p> | <p><code>storage aggregate object-store modify</code> con la <code>-tiering-fullness-threshold</code> parámetro en el nivel de privilegio avanzado</p> |
| <p>Muestre el umbral para recuperar espacio no referenciado para FabricPool</p> | <p><code>storage aggregate object-store show 0.</code> <code>storage aggregate object-store show-space</code> con el <code>-unreclaimed-space-threshold</code> parámetro en el nivel de privilegio avanzado</p> |

Movilidad de datos de SVM

Información general sobre movilidad de datos de SVM

A partir de ONTAP 9.10.1, los administradores del clúster pueden reubicar de forma no

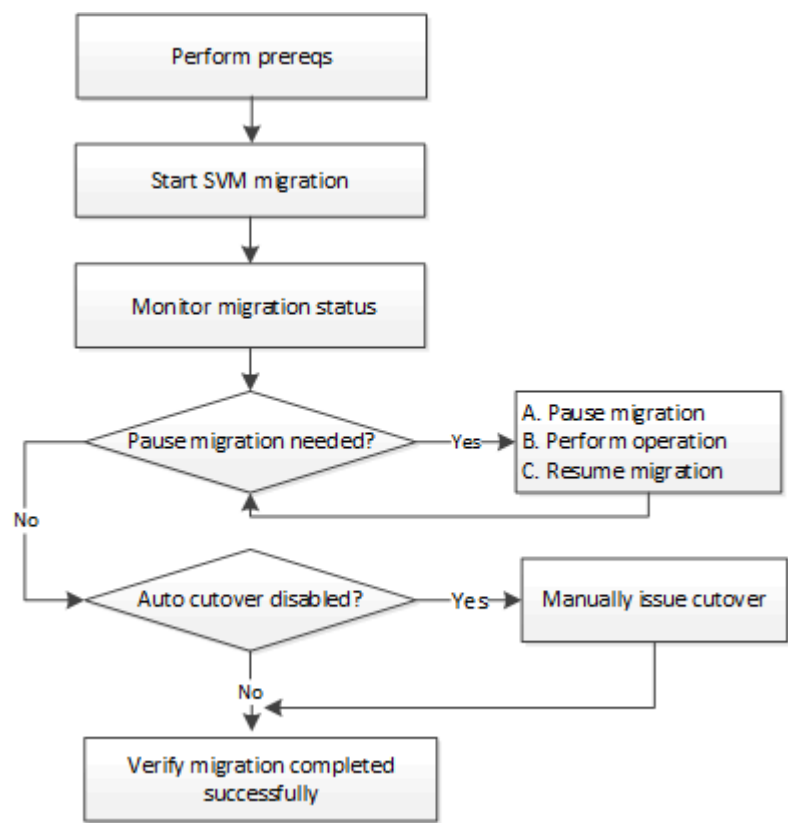
disruptiva una SVM desde un clúster de origen a un clúster de destino para gestionar la capacidad y el balanceo de carga, o para permitir actualizaciones de equipos o consolidaciones de centros de datos mediante la interfaz de línea de comandos de ONTAP.

Esta funcionalidad de reubicación de SVM no disruptiva es compatible con las plataformas AFF en ONTAP 9.10.1 y 9.11.1. A partir de ONTAP 9.12.1, esta funcionalidad es compatible tanto con las plataformas FAS como AFF y los agregados híbridos.

El nombre y el UUID de la SVM no cambian después de la migración, así como el nombre de la LIF de datos, la dirección IP y los nombres de objetos, como el nombre del volumen. El UUID de los objetos de la SVM será diferente.

Flujo de trabajo de migración de SVM

El diagrama muestra el flujo de trabajo típico para una migración de SVM. Puede iniciar una migración de SVM desde el clúster de destino. Puede supervisar la migración desde el origen o desde el destino. Puede realizar una transición manual o una transición automática. De forma predeterminada, se realiza una transición automática.



Compatibilidad con la plataforma de migración de SVM

| Familia de controladoras | Versiones de ONTAP admitidas |
|--------------------------|--------------------------------------|
| AFF A-Series | ONTAP 9.10.1 y posteriores |
| Serie C de AFF | ONTAP 9.12.1, revisión 4 y posterior |
| FAS | ONTAP 9.12.1 y versiones posteriores |



Cuando se migra desde un clúster AFF a un clúster FAS con agregados híbridos, la ubicación automática del volumen intentará realizar una coincidencia de agregado similar a como la de. Por ejemplo, si el clúster de origen tiene 60 volúmenes, la ubicación del volumen intentará encontrar un agregado de AFF en el destino para colocar los volúmenes. Si no hay espacio suficiente en los agregados de AFF, los volúmenes se colocarán en agregados con discos no flash.

Soporte de escalabilidad con versión de ONTAP

| Versión de ONTAP | Pares DE ALTA DISPONIBILIDAD en origen y destino |
|------------------|--|
| ONTAP 9.14.1 | 12 |
| ONTAP 9.13.1 | 6 |
| ONTAP 9.11.1 | 3 |
| ONTAP 9.10.1 | 1 |

Requisitos de rendimiento de la infraestructura de red para el tiempo de ida y vuelta (RTT) de TCP entre el clúster de origen y el de destino

Según la versión de ONTAP instalada en el clúster, la red que conecte los clústeres de origen y destino debe tener un tiempo máximo de ida y vuelta tal y como se indica:

| Versión de ONTAP | RTT máxima |
|--------------------------------------|------------|
| ONTAP 9.12.1 y versiones posteriores | 10 ms |
| ONTAP 9.11.1 y anteriores | 2 ms |

Volúmenes máximos admitidos por SVM

| Origen | Destino | ONTAP 9.14.1 | ONTAP 9.13.1 | ONTAP 9.12.1 | ONTAP 9.11.1 y anteriores |
|--------|---------|--------------|--------------|--------------|---------------------------|
| AFF | AFF | 400 | 200 | 100 | 100 |
| FAS | FAS | 80 | 80 | 80 | N.A. |
| FAS | AFF | 80 | 80 | 80 | N.A. |
| AFF | FAS | 80 | 80 | 80 | N.A. |

Requisitos previos

Antes de iniciar una migración de SVM, debe cumplir los siguientes requisitos previos:

- Debe ser un administrador de clústeres.
- ["Los clústeres de origen y destino deben tener una relación entre sí"](#).
- Los clústeres de origen y destino deben tener SnapMirror síncrono ["licencia instalada"](#). Esta licencia se incluye con ["ONTAP One"](#).
- Todos los nodos del clúster de origen deben ejecutar ONTAP 9.10.1 o una versión posterior. Para obtener información sobre la compatibilidad de controladoras de cabina ONTAP específicas, consulte ["Hardware Universe"](#).

- Todos los nodos del clúster de origen deben ejecutar la misma versión de ONTAP.
- Todos los nodos del clúster de destino deben ejecutar la misma versión de ONTAP.
- El clúster de destino debe tener la misma o no más de dos versiones de clúster efectivas (ECV) principales más recientes que el clúster de origen.
- Los clústeres de origen y destino deben admitir la misma subred IP para el acceso a la LIF de datos.
- La SVM de origen debe contener un número menor que el [número máximo de volúmenes de datos admitidos para la versión](#).
- Debe haber disponible espacio suficiente para la ubicación de volúmenes en el destino
- Onboard Key Manager se debe configurar en el destino si la SVM de origen tiene volúmenes cifrados

Mejor práctica

Al realizar una migración de SVM, se recomienda dejar un margen de CPU del 30 % en el clúster de origen y el de destino para habilitar la ejecución de la carga de trabajo de CPU.

Operaciones de SVM


Debe comprobar si existen operaciones que puedan entrar en conflicto con una migración de SVM:


- No hay operaciones de conmutación por error en curso
- WAFLIRON no se puede ejecutar
- La huella dactilar no está en curso
- No se están ejecutando Vol Move, rehost, clone, create, convert o Analytics

Funciones admitidas y no admitidas

En la tabla se indican las funciones de ONTAP compatibles con la movilidad de datos de SVM y las versiones de ONTAP en las que está disponible la compatibilidad.

| Función | Se admite la primera versión | Comentarios |
|---|------------------------------|---|
| Protección autónoma de ransomware | ONTAP 9.12.1 | |
| Cloud Volumes ONTAP | No admitido | |
| Gestor de claves externas | ONTAP 9.11.1 | |
| FabricPool | ONTAP 9.11.1 | Más información acerca de Soporte de FabricPool . |
| Relación de abanico (el origen de migración tiene un volumen de origen de SnapMirror con más de un destino) | ONTAP 9.11.1 | |
| FC SAN | No admitido | |
| Flash Pool | ONTAP 9.12.1 | |

| | | |
|--|--------------|--|
| Volúmenes de FlexCache | No admitido | |
| FlexGroup | No admitido | |
| Directivas IPsec | No admitido | |
| LIF IPv6 | No admitido | |
| San iSCSI | No admitido | |
| Replicación de la programación de trabajos | ONTAP 9.11.1 | En ONTAP 9.10.1, las programaciones de trabajos no se replican durante la migración y se deben crear manualmente en el destino. A partir de ONTAP 9.11.1, las programaciones de tareas que utiliza el origen se replican automáticamente durante la migración. |
| Mirroring con carga compartida | No admitido | |
| SVM de MetroCluster | No admitido | Aunque la migración de SVM no admite la migración de SVM de MetroCluster, es posible que se pueda usar la replicación asíncrona de SnapMirror para "Migre una SVM en una configuración MetroCluster" . Debe tener en cuenta que el proceso descrito para migrar una SVM a una configuración de MetroCluster es <i>NOT</i> un método no disruptivo. |
| Cifrado de agregados de NetApp (NAE) | No admitido | La migración no está soportada desde un origen sin cifrar a un destino cifrado. |
| Configuraciones de NDMP | No admitido | |
| Cifrado de volúmenes de NetApp (NVE) | ONTAP 9.10.1 | |
| Registros de auditoría de NFS y SMB | ONTAP 9.13.1 | <div>  <p>El redireccionamiento del registro de auditoría solo está disponible en modo cloud. Para la migración de SVM en las instalaciones con auditoría habilitada, debe deshabilitar la auditoría en la SVM de origen y, a continuación, llevar a cabo la migración.</p> </div> <p>Antes de la migración de SVM:</p> <ul style="list-style-type: none"> • "La redirección de registros de auditoría debe estar habilitada en el clúster de destino". • "La ruta de destino del registro de auditoría de la SVM de origen debe crearse en el clúster de destino". |
| NFS v3, NFS v4,1 y NFS v4,2 | ONTAP 9.10.1 | |
| NFS v4,0 | ONTAP 9.12.1 | |
| NFSv4,1 con pNFS | ONTAP 9.14.1 | |

| | | |
|--|--------------|---|
| NVMe sobre Fabric | No admitido | |
| Gestor de claves incorporado (OKM) con modo Common Criteria habilitado en el clúster de origen | No admitido | |
| Qtrees | ONTAP 9.14.1 | |
| Cuotas | ONTAP 9.14.1 | |
| S3 | No admitido | |
| Protocolo de SMB | ONTAP 9.12.1 | Las migraciones SMB son disruptivas y requieren una actualización de cliente posterior a la migración. |
| Relaciones de SnapMirror Cloud | ONTAP 9.12.1 | A partir de ONTAP 9.12.1, cuando se migra una SVM con relaciones de SnapMirror Cloud, el clúster de destino debe tener el " Licencia de SnapMirror Cloud " instalado y debe tener suficiente capacidad disponible para admitir el desplazamiento de capacidad de los volúmenes que se reflejan al cloud. |
| Destino asíncrono de SnapMirror | ONTAP 9.12.1 | |
| Origen asíncrono de SnapMirror | ONTAP 9.11.1 | <ul style="list-style-type: none"> • Las transferencias pueden continuar con normalidad en las relaciones de SnapMirror de FlexVol durante la mayor parte de la migración. • Todas las transferencias continuas se cancelan durante la transición y las nuevas transferencias fallan durante la transición. Además, no se pueden reiniciar hasta que finalice la migración. • Las transferencias programadas que se cancelaron o omitieron durante la migración no se inician automáticamente una vez que finaliza la migración. <div>  <p>Cuando se migra el origen de SnapMirror, ONTAP no impide que se elimine el volumen después de la migración hasta que se realice la actualización de SnapMirror. Esto sucede debido a que la información relacionada con SnapMirror para volúmenes de origen de SnapMirror migrados solo está disponible una vez finalizada la migración y una vez que se lleve a cabo la primera actualización.</p> </div> |
| Configuración de SMTape | No admitido | |

| | | |
|---|--------------|--|
| SnapLock | No admitido | |
| Continuidad del negocio de SnapMirror | No admitido | |
| Relaciones entre iguales de SVM de SnapMirror | ONTAP 9.12.1 | |
| Recuperación ante desastres de SVM con SnapMirror | No admitido | |
| SnapMirror síncrono | No admitido | |
| Copia Snapshot | ONTAP 9.10.1 | |
| Bloqueo de copias snapshot a prueba de manipulaciones | ONTAP 9.14.1 | El bloqueo de copia snapshot a prueba de manipulaciones no equivale a SnapLock. SnapLock no se admite. |
| LIF IP virtuales/BGP | No admitido | |
| Virtual Storage Console 7,0 y versiones posteriores | No admitido | VSC forma parte del "Herramientas de ONTAP para el dispositivo virtual de VMware vSphere" A partir de VSC 7,0. |
| Clones de volúmenes | No admitido | |
| VStorage | No admitido | |

Soporte de FabricPool

La migración de SVM se admite con volúmenes en FabricPools para las siguientes plataformas:

- Plataforma Azure NetApp Files. Todas las políticas de organización en niveles son compatibles (solo Snapshot, automático, all y ninguna).
- Plataforma en las instalaciones. Solo se admite la política de organización en niveles de volúmenes «ninguno».

Operaciones admitidas durante la migración

En la siguiente tabla se indican las operaciones de volumen admitidas dentro de la SVM migradora según el estado de migración:

| Operación de volumen | Estado de migración de SVM | | |
|---|----------------------------|-----------|-------------|
| | En curso | Pausa | Cutover |
| Cree | No permitido | Permitido | No admitido |
| Eliminar | No permitido | Permitido | No admitido |
| Desactivación de análisis del sistema de archivos | Permitido | Permitido | No admitido |
| Activación de análisis del sistema de archivos | No permitido | Permitido | No admitido |
| Modificar | Permitido | Permitido | No admitido |
| Sin conexión/En línea | No permitido | Permitido | No admitido |

| | | | |
|--|--------------|-----------|-------------|
| Mover/volver a alojar | No permitido | Permitido | No admitido |
| Crear/modificar qtree | No permitido | Permitido | No admitido |
| Crear/modificar cuota | No permitido | Permitido | No admitido |
| Cambiar el nombre | No permitido | Permitido | No admitido |
| Cambie el tamaño | Permitido | Permitido | No admitido |
| Restringir | No permitido | Permitido | No admitido |
| Modificar los atributos de copia Snapshot | Permitido | Permitido | No admitido |
| Modificación de eliminación automática de copia Snapshot | Permitido | Permitido | No admitido |
| Crear copias Snapshot | Permitido | Permitido | No admitido |
| Eliminación de copia Snapshot | Permitido | Permitido | No admitido |
| Restaurar archivo desde la copia snapshot | Permitido | Permitido | No admitido |

Migre un SVM

Una vez completada la migración de SVM, los clientes se pasan al clúster de destino automáticamente y se elimina la SVM innecesaria del clúster de origen. La transición automática y la limpieza automática de la fuente están activadas de manera predeterminada. Si es necesario, puede deshabilitar la transición automática del cliente para suspender la migración antes de que se produzca la transición y también puede deshabilitar la limpieza automática de la SVM de origen.

- Puede utilizar el `-auto-cutover false` opción de suspender la migración cuando normalmente se produce la transición automática del cliente y, a continuación, llevar a cabo la transposición manualmente más adelante.

Transposición manual de clientes tras la migración de SVM

- Puede utilizar el privilegio `Advance -auto-source-cleanup false` Opción para deshabilitar la eliminación de la SVM de origen después de la transición y, a continuación, activar la limpieza del origen manualmente más adelante, después de la transición.

Quite manualmente la SVM de origen tras la transición

Migre una SVM con la transición automática habilitada

De forma predeterminada, los clientes se pasan al clúster de destino automáticamente cuando finaliza la migración y se elimina la SVM innecesaria del clúster de origen.

Pasos

1. Desde el clúster de destino, ejecute las comprobaciones previas de la migración:

```
dest_cluster> vserver migrate start -vserver SVM_name -source-cluster
cluster_name -check-only true
```

2. Desde el clúster de destino, inicie la migración SVM:

```
dest_cluster> vserver migrate start -vserver SVM_name -source-cluster cluster_name
```

3. Compruebe el estado de la migración:

```
dest_cluster> vserver migrate show
```

El estado muestra Migrate-Complete cuando termine la migración de SVM.

Migre una SVM con la transición automática del cliente deshabilitada

Puede utilizar la opción `-auto-transposición false` para suspender la migración cuando se produce normalmente la transición automática del cliente y luego realizar manualmente la transición posteriormente. Consulte [Transposición manual de clientes tras la migración de SVM](#).

Pasos

1. Desde el clúster de destino, ejecute las comprobaciones previas de la migración:

```
dest_cluster> vserver migrate start -vserver SVM_name -source-cluster cluster_name -check-only true
```

2. Desde el clúster de destino, inicie la migración SVM:

```
dest_cluster> vserver migrate start -vserver SVM_name -source-cluster cluster_name -auto-cutover false
```

3. Compruebe el estado de la migración:

```
dest_cluster> vserver migrate show
```

El estado muestra Listo para transposición cuando la migración SVM completa las transferencias de datos asíncronas y está lista para la operación de transposición.

Migre un SVM con la limpieza de origen deshabilitada

Puede utilizar la opción `Advance Privilege -auto-source-cleaned false` para deshabilitar la eliminación de la SVM de origen después de la transición y, a continuación, activar la limpieza de origen manualmente más tarde, después de la transición. Consulte [Quite manualmente la SVM de origen](#).

Pasos

1. Desde el clúster de destino, ejecute las comprobaciones previas de la migración:

```
dest_cluster*> vserver migrate start -vserver SVM_name -source-cluster cluster_name -check-only true
```

2. Desde el clúster de destino, inicie la migración SVM:

```
dest_cluster*> vserver migrate start -vserver SVM_name -source-cluster cluster_name -auto-source-cleanup false
```

3. Compruebe el estado de la migración:

```
dest_cluster*> vserver migrate show
```

El estado muestra una limpieza lista para el origen cuando la transición de la migración SVM ha finalizado, y está lista para quitar la SVM en el clúster de origen.

Supervisar la migración de volúmenes

Además de supervisar la migración general de SVM con el `vserver migrate show` Comando, puede supervisar el estado de migración de los volúmenes que contiene la SVM.

Pasos

1. Comprobar el estado de migración de volumen:

```
dest_clust> vserver migrate show-volume
```

Detenga y reanude la migración de SVM

Puede que desee pausar una migración de SVM antes de que comience la transición de la migración. Puede pausar una migración de SVM mediante el `vserver migrate pause` comando.

Pausar la migración

Puede pausar una migración de SVM antes de que comience la transición del cliente mediante el `vserver migrate pause` comando.

Algunos cambios de configuración están restringidos cuando hay una operación de migración en curso; sin embargo, a partir de ONTAP 9.12.1, puede pausar una migración para corregir algunas configuraciones restringidas y para algunos estados fallidos, de modo que pueda solucionar los problemas de configuración que podrían haber causado el error. Algunos de los estados de errores que se pueden corregir al pausar la migración de SVM incluyen los siguientes:

- error en la configuración
- error al migrar

Pasos

1. Desde el clúster de destino, detenga la migración:

```
dest_cluster> vserver migrate pause -vserver <vserver name>
```

Reanudar las migraciones

Cuando esté listo para reanudar una migración de SVM en pausa o cuando ocurra errores en una migración de SVM, puede usar el `vserver migrate resume` comando.

Paso

1. Reanudar la migración de SVM:

```
dest_cluster> vserver migrate resume
```

2. Compruebe que la migración de SVM se ha reanudado y supervise el progreso:

```
dest_cluster> vserver migrate show
```

Cancele una migración de SVM

Si necesita cancelar una migración de SVM antes de que finalice, puede usar el `vserver migrate abort` comando. Solo es posible cancelar una migración de SVM cuando la operación se encuentra en estado de pausa o con errores. No es posible cancelar una migración de SVM cuando el estado es "transposición-iniciada" o una vez completada la transposición. No puede utilizar el `abort` Opción cuando hay una migración de SVM en curso.

Pasos

1. Compruebe el estado de la migración:

```
dest_cluster> vserver migrate show -vserver <vserver name>
```

2. Cancele la migración:

```
dest_cluster> vserver migrate abort -vserver <vserver name>
```

3. Compruebe el progreso de la operación de cancelación:

```
dest_cluster> vserver migrate show
```

El estado de migración muestra migración-anulación mientras la operación de cancelación está en curso. Cuando se completa la operación de cancelación, el estado de migración no muestra nada.

Corte manual de los clientes

De forma predeterminada, la transición del cliente al clúster de destino se realiza automáticamente después de que la migración de SVM alcanza el estado "Listo para transposición". Si elige deshabilitar la transición automática del cliente, debe realizar la transición manualmente del cliente.

Pasos

1. Ejecución manual de la transición del cliente:

```
dest_cluster> vserver migrate cutover -vserver <vserver name>
```

2. Comprobar el estado de la operación de transición:

```
dest_cluster> vserver migrate show
```

Quite manualmente la SVM de origen tras la transición del cliente

Si ha realizado la migración de SVM con la limpieza de origen deshabilitada, puede quitar la SVM de origen manualmente una vez que finaliza la transición del cliente.

Pasos

1. Compruebe que el estado esté listo para la limpieza del origen:

```
dest_cluster> vserver migrate show
```

2. Limpie la fuente:

```
dest_cluster> vserver migrate source-cleanup -vserver <vserver_name>
```

Gestión de parejas de HA

Información general sobre la gestión de parejas de HA

Los nodos de clúster están configurados en pares de alta disponibilidad para tolerancia a fallos y operaciones no disruptivas. Si un nodo falla o si necesita desconectar un nodo para realizar un mantenimiento rutinario, su partner puede tomar el control de su almacenamiento y seguir sirviendo datos. El partner devuelve el almacenamiento cuando el nodo vuelve a estar online.

La configuración de controladoras de parejas de alta disponibilidad consta de un par de controladoras de almacenamiento FAS/AFF coincidentes (nodo local y nodo asociado). Cada uno de estos nodos está conectado a las bandejas de discos del otro. Cuando uno de los nodos de una pareja de alta disponibilidad encuentra un error y detiene el procesamiento de datos, su compañero detecta el estado fallido del partner y asume todo el procesamiento de los datos de esa controladora.

Takeover es el proceso en el que un nodo asume el control sobre el almacenamiento de su partner.

Giveback es el proceso en el que el almacenamiento se devuelve al partner.

De forma predeterminada, las adquisiciones se realizan automáticamente en cualquiera de las siguientes situaciones:

- Se produce un fallo del sistema o software en un nodo que provoca una caída en alarma. Las controladoras de parejas de alta disponibilidad conmutan automáticamente al nodo de su partner. Una vez que el partner se ha recuperado de la alarma y se ha iniciado, el nodo realiza automáticamente una devolución, devolviendo al partner al funcionamiento normal.
- Se produce un fallo del sistema en un nodo y el nodo no se puede reiniciar. Por ejemplo, cuando un nodo falla debido a una pérdida de alimentación, las controladoras de parejas de alta disponibilidad conmuta automáticamente a su nodo de partner y sirven los datos de la controladora de almacenamiento superviviente.



Si el almacenamiento para un nodo también pierde potencia al mismo tiempo, no será posible una toma de control estándar.

- No se reciben mensajes de latido del compañero del nodo. Esto podría suceder si el partner experimentó

un error de hardware o software (por ejemplo, un fallo de interconexión) que no dio lugar a una situación de pánico, pero todavía impidió que funcionara correctamente.

- Detenga uno de los nodos sin usar el `-f` o. `-inhibit-takeover true` parámetro.



En un clúster de dos nodos con un clúster de alta disponibilidad habilitado, detener o reiniciar un nodo mediante el `-inhibit-takeover true` El parámetro hace que ambos nodos dejen de servir datos a menos que deshabilite primero el clúster de alta disponibilidad y asigne un valor épsilon al nodo que desee permanecer en línea.

- Uno de los nodos se reinicia sin usar el `-inhibit-takeover true` parámetro. (La `-onboot` parámetro de `storage failover` el comando está habilitado de forma predeterminada.)
- El dispositivo de gestión remota (Service Processor) detecta un fallo del nodo asociado. Esto no es aplicable si deshabilita la toma de control asistida por hardware.

También puede iniciar manualmente tomas de control con el `storage failover takeover` comando.

Mejoras en la resiliencia y el diagnóstico de clústeres

A partir de ONTAP 9.9.1, las siguientes adiciones de resiliencia y diagnóstico mejoran el funcionamiento del clúster:

- **Monitoreo y evitación de puertos:** En configuraciones de clúster conmutado de dos nodos, el sistema evita los puertos que experimentan pérdida total de paquetes (pérdida de conectividad). En ONTAP 9.8.1 y versiones anteriores, esta funcionalidad solo estaba disponible en configuraciones conmutadas.
- *** Failover automático de nodos*:** Si un nodo no puede servir datos a través de su red de clúster, ese nodo no debe poseer ningún disco. En lugar de eso, su partner de alta disponibilidad debería asumir el control si el partner está en buen estado.
- **Comandos para analizar problemas de conectividad:** Utilice el siguiente comando para mostrar qué rutas de cluster están experimentando pérdida de paquetes: `network interface check cluster-connectivity show`

Cómo funciona la toma de control asistida por hardware

Habilitada de forma predeterminada, la función de toma de control asistida por hardware puede acelerar el proceso de toma de control utilizando el dispositivo de gestión remota de un nodo (Service Processor).

Cuando el dispositivo de gestión remota detecta un fallo, inicia rápidamente la toma de control en lugar de esperar a que ONTAP reconozca que el latido del partner se ha detenido. Si se produce un fallo sin esta función habilitada, el partner espera hasta que se dé cuenta de que el nodo ya no está dando un latido de corazón, confirma la pérdida del latido del corazón e inicia la toma de control.

La función de toma de control asistida por hardware utiliza el siguiente proceso para evitar que se espere:

1. El dispositivo de administración remota supervisa el sistema local para detectar ciertos tipos de errores.
2. Si se detecta un fallo, el dispositivo de gestión remota envía inmediatamente una alerta al nodo asociado.
3. Al recibir la alerta, el partner inicia la toma de control.

Eventos del sistema que activan la toma de control asistida por hardware

El nodo asociado puede generar una toma de control en función del tipo de alerta que reciba del dispositivo de gestión remota (Service Processor).

| Alerta | ¿Toma de control iniciada al recibirse? | Descripción |
|--------------------|---|--|
| reboot_anormal | No | Se produjo un reinicio anormal del nodo. |
| l2_watchdog_reset | Sí | El hardware del guardián del sistema ha detectado un restablecimiento L2. El dispositivo de administración remota detectó una falta de respuesta de la CPU del sistema y reinició el sistema. |
| pérdida_de_latido | No | El dispositivo de gestión remota ya no recibe el mensaje de latido del nodo. Esta alerta no hace referencia a los mensajes de latido entre los nodos del par de alta disponibilidad; hace referencia al latido entre el nodo y su dispositivo de gestión remota local. |
| mensaje_periódico | No | Se envía un mensaje periódico durante una operación normal de toma de control asistida por hardware. |
| power_cycle_via_sp | Sí | El dispositivo de gestión remota apague y encienda el sistema. |
| pérdida_potencia | Sí | Se produjo una pérdida de alimentación en el nodo. El dispositivo de gestión remota tiene una fuente de alimentación que mantiene la alimentación durante un corto período después de una pérdida de alimentación, lo que le permite informar de la pérdida de alimentación al partner. |
| power_off_via_sp | Sí | El dispositivo de gestión remota apagó el sistema. |
| reset_via_sp | Sí | El dispositivo de administración remota restablece el sistema. |
| prueba | No | Se envía un mensaje de prueba para verificar una operación de toma de control asistida por hardware. |

Cómo funciona la toma de control y la devolución automáticas

Las operaciones de toma de control y devolución automáticas pueden funcionar juntas para reducir y evitar las interrupciones del servicio cliente.

De forma predeterminada, si uno de los nodos de la pareja de alta disponibilidad produce una alarma, se reinicia o se detiene, el nodo del partner automáticamente sustituye y devuelve el almacenamiento cuando el nodo afectado se reinicia. A continuación, el par de alta disponibilidad reanuda su estado operativo normal.

También se pueden producir tomas automáticas si uno de los nodos deja de responder.

La devolución automática se produce de forma predeterminada. Si prefiere controlar el impacto de devolución en los clientes, puede desactivar la devolución automática y utilizar la `storage failover modify -auto`

`-giveback false -node <node>` comando. Antes de realizar la devolución automática (independientemente de lo que la haya activado), el nodo del partner espera una cantidad fija de tiempo, controlada por el `-delay- seconds` parámetro de `storage failover modify` comando. El retardo predeterminado es de 600 segundos. Al retrasar la devolución, el proceso provoca dos breves interrupciones del servicio: Una durante la toma de control y otra durante la devolución.

Este proceso evita una única interrupción prolongada que incluye el tiempo necesario para:

- La operación de toma de control
- El nodo tomado en arranque hasta el punto en el que está listo para la devolución
- La operación de devolución

Si la devolución automática falla en cualquiera de los agregados que no son raíz, el sistema realiza automáticamente dos intentos adicionales para completar la devolución.



Durante el proceso de toma de control, el proceso de devolución automática se inicia antes de que el nodo del partner esté listo para el retorno al nodo principal. Cuando caduca el límite de tiempo del proceso de devolución automática y el nodo del partner aún no está listo, el temporizador se reinicia. Como resultado, el tiempo entre el nodo del partner que está preparado y la devolución real que se está realizando puede ser más corto que el tiempo de devolución automática.

Qué sucede durante la toma de control

Cuando un nodo toma el control de su compañero, sigue proporcionando y actualizando datos en los agregados y volúmenes del partner.

Los siguientes pasos ocurren durante el proceso de toma de control:

1. Si la toma de control negociada está iniciada por el usuario, los datos agregados se mueven desde el nodo del partner al nodo que está realizando la toma de control. Se produce una breve interrupción del servicio cuando el propietario actual de cada agregado (excepto el agregado raíz) cambia a el nodo de toma de control. Esta interrupción es más breve que una interrupción que se produce durante una toma de control sin necesidad de reubicar agregados.



Una toma negociada durante el pánico no puede ocurrir en el caso de un pánico. Una toma de control puede ser el resultado de un fallo no asociado a una caída del pánico. Un fallo se experimenta cuando se pierde la comunicación entre un nodo y su compañero, también llamado pérdida de latido. Si se produce una toma de control debido a un fallo, la interrupción del servicio podría tardar más porque el nodo asociado necesita tiempo para detectar la pérdida de latido.

- Puede supervisar el progreso con el `storage failover show-takeover` comando.
- Puede evitar la reubicación de agregados durante esta instancia de toma de control mediante la `-bypass-optimization` con el `storage failover takeover` comando.

Los agregados se reubican en serie durante las operaciones de toma de control planificadas para reducir las interrupciones del cliente. Si se omite la reubicación de agregados, se produce una interrupción del servicio del cliente mayor durante los eventos de toma de control planificados.

2. Si la toma de control iniciada por el usuario es una toma de control negociada, el nodo de destino se cierra con dignidad, seguido de la toma de control del agregado raíz del nodo de destino y de cualquier

agregado que no se haya reubicado en el paso 1.

3. Las LIF de datos (interfaces lógicas) migran desde el nodo de destino al nodo de toma de control, o a cualquier otro nodo del clúster según las reglas de conmutación al nodo de respaldo de LIF. Puede evitar la migración de LIF mediante el `-skip-lif-migration` con el `storage failover takeover` comando. En caso de toma de control iniciada por el usuario, los LIF de datos se migran antes de que se inicie la toma de control del almacenamiento. En caso de alarma o fallo, los LIF de datos y el almacenamiento se migran al mismo tiempo.
4. Las sesiones SMB existentes se desconectan cuando se produce la toma de control.



Debido a la naturaleza del protocolo SMB, todas las sesiones SMB se interrumpen (a excepción de las sesiones SMB 3.0 conectadas a recursos compartidos con la propiedad Continuous Availability establecida). Las sesiones de SMB 1.0 y SMB 2.x no pueden volver a conectarse tras un evento de toma de control; por lo tanto, la toma de control es disruptiva y podrían producirse algunas pérdidas de datos.

5. Las sesiones SMB 3.0 que se establecen para recursos compartidos con la propiedad Continuous Availability habilitada pueden volver a conectarse a los recursos compartidos desconectados tras un evento de toma de control. Si su sitio utiliza conexiones SMB 3.0 a Microsoft Hyper-V y la propiedad de disponibilidad continua está activada en los recursos compartidos asociados, las tomas de control no causan interrupciones en dichas sesiones.

Qué sucede si un nodo que realiza una toma de control produce una alarma

Si el nodo que está realizando la toma de control produce una alarma en los 60 segundos tras iniciar la toma de control, se producen los siguientes eventos:

- El nodo que entró en pánico se reinicia.
- Después de reiniciar, el nodo realiza operaciones de recuperación automática y ya no se encuentra en modo de toma de control.
- La conmutación por error está deshabilitada.
- Si el nodo sigue teniendo algunos de los agregados del partner, tras habilitar la conmutación al nodo de respaldo del almacenamiento, devuelve estos agregados al partner mediante el `storage failover giveback` comando.

Qué sucede durante la devolución

El nodo local devuelve la propiedad al nodo del partner cuando se resuelven los problemas, cuando el nodo del partner arranca o cuando se inicia la devolución.

El siguiente proceso tiene lugar en una operación de devolución normal. En esta discusión, el nodo A ha tomado el control del nodo B. Se han resuelto todos los problemas en el nodo B y está listo para reanudar el servicio de datos.

1. Los problemas en el nodo B se resuelven y muestra el siguiente mensaje: `Waiting for giveback`
2. La devolución se inicia mediante `storage failover giveback` comando o mediante devolución automática si el sistema está configurado para él. Esto inicia el proceso de devolver la propiedad de los agregados y volúmenes del nodo B desde el nodo A al nodo B.
3. El nodo A devuelve primero el control del agregado raíz.
4. El nodo B completa el proceso de arranque hasta su estado operativo normal.

5. En cuanto el nodo B llega al punto del proceso de arranque en el que puede aceptar los agregados no raíz, el nodo A devuelve la propiedad de los otros agregados, uno a la vez, hasta que se completa la devolución. Puede supervisar el progreso de la devolución mediante el `storage failover show-giveback` comando.



La `storage failover show-giveback` el comando no muestra (ni está previsto) información acerca de todas las operaciones que se producen durante la operación de devolución de la conmutación por error del almacenamiento. Puede utilizar el `storage failover show` comando para mostrar detalles adicionales acerca del estado actual de la conmutación al respaldo del nodo, como si el nodo está totalmente funcional, la toma de control es posible y la devolución está completa.

La I/O se reanuda para cada agregado una vez que se ha completado el retorno para ese agregado, lo que reduce su ventana de interrupción del servicio general.

Política de ALTA DISPONIBILIDAD y su efecto en la toma de control y el retorno al nodo primario

ONTAP asigna automáticamente una política de alta disponibilidad del director financiero (recuperación tras fallos de la controladora) y de la recuperación tras fallos del almacenamiento en un agregado. Esta política determina la forma en que se producen las operaciones de conmutación por error del almacenamiento para el agregado y sus volúmenes.

Las dos opciones, CFO y SFO, determinan la secuencia de control de agregados que utiliza ONTAP durante las operaciones de recuperación tras fallos y recuperación del almacenamiento.

Aunque los términos CFO y SFO se utilizan a veces de manera informal para referirse a las operaciones de conmutación por error (toma de control y retorno al nodo primario) del almacenamiento, realmente representan la política de alta disponibilidad asignada a los agregados. Por ejemplo, los términos agregado SFO o agregado CFO simplemente se refieren a la asignación de la normativa de alta disponibilidad del agregado.

Las políticas de ALTA DISPONIBILIDAD afectan a las operaciones de toma de control y devolución de la siguiente manera:

- Los agregados creados en los sistemas ONTAP (excepto en el agregado raíz que contiene el volumen raíz) tienen una política de alta disponibilidad de SFO. La toma de control iniciada manualmente se optimiza para mejorar el rendimiento reubicando los agregados de SFO (no raíz) en serie en el partner antes de la toma de control. Durante el proceso de devolución, los agregados se devuelven en serie después de iniciar el sistema de recuperación y las aplicaciones de gestión se encuentran en línea, lo que permite al nodo recibir sus agregados.
- Dado que las operaciones de reubicación de agregados implican la reasignación de la propiedad de disco agregado y el control de movimiento de un nodo a su compañero, solo los agregados con una política de alta disponibilidad de SFO son aptos para la reubicación de agregados.
- El agregado raíz siempre tiene una política de alta disponibilidad de CFO y se devuelve al inicio de la operación de devolución. Esto es necesario para permitir el arranque del sistema de toma de control. El resto de agregados se devuelven en serie una vez que el sistema de recuperación completa el proceso de arranque y las aplicaciones de gestión se encuentran en línea, lo que permite al nodo recibir sus agregados.



Cambiar la política de alta disponibilidad de un agregado de SFO a CFO es una operación de modo de mantenimiento. No modifique esta configuración a menos que un representante de soporte al cliente lo indique.

Cómo afectan las actualizaciones en segundo plano a la toma de control y al retorno al nodo

Las actualizaciones en segundo plano del firmware de disco afectarán a la toma de control, el retorno al nodo primario y las operaciones de reubicación de agregados de alta disponibilidad de forma diferente, en función de cómo se inicien esas operaciones.

En la lista siguiente se describe cómo las actualizaciones del firmware del disco en segundo plano afectan a la toma de control, el retorno al nodo primario y la reubicación de agregados:

- Si se produce una actualización del firmware del disco en segundo plano en un disco de cualquiera de los nodos, las operaciones de toma de control iniciadas manualmente se retrasan hasta que la actualización del firmware del disco finalice en dicho disco. Si la actualización del firmware del disco en segundo plano tarda más de 120 segundos, se cancelan las operaciones de toma de control y se deben reiniciar manualmente una vez finalizada la actualización del firmware del disco. Si la toma de control se ha iniciado con `-bypass-optimization` parámetro de `storage failover takeover` comando establecido en `true`, la actualización del firmware del disco en segundo plano que se produce en el nodo de destino no afecta a la toma de control.
- Si se produce una actualización de firmware de disco en segundo plano en un disco del nodo de origen (o toma de control) y la toma de control se inició manualmente con el `-options` parámetro de `storage failover takeover` comando establecido en `immediate`, las operaciones de toma de control se inician inmediatamente.
- Si se produce una actualización del firmware del disco en segundo plano en un disco de un nodo y produce una alarma, la conmutación por error del nodo que ha entran en pánico se inicia de inmediato.
- Si se está produciendo una actualización del firmware del disco en segundo plano en un disco de cualquiera de los nodos, la restauración de los agregados de datos se retrasa hasta que la actualización del firmware del disco finaliza en ese disco.
- Si la actualización del firmware del disco en segundo plano tarda más de 120 segundos, se cancelan las operaciones de devolución y se deben reiniciar manualmente una vez finalizada la actualización del firmware del disco.
- Si se está produciendo una actualización de firmware de disco en segundo plano en un disco de cualquiera de los nodos, las operaciones de reubicación de agregados se retrasan hasta que la actualización del firmware del disco finalice en ese disco. Si la actualización del firmware del disco en segundo plano tarda más de 120 segundos, se cancelan las operaciones de reubicación de agregados y se deben reiniciar manualmente una vez finalizada la actualización del firmware de disco. Si se inició la reubicación de agregados con el `-override-destination-checks` de la `storage aggregate relocation` comando establecido en `true`, la actualización del firmware del disco en segundo plano que se produce en el nodo de destino no afecta a la reubicación de agregados.

Comandos de toma de control automática

La toma de control automática está habilitada de forma predeterminada en todas las plataformas FAS, AFF y ASA de NetApp compatibles. Es posible que deba cambiar el comportamiento y el control predeterminados cuando se producen las tomas automáticas cuando el nodo del partner se reinicia, produce una alarma o se detiene.

| | |
|--|--|
| Si desea que la toma de control se produzca automáticamente cuando el nodo asociado... | Se usa este comando... |
| Reinicia o detiene | <code>storage failover modify -node nodename -onreboot true</code> |

| | |
|---------|---|
| Pánicos | <code>storage failover modify -node nodename -onpanic true</code> |
|---------|---|

Habilite la notificación por correo electrónico si la funcionalidad de toma de control está deshabilitada

Para recibir una notificación con aviso si la función de toma de control se desactiva, debe configurar el sistema para activar la notificación automática de correo electrónico para los mensajes EMS de "takeover impossible":

- `ha.takeoverImpVersion`
- `ha.takeoverImpLowMem`
- `ha.takeoverImpDegraded`
- `ha.takeoverImpUnsync`
- `ha.takeoverImpIC`
- `ha.takeoverImpHotShelf`
- `ha.takeoverImpNotDef`

Comandos de devolución automática

De forma predeterminada, el nodo del partner de recuperación vuelve a ofrecer almacenamiento automáticamente cuando el nodo externo vuelve a estar en línea, por lo que restaura la relación de pareja de alta disponibilidad. En la mayoría de los casos, este es el comportamiento deseado. Si necesita desactivar la devolución automática, por ejemplo, si desea investigar la causa de la toma de control antes de dar vuelta, debe conocer la interacción de la configuración no predeterminada.

| Si desea... | Se usa este comando... |
|--|--|
| Habilite la devolución automática para que la devolución se produzca en cuanto arranca el nodo tomado, alcanza el estado esperando devolución y el retraso antes de que caduque el periodo de restauración automática. El valor predeterminado es TRUE. | <code>storage failover modify -node nodename -auto-giveback true</code> |
| Desactivar devolución automática. El valor predeterminado es TRUE. Nota: al establecer este parámetro en FALSE no se desactiva la devolución automática después de la toma de control en caso de pánico; la devolución automática después de la toma de control en caso de pánico debe estar desactivada estableciendo la <code>-auto-giveback-after-panic</code> parámetro a false. | <code>storage failover modify -node nodename -auto-giveback false</code> |

| | |
|---|--|
| Deshabilite la devolución automática después de tomar el control de pánico (esta configuración está habilitada de forma predeterminada). | <code>storage failover modify -node nodename -auto-giveback-after-panic false</code> |
| Retrasar la devolución automática durante un número de segundos especificado (el valor predeterminado es 600). Esta opción determina el tiempo mínimo que un nodo permanece durante la toma de control antes de realizar una devolución automática. | <code>storage failover modify -node nodename -delay-seconds seconds</code> |

De qué manera las variaciones del comando de modificación de la conmutación por error del almacenamiento afectan a la devolución automática

El funcionamiento de la devolución automática depende de la forma en que se configuren los parámetros del comando de modificación de la conmutación por error del almacenamiento.

En la siguiente tabla, se enumeran los ajustes predeterminados del `storage failover modify` parámetros de comando que se aplican a eventos de toma de control no causados por una alarma.

| Parámetro | Configuración predeterminada |
|----------------------------------|---|
| <code>-auto-giveback true</code> | <code>false</code> |
| <code>true</code> | <code>-delay-seconds integer (seconds)</code> |
| 600 | <code>-onreboot true</code> |
| <code>false</code> | <code>true</code> |

En la siguiente tabla se describen cómo las combinaciones de `-onreboot` y `-auto-giveback` los parámetros afectan la devolución automática para eventos de toma de control que no están causados por una alarma.

| <code>storage failover modify</code> parámetros utilizados | Causa de la toma de control | ¿Se produce la devolución automática? |
|---|-----------------------------|---|
| <code>-onreboot true</code> <code>-auto-giveback true</code> | comando reboot | Sí |
| Comando detenido o operación de ciclo de encendido emitido por el Service Processor | Sí | <code>-onreboot true</code> <code>-auto-giveback false</code> |
| comando reboot | Sí | Comando detenido o operación de ciclo de encendido emitido por el Service Processor |

| | | |
|---|---|----------------|
| No | <code>-onreboot false</code> <code>-auto-giveback true</code> | comando reboot |
| N.A. En este caso, no se produce la toma de control | Comando detenido o operación de ciclo de encendido emitido por el Service Processor | Sí |
| <code>-onreboot false</code> <code>-auto-giveback false</code> | comando reboot | No |

La `-auto-giveback` el parámetro controla el retorno tras el pánico y todos los demás tovers automáticos. Si la `-onreboot` el parámetro se establece en `true` y la toma de control se produce debido al reinicio, entonces se realiza siempre la devolución automática, independientemente de si la `-auto-giveback` el parámetro se establece en `true`.

La `-onreboot` El parámetro se aplica a los reinicios y los comandos de detención emitidos desde ONTAP. Cuando la `-onreboot` el parámetro se establece en `false`, la toma de control no se produce en caso de reiniciar el nodo. Por lo tanto, no se puede producir una devolución automática, independientemente de si `-auto-giveback` el parámetro se establece en `true`. Se produce una interrupción del cliente.

Los efectos de las combinaciones de parámetros de devolución automática que se aplican a situaciones de pánico.

En la siguiente tabla, se muestra el `storage failover modify` parámetros de comando que se aplican a situaciones de pánico:

| Parámetro | Configuración predeterminada |
|--|--|
| <code>`-onpanic _true</code> | <code>false_`</code> |
| <code>true</code> | <code>`-auto-giveback-after-panic _true</code> |
| <code>false_`</code> (Privilegio: Avanzado) | <code>true</code> |
| <code>`-auto-giveback _true</code> | <code>false_`</code> |

En la siguiente tabla se describe cómo las combinaciones de parámetros del `storage failover modify` comando que afecta la devolución automática en situaciones de emergencia.

| <code>storage failover</code> parámetros utilizados | ¿Se produce una devolución automática después de una alarma? |
|--|--|
| <code>-onpanic true</code> <code>-auto-giveback true</code> <code>-auto-giveback-after-panic true</code> | Sí |

| | |
|---|----|
| -onpanic true -auto-giveback true -auto-giveback-after-panic false | Sí |
| -onpanic true -auto-giveback false -auto-giveback-after-panic true | Sí |
| -onpanic true -auto-giveback false -auto-giveback-after-panic false | No |
| -onpanic false Si -onpanic se establece en false, la toma de control/devolución no se produce, independientemente del valor establecido para -auto-giveback o. -auto-giveback -after-panic | No |



Una toma de control puede ser el resultado de un fallo no asociado a una caída del pánico. Se experimenta un *failure* cuando se pierde la comunicación entre un nodo y su compañero, también llamado *beat loss*. Si se produce una toma de control debido a un error, la devolución se controla mediante la `-onfailure` en lugar de `-auto-giveback-after-panic` parameter.



Cuando un nodo produce una alarma, envía un paquete de alarma a su nodo compañero. Si por algún motivo el nodo del partner no recibe el paquete de pánico, el pánico se puede interpretar como un fallo. Sin recibir el paquete de pánico, el nodo asociado sólo sabe que la comunicación se ha perdido, y no sabe que ha ocurrido un pánico. En este caso, el nodo del partner procesa la pérdida de comunicación como un fallo en lugar de una alarma, y la devolución se controla mediante `-onfailure` parámetro (y no por la `-auto-giveback -after-panic` parameter).

Para obtener más detalles sobre todos `storage failover modify` parámetros, consulte "[Páginas de manual de ONTAP](#)".

Comandos de toma de control manual

Puede realizar la toma de control manualmente cuando necesite realizar tareas de mantenimiento en el partner y en otras situaciones similares. En función del estado del partner, el comando que utilice para realizar la toma de control varía.

| Si desea... | Se usa este comando... |
|--|---|
| Tome el control del nodo del partner | <code>storage failover takeover</code> |
| Supervisar el progreso de la toma de control mientras los agregados del partner se mueven al nodo que realiza la toma de control | <code>storage failover show-takeover</code> |
| Muestra el estado de conmutación por error de almacenamiento de todos los nodos del clúster | <code>storage failover show</code> |

| | |
|--|--|
| Tomar el control del nodo del partner sin migrar las LIF | <code>storage failover takeover -skip-lif -migration-before-takeover true</code> |
| Hágase cargo del nodo del partner incluso si hay un error de coincidencia del disco | <code>storage failover takeover -skip-lif -migration-before-takeover true</code> |
| Asuma el nodo del partner incluso si hay una discrepancia en la versión de ONTAP Nota: Esta opción solo se utiliza durante el proceso de actualización de ONTAP no disruptivo. | <code>storage failover takeover -option allow -version-mismatch</code> |
| Asuma el control del nodo de partner sin realizar la reubicación de agregados | <code>storage failover takeover -bypass -optimization true</code> |
| Toma el control del nodo de partner antes de que el partner tenga tiempo para cerrar sus recursos de almacenamiento perfectamente | <code>storage failover takeover -option immediate</code> |

Antes de emitir el comando de conmutación al nodo de respaldo de almacenamiento con la opción inmediata, debe migrar las LIF de datos a otro nodo mediante el comando siguiente:

```
network interface migrate-all -node node
```



Si especifica el `storage failover takeover -option immediate` Comando sin primero migrar las LIF de datos, la migración de la LIF de datos del nodo se retrasa significativamente aunque la `skip-lif-migration-before-takeover` opción no especificada.

De forma similar, si especifica la opción inmediato, se omite la optimización negociada de toma de control aunque la opción `bypass-Optimization` esté establecida en *false*.

Traslado del épsilon para determinadas adquisiciones iniciadas manualmente

Debería mover épsilon si espera que cualquier toma de control iniciada manualmente podría provocar que su sistema de almacenamiento falle un nodo inesperado durante una pérdida de quórum en todo el clúster.

Acerca de esta tarea

Para realizar tareas de mantenimiento planificadas, debe hacerse el control de uno de los nodos de un par de alta disponibilidad. Se debe mantener el quorum en todo el clúster para evitar interrupciones no planificadas en los datos del cliente para los nodos restantes. En algunos casos, la toma de control puede provocar un cluster que es un fallo inesperado de nodo lejos de la pérdida de quórum en todo el cluster.

Esto puede suceder si el nodo que se está tomando está épsilon o si el nodo con épsilon no está en buen estado. Para mantener un clúster más resiliente, se puede transferir épsilon a un nodo en buen estado que no se vaya a transferir.

Normalmente, este sería el partner de alta disponibilidad.

Solo los nodos sanos y aptos participan en la votación de quórum. Para mantener el quórum en todo el clúster, se necesitan más de $N/2$ votos (donde N representa la suma de nodos en línea sanos y elegibles). En los clusters

con un número par de nodos online, épsilon añade una ponderación adicional para mantener quórum para el nodo al que está asignado.



Aunque la formación de cluster puede modificarse mediante el `cluster modify -eligibility false` comando, debe evitar esto excepto en situaciones como restaurar la configuración del nodo o realizar un mantenimiento prolongado de los nodos. Si establece un nodo que no cumple los requisitos, deja de servir datos DE SAN hasta que el nodo se restablece a apto y se reinicia. El acceso a datos NAS al nodo también puede verse afectado cuando el nodo no cumple con los requisitos.

Pasos

1. Compruebe el estado del clúster y confirme que un nodo en buen estado no está ocupado con épsilon:
 - a. Cambie al nivel de privilegio avanzado y confirme que desea continuar cuando aparezca el símbolo del sistema del modo avanzado (*>):

```
set -privilege advanced
```

- b. Determine qué nodo tiene épsilon:

```
cluster show
```

En el siguiente ejemplo, Node1 mantiene épsilon:

| Nodo | Salud | Condiciones | Épsilon |
|-------|-----------|-------------|-----------|
| node1 | verdadero | verdadero | verdadero |
| 2 | verdadero | verdadero | falso |

+

Si el nodo que desea sustituir no tiene un valor épsilon, continúe con el paso 4.

2. Elimine el valor épsilon del nodo que desee sustituir:

```
cluster modify -node Node1 -epsilon false
```

3. Asigne épsilon al nodo del partner (en este ejemplo, Node2):

```
cluster modify -node Node2 -epsilon true
```

4. Realice la operación de toma de control:

```
storage failover takeover -ofnode node_name
```

5. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

Comandos de devolución manual

Puede realizar una devolución normal, una devolución del nodo en la que termina los procesos en el nodo asociado o una devolución forzada.



Antes de realizar una devolución del control, debe quitar las unidades con errores en el sistema tomado-encima como se describe en ["Gestión de discos y agregados"](#).

Si se interrumpe la devolución

Si el nodo de toma de control experimenta un fallo o una interrupción del servicio de alimentación durante el proceso de devolución, este proceso se detiene y el nodo de toma de control regresa al modo de toma de control hasta que se repara el error o se restaura la alimentación.

Sin embargo, esto depende de la etapa de devolución en la que se haya producido el fallo. Si el nodo encontró un fallo o una interrupción del servicio de alimentación durante el estado de devolución parcial (después de haber devuelto el agregado raíz), no regresará al modo de toma de control. En su lugar, el nodo vuelve al modo de devolución parcial. Si esto ocurre, complete el proceso repitiendo la operación de devolución.

Si el retorno se ha vetado

Si se ha vetado la devolución, debe comprobar los mensajes EMS para determinar la causa. Dependiendo de la razón o de las razones, puede decidir si puede anular de forma segura los vetos.

La `storage failover show-giveback` el comando muestra el progreso de la devolución y muestra qué subsistema vetó la devolución, si la hubiera. Los vetos blandos pueden ser anulados, mientras que los vetos duros no pueden ser, incluso si son forzados. En las siguientes tablas se resumen los vetos suaves que no deben anularse, junto con las soluciones recomendadas.

Puede consultar los detalles de EMS de cualquier veto de devolución utilizando el siguiente comando:

```
event log show -node * -event gb*
```

Devolución del agregado raíz

Estos vetos no se aplican a las operaciones de reubicación de agregados:

| Vetoque módulo subsistema | Solución alternativa |
|---------------------------|---|
| nivel_bajo_vfiler | <p>Finalice las sesiones SMB que causan el veto o apague la aplicación SMB que estableció las sesiones abiertas.</p> <p>Reemplazar este veto puede provocar que la aplicación que utiliza SMB se desconecte abruptamente y pierda datos.</p> |
| Comprobación del disco | <p>Todos los discos fallidos o omitidos se deben eliminar antes de intentar realizar la devolución. Si se están saneando los discos, debería esperar hasta que finalice la operación.</p> <p>Si se anula este veto, se podría producir una interrupción del servicio provocada por agregados o volúmenes que se desconectarán debido a conflictos de reserva o discos inaccesibles.</p> |

Recuperación de los agregados SFO

Estos vetos no se aplican a las operaciones de reubicación de agregados:

| | |
|-------------------------------------|---|
| Vetoque módulo subsistema | Solución alternativa |
| Gestor de bloqueos | <p>Apague con dignidad las aplicaciones SMB que tienen archivos abiertos o mueva esos volúmenes a un agregado diferente.</p> <p>Sobrescribir este veto produce una pérdida de estado de bloqueo de SMB, lo que provoca interrupciones y pérdida de datos.</p> |
| Bloquear OPERACIONES NO DISRUPTIVAS | <p>Espere hasta que los bloqueos estén reflejados.</p> <p>Anular este veto provoca interrupciones en las máquinas virtuales de Microsoft Hyper-V.</p> |
| RAID | <p>Compruebe los mensajes EMS para determinar la causa del veto:</p> <p>Si el veto se debe a nvfile, coloque los volúmenes y los agregados offline en línea.</p> <p>Si las operaciones de adición de discos o de reasignación de la propiedad de discos están en curso, espere hasta que hayan finalizado.</p> <p>Si el veto se debe a un conflicto de nombre de agregado o UUID, solucione y resuelva el problema.</p> <p>Si el veto se debe a una resincronización de espejo, verificación de espejo o discos sin conexión, el veto puede anularse y la operación se reinicia después de la devolución.</p> |
| Inventario de discos | <p>Solucione problemas para identificar y resolver la causa del problema.</p> <p>Es posible que el nodo de destino no pueda ver discos que pertenecen a un agregado que se está migrando.</p> <p>Los discos inaccesibles pueden provocar agregados o volúmenes inaccesibles.</p> |
| Operación de movimiento de volumen | <p>Solucione problemas para identificar y resolver la causa del problema.</p> <p>Este veto impide que la operación de desplazamiento de volumen se aborte durante la fase de transposición importante. Si el trabajo se cancela durante la transición, es posible que el volumen no se pueda acceder a él.</p> |

Comandos para realizar una devolución del control manual

Puede iniciar manualmente un retorno al nodo en una pareja de alta disponibilidad para devolver el almacenamiento al propietario original tras completar el mantenimiento o resolver cualquier problema que provoque la toma de control.

| | |
|-------------|------------------------|
| Si desea... | Se usa este comando... |
|-------------|------------------------|

| | |
|--|--|
| Conceda de nuevo almacenamiento a un nodo asociado | <code>storage failover giveback -ofnode nodename</code> |
| Recupere el almacenamiento aunque el partner no esté en el modo de devolución | <code>storage failover giveback -ofnode nodename -require-partner-waiting false</code> No utilice esta opción a menos que se acepte una interrupción del cliente más larga. |
| Devolver el almacenamiento aunque los procesos veten la operación de devolución (forzar la devolución) | <code>storage failover giveback -ofnode nodename -override-vetoes true</code> El uso de esta opción puede provocar una interrupción del servicio del cliente mayor o agregados y volúmenes que no se conecten tras esta devolución. |
| Proporcione solo los agregados CFO (el agregado raíz). | <code>storage failover giveback -ofnode nodename -only-cfo-aggregates true</code> |
| Supervise el progreso de la devolución después de emitir el comando retorno | <code>storage failover show-giveback</code> |

Prueba de toma de control y retorno al nodo primario

Después de configurar todos los aspectos de su par de alta disponibilidad, debe verificar que funciona como se espera para mantener un acceso ininterrumpido al almacenamiento de ambos nodos durante las operaciones de toma de control y devolución. Durante el proceso de toma de control, el nodo local (o de toma de control) debe seguir prestando servicio a los datos que normalmente proporciona el nodo del partner. Durante la devolución, el control y la entrega del almacenamiento del partner deben volver al nodo del partner.

Pasos

1. Revise el cableado en los cables de interconexión de alta disponibilidad para asegurarse de que sean seguros.
2. Compruebe que puede crear y recuperar archivos en ambos nodos para cada protocolo con licencia.
3. Introduzca el siguiente comando:

```
storage failover takeover -ofnode partnernode
```

Consulte la página man para obtener más detalles del comando.

4. Escriba uno de los siguientes comandos para confirmar que se ha producido la conmutación por error:

```
storage failover show-takeover
```

```
storage failover show
```

Si tiene `storage failover` de comandos `-auto-giveback` opción habilitada:

| Nodo | Como partner | Toma de control posible | Descripción del estado |
|--------|--------------|-------------------------|--|
| nodo 1 | nodo 2 | - | Esperando devolución |
| nodo 2 | nodo 1 | falso | Durante la toma de control, la devolución automática se iniciará en número de segundos |

Si tiene `storage failover` de comandos `-auto-giveback` opción deshabilitada:

| Nodo | Como partner | Toma de control posible | Descripción del estado |
|--------|--------------|-------------------------|----------------------------|
| nodo 1 | nodo 2 | - | Esperando devolución |
| nodo 2 | nodo 1 | falso | Durante la toma de control |

5. Muestre todos los discos que pertenecen al nodo asociado (Node2) que el nodo de toma de control (Node1) puede detectar:

```
storage disk show -home node2 -ownership
```

El siguiente comando muestra todos los discos que pertenecen a Node2 que Node1 puede detectar:

```
cluster::> storage disk show -home node2 -ownership
```

| Disco | Agregado | Inicio | Propietario | Recuperación ante desastres en casa | ID de casa | ID del propietario | ID de inicio de recuperación ante desastres | Reservador | Piscina |
|-------|----------|--------|-------------|-------------------------------------|------------|--------------------|---|------------|-----------|
| 1.0.2 | - | 2 | 2 | - | 4078312453 | 4078312453 | - | 4078312452 | Piscina 0 |
| 1.0.3 | - | 2 | 2 | - | 4078312453 | 4078312453 | - | 4078312452 | Piscina 0 |

6. CConfirme que el nodo de respaldo (Node1) controla los agregados del nodo principal (Node2):

```
aggr show -fields home-id,home-name,is-home
```

| agregado | id de casa | casa-nameh | es-casa |
|----------|------------|------------|-----------|
| aggr0_1 | 2014942045 | nodo 1 | verdadero |
| aggr0_2 | 4078312453 | 2 | falso |

| | | | |
|---------|------------|--------|-----------|
| aggr1_1 | 2014942045 | nodo 1 | verdadero |
| aggr1_2 | 4078312453 | 2 | falso |

Durante la toma de control, el valor «'is-home'» de los agregados del nodo partner es FALSE.

7. Devolver el servicio de datos del nodo del partner cuando muestre el mensaje «'esperando devolución'»:

```
storage failover giveback -ofnode partnernode
```

8. Escriba uno de los siguientes comandos para observar el progreso de la operación de devolución del nodo:

```
storage failover show-giveback
```

```
storage failover show
```

9. Continúe, dependiendo de si ha visto el mensaje de que la devolución se ha completado correctamente:

| | |
|--|---|
| Si toma de control y retorno al nodo primario... | Realice lo siguiente... |
| Se han completado correctamente | Repita del paso 2 al paso 8 en el nodo asociado. |
| Error | Corrija el fallo de toma de control o devolución y repita este procedimiento. |

Comandos para supervisar una pareja de alta disponibilidad

Puede usar los comandos ONTAP para supervisar el estado de la pareja de ha. Si se produce una toma de control, también puede determinar la causa de la toma de control.

| | |
|--|---|
| Si desea comprobar | Utilice este comando |
| Tanto si la conmutación por error está habilitada como si se ha producido, o por qué no es posible la conmutación por error actualmente | <code>storage failover show</code> |
| Vea los nodos en los que está habilitado la configuración de conmutación por error de almacenamiento en modo HA Debe establecer el valor como HA para que el nodo participe en una configuración de conmutación por error de almacenamiento (par de alta disponibilidad). | <code>storage failover show -fields mode</code> |
| Si la toma de control asistida por hardware está habilitada | <code>storage failover hwassist show</code> |
| Historial de eventos de toma de control asistida por hardware que se han producido | <code>storage failover hwassist stats show</code> |
| El progreso de una operación de toma de control a medida que los agregados del partner se mueven al nodo que realiza la toma de control | <code>storage failover show-takeover</code> |

| | |
|---|---|
| El progreso de una operación de devolución al devolver agregados al nodo asociado | <code>storage failover show-giveback</code> |
| Si un agregado se muestra a raíz durante las operaciones de toma de control o devolución | <code>aggregate show -fields home-id,owner-id,home-name,owner-name,is-home</code> |
| Si la alta disponibilidad del clúster está habilitada (solo se aplica a clústeres de dos nodos) | <code>cluster ha show</code> |
| Estado de alta disponibilidad de los componentes de un par de alta disponibilidad (en sistemas que usan el estado de alta disponibilidad) | <code>ha-config show</code> Este es un comando de modo de mantenimiento. |

estados de nodo que se muestran con comandos `show-type` de conmutación al nodo de respaldo del almacenamiento

En la siguiente lista se describen los estados del nodo que el `storage failover show` se muestra el comando.

| Estado del nodo | Descripción |
|---|--|
| Conectado a nombre_partner, toma de control automática deshabilitada. | La interconexión de alta disponibilidad es activa y puede transmitir datos al nodo asociado. Se ha deshabilitado la toma de control automática del partner. |
| Esperando nombre_partner, restauración de los discos de repuesto del partner pendientes. | El nodo local no puede intercambiar información con el nodo compañero a través de la interconexión de alta disponibilidad. La devolución de los agregados de la OFS al partner se ha completado, pero los discos de reserva del partner siguen siendo propiedad del nodo local. <ul style="list-style-type: none"> • Ejecute el <code>storage failover show-giveback</code> comando para obtener más información. |
| Esperando nombre_partner. Esperando la sincronización de bloqueo del partner. | El nodo local no puede intercambiar información con el nodo asociado a través de la interconexión de alta disponibilidad; está esperando a que se produzca la sincronización de bloqueo del partner. |
| Esperando nombre_partner. Esperando a que las aplicaciones del clúster se conecten en el nodo local. | El nodo local no puede intercambiar información con el nodo asociado a través de la interconexión de alta disponibilidad; mientras espera a que las aplicaciones de clúster se conecten. |
| Toma de control programada. El nodo de destino reubica sus agregados de SFO durante la preparación de la toma de control. | Se inició el procesamiento de la toma de control. El nodo de destino se está reubicando la propiedad de sus agregados de SFO durante la preparación para la toma de control. |

| | |
|--|---|
| Toma de control programada. El nodo de destino ha reubicado sus agregados SFO durante la preparación de la toma de control. | Se inició el procesamiento de la toma de control. El nodo de destino ha reubicado la propiedad de sus agregados SFO para prepararse para la toma de control. |
| Toma de control programada. Esperando para deshabilitar las actualizaciones del firmware del disco en segundo plano en el nodo local. Hay una actualización de firmware en curso en el nodo. | Se inició el procesamiento de la toma de control. El sistema está esperando a que se completen operaciones de actualización del firmware de los discos en segundo plano en el nodo local. |
| Reubicación de los agregados de SFO para hacer frente al nodo en la preparación de la toma de control | El nodo local está reubicando la propiedad de sus agregados de la OFS al nodo de toma de control como preparación para la toma de control. |
| Se reubicaron los agregados de SFO para hacer frente al nodo. A la espera de que se tome el control del nodo. | Se ha completado la reubicación de la propiedad de los agregados de la OFS del nodo local al nodo de toma de control. El sistema está esperando a que el nodo de toma de control. |
| Reubicando los agregados de SFO en partner_NAME. Esperando para deshabilitar las actualizaciones del firmware del disco en segundo plano en el nodo local. Hay una actualización de firmware en curso en el nodo. | La reubicación de la propiedad de los agregados de la OFS del nodo local al nodo de toma de control está en curso. El sistema está esperando a que se completen operaciones de actualización del firmware de los discos en segundo plano en el nodo local. |
| Reubicando los agregados de SFO en partner_NAME. Esperando a deshabilitar las actualizaciones de firmware del disco en segundo plano para nombre_partner. Hay una actualización de firmware en curso en el nodo. | La reubicación de la propiedad de los agregados de la OFS del nodo local al nodo de toma de control está en curso. El sistema está esperando a que se completen operaciones de actualización del firmware del disco en segundo plano en el nodo del partner. |
| Conectado a nombre_partner. Se ha anulado el intento de toma de control anterior debido a este motivo. El nodo local posee algunos de los agregados SFO del partner. Vuelva a emitir la toma de control del partner con el <code>-bypass-optimization</code> parámetro establecido en true para la toma de control de los agregados restantes, o emita una devolución del partner para devolver los agregados reubicados. | <p>La interconexión de alta disponibilidad es activa y puede transmitir datos al nodo asociado. El intento de toma de control anterior se canceló debido al motivo mostrado bajo el motivo. El nodo local posee algunos de los agregados SFO de su partner.</p> <ul style="list-style-type: none"> • Vuelva a emitir la toma de control del nodo asociado, estableciendo el parámetro <code>-bypass-optimization</code> en true para tomar posesión de los agregados SFO restantes, o realice una devolución del partner para devolver los agregados reubicados. |

| | |
|---|--|
| <p>Conectado a nombre_partner. Se canceló el intento de toma de control anterior. El nodo local posee algunos de los agregados SFO del partner. Vuelva a emitir la toma de control del partner con el -bypass-optimization parámetro establecido en true para la toma de control de los agregados restantes, o emita una devolución del partner para devolver los agregados reubicados.</p> | <p>La interconexión de alta disponibilidad es activa y puede transmitir datos al nodo asociado. Se canceló el intento de toma de control anterior. El nodo local posee algunos de los agregados SFO de su partner.</p> <ul style="list-style-type: none"> • Vuelva a emitir la toma de control del nodo asociado, estableciendo el parámetro -bypass-optimization en true para tomar posesión de los agregados SFO restantes, o realice una devolución del partner para devolver los agregados reubicados. |
| <p>Esperando nombre_partner. Se ha anulado el intento de toma de control anterior debido a este motivo. El nodo local posee algunos de los agregados SFO del partner. Vuelva a emitir la toma de control del partner con el parámetro "-bypass-Optimization" establecido en true para tomar el control de los agregados restantes, o emita una devolución del partner para devolver los agregados reubicados.</p> | <p>El nodo local no puede intercambiar información con el nodo compañero a través de la interconexión de alta disponibilidad. El intento de toma de control anterior se canceló debido al motivo mostrado bajo el motivo. El nodo local posee algunos de los agregados SFO de su partner.</p> <ul style="list-style-type: none"> • Vuelva a emitir la toma de control del nodo asociado, estableciendo el parámetro -bypass-optimization en true para tomar posesión de los agregados SFO restantes, o realice una devolución del partner para devolver los agregados reubicados. |
| <p>Esperando nombre_partner. Se canceló el intento de toma de control anterior. El nodo local posee algunos de los agregados SFO del partner. Vuelva a emitir la toma de control del partner con el parámetro "-bypass-Optimization" establecido en true para tomar el control de los agregados restantes, o emita una devolución del partner para devolver los agregados reubicados.</p> | <p>El nodo local no puede intercambiar información con el nodo compañero a través de la interconexión de alta disponibilidad. Se canceló el intento de toma de control anterior. El nodo local posee algunos de los agregados SFO de su partner.</p> <ul style="list-style-type: none"> • Vuelva a emitir la toma de control del nodo asociado, estableciendo el parámetro -bypass-optimization en true para tomar posesión de los agregados SFO restantes, o realice una devolución del partner para devolver los agregados reubicados. |
| <p>Conectado a nombre_partner. Se canceló el intento de toma de control anterior porque no se pudo deshabilitar la actualización del firmware del disco en segundo plano (BDFU) en el nodo local.</p> | <p>La interconexión de alta disponibilidad es activa y puede transmitir datos al nodo asociado. Se canceló el intento de toma de control anterior porque la actualización del firmware del disco en segundo plano en el nodo local no estaba deshabilitada.</p> |
| <p>Conectado a nombre_partner. Se ha anulado el intento de toma de control anterior debido a este motivo.</p> | <p>La interconexión de alta disponibilidad es activa y puede transmitir datos al nodo asociado. El intento de toma de control anterior se canceló debido al motivo mostrado bajo el motivo.</p> |

| | |
|---|---|
| Esperando nombre_partner. Se ha anulado el intento de toma de control anterior debido a este motivo. | El nodo local no puede intercambiar información con el nodo compañero a través de la interconexión de alta disponibilidad. El intento de toma de control anterior se canceló debido al motivo mostrado bajo el motivo. |
| Conectado a nombre_partner. Se ha anulado el intento de toma de control anterior por nombre_partner porque el motivo. | La interconexión de alta disponibilidad es activa y puede transmitir datos al nodo asociado. El intento de toma de control anterior del nodo partner se canceló debido al motivo que muestra motivo. |
| Conectado a nombre_partner. Se ha anulado el intento de toma de control anterior por nombre_partner. | La interconexión de alta disponibilidad es activa y puede transmitir datos al nodo asociado. Se canceló el intento de toma de control anterior del nodo partner. |
| Esperando nombre_partner. Se ha anulado el intento de toma de control anterior por nombre_partner porque el motivo. | El nodo local no puede intercambiar información con el nodo compañero a través de la interconexión de alta disponibilidad. El intento de toma de control anterior del nodo partner se canceló debido al motivo que muestra motivo. |
| Error del retorno anterior en el módulo: Nombre del módulo. La devolución automática se iniciará en número de segundos. | <p>Error en el intento de devolución anterior en module_name. La devolución automática del control se iniciará en el número de segundos.</p> <ul style="list-style-type: none"> • Ejecute el <code>storage failover show-giveback</code> comando para obtener más información. |
| El nodo posee agregados de los partners como parte del procedimiento de actualización de controladora sin interrupciones. | El nodo posee los agregados de su partner debido al procedimiento de actualización de controladoras sin interrupciones actualmente en curso. |
| Conectado a nombre_partner. El nodo posee agregados que pertenecen a otro nodo del clúster. | La interconexión de alta disponibilidad es activa y puede transmitir datos al nodo asociado. El nodo posee agregados que pertenecen a otro nodo del clúster. |
| Conectado a nombre_partner. Esperando la sincronización de bloqueo del partner. | La interconexión de alta disponibilidad es activa y puede transmitir datos al nodo asociado. El sistema está esperando a que se complete la sincronización del bloqueo del partner. |
| Conectado a nombre_partner. Esperando a que las aplicaciones del clúster se conecten en el nodo local. | La interconexión de alta disponibilidad es activa y puede transmitir datos al nodo asociado. El sistema está esperando a que las aplicaciones de clúster estén conectadas en el nodo local. |

| | |
|--|---|
| No modo de alta disponibilidad, reinicie para utilizar NVRAM completa. | <p>No es posible recuperar el sistema de almacenamiento. La opción de modo de alta disponibilidad está configurada como non_ha.</p> <ul style="list-style-type: none"> • Debe reiniciar el nodo para utilizar toda su NVRAM. |
| Modo no de alta disponibilidad. Reinicie el nodo para activar alta disponibilidad. | <p>No es posible recuperar el sistema de almacenamiento.</p> <ul style="list-style-type: none"> • El nodo se debe reiniciar para habilitar la funcionalidad de alta disponibilidad. |
| Modo no de alta disponibilidad. | <p>No es posible recuperar el sistema de almacenamiento. La opción de modo de alta disponibilidad está configurada como non_ha.</p> <ul style="list-style-type: none"> • Debe ejecutar el <code>storage failover modify -mode ha -node nodename</code> Comando en ambos nodos de la pareja de ha y, a continuación, reinicie los nodos para habilitar la funcionalidad de alta disponibilidad. |

Comandos para habilitar y deshabilitar la conmutación al nodo de respaldo del almacenamiento

Utilice los siguientes comandos para habilitar y deshabilitar la funcionalidad de conmutación al nodo de respaldo del almacenamiento.

| Si desea... | Se usa este comando... |
|--------------------------------|---|
| Habilite la toma de control | <code>storage failover modify -enabled true -node <i>nodename</i></code> |
| Deshabilite la toma de control | <code>storage failover modify -enabled false -node <i>nodename</i></code> |



Solo debe deshabilitar la conmutación por error del almacenamiento si es necesario como parte de un procedimiento de mantenimiento.

Detenga o reinicie un nodo sin iniciar la toma de control en un clúster de dos nodos

Detuvo o reiniciar un nodo en un clúster de dos nodos sin iniciar la toma de control cuando realiza determinado mantenimiento de hardware en un nodo o una bandeja y desea limitar el tiempo de inactividad manteniendo el nodo del partner en funcionamiento. o cuando hay problemas que impiden la toma de control manual y desea mantener los agregados del nodo asociado en funcionamiento y sirviendo datos. Además, si el soporte técnico le ayuda a solucionar problemas, es posible que tenga que

realizar este procedimiento como parte de dichos esfuerzos.

Acerca de esta tarea

- Antes de inhibir la toma de control (mediante el `-inhibit-takeover true` Parámetro), deshabilita el clúster ha.



- En un clúster de dos nodos, el clúster de alta disponibilidad garantiza que se produzca un error en un nodo que no deshabilite el clúster. Sin embargo, si no deshabilita la alta disponibilidad del clúster antes de usar el `-inhibit-takeover true` parámetro, ambos nodos dejan de servir datos.
- Si intenta detener o reiniciar un nodo antes de deshabilitar la alta disponibilidad del clúster, ONTAP emite una advertencia y le indica que debe deshabilitar la alta disponibilidad del clúster.

- Migra LIF (interfaces lógicas) al nodo del partner que desea mantener en línea.
- Si en el nodo que va a detener o reiniciar hay agregados que desea conservar, los mueve al nodo que desea permanecer en línea.

Pasos

1. Compruebe que ambos nodos estén en buen estado:

```
cluster show
```

Para ambos nodos, `true` aparece en la `Health` columna.

```
cluster::> cluster show
Node           Health  Eligibility
-----
node1          true   true
node2          true   true
```

2. Migre todos los LIF del nodo que detendrá o reiniciará al nodo compañero:

```
network interface migrate-all -node node_name
```

3. Si en el nodo que va a detener o reiniciar hay agregados que desea mantener en línea cuando el nodo está inactivo, reubicarlos al nodo del compañero; de lo contrario, vaya al siguiente paso.

- a. Muestre los agregados del nodo que detendrá o reiniciará:

```
storage aggregates show -node node_name
```

Por ejemplo, el nodo 1 es el nodo que se detuvo o reiniciando:

```
cluster::> storage aggregates show -node node1
Aggregate Size Available Used% State #Vols Nodes RAID
Status
-----
aggr0_node_1_0
744.9GB 32.68GB 96% online 2 node1 raid_dp,
normal
aggr1 2.91TB 2.62TB 10% online 8 node1 raid_dp,
normal
aggr2 4.36TB 3.74TB 14% online 12 node1 raid_dp,
normal
test2_aggr 2.18TB 2.18TB 0% online 7 node1 raid_dp,
normal
4 entries were displayed.
```

b. Mueva los agregados al nodo partner:

```
storage aggregate relocation start -node node_name -destination node_name
-aggregate-list aggregate_name
```

Por ejemplo, los agregados aggr1, aggr2 y test2_aggr se están moviendo del nodo 1 al nodo 2:

```
storage aggregate relocation start -node node1 -destination node2 -aggregate
-list aggr1,aggr2,test2_aggr
```

4. Deshabilitar clúster de alta disponibilidad:

```
cluster ha modify -configured false
```

La salida de retorno confirma que ha está desactivada: Notice: HA is disabled



Esta operación no deshabilita la conmutación al nodo de respaldo del almacenamiento.

5. Detenga o reinicie el sistema e impida la toma de control del nodo de destino mediante el uso del comando correspondiente:

- ° `system node halt -node node_name -inhibit-takeover true`
- ° `system node reboot -node node_name -inhibit-takeover true`



En el resultado del comando, verá una advertencia preguntándole si desea continuar, introduzca `y`.

6. Compruebe que el nodo que sigue estando conectado esté en buen estado (mientras el partner está

inactivo):
`cluster show`

Para el nodo en línea: `true` aparece en la `Health` columna.



En el resultado del comando, verá una advertencia de que alta disponibilidad del clúster no está configurado. Puede ignorar la advertencia en este momento.

7. Realice las acciones que le requerían para detener o reiniciar el nodo.
8. Arrancar el nodo desconectar desde el símbolo del sistema DEL CARGADOR:
`boot_ontap`

9. Compruebe que ambos nodos estén en buen estado:
`cluster show`

Para ambos nodos, `true` aparece en la `Health` columna.



En el resultado del comando, verá una advertencia de que alta disponibilidad del clúster no está configurado. Puede ignorar la advertencia en este momento.

10. Volver a habilitar el clúster de alta disponibilidad:
`cluster ha modify -configured true`
11. Si anteriormente de este procedimiento reubica los agregados al nodo del partner, moverlos de nuevo a su nodo de origen; de lo contrario, vaya al siguiente paso:
`storage aggregate relocation start -node node_name -destination node_name -aggregate-list aggregate_name`

Por ejemplo, los agregados `aggr1`, `aggr2` y `test2_aggr` se están moviendo del nodo 2 al nodo 1:

```
storage aggregate relocation start -node node2 -destination node1 -aggregate -list aggr1,aggr2,test2_aggr
```

12. Revertir los LIF a sus puertos raíz:
 - a. Vea los LIF que no están en casa:
`network interface show -is-home false`
 - b. Si hay LIF sin hogar que no se migraron desde el nodo inactivo, compruebe que es seguro moverlas antes de revertir.
 - c. Si puede hacerlo con seguridad, revierte el inicio de todos los LIF.
`network interface revert *`

Gestión de API de REST con System Manager

Gestión de API de REST con System Manager

El registro de la API DE REST captura las llamadas API que System Manager emite a ONTAP. Puede utilizar el registro para comprender la naturaleza y la secuencia de las llamadas necesarias para realizar las distintas tareas administrativas de ONTAP.

Cómo System Manager utiliza la API de REST y el registro de la API

Hay varias maneras en que System Manager envía las llamadas API DE REST a ONTAP.

Cuándo utiliza System Manager las llamadas API

Estos son los ejemplos más importantes de cuándo System Manager emite las llamadas a la API DE REST de ONTAP.

Actualización automática de páginas

System Manager emite automáticamente llamadas de API en segundo plano para actualizar la información mostrada, como en la página de la consola.

Mostrar acción por usuario

Se generan una o más llamadas API cuando se muestra un recurso de almacenamiento específico o una colección de recursos de la interfaz de usuario de System Manager.

Actualizar la acción por el usuario

Una llamada API se emite cuando se añade, modifica o elimina un recurso de ONTAP de la interfaz de usuario de System Manager.

Volver a emitir una llamada API

También puede volver a emitir manualmente una llamada API haciendo clic en una entrada de registro. Esto muestra la salida JSON sin configurar de la llamada.


Más información

- ["Documentos de automatización de ONTAP 9"](#)

Acceder al registro de la API de REST

Es posible acceder al registro que contiene un registro de las llamadas de la API DE REST de ONTAP que realiza System Manager. Al mostrar el registro, también puede volver a emitir llamadas API y revisar el resultado.

Pasos

1. En la parte superior de la página, haga clic en  Para mostrar el registro de la API de REST.

Las entradas más recientes se muestran en la parte inferior de la página.
2. A la izquierda, haga clic en **PANEL** y observe las nuevas entradas que se están creando para las llamadas API emitidas para actualizar la página.
3. Haga clic en **STORAGE** y, a continuación, en **Qtrees**.

Esto hace que System Manager emita una llamada de API específica para recuperar una lista de los qtrees.

4. Busque la entrada de registro que describe la llamada API que tiene el formato:

GET /api/storage/qtrees

Verá parámetros de consulta HTTP adicionales incluidos con la entrada, por ejemplo `max_records`.

5. Haga clic en la entrada log para volver a emitir la llamada GET API y mostrar la salida JSON sin configurar.

Ejemplo

```
{
  "records": [
    {
      "svm": {
        "uuid": "19507946-e801-11e9-b984-00a0986ab770",
        "name": "SMQA",
        "_links": {
          "self": {
            "href": "/api/svm/svms/19507946-e801-11e9-b984-00a0986ab770"
          }
        }
      },
      "volume": {
        "uuid": "1e173258-f98b-11e9-8f05-00a0986abd71",
        "name": "vol_vol_test2_dest_dest",
        "_links": {
          "self": {
            "href": "/api/storage/volumes/1e173258-f98b-11e9-8f05-00a0986abd71"
          }
        }
      },
      "id": 1,
      "name": "test2",
      "security_style": "mixed",
      "unix_permissions": 777,
      "export_policy": {
        "name": "default",
        "id": 12884901889,
        "_links": {
          "self": {
            "href": "/api/protocols/nfs/export-policies/12884901889"
          }
        }
      },
      "path": "/vol_vol_test2_dest_dest/test2",
      "_links": {
        "self": {

```



```
      "href": "/api/storage/qtrees/1e173258-f98b-11e9-8f05-00a0986abd71/1"
    }
  },
],
"num_records": 1,
"_links": {
  "self": {
    "href":
"/api/storage/qtrees?max_records=20&fields=*&name=!%22%22"
  }
}
```

Administración de volúmenes

Gestión de volúmenes y LUN con System Manager

Información general de administración de volúmenes con System Manager

A partir de ONTAP 9.7, puede usar System Manager para gestionar el almacenamiento lógico, como volúmenes y LUN de FlexVol, qtrees, eficiencia de almacenamiento y cuotas.

Si utiliza la versión clásica de System Manager (disponible solo en ONTAP 9.7 y versiones anteriores), consulte ["Gestión del almacenamiento lógico"](#)

Gestione los volúmenes

Información general sobre la gestión de volúmenes





Después de mostrar una lista de volúmenes en System Manager, puede realizar varias acciones para gestionar los volúmenes.



Pasos

1. En System Manager, haga clic en **almacenamiento > volúmenes**.

Se muestra la lista de volúmenes.

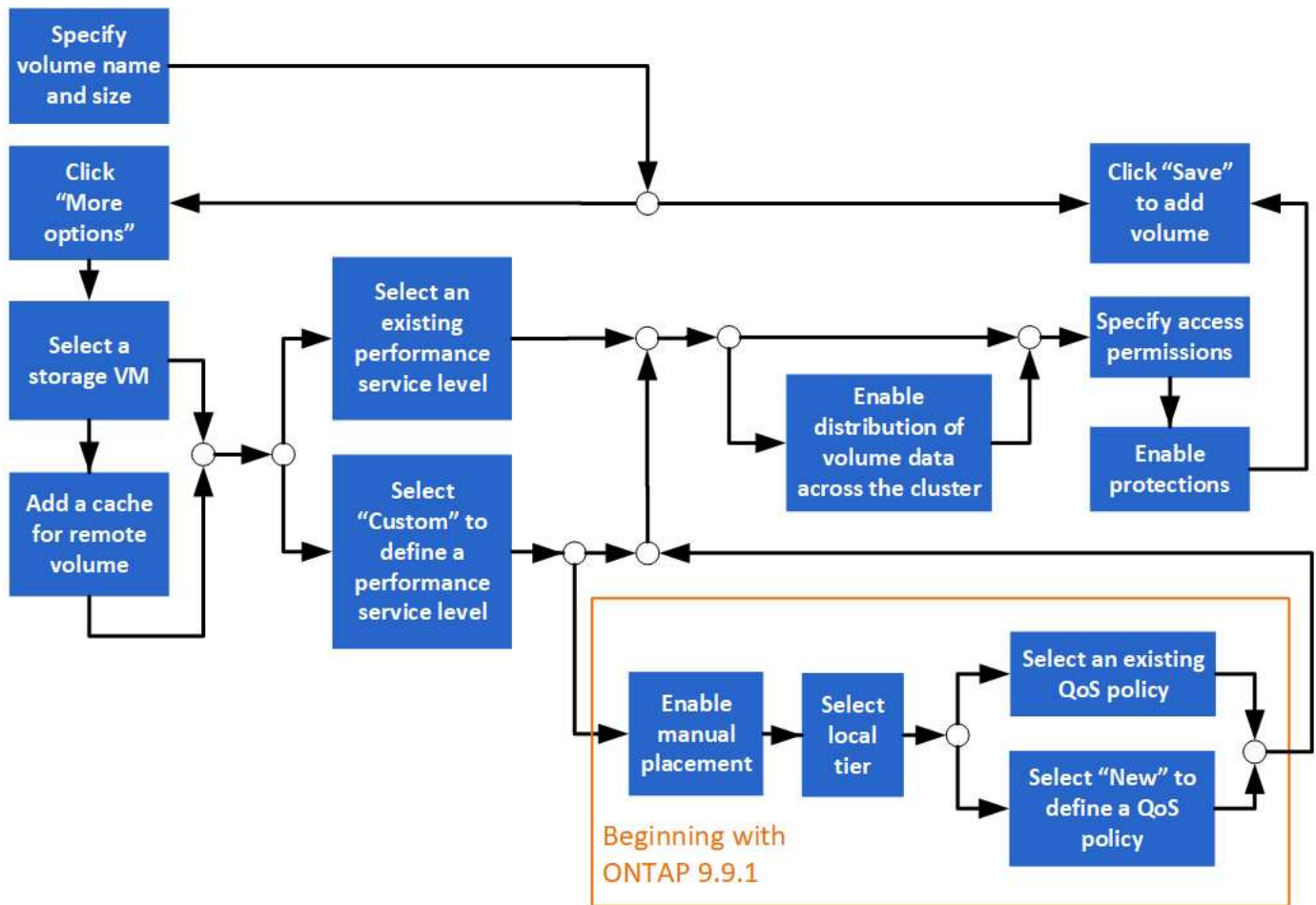
2. Puede realizar lo siguiente:

| Para realizar esta tarea... | Realice estas acciones... |
|-----------------------------|--|
| Añadir un volumen | Haga clic en  Add . Consulte "Añadir un volumen" . |
| Gestione varios volúmenes | <p>Active las casillas junto a los volúmenes.</p> <ul style="list-style-type: none">• Haga clic en  Delete para eliminar los volúmenes seleccionados.• Haga clic en  Protect para asignar una política de protección a los volúmenes seleccionados.• Haga clic en  More para seleccionar una de las siguientes acciones a realizar en todos los volúmenes seleccionados:<ul style="list-style-type: none">◦ Habilite la cuota◦ Desconectar◦ Mover◦ Mostrar volúmenes eliminados |

| | |
|--|---|
| <p>Gestione un único volumen</p> | <p>Junto al volumen, haga clic en , a continuación, seleccione una de las siguientes acciones que desee realizar:</p> <ul style="list-style-type: none"> • Editar • Cambiar el tamaño (a partir de ONTAP 9.10.1 y solo para volúmenes en línea y volúmenes FlexVol de DP) • Eliminar • Clonar • Desconectar (o conectar) • Habilitar cuota (o deshabilitar cuota) • Editar política de exportación • Edite la ruta de montaje • Mover • Edite la configuración de Cloud Tier • Proteger |
| <p>Cambiar el nombre de un volumen</p> | <p>Se puede cambiar el nombre de un volumen en la página de información general.</p> <p>Haga clic en  junto al nombre del volumen y, a continuación, modifique el nombre del volumen.</p> |

Añadir un volumen

Puede crear un volumen y añadirlo a una máquina virtual de almacenamiento existente que se configure para el servicio NFS o SMB.



Antes de empezar

- Debe haber un equipo virtual de almacenamiento configurado para servicio NFS o SMB en el clúster.
- A partir de ONTAP 9.13.1, puede habilitar los análisis de capacidad y el seguimiento de actividades de forma predeterminada en volúmenes nuevos. En System Manager, puede gestionar la configuración predeterminada en el nivel del clúster o de máquina virtual de almacenamiento. Para obtener más información, consulte [Active File System Analytics](#).

Pasos

1. Vaya a **almacenamiento > volúmenes**.
2. Seleccione **+ Add**.
3. Especifique un nombre y un tamaño para el volumen.
4. Realice uno de los siguientes pasos:

| Seleccione este botón... | Para realizar esta acción... |
|--------------------------|---|
| Guardar | El volumen se crea y se añade con los valores predeterminados del sistema. No se requieren pasos adicionales. |
| Más opciones | Vaya a Paso 5 para definir las especificaciones del volumen. |

5. se muestran el nombre y el tamaño del volumen si los ha especificado previamente. De lo contrario, introduzca el nombre y el tamaño.
6. Seleccione una máquina virtual de almacenamiento de la lista desplegable.

Solo se muestran las máquinas virtuales de almacenamiento configuradas con el protocolo NFS. Si sólo hay disponible un equipo virtual de almacenamiento configurado con el protocolo NFS, no se muestra el campo **Storage VM**.

7. Para agregar una memoria caché para el volumen remoto, seleccione **Agregar una memoria caché para el volumen remoto** y especifique los siguientes valores:
 - Seleccione un clúster.
 - Seleccione una máquina virtual de almacenamiento.
 - Seleccione el volumen que desea que sea un volumen de caché.
8. En la sección **almacenamiento y optimización**, especifique los siguientes valores:
 - a. La capacidad del volumen ya se muestra, pero es posible modificarla.
 - b. En el campo **nivel de servicio de rendimiento**, seleccione un nivel de servicio:

| Al seleccionar este nivel de servicio... | Esto ocurre... |
|---|--|
| Un nivel de servicio existente, como «extremo», «rendimiento» o «valor». Solo se muestran los niveles de servicio válidos para la plataforma del sistema (AFF, FAS, etc.). | Se seleccionan automáticamente un nivel o niveles locales. Vaya a. [step9] . |
| Personalizado | Vaya a. paso 8c para definir un nuevo nivel de servicio. |

- c. a partir de ONTAP 9.9.1, puede usar System Manager para seleccionar manualmente el nivel local en el que desea colocar el volumen que va a crear (si ha seleccionado el nivel de servicio "personalizado").



Esta opción no está disponible si selecciona **Agregar como caché para un volumen remoto o distribuir datos de volumen a través del clúster** (consulte a continuación).

| Cuando usted hace esta elección... | Realice estos pasos... |
|------------------------------------|---|
| Colocación manual | La ubicación manual está activada. La selección distribuir datos de volumen a través del clúster está desactivada (véase a continuación). Vaya a. Step 8d para completar el proceso. |
| Sin selección | La ubicación manual no está activada. El nivel local se selecciona automáticamente. Vaya a. [step9] . |

- a. Seleccione un nivel local en el menú desplegable.
 - b. Seleccione una política de calidad de servicio.

Seleccione "existente" para elegir entre una lista de directivas existentes o seleccione "Nuevo" para introducir las especificaciones de una nueva política.

9. [\[\[paso 9,Paso 9\]\]](#) en la sección **Opciones de optimización**, determine si desea distribuir los datos de volumen en el clúster:

| | |
|---|--|
| Cuando usted hace esta elección... | Esto ocurre... |
| Distribuya datos de volumen a través del cluster | El volumen que va a añadir se convierte en volumen FlexGroup. Esta opción no está disponible si ha seleccionado anteriormente colocación manual . |
| Sin selección | De forma predeterminada, el volumen que va a añadir se convierte en volumen FlexVol. |

10. En la sección **permisos de acceso**, especifique los permisos de acceso para los protocolos para los que está configurado el volumen.

A partir de ONTAP 9.11.1, el nuevo volumen no se podrá compartir de forma predeterminada. Para especificar los permisos de acceso predeterminados, asegúrese de que se activan las siguientes casillas de verificación:

- **Exportar a través de NGS:** Crea el volumen con la política de exportación "predeterminada" que otorga a los usuarios acceso total a los datos.
- **Compartir a través de SMB/CIFS:** Crea un recurso compartido con un nombre generado automáticamente, que se puede editar. El acceso se concede a «'todos'». También puede especificar el nivel de permiso.

11. En la sección **Protección**, especifique las protecciones para el volumen.

- A partir de ONTAP 9.12.1, puede seleccionar **Habilitar copias snapshot (locales)** y elegir una política de copia snapshot en lugar de usar la predeterminada.
- Si selecciona **Activar SnapMirror (local o remoto)**, especifique la directiva de protección y la configuración del clúster de destino en las listas desplegables.

12. Seleccione **Guardar**.

El volumen se crea y se añade al clúster y a la máquina virtual de almacenamiento.



También puede guardar las especificaciones de este volumen en un libro de aplicaciones de Ansible. Para obtener más información, visite ["Utilice libros de aplicaciones Ansible para añadir o editar volúmenes o LUN"](#).

Asigne etiquetas a volúmenes

A partir de ONTAP 9.14.1, puede usar System Manager para asignar etiquetas a volúmenes a fin de identificar objetos que pertenecen a una categoría, como proyectos o centros de costes.

Acerca de esta tarea

Puede asignar una etiqueta a un volumen. En primer lugar, debe definir y agregar la etiqueta. A continuación, también puede editar o eliminar la etiqueta.

Las etiquetas se pueden añadir al crear un volumen o más adelante se pueden añadir.

Usted define una etiqueta especificando una clave y asociando un valor a ella usando el formato "key:value". Por ejemplo: "dispt:engineering" o "location:san-jose".

Debe tenerse en cuenta lo siguiente al crear etiquetas:

- Las claves tienen una longitud mínima de un carácter y no pueden ser nulas. Los valores pueden ser nulos.
- Una clave se puede emparejar con varios valores separando los valores con una coma, por ejemplo, "location:san-jose,toronto"
- Las etiquetas se pueden usar para varios recursos.
- Las teclas deben comenzar por una letra minúscula.
- Las etiquetas asignadas a los volúmenes se eliminarán cuando se elimine el volumen.
- Las etiquetas no se recuperan si un volumen se recupera de la cola de recuperación.
- Las etiquetas se conservan si el volumen se mueve o se clona.
- Las etiquetas que se asignan a máquinas virtuales de almacenamiento en una relación de recuperación de desastres se replican en el volumen del sitio del partner.

Pasos


Para administrar etiquetas, realice los siguientes pasos:

1. En System Manager, haga clic en **Volúmenes** y, a continuación, seleccione el volumen al que desea agregar una etiqueta.

Las etiquetas se enumeran en la sección **Tags**.

2. Haga clic en **Administrar etiquetas** para modificar las etiquetas existentes o agregar otras nuevas.

Puede agregar, editar o eliminar las etiquetas.

| Para realizar esta acción... | Realice estos pasos... |
|------------------------------|--|
| Agregar una etiqueta | <ol style="list-style-type: none"> a. Haga clic en Añadir etiqueta. b. Especifique una clave y su valor o valores (separe varios valores con comas). c. Haga clic en Guardar. |
| Editar una etiqueta | <ol style="list-style-type: none"> a. Modifique el contenido en los campos Key y values (opcional). b. Haga clic en Guardar. |
| Eliminar una etiqueta | <ol style="list-style-type: none"> a. Haga clic en  junto a la etiqueta que desea eliminar. |

Recuperar volúmenes eliminados

Si ha eliminado por error uno o varios volúmenes de FlexVol, puede usar System Manager para recuperar estos volúmenes. A partir de ONTAP 9.8, también es posible recuperar volúmenes de FlexGroup con System Manager. También es posible eliminar los volúmenes de forma permanente. Para ello, se deben purgar los volúmenes.

El tiempo de retención de volúmenes se puede establecer en el nivel de una máquina virtual de almacenamiento. De manera predeterminada, el tiempo de retención de volumen se establece en 12 horas.

Selección de volúmenes eliminados

Pasos

1. Haga clic en **almacenamiento > volúmenes**.
2. Haga clic en **más > Mostrar volúmenes eliminados**.
3. Seleccione los volúmenes y haga clic en la acción que desee para recuperar o eliminar de forma permanente los volúmenes.

Restablecimiento de las configuraciones de volumen

Al eliminar un volumen, se eliminan las configuraciones asociadas del volumen. La recuperación de un volumen no restablece todas las configuraciones. Realice las siguientes tareas manualmente después de recuperar un volumen para que el volumen vuelva a su estado original:

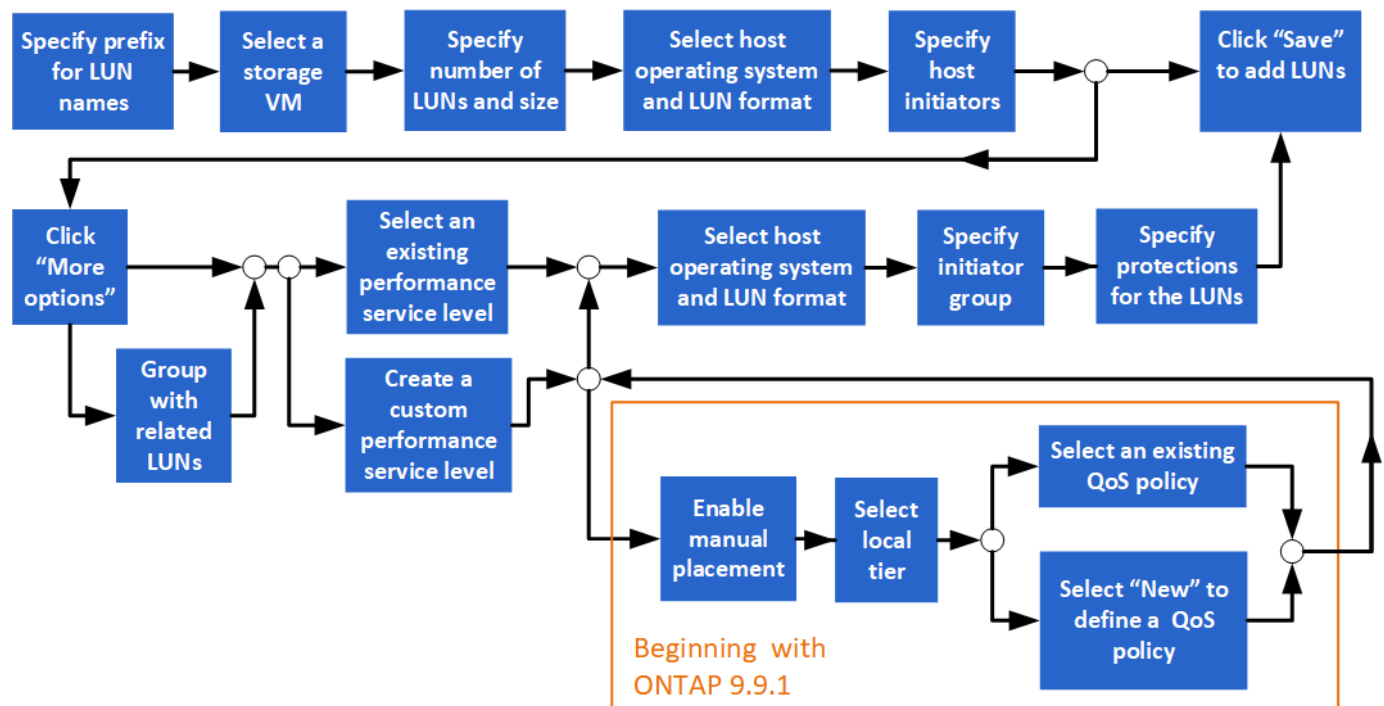
Pasos

1. Cambie el nombre del volumen.
2. Configure una ruta de unión (NAS).
3. Crear asignaciones para las LUN en el volumen (SAN).
4. Asocie una política de Snapshot y una política de exportación al volumen.
5. Se deben añadir nuevas reglas de política de cuotas para el volumen.
6. Añada una política de CALIDAD de SERVICIO para el volumen.

Gestionar las LUN

Puede crear LUN y añadirlos a un equipo virtual de almacenamiento existente que se configura con el protocolo SAN. También puede agrupar LUN o cambiarles el nombre.

Añada LUN



Antes de comenzar

En el clúster debe haber un equipo virtual de almacenamiento configurado para servicio SAN.

Pasos

1. Vaya a **almacenamiento > LUN**.
2. Haga clic en **+ Add**.
3. Especifique un prefijo que se utilizará al inicio de cada nombre de LUN. (Si solo crea una LUN, introduzca el nombre de la LUN.)
4. Seleccione una máquina virtual de almacenamiento de la lista desplegable.

Solo se muestran las máquinas virtuales de almacenamiento configuradas para el protocolo SAN. Si sólo hay disponible un equipo virtual de almacenamiento configurado para el protocolo SAN, no se mostrará el campo **Storage VM**.

5. Indique cuántas LUN desea crear y el tamaño de cada LUN.
6. Seleccione el sistema operativo host y el formato de LUN en las listas desplegables.
7. Introduzca los iniciadores de host y sepárelos con comas.
8. Ejecute una de las siguientes acciones:

| Haga clic en este botón... | Para realizar esta acción... |
|----------------------------|---|
| Guardar | Las LUN se crean con las especificaciones que ha introducido. Los valores predeterminados del sistema se utilizan para otras especificaciones. No se requieren pasos adicionales. |
| Más opciones | Vaya a Paso 9 A fin de definir especificaciones adicionales para las LUN. |

9. ☐ el prefijo de LUN ya se muestra si lo ha introducido anteriormente, pero puede modificarlo. De lo contrario, introduzca el prefijo.
10. Seleccione una máquina virtual de almacenamiento de la lista desplegable.

Solo se muestran las máquinas virtuales de almacenamiento configuradas para el protocolo SAN. Si sólo hay disponible un equipo virtual de almacenamiento configurado para el protocolo SAN, no se mostrará el campo **Storage VM**.

11. Determine cómo desea agrupar las LUN:

| Cuando usted hace esta elección... | Esto ocurre... |
|------------------------------------|---|
| Grupo con LUN relacionadas | Los LUN se agruparán junto con las LUN relacionadas en un volumen existente del equipo virtual de almacenamiento. |
| Sin selección | Los LUN se agruparán en un volumen llamado "contenedor". |

12. En la sección **almacenamiento y optimización**, especifique los siguientes valores:
 - a. El número y la capacidad de las LUN ya aparecen si las ha introducido anteriormente, pero puede modificarlas. De lo contrario, introduzca los valores.
 - b. En el campo **nivel de servicio de rendimiento**, seleccione un nivel de servicio:

| Al seleccionar este nivel de servicio... | Esto ocurre... |
|--|----------------|
|--|----------------|

| | |
|---|---|
| Un nivel de servicio existente, como «extremo», «rendimiento» o «valor». | Se selecciona automáticamente un nivel local. Vaya a. Paso 13 . |
| Solo se muestran los niveles de servicio válidos para la plataforma del sistema (AFF, FAS, etc.). | |
| Personalizado | Vaya a. paso 12c para definir un nuevo nivel de servicio. |

- c. a partir de ONTAP 9.9.1, puede usar System Manager para seleccionar manualmente el nivel local en el que desea colocar las LUN que crea (si ha seleccionado el nivel de servicio "personalizado").

| | |
|------------------------------------|---|
| Cuando usted hace esta elección... | Realice estos pasos... |
| Colocación manual | La ubicación manual está activada. Vaya a. Step 12d para completar el proceso. |
| Sin selección | La selección manual no está activada. El nivel local se selecciona automáticamente. Vaya a. Paso 13 . |

- d. Seleccione un nivel local en el menú desplegable.
- e. Seleccione una política de calidad de servicio.

Seleccione "existente" para elegir entre una lista de directivas existentes o seleccione "Nuevo" para introducir las especificaciones de una nueva política.

13. en la sección **Información del host**, el sistema operativo host y el formato LUN ya se muestran, pero puede modificarlos.

14. En **asignación de host**, seleccione el tipo de iniciadores para las LUN:

- **Grupo iniciador existente:** Seleccione un iGroup para la lista que se muestra.
- **Nuevo iGroup usando iGroups existentes:** Especifique el nombre del nuevo grupo y seleccione el grupo o grupos que desea usar para crear el nuevo grupo.
- **Iniciadores de host:** Especifique un nombre del nuevo iGroup y haga clic en **+Agregar iniciador** para agregar iniciadores al grupo.

15. En la sección **Protección**, especifique las protecciones para los LUN.

Si selecciona **Activar SnapMirror (local o remoto)**, especifique la directiva de protección y la configuración del clúster de destino en las listas desplegables.

16. Haga clic en **Guardar**.

Las LUN se crean y se añaden al clúster y a la máquina virtual de almacenamiento.




También puede guardar las especificaciones de estas LUN en un libro de aplicaciones de Ansible. Para obtener más información, visite ["Utilice libros de aplicaciones Ansible para añadir o editar volúmenes o LUN"](#).

Cambiar el nombre a una LUN

Puede cambiar el nombre de un LUN en la página de descripción general.

Pasos

1. En el Administrador del sistema, haga clic en **LUN**.
2. Haga clic en  Junto al nombre de la LUN cuyo nombre desea cambiar y, a continuación, modifique el nombre de la LUN.
3. Haga clic en **Guardar**.

Amplíe el almacenamiento

Con System Manager, puede aumentar el tamaño del volumen o LUN para que haya más espacio disponible para el host. El tamaño de una LUN no puede superar el tamaño del volumen que contiene.

A partir de ONTAP 9.12.1, al introducir la nueva capacidad de un volumen, la ventana **Cambiar tamaño de volumen** muestra el impacto que tendrá el cambio de tamaño del volumen en el espacio de datos y la reserva de copia Snapshot.

- [Aumente el tamaño de un volumen](#)
- [Aumentar el tamaño de una LUN](#)


Además, puede agregar un LUN a un volumen existente. Los procesos son diferentes cuando se utiliza System Manager con ONTAP 9.7 o 9.8

- [Agregar un LUN a un volumen existente \(ONTAP 9.7\)](#)
- [8\)](#)

Además, a partir de ONTAP 9.8, es posible usar System Manager para añadir un LUN a un volumen existente.


Aumente el tamaño de un volumen

Pasos

1. Haga clic en **almacenamiento > volúmenes**.
2. Pase el ratón sobre el nombre del volumen que desea aumentar su tamaño.
3. Haga clic en .
4. Seleccione **Editar**.
5. Aumente el valor de capacidad.
6. Consulte los detalles de **espacio de datos existente** y **Nuevo** y la reserva de Snapshot.

Aumentar el tamaño de una LUN

Pasos

1. Haga clic en **almacenamiento > LUN**.
2. Pase el ratón sobre el nombre de la LUN que desea aumentar su tamaño.
3. Haga clic en .

4. Seleccione **Editar**.
5. Aumente el valor de capacidad.

Agregar un LUN a un volumen existente (ONTAP 9.7)

Para usar System Manager con ONTAP 9.7 para añadir una LUN a un volumen existente, primero debe cambiar a la vista clásica.

Pasos

1. Inicie sesión en System Manager en ONTAP 9.7.
2. Haga clic en **Vista clásica**.
3. Seleccione **almacenamiento > LUN > Crear**
4. Especifique los detalles para crear la LUN.
5. Especifique el volumen o qtree existentes al que se debe añadir la LUN.

Añadir un LUN a un volumen existente (ONTAP 9,8)

A partir de ONTAP 9.8, puede usar System Manager para añadir una LUN a un volumen existente que ya tenga al menos una LUN.

Pasos

1. Haga clic en **almacenamiento > LUN**.
2. Haga clic en **Agregar+**.
3. Complete los campos en la ventana **Agregar LUN**.
4. Seleccione **más opciones**.
5. Seleccione la casilla de verificación con la etiqueta **Grupo con LUN** relacionadas.
6. En el campo desplegable, seleccione el LUN existente en el volumen al que desea añadir otro LUN.
7. Complete el resto de los campos. Para **asignación de host**, haga clic en uno de los botones de opción:
 - **IGroup existente** le permite seleccionar un grupo existente de una lista.
 - **Nuevo iGroup** le permite introducir un nuevo grupo en el campo.

Ahorre espacio de almacenamiento mediante la compresión, la compactación y la deduplicación

En el caso de volúmenes en clústeres que no son de AFF, puede ejecutar deduplicación, compresión de datos y compactación de datos en conjunto o de forma independiente para lograr un ahorro de espacio óptimo.

- La deduplicación elimina los bloques de datos duplicados.
- La compresión de datos comprime los bloques de datos para reducir la cantidad de almacenamiento físico necesaria.
- La compactación de datos almacena más datos en menos espacio para aumentar la eficiencia del almacenamiento.



Estas tareas son compatibles para volúmenes en clústeres que no son de AFF. A partir de ONTAP 9.2, todas las funciones de eficiencia del almacenamiento en línea, como la deduplicación inline y la compresión inline, se habilitan de forma predeterminada en los volúmenes AFF.

Pasos

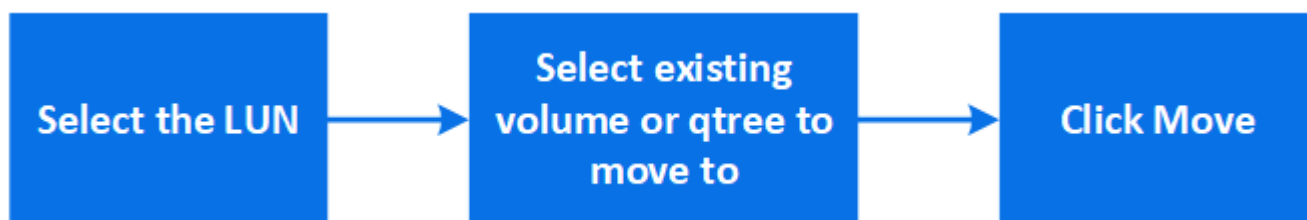
1. Haga clic en **almacenamiento > volúmenes**.
2. Junto al nombre del volumen para el que desea guardar el almacenamiento, haga clic en **:**.
3. Haga clic en **Editar** y desplácese a **eficiencia de almacenamiento**.
4. *Optional:* Si desea activar la deduplicación en segundo plano, asegúrese de que la casilla de verificación esté activada.
5. *Optional:* Si desea habilitar la compresión en segundo plano, especifique la directiva de eficiencia del almacenamiento y asegúrese de que la casilla de verificación esté activada.
6. *Optional:* Si desea activar la compresión en línea, asegúrese de que la casilla de verificación esté activada.

Equilibre las cargas moviendo LUN

Puede mover una LUN a otro volumen de la máquina virtual de almacenamiento para equilibrar la carga, o bien puede moverla a un volumen con un nivel de servicio de mayor rendimiento para mejorar el rendimiento.

Restricciones de movimiento

- No se puede mover una LUN a un qtree dentro del mismo volumen.
- No se puede mover un LUN creado a partir de un archivo con la CLI con System Manager.
- Las LUN que están en línea y sirviendo datos no se pueden mover.
- No se pueden mover los LUN si el espacio asignado en el volumen de destino no puede contener la LUN (aunque el crecimiento automático esté habilitado en el volumen).
- Las LUN de volúmenes de SnapLock no se pueden mover con System Manager.



Pasos

1. Haga clic en **almacenamiento > LUN**.
2. Seleccione la LUN que desea mover y haga clic en **mover**.
3. Seleccione un volumen existente al que desea mover el LUN. Si el volumen contiene qtrees, seleccione el qtree.



Mientras la operación de movimiento está en curso, la LUN se muestra tanto en el volumen de origen como en el de destino.

Equilibre las cargas moviendo volúmenes a otro nivel

A partir de ONTAP 9.8, se puede usar System Manager para mover un volumen a otro nivel para equilibrar la carga.

A partir de ONTAP 9.9.1, también puede mover volúmenes en función del análisis del almacenamiento de datos activo e inactivo. Para obtener más información, consulte ["Descripción general de File System Analytics"](#).

Pasos

1. Haga clic en **almacenamiento > volúmenes**.
2. Seleccione el volumen o los volúmenes que desea mover y, a continuación, haga clic en **mover**.
3. Seleccione el nivel existente (agregado) al que desee mover los volúmenes.

Utilice libros de aplicaciones Ansible para añadir o editar volúmenes o LUN

A partir de ONTAP 9.9.1, puede usar las Libros de estrategia de Ansible con System Manager cuando quiera añadir o editar volúmenes o LUN.

Esta función le permite utilizar la misma configuración varias veces o utilizar la misma configuración con ligeros cambios al añadir o editar volúmenes o LUN.

Habilite o deshabilite los libros de aplicaciones de Ansible

Puede habilitar o deshabilitar el uso de las Libros de estrategia de Ansible con System Manager.

Pasos

1. En System Manager, vaya a la configuración de la interfaz de usuario en la página de configuración del clúster:

Clúster > Configuración

2. En **Configuración de la interfaz de usuario**, cambie el interruptor deslizante a "Activado" o "Desactivado".

Guardar una configuración de volumen en un libro de aplicaciones de Ansible

Al crear o modificar la configuración de un volumen, puede guardar la configuración como archivos del libro de aplicaciones de Ansible.

Pasos

1. Añada o edite el volumen:

Volumen > Añadir (o Volumen > Editar)

2. Especifique o edite los valores de configuración del volumen.
3. Seleccione **Guardar en la tableta Ansible PlayBook** para guardar la configuración en los archivos de la tableta Ansible PlayBook.

Se descarga un archivo zip que contiene los siguientes archivos:

- **variable.yaml**: Los valores introducidos o modificados para añadir o editar el volumen.

- **volumeAdd.yaml** (o. **volumeEdit.yaml**): Los casos de prueba necesarios para crear o modificar los valores al leer las entradas del `variable.yaml` archivo.

Guarde una configuración de LUN en un libro de aplicaciones de Ansible

A la hora de crear o modificar la configuración de un LUN, puede guardar la configuración como archivos del libro de aplicaciones de Ansible.

Pasos

1. Añada o edite la LUN:

LUN > Agregar (o **LUN > Editar**)

2. Especifique o edite los valores de configuración de la LUN.
3. Seleccione **Guardar en la tableta Ansible PlayBook** para guardar la configuración en los archivos de la tableta Ansible PlayBook:


Se descarga un archivo zip que contiene los siguientes archivos:

- **variable.yaml**: Los valores introducidos o modificados para agregar o editar la LUN.
- **lunAdd.yaml** (o. **lunEdit.yaml**): Los casos de prueba necesarios para crear o modificar los valores al leer las entradas del `variable.yaml` archivo.

Descargue los archivos del libro de aplicaciones de Ansible a partir de los resultados de búsquedas globales

Puede descargar archivos del libro de aplicaciones de Ansible cuando realice una búsqueda global.

Pasos

1. En el campo de búsqueda, introduzca "VOLUME", "LUN" o "PlayBook".
2. Encuentre el resultado de la búsqueda, "Volume Management (libro de aplicaciones de Ansible)" o "LUN Management (libro de aplicaciones de Ansible)".
3. Haga clic en  Para descargar los archivos del libro de aplicaciones de Ansible.

Trabaje con archivos del libro de aplicaciones de Ansible

Los archivos del libro de aplicaciones de Ansible se pueden modificar y ejecutar para especificar configuraciones de volúmenes y LUN.

Acerca de esta tarea

Se utilizan dos archivos para realizar una operación (ya sea un "add" o un "edit"):

| Si desea... | Usar este archivo variable... | Y usar este archivo de ejecución... |
|-------------------|-------------------------------|-------------------------------------|
| Añadir un volumen | volumeAdd-variable.yaml | valueAdd.yaml |
| Editar un volumen | volumeEdit-variable.yaml | volumeEdit.yaml |
| Agregar una LUN | lunAdd-variable.yaml | lunAdd.yaml |
| Editar una LUN | lunEdit-variable.yaml | lunEdit.yaml |

Pasos

1. Modifique el archivo de variables.

El archivo contiene los distintos valores que se utilizan para configurar el volumen o LUN.

- Si no cambia los valores, déjelo comentado.
- Si modifica los valores, elimine los comentarios.

2. Ejecute el archivo de ejecución asociado.

El archivo RUN contiene los casos de prueba necesarios para crear o modificar los valores al leer las entradas del archivo variable.

3. Introduzca sus credenciales de inicio de sesión de usuario.

Gestione las políticas de eficiencia del almacenamiento

A partir de ONTAP 9.8, puede usar System Manager para habilitar, deshabilitar, agregar, editar o eliminar políticas de eficiencia para máquinas virtuales de almacenamiento en sistemas FAS.



Esta función no está disponible en los sistemas AFF.

Pasos

1. Seleccione **almacenamiento > Storage VMs**
2. Seleccione la máquina virtual de almacenamiento para la que desee gestionar políticas de eficiencia.
3. En la ficha **Configuración**, seleccione → En la sección **Política de eficiencia**. Se muestran las políticas de eficiencia para esa máquina virtual de almacenamiento.

Es posible realizar las siguientes tareas:

- **Activar o desactivar** una política de eficiencia haciendo clic en el botón de alternar de la columna Estado.
- **Agregue** una política de eficiencia haciendo clic en **Add+**.
- **Edite** una política de eficiencia haciendo clic en A la derecha del nombre de la directiva y seleccione **Editar**.
- **Eliminar** una política de eficiencia haciendo clic en A la derecha del nombre de la política y seleccione **Eliminar**.

Lista de políticas de eficiencia

• Auto

Especifica que la deduplicación se ejecuta continuamente en segundo plano. Esta política se establece para todos los volúmenes nuevos y para todos los volúmenes actualizados que no se configuraron manualmente para la deduplicación en segundo plano. Si cambia la política a «default» o a otra política, la política «auto» queda desactivada.

Si un volumen pasa de un sistema distinto de AFF a un sistema AFF, la política «'auto'» se habilita de forma predeterminada en el nodo de destino. Si un volumen pasa de un nodo AFF a uno distinto de AFF, la política «'auto'» del nodo de destino se reemplaza de forma predeterminada por la política «'solo en línea'».

- **Política**

Especifica el nombre de una política de eficiencia.

- **Estado**

Especifica el estado de una política de eficiencia. El estado puede ser uno de los siguientes:

- **Activado**

Especifica que la política de eficiencia se puede asignar a una operación de deduplicación.

- **Deshabilitado**

Especifica que la directiva de eficiencia está desactivada. Puede habilitar la política mediante el menú desplegable de estado y asignarla después a una operación de deduplicación.

- **Ejecutar por**

Especifica si la política de eficiencia del almacenamiento se ejecuta en función de una programación o de un valor de umbral (umbral de cambio).

- **Política de QoS**

Especifica el tipo de calidad de servicio para la política de eficiencia del almacenamiento. El tipo de calidad de servicio puede ser uno de los siguientes:

- **Información previa**

Especifica que la política de calidad de servicio se ejecuta en segundo plano, lo que reduce el impacto potencial en el rendimiento de las operaciones del cliente.

- **El mejor esfuerzo**

Especifica que la política de calidad de servicio se ejecuta cuando se realiza el mejor esfuerzo, lo que le permite maximizar la utilización de los recursos del sistema.

- **Tiempo de ejecución máximo**

Especifica la duración máxima en tiempo de ejecución de una política de eficiencia. Si no se especifica este valor, la política de eficiencia se ejecuta hasta que la operación se completa.

El área Detalles

El área que se encuentra debajo de la lista de políticas de eficiencia muestra información adicional sobre la política de eficiencia seleccionada, incluidos el nombre de la programación y los detalles de la programación de una política basada en programación, y el valor de umbral de la política basada en umbrales.

Gestionar recursos mediante cuotas

A partir de ONTAP 9.7, puede configurar y gestionar las cuotas de uso con System Manager.

Si utiliza la interfaz de línea de comandos de ONTAP para configurar y gestionar cuotas de uso, consulte

"Gestión de almacenamiento lógico".

Si utiliza System Manager heredado de OnCommand para ONTAP 9.7 y versiones anteriores para configurar y gestionar cuotas de uso, consulte la siguiente sección para su versión:

- ["Documentación de ONTAP 9.6 y 9.7"](#)
- ["Documentación de ONTAP 9,5"](#)
- ["Documentación de ONTAP 9,4"](#)
- ["Documentación de ONTAP 9,3"](#)
- ["Documentación archivada de ONTAP 9.2"](#)
- ["Documentación archivada de ONTAP 9,0"](#)

Información general sobre cuotas

Las cuotas proporcionan una forma de restringir o realizar un seguimiento del espacio en disco y del número de archivos que usan los usuarios, grupos o qtrees. Las cuotas se aplican a un volumen o qtree concreto.

Puede utilizar las cuotas para realizar un seguimiento y limitar el uso de los recursos en volúmenes y proporcionar una notificación cuando el uso de los recursos alcance niveles específicos.

Las cuotas pueden ser suaves o duras. Las cuotas blandas hacen que ONTAP envíe una notificación cuando se superen los límites especificados y las cuotas rígidas evitan que una operación de escritura tenga éxito cuando se superen los límites especificados.

Establezca cuotas para limitar el uso de recursos

Añada cuotas para limitar la cantidad de espacio en disco que puede utilizar el destino de cuota.

Puede establecer un límite duro y un límite suave para una cuota.

Las cuotas estrictas imponen un límite duro a los recursos del sistema; cualquier operación que pueda resultar en superar el límite falla. Las cuotas suaves envían un mensaje de advertencia cuando el uso de recursos alcanza un cierto nivel, pero no afectan a las operaciones de acceso a datos, por lo que puede tomar las medidas adecuadas antes de que se supere la cuota.

Pasos

1. Haga clic en **almacenamiento > cuotas**.
2. Haga clic en **Agregar**.

Clone volúmenes y LUN para realizar pruebas

Puede clonar volúmenes y LUN para crear copias temporales y editables para las pruebas. Los clones reflejan el estado actual de los datos, un momento específico. También puede utilizar clones para proporcionar a los usuarios adicionales acceso a los datos sin tener que darles acceso a los datos de producción.




La licencia de FlexClone debe ser **"instalado"** en el sistema de almacenamiento.

Clonar un volumen

Cree un clon de un volumen de la siguiente manera:

Pasos


1. Haga clic en **almacenamiento > volúmenes**.
2. Haga clic en  junto al nombre del volumen que desea clonar.
3. Seleccione **Clonar** de la lista.
4. Especifique un nombre para el clon y complete las otras selecciones.
5. Haga clic en **Clonar** y compruebe que el clon de volumen aparece en la lista de volúmenes.

Como alternativa, puede clonar un volumen desde **Descripción general** que aparece cuando se visualizan los detalles del volumen.

Clonar una LUN

Cree un clon de una LUN de la siguiente manera:

Pasos

1. Haga clic en **almacenamiento > LUN**.
2. Haga clic en  Junto al nombre de la LUN que desea clonar.
3. Seleccione **Clonar** de la lista.
4. Especifique un nombre para el clon y complete las otras selecciones.
5. Haga clic en **Clonar** y compruebe que el clon LUN aparece en la lista de LUN.

Como alternativa, puede clonar una LUN desde **Descripción general** que aparece cuando ve los detalles de la LUN.

Cuando crea un clon de LUN, System Manager habilita automáticamente la eliminación del clon cuando se necesita espacio.

Busque, filtre y ordene información en System Manager

Puede buscar varias acciones, objetos y temas de información en System Manager. También puede buscar entradas específicas en los datos de la tabla.

System Manager proporciona dos tipos de búsqueda:

- [Búsqueda global](#)

Cuando introduce un argumento de búsqueda en el campo en la parte superior de cada página, System Manager busca coincidencias en toda la interfaz para buscar coincidencias. A continuación, puede ordenar y filtrar los resultados.

A partir de ONTAP 9.12.1, System Manager también proporciona resultados de búsqueda en el sitio de soporte de NetApp para proporcionar enlaces a información de soporte relevante.

- [Búsqueda en grid de tabla](#)

A partir de ONTAP 9.8, cuando se introduce un argumento de búsqueda en el campo de la parte superior

de una cuadrícula de tabla, System Manager sólo busca las columnas y filas de esa tabla para buscar coincidencias.

Búsqueda global

En la parte superior de cada página de System Manager, puede utilizar un campo de búsqueda global para buscar varios objetos y acciones en la interfaz. Por ejemplo, puede buscar diferentes objetos por nombre, páginas disponibles en la columna del navegador (en el lado izquierdo), varios elementos de acción, como "Añadir volumen" o "Agregar licencia", y vínculos a temas de ayuda externos. También puede filtrar y ordenar los resultados.



Para obtener mejores resultados, realice búsquedas, filtrado y ordenación un minuto después de iniciar sesión y cinco minutos después de crear, modificar o eliminar un objeto.

Obtención de resultados de búsqueda

La búsqueda no distingue mayúsculas de minúsculas. Puede introducir diversas cadenas de texto para buscar la página, las acciones o los temas de información que necesite. Se muestran hasta 20 resultados. Si se encuentran más resultados, puede hacer clic en **Mostrar más** para ver todos los resultados. Los siguientes ejemplos describen las búsquedas típicas:

| Tipo de búsqueda | Cadena de búsqueda de ejemplo | Ejemplos de resultados de búsqueda |
|------------------------------|-------------------------------|--|
| Por nombre de objeto | vol_ | vol_lun_dest en máquina virtual de almacenamiento: svm0 (volumen) /Vol/vol...est1/lun en máquinas virtuales de almacenamiento: svm0 (LUN) svm0:vol_lun_DEST1 rol: Destino (Relación) |
| Por ubicación en la interfaz | volumen | Añadir volumen (acción) Protección – Descripción general (Página) Recuperar volumen eliminado (Ayuda) |
| Por acciones | agregar | Añadir volumen (acción) Red: Descripción general (página) Expandir volúmenes y LUN (Ayuda) |
| Por contenido de ayuda | san | Descripción general del almacenamiento (Página) Descripción general de SAN (ayuda) Provisionamiento de almacenamiento SAN para bases de datos (Ayuda) |



Resultados de búsqueda global del sitio de soporte de NetApp

A partir de ONTAP 9.12.1, para los usuarios registrados en Active IQ, System Manager muestra otra columna de resultados que proporciona enlaces a información del sitio de soporte de NetApp, incluida la información de productos de System Manager.

Los resultados de búsqueda contienen la siguiente información:

- **Título** de la información que es un enlace al documento en formato HTML, PDF, EPUB u otro formato.
- **Tipo de contenido**, que identifica si es un tema de documentación de producto, un artículo de base de conocimientos u otro tipo de información.
- **Descripción del resumen** del contenido.
- **Fecha de creación** cuando fue publicada por primera vez.
- **Fecha actualizada** cuando se actualizó por última vez.

Es posible realizar las siguientes acciones:

| Acción | Resultado |
|---|--|
| Haga clic en Administrador del sistema ONTAP y, a continuación, escriba texto en el campo de búsqueda. | Los resultados de búsqueda incluyen información del sitio de soporte de NetApp sobre System Manager. |
| Haga clic en todos los productos y escriba texto en el campo de búsqueda. | Los resultados de búsqueda incluyen información del sitio de soporte de NetApp para todos los productos de NetApp, no solo para System Manager. |
| Haga clic en un resultado de búsqueda. | La información del sitio de soporte de NetApp se muestra en una ventana o una pestaña separadas del navegador. |
| Haga clic en Ver más resultados . | Si hay más de diez resultados, puede hacer clic en Ver más resultados después del décimo resultado para ver más resultados. Cada vez que haga clic en Ver más resultados , se mostrarán otros diez resultados, si están disponibles. |
| Copie el vínculo. | El vínculo se copia en el portapapeles. Puede pegar el vínculo en un archivo o en una ventana del explorador. |
| Haga clic en  . | El panel en el que se muestran los resultados está anclado de manera que permanece visible cuando se trabaja en otro panel. |
| Haga clic en  . | El panel de resultados ya no está fijado y se cierra. |


Filtrado de resultados de búsqueda

Puede restringir los resultados con filtros, como se muestra en los ejemplos siguientes:

| Filtro | Sintaxis | Cadena de búsqueda de ejemplo |
|----------------------|---------------------------------------|-------------------------------|
| Por tipo de objeto | <type>:<objectName> | volume: vol_2 |
| Por tamaño de objeto | <type> <size-symbol> <number> <units> | lun<500 mb |
| Por discos rotos | «disco roto» o «disco incorrecto» | disco mal saludable |

| | | |
|-----------------------------|--------------|---------------|
| Mediante la interfaz de red | <IP address> | 172.22.108.21 |
|-----------------------------|--------------|---------------|

Ordenar resultados de búsqueda

Cuando se visualizan todos los resultados de la búsqueda, se ordenan alfabéticamente. Para ordenar los resultados, haga clic en  **Filter** y seleccionando cómo desea ordenar los resultados.

Búsqueda en grid de tabla

A partir de ONTAP 9.8, cada vez que System Manager muestra información en formato de cuadrícula de tabla, aparece un botón de búsqueda en la parte superior de la tabla.

Al hacer clic en **Buscar**, aparece un campo de texto en el que puede introducir un argumento de búsqueda. System Manager busca en toda la tabla y muestra sólo las filas que contienen texto que coincide con el argumento de búsqueda.

Puede utilizar un asterisco (*) como carácter "comodín" como sustituto de caracteres. Por ejemplo, busque `vol1*` puede proporcionar filas que contengan lo siguiente:

- vol_122_D9
- vol_lun_dest1
- vol2866
- volspec1
- volum_dest_765
- volumen
- volumen_new4
- volume9987

Mediciones de capacidad en System Manager

La capacidad del sistema se puede medir como espacio físico o como espacio lógico. A partir de ONTAP 9,7, System Manager proporciona mediciones de la capacidad física y lógica.

Las diferencias entre las dos mediciones se explican en las siguientes descripciones:

- **Capacidad física:** El espacio físico se refiere a los bloques físicos de almacenamiento utilizados en el volumen o nivel local. El valor de la capacidad física utilizada suele ser menor que el valor de la capacidad lógica utilizada debido a la reducción de datos de funciones de eficiencia del almacenamiento (como la deduplicación y la compresión).
- **Capacidad lógica:** El espacio lógico se refiere al espacio utilizable (los bloques lógicos) en un volumen o nivel local. El espacio lógico hace referencia a cómo se puede utilizar el espacio teórico, sin tener en cuenta los resultados de la deduplicación o la compresión. El valor del espacio lógico utilizado procede de la cantidad de espacio físico utilizado más el ahorro derivado de las funciones de eficiencia del almacenamiento (como la deduplicación y compresión) que se han configurado. Esta medición suele ser mayor que la capacidad física utilizada porque incluye copias Snapshot, clones y otros componentes, y no refleja la compresión de datos ni otras reducciones del espacio físico. Por lo tanto, la capacidad lógica total podría ser mayor que el espacio provisionado.



En System Manager, las representaciones de capacidad no dan cuenta de las capacidades de niveles de almacenamiento raíz (agregado).

Mediciones de capacidad utilizada

Las mediciones de la capacidad utilizada se muestran de forma diferente según la versión de System Manager que se esté usando, como se explica en la siguiente tabla:

| La versión de System Manager | Término utilizado para capacidad | El tipo de capacidad a la que se hace referencia |
|------------------------------|----------------------------------|---|
| 9.9.1 y posterior | Lógica utilizada | El espacio lógico utilizado si se habilitó la configuración de eficiencia del almacenamiento) |
| 9.7 y 9.8 | Utilizado | El espacio lógico utilizado (si se ha habilitado la configuración de eficiencia del almacenamiento) |
| 9,5 y 9,6 (Vista clásica) | Utilizado | El espacio físico utilizado |

Términos de medición de capacidad

Los siguientes términos se utilizan cuando se describe la capacidad:

- **Capacidad asignada:** La cantidad de espacio que se ha asignado para volúmenes en una VM de almacenamiento.
- **Disponible:** La cantidad de espacio físico disponible para almacenar datos o para aprovisionar volúmenes en una VM de almacenamiento o en un nivel local.
- **Capacidad en volúmenes:** La suma del almacenamiento usado y el almacenamiento disponible de todos los volúmenes en una VM de almacenamiento.
- **Datos del cliente:** La cantidad de espacio utilizado por los datos del cliente (ya sea físico o lógico).
 - A partir de ONTAP 9.13.1, la capacidad utilizada por los datos del cliente se conoce como **Lógica utilizada**, y la capacidad utilizada por las copias snapshot se muestra por separado.
 - En ONTAP 9.12.1 y versiones anteriores, la capacidad utilizada por los datos del cliente añadidos a la capacidad utilizada por las copias snapshot se denomina **Lógica usada**.
- **Comprometido:** La cantidad de capacidad comprometida para un nivel local.
- **Reducción de datos:**
 - A partir de ONTAP 9.13.1, las relaciones de reducción de datos se muestran de la siguiente manera:
 - El valor de reducción de datos que se muestra en el panel **Capacity** es la relación entre el espacio utilizado lógico y el espacio físico utilizado sin tener en cuenta las reducciones significativas que se obtienen al utilizar funciones de eficiencia del almacenamiento, como las copias Snapshot.
 - Al mostrar el panel de detalles, verá tanto la relación que se muestra en el panel de vista general como la relación general de todos los espacios utilizados lógicos en comparación con el espacio utilizado físico. Este valor, conocido como **con las copias Snapshot**, incluye los beneficios derivados del uso de las copias Snapshot y otras funciones de eficiencia del almacenamiento.

- En ONTAP 9.12.1 y versiones anteriores, las proporciones de reducción de datos se muestran de la siguiente forma:

- El valor de reducción de datos que se muestra en el panel **Capacidad** es la relación general de todo el espacio utilizado lógico en comparación con el espacio físico utilizado, e incluye los beneficios derivados del uso de copias Snapshot y otras funciones de eficiencia del almacenamiento.
- Cuando se muestra el panel de detalles, se ve tanto la relación **general** que se muestra en el panel de visión general como la relación del espacio usado lógico utilizado solo por los datos del cliente en comparación con el espacio usado físico utilizado solo por los datos del cliente, denominado **sin copias Snapshot y clones**.

- **Lógica usada:**

- A partir de ONTAP 9.13.1, la capacidad utilizada por los datos del cliente se conoce como **Lógica utilizada**, y la capacidad utilizada por las copias snapshot se muestra por separado.
- En ONTAP 9.12.1 y versiones anteriores, la capacidad utilizada por los datos del cliente añadidos a la capacidad utilizada por las copias snapshot se conoce como **Lógica usada**.

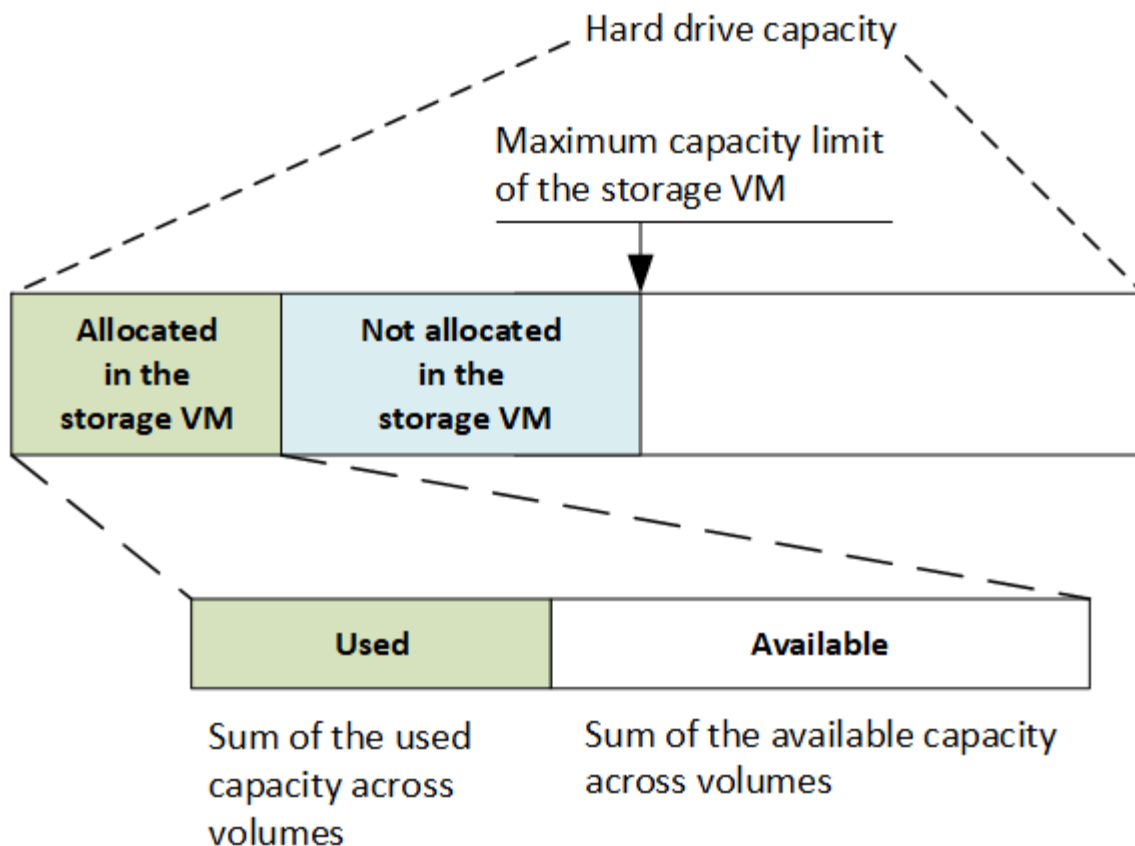
- *** % Lógico utilizado***: El porcentaje de la capacidad lógica utilizada actual en comparación con el tamaño aprovisionado, excluyendo las reservas Snapshot. Este valor puede ser mayor que el 100%, ya que incluye ahorros de eficiencia en el volumen.
- **Capacidad máxima**: La cantidad máxima de espacio asignado para volúmenes en una VM de almacenamiento.
- **Físico utilizado**: La cantidad de capacidad utilizada en los bloques físicos de un volumen o nivel local.
- **Uso físico %**: El porcentaje de capacidad utilizada en los bloques físicos de un volumen en comparación con el tamaño aprovisionado.
- **Capacidad suministrada**: Un sistema de archivos (volumen) que ha sido asignado desde un sistema Cloud Volumes ONTAP y está listo para almacenar datos de usuario o aplicación.
- **Reservado**: Cantidad de espacio reservado para volúmenes ya aprovisionados en un nivel local.
- **Usado**: La cantidad de espacio que contiene datos.
- **Usado y reservado**: La suma del espacio físico utilizado y reservado.

La capacidad de una máquina virtual de almacenamiento

La capacidad máxima de una máquina virtual de almacenamiento se determina por el espacio total asignado para los volúmenes más el espacio sin asignar restante.

- El espacio asignado para los volúmenes es la suma de la capacidad utilizada y la suma de la capacidad disponible de los volúmenes de FlexVol, FlexGroup Volumes y FlexCache Volumes.
- La capacidad de los volúmenes se incluye en las sumas, incluso cuando están restringidos, sin conexión o en la cola de recuperación después de su eliminación.
- Si los volúmenes se configuran con el crecimiento automático, el valor máximo de tamaño automático del volumen se usa en las sumas. Sin crecimiento automático, la capacidad real del volumen se usa en las sumas.

En el siguiente gráfico se explica cómo la medición de la capacidad entre volúmenes se relaciona con el límite de capacidad máxima.



A partir de ONTAP 9.13.1, los administradores de clúster pueden ["Habilite un límite de capacidad máxima para una máquina virtual de almacenamiento"](#). Sin embargo, no es posible establecer límites de almacenamiento para una máquina virtual de almacenamiento que contiene volúmenes para la protección de datos, en una relación de SnapMirror o en una configuración de MetroCluster. Además, no es posible configurar cuotas para superar la capacidad máxima de un equipo virtual de almacenamiento.

Una vez establecido el límite de capacidad máxima, no se puede cambiar a un tamaño inferior a la capacidad asignada actualmente.

Cuando una máquina virtual de almacenamiento alcanza su límite máximo de capacidad, no se pueden ejecutar ciertas operaciones. System Manager proporciona sugerencias para los siguientes pasos de ["Insights"](#).

Unidades de medida de capacidad

System Manager calcula la capacidad de almacenamiento en función de unidades binarias de 1024 (2^{10}) bytes.

- A partir de ONTAP 9.10.1, las unidades de capacidad de almacenamiento se muestran en System Manager como KiB, MiB, GiB, TiB y PiB.
- En ONTAP 9.10.0 y versiones anteriores, estas unidades se muestran en System Manager como KB, MB, GB, TB y PB.



Las unidades utilizadas en System Manager para el rendimiento siguen siendo KB/s, MB/s, GB/s, TB/s y PB/s en todas las versiones de ONTAP.

| Unidad de capacidad mostrada en System Manager para ONTAP 9.10.0 y versiones anteriores | Unidad de capacidad mostrada en System Manager para ONTAP 9.10.1 y versiones posteriores | Cálculo | Valor en bytes |
|---|--|----------------------------------|-----------------------------|
| KB | KiB | 1024 | 1024 bytes |
| MB | MiB | 1024 * 1024 | 1.048.576 bytes |
| GB | GiB | 1024 * 1024 * 1024 | 1.073.741.824 bytes |
| TB | TiB | 1024 * 1024 * 1024 * 1024 | 1.099.511.627.776 bytes |
| PB | PiB | 1024 * 1024 * 1024 * 1024 * 1024 | 1.125.899.906.842.624 bytes |

Información relacionada

["Supervise la capacidad en System Manager"](#)

["Generación de informes sobre el espacio lógico y cumplimiento para volúmenes"](#)

Gestión de almacenamiento lógico con CLI

Información general sobre la gestión de almacenamiento lógico con la CLI

Mediante la interfaz de línea de comandos de ONTAP, puede crear y gestionar volúmenes de FlexVol, utilizar la tecnología FlexClone para crear copias eficientes de volúmenes, archivos y LUN, crear qtrees y cuotas y gestionar funciones de eficiencia como la deduplicación y la compresión.

Debe utilizar estos procedimientos en las siguientes circunstancias:

- Quiere comprender el rango de funcionalidades de volumen de ONTAP FlexVol y las funciones de eficiencia del almacenamiento.
- Desea usar la interfaz de línea de comandos (CLI), no System Manager ni una herramienta de secuencias de comandos automatizadas.

Cree y gestione volúmenes

Cree un volumen

Puede crear un volumen y especificar su punto de unión y otras propiedades mediante la `volume create` comando.

Acerca de esta tarea

Un volumen debe incluir una *ruta de unión* para que sus datos estén disponibles para los clientes. Puede

especificar la ruta de unión cuando cree un nuevo volumen. Si crea un volumen sin especificar una ruta de unión, debe *Mount* el volumen en el espacio de nombres de la SVM mediante el `volume mount` comando.

Antes de empezar

- La SVM del nuevo volumen y el agregado que suministrará almacenamiento al volumen ya deben existir.
- Si la SVM tiene una lista de agregados asociados, el agregado debe incluirse en la lista.
- A partir de ONTAP 9.13.1, se pueden crear volúmenes con análisis de capacidad y seguimiento de actividades habilitados. Para activar la capacidad o el seguimiento de actividades, emita el `volume create` comando con `-analytics-state 0`. `-activity-tracking-state` establezca en `on`.

Para obtener más información sobre el análisis de capacidad y el seguimiento de actividades, consulte [Active File System Analytics](#).

Pasos

1. Cree un volumen:

```
volume create -vserver svm_name -volume volume_name -aggregate aggregate_name  
-size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed} -user  
user_name_or_number -group group_name_or_number -junction-path junction_path  
[-policy export_policy_name]
```

La `-security style`, `-user`, `-group`, `-junction-path`, y `-policy` Las opciones son sólo para espacios de nombres NAS.

Las opciones para `-junction-path` son las siguientes:

- Directamente bajo la raíz, por ejemplo, `/new_vol`

Puede crear un nuevo volumen y especificar que se monte directamente en el volumen raíz de SVM.

- En un directorio existente, por ejemplo, `/existing_dir/new_vol`

Puede crear un nuevo volumen y especificar que se monte en un volumen existente (en una jerarquía existente), expresado como un directorio.

Si desea crear un volumen en un nuevo directorio (en una nueva jerarquía debajo de un nuevo volumen), por ejemplo, `/new_dir/new_vol`, Entonces debe crear primero un nuevo volumen principal que se junte al volumen raíz de la SVM. A continuación, creará el nuevo volumen secundario en la ruta de unión del nuevo volumen principal (nuevo directorio).

2. Compruebe que el volumen se ha creado con el punto de unión deseado:

```
volume show -vserver svm_name -volume volume_name -junction
```

Ejemplos

El siguiente comando crea un nuevo volumen llamado `users1` en la SVM `vs1.example.com` y el agregado `aggr1`. El nuevo volumen está disponible en `/users`. El tamaño del volumen es de 750 GB y su garantía de volumen es del tipo volumen (de forma predeterminada).

```
cluster1::> volume create -vserver vs1.example.com -volume users1
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1.example.com -volume users1 -junction
```

| Vserver | Volume | Active | Junction Path | Junction Path Source |
|-----------------|--------|--------|---------------|----------------------|
| vs1.example.com | users1 | true | /users | RW_volume |

El siguiente comando crea un nuevo volumen denominado «'home4'» en la SVM «'vs1.example.com'» y el agregado «'aggr1'». El directorio /eng/ Ya existe en el espacio de nombres para el SVM vs1 y el nuevo volumen estará disponible en /eng/home, que se convierte en el directorio principal de /eng/ espacio de nombres. El volumen tiene un tamaño de 750 GB y su garantía de volumen es de tipo volume (de forma predeterminada).

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
```

| Vserver | Volume | Active | Junction Path | Junction Path Source |
|-----------------|--------|--------|---------------|----------------------|
| vs1.example.com | home4 | true | /eng/home | RW_volume |

Habilite el soporte de grandes volúmenes y archivos de gran tamaño

A partir de ONTAP 9.12.1 P2, puede crear un nuevo volumen o modificar un volumen existente para permitir la compatibilidad con un tamaño de volumen máximo de 300TB TB y un tamaño máximo de archivo (LUN) de 128TB TB.

Antes de empezar

- ONTAP 9.12.1 P2 o posterior se instala en el clúster.
- Si habilita la compatibilidad con volúmenes grandes en el clúster de origen en una relación de SnapMirror, debe tener ONTAP 9.12.1 P2 o una versión posterior instalada en el clúster que aloja el volumen de origen y el clúster que aloja el volumen de destino.
- Es un administrador de clústeres o de SVM.

Cree un nuevo volumen

Paso

1. Cree un volumen con compatibilidad de grandes volúmenes y archivos habilitada:

```
volume create -vserver _svm_name_ -volume _volume_name_ -aggregate  
_aggregate_name_ -is-large-size-enabled true
```

Ejemplo

En el siguiente ejemplo, se crea un nuevo volumen con compatibilidad con volúmenes grandes y tamaño de archivo habilitada.

```
volume create -vserver vs1 -volume big_vol1 -aggregate aggr1 -is-large  
-size-enabled true
```

Modifique un volumen existente

Paso

1. Modifique un volumen para habilitar el soporte de archivos y volúmenes grandes:

```
volume modify -vserver _svm_name_ -volume _volume_name_ -is-large-size  
-enabled true
```

Ejemplo

En el siguiente ejemplo se modifica un volumen existente para admitir volúmenes y tamaños de archivo grandes.

```
volume modify -vserver vs2 -volume data_vol -is-large-size-enabled true
```

Información relacionada

- ["Cree un volumen"](#)
- ["Referencia de comandos"](#)

Volúmenes SAN

Acerca de VOLÚMENES SAN

ONTAP proporciona tres opciones básicas de aprovisionamiento de volúmenes: Aprovisionamiento ligero, aprovisionamiento ligero y aprovisionamiento ligero. Cada opción utiliza diferentes formas de gestionar el espacio de volumen y los requisitos de espacio para las tecnologías de uso compartido de bloques de ONTAP. Comprender cómo funcionan las opciones le permite elegir la mejor opción para su entorno.



No se recomienda colocar LUN DE SAN y recursos compartidos de NAS en el mismo volumen de FlexVol. Debería aprovisionar volúmenes FlexVol independientes específicamente para sus LUN DE SAN y debería aprovisionar volúmenes FlexVol independientes específicamente para sus recursos compartidos NAS. Esto simplifica la gestión y la replicación y es similar a la forma en la que los volúmenes de FlexVol son compatibles con Active IQ Unified Manager (anteriormente, Unified Manager de OnCommand).

Aprovisionamiento ligero para volúmenes

Cuando se crea un volumen con Thin Provisioning, ONTAP no reserva ningún espacio adicional cuando se crea el volumen. A medida que se escriben datos en el volumen, el volumen solicita el almacenamiento que necesita del agregado para acomodar la operación de escritura. El uso de volúmenes con aprovisionamiento ligero le permite comprometer en exceso su agregado, lo que introduce la posibilidad de que el volumen no pueda asegurar el espacio que necesita cuando el agregado se queda sin espacio libre.

Para crear un volumen de FlexVol con aprovisionamiento fino, debe configurar su `-space-guarantee` opción a `none`.

Aprovisionamiento grueso para volúmenes

Cuando se crea un volumen con aprovisionamiento grueso, ONTAP reserva suficiente almacenamiento del agregado para garantizar que cualquier bloque del volumen se pueda escribir en cualquier momento. Cuando configura un volumen para utilizar este tipo de aprovisionamiento, puede emplear cualquiera de las funcionalidades de eficiencia del almacenamiento de ONTAP, como la compresión y la deduplicación, para compensar los mayores requisitos de almacenamiento inicial.

Para crear un volumen FlexVol con aprovisionamiento grueso, configure su `-space-slo` (objetivo de nivel de servicio) opción a `thick`.

Aprovisionamiento para volúmenes semigruesos

Cuando se crea un volumen que utiliza aprovisionamiento grueso, ONTAP establece un espacio de almacenamiento aparte del agregado para tener en cuenta el tamaño del volumen. Si el volumen se está quedando sin espacio libre porque las tecnologías de uso compartido de bloques lo están utilizando, ONTAP realiza un esfuerzo para eliminar objetos de datos de protección (copias Snapshot y archivos FlexClone y LUN) para liberar el espacio en el que se encuentran. Siempre que ONTAP pueda eliminar los objetos de datos de protección con la rapidez suficiente como para responder al ritmo del espacio requerido para las sobrescrituras, las operaciones de escritura siguen teniendo éxito. Esto se denomina «mejor esfuerzo».



No puede emplear tecnologías de eficiencia del almacenamiento como deduplicación, compresión y compactación en un volumen que utiliza aprovisionamiento de grosor medio.

Para crear un volumen de FlexVol con aprovisionamiento semigrueso, establezca su configuración `-space-slo` (objetivo de nivel de servicio) opción a `semi-thick`.

Utilice con archivos y LUN reservados en el espacio

Un archivo o LUN con reserva de espacio es uno para el cual se asigna el almacenamiento cuando se crea. Históricamente, NetApp ha utilizado el término «LUN aprovisionada mediante thin provisioning» para indicar una LUN para la que se ha deshabilitado la reserva de espacio (LUN sin reservar espacio).



Los archivos sin espacio reservado no se denominan normalmente «ficheros con thin provisioning».

En la tabla siguiente se resumen las principales diferencias en cómo pueden utilizarse las tres opciones de aprovisionamiento de volúmenes con archivos y LUN con espacio reservado:

| Aprovisionamiento de volúmenes | Reserva de espacio de archivos/LUN | Sobrescrituras | Datos de protección 2 | Eficiencia del almacenamiento 3 |
|--------------------------------|------------------------------------|------------------|-----------------------|---------------------------------|
| Grueso | Compatible | Garantizado 1 | Garantizado | Compatible |
| Fino | Sin efecto | Ninguno | Garantizado | Compatible |
| Semi-grueso | Compatible | Mejor esfuerzo 1 | El mejor esfuerzo | No admitido |

Notas

1. La capacidad para garantizar sobrescrituras o proporcionar una garantía de sobrescritura de mejor esfuerzo requiere que la reserva de espacio esté habilitada en la LUN o el archivo.
2. Los datos de protección incluyen copias Snapshot, y los archivos FlexClone y LUN marcados para su eliminación automática (clones de backup).
3. La eficiencia del almacenamiento incluye deduplicación, compresión, cualquier archivo FlexClone y LUN no marcados para su eliminación automática (clones activos), y subarchivos FlexClone (utilizados para la descarga de copia).

Compatibilidad con LUN aprovisionados mediante thin provisioning de SCSI

ONTAP admite LUN T10 SCSI con thin provisioning, así como LUN con thin provisioning de NetApp. El thin provisioning SCSI T10 permite que las aplicaciones host admitan funciones SCSI como la reclamación de espacio de LUN y las funcionalidades de supervisión de espacio de LUN para entornos de bloques. El thin provisioning SCSI T10 debe ser compatible con su software host SCSI.

Se utiliza `ONTAP space-allocation Configuración` para habilitar o deshabilitar la compatibilidad con thin provisioning T10 en una LUN. Se utiliza `ONTAP space-allocation enable Configuración` para habilitar thin provisioning SCSI T10 en una LUN.

La `[-space-allocation {enabled|disabled}]` En el manual de referencia de comandos de la ONTAP encontrará más información para habilitar o deshabilitar la compatibilidad con el thin provisioning T10 y para habilitar el aprovisionamiento ligero SCSI T10 en una LUN.

"Comandos de ONTAP 9"

Configure las opciones de aprovisionamiento del volumen

Puede configurar un volumen para thin provisioning, thick provisioning o semi-thick provisioning.

Acerca de esta tarea

Ajuste de `-space-slo` opción a. `thick` garantiza lo siguiente:

- El volumen completo se preasigna en el agregado. No puede utilizar el `volume create` o `volume modify` para configurar el volumen `-space-guarantee` opción.
- se reserva el 100% del espacio requerido para sobrescrituras. No puede utilizar el `volume modify` para configurar el volumen `-fractional-reserve` opción

Ajuste de `-space-slo` opción a `semi-thick` garantiza lo siguiente:

- El volumen completo se preasigna en el agregado. No puede utilizar el `volume create` o `volume modify` para configurar el volumen `-space-guarantee` opción.
- No hay espacio reservado para sobrescrituras. Puede utilizar el `volume modify` para configurar el volumen `-fractional-reserve` opción.
- La eliminación automática de copias Snapshot está habilitada.

Paso

1. Configure las opciones de aprovisionamiento del volumen:

```
volume create -vserver vs1 -volume vol1 -aggregate
aggregate_name -space-slo none|thick|semi-thick -space-guarantee none|volume
```

La `-space-guarantee` de forma predeterminada, la opción es `none` Para sistemas AFF y volúmenes DP distintos de AFF. De lo contrario, se establece de forma predeterminada en `volume`. Para los volúmenes de FlexVol existentes, utilice `volume modify` para configurar las opciones de aprovisionamiento.

El siguiente comando configura vol1 en SVM vs1 para thin provisioning:

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-guarantee
none
```

El siguiente comando configura vol1 en SVM vs1 para el aprovisionamiento grueso:

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-slo thick
```

El siguiente comando configura vol1 en SVM vs1 para un aprovisionamiento semigrueso:

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-slo semi-
thick
```

Determine el uso del espacio en un volumen o un agregado

Habilitar una función en ONTAP podría consumir más espacio del esperado. ONTAP le ayuda a determinar cómo se consume el espacio proporcionando tres perspectivas desde las cuales ver espacio: El volumen, la huella de un volumen dentro del agregado y el agregado.

Un volumen puede quedarse sin espacio debido al consumo de espacio o al espacio insuficiente en el

volumen, agregado o una combinación de ambos. Al ver un desglose orientado a las características del uso de espacio desde diferentes perspectivas, puede evaluar qué características puede que desee ajustar o desactivar, o si debe realizar otra acción (como aumentar el tamaño del agregado o volumen).

Puede ver los detalles del uso del espacio desde cualquiera de estas perspectivas:

- El uso de espacio del volumen

Desde esta perspectiva, se ofrecen detalles sobre el uso de espacio en el volumen, incluido el uso por parte de las copias Snapshot.

Utilice la `volume show-space` comando para ver el uso de espacio de un volumen.

A partir de ONTAP 9.14.1, en volúmenes con [Eficiencia del almacenamiento sensible a la temperatura \(TSSE\)](#) habilitada, la cantidad de espacio utilizado en el volumen informado por el `volume show-space -physical used` Comando incluye el ahorro de espacio obtenido como resultado de la TSSE.

- La huella del volumen dentro del agregado

En esta perspectiva, se proporciona información detallada acerca de la cantidad de espacio que cada volumen utiliza en el agregado que contiene, incluidos los metadatos del volumen.

Utilice la `volume show-footprint` comando para ver la huella de un volumen con el agregado.

- Uso de espacio del agregado

Esta perspectiva incluye los totales del espacio físico utilizado por el volumen de todos los volúmenes contenidos en el agregado, el espacio reservado para las copias Snapshot agregadas y otros metadatos agregados.

WAFL reserva el 10% del espacio total en disco para el rendimiento y los metadatos a nivel de agregado. El espacio utilizado para mantener los volúmenes del agregado sale de la reserva de WAFL y no se puede cambiar.

A partir de ONTAP 9.12.1, la reserva de WAFL para agregados superiores a 30TB TB se ha reducido del 10 % al 5 % para las plataformas AFF y para las plataformas FAS500f. A partir de ONTAP 9.14.1, esta misma reducción se aplica a los agregados en todas las plataformas de FAS, lo que da como resultado un 5 % más de espacio utilizable en los agregados.

Utilice la `storage aggregate show-space` comando para ver el uso del espacio del agregado.

Ciertas funciones, como los respaldos en cinta y la deduplicación, usan espacio para los metadatos tanto del volumen como directamente desde el agregado. Estas funciones muestran un uso de espacio diferente entre las perspectivas de espacio del volumen y la huella del volumen.

Información relacionada

- ["Artículo de la base de conocimientos: Uso del espacio"](#)
- ["Libere hasta un 5 % de su capacidad de almacenamiento actualizando a ONTAP 9.12.1"](#)

Elimine copias Snapshot automáticamente

Puede definir y habilitar una política para eliminar automáticamente copias Snapshot y LUN FlexClone. La eliminación automática de copias Snapshot y LUN de FlexClone

puede ayudarle a gestionar la utilización del espacio.

Acerca de esta tarea

Puede eliminar automáticamente copias Snapshot de volúmenes de lectura y escritura y LUN FlexClone de volúmenes principales de lectura y escritura. No puede configurar la eliminación automática de las copias Snapshot de volúmenes de solo lectura, por ejemplo, volúmenes de destino de SnapMirror.

Paso

1. Defina y habilite una política para eliminar automáticamente copias de Snapshot mediante el `volume snapshot autodelete modify` comando.

Consulte `volume snapshot autodelete modify` manual para obtener información acerca de los parámetros que se pueden utilizar con este comando para definir una directiva que se ajuste a sus necesidades.

El siguiente comando permite eliminar automáticamente las copias Snapshot y establece el activador en `snap_reserve` Para el volumen `vol3`, que forma parte de la máquina virtual de almacenamiento (SVM) de `vs0.example.com`:

```
cluster1::> volume snapshot autodelete modify -vserver vs0.example.com
-volume vol3 -enabled true -trigger snap_reserve
```

El siguiente comando permite la eliminación automática de las copias Snapshot y de las LUN FlexClone marcadas para la eliminación automática del volumen `vol3`, que forma parte de la máquina virtual de almacenamiento (SVM) `vs0.example.com`:

```
cluster1::> volume snapshot autodelete modify -vserver vs0.example.com
-volume vol3 -enabled true -trigger volume -commitment try -delete-order
oldest_first -destroy-list lun_clone,file_clone
```



Las copias Snapshot a nivel de agregado funcionan de forma diferente que las copias Snapshot a nivel de volumen y ONTAP las gestiona automáticamente. La opción para eliminar las copias Snapshot del agregado está siempre habilitada y ayuda a gestionar el uso de espacio.

Si el parámetro `trigger` está establecido en `snap_reserve` En el caso de un agregado, las copias de Snapshot se mantienen hasta que el espacio reservado supera el umbral de capacidad. Por lo tanto, aunque el parámetro `trigger` no esté establecido en `snap_reserve`, El espacio utilizado por la copia Snapshot en el comando se mostrará como 0 Dado que estas copias Snapshot se eliminan automáticamente. Además, el espacio utilizado por las copias Snapshot en un agregado se considera libre y se incluye en el parámetro de espacio disponible del comando.

Configure los volúmenes para que proporcionen automáticamente más espacio cuando se llenen

Cuando se llena los volúmenes de FlexVol, ONTAP puede usar varios métodos para intentar obtener automáticamente más espacio libre para el volumen. Puede elegir los métodos que puede utilizar ONTAP y el orden en que, en función de los requisitos que

imponga su aplicación y arquitectura de almacenamiento.

Acerca de esta tarea

ONTAP puede proporcionar automáticamente más espacio libre para un volumen completo mediante uno o ambos métodos:

- Aumente el tamaño del volumen (conocido como *crecimiento automático*).

Este método resulta útil si el agregado que contiene el volumen tiene espacio suficiente para admitir un volumen mayor. Puede configurar ONTAP para establecer un tamaño máximo del volumen. El aumento se activa automáticamente en función de la cantidad de datos que se escriben en el volumen en relación con la cantidad actual de espacio usado y todos los umbrales establecidos.

El crecimiento automático no se activa para admitir la creación de copias de Snapshot. Si se intenta crear una copia Snapshot y hay espacio insuficiente, se produce un error en la creación de la copia Snapshot, incluso con el crecimiento automático habilitado.

- Elimine copias snapshot, archivos FlexClone o LUN FlexClone.

Por ejemplo, puede configurar ONTAP para eliminar automáticamente copias Snapshot que no están vinculadas a las copias Snapshot en volúmenes o LUN clonados, o puede definir qué copias Snapshot desea que ONTAP elimine primero, es decir, las copias Snapshot más antiguas o más recientes. También puede determinar cuándo ONTAP debe empezar a eliminar copias Snapshot; por ejemplo, cuando el volumen está casi lleno o cuando la reserva Snapshot del volumen está casi completa.

Si habilita ambos métodos, puede especificar el método que ONTAP intenta primero cuando un volumen está casi lleno. Si el primer método no proporciona suficiente espacio adicional al volumen, ONTAP intenta el otro método a continuación.

De forma predeterminada, ONTAP intenta aumentar primero el tamaño del volumen. En la mayoría de los casos, es preferible la configuración predeterminada porque cuando se elimina una copia Snapshot, no puede restaurarse. Sin embargo, si necesita evitar aumentar el tamaño de un volumen siempre que sea posible, puede configurar ONTAP para eliminar copias Snapshot antes de aumentar el tamaño del volumen.

Pasos

1. Si desea que ONTAP intente aumentar el tamaño del volumen al llenarse, habilite la funcionalidad de crecimiento automático del volumen mediante el uso de `volume autosize` comando con `grow` modo.

Recuerde que, cuando el volumen crece, consume más espacio libre de su agregado asociado. Si depende de la capacidad del volumen para crecer cuando sea necesario, debe supervisar el espacio libre en el agregado asociado y agregar más cuando sea necesario.

2. Si desea que ONTAP elimine copias Snapshot, archivos FlexClone o LUN FlexClone cuando el volumen se llene, habilite la eliminación automática para esos tipos de objetos.
3. Si se habilitó la funcionalidad de crecimiento automático de volúmenes y una o varias funcionalidades de eliminación automática, seleccione el primer método que debe usar ONTAP para proporcionar espacio libre a un volumen mediante el uso de `volume modify` con el `-space-mgmt-try-first` opción.

Para especificar si desea aumentar el tamaño del volumen primero (la opción predeterminada), utilice `volume_grow`. Para especificar primero la eliminación de copias Snapshot, utilice `snap_delete`.

Configure los volúmenes para que aumenten y reduzcan su tamaño automáticamente

Puede configurar volúmenes FlexVol para que crezcan y reduzcan automáticamente en función del espacio que necesite actualmente. El crecimiento automático ayuda a evitar que un volumen se quede sin espacio si el agregado puede suministrar más espacio. La reducción automática evita que un volumen sea mayor de lo necesario y libera espacio en el agregado para que lo usen otros volúmenes.

Lo que necesitará

El volumen FlexVol debe estar en línea.

Acerca de esta tarea

La autoreducción sólo se puede utilizar en combinación con el crecimiento automático para satisfacer las cambiantes demandas de espacio y no está disponible solo. Cuando se habilita la función de reducción automática, ONTAP gestiona automáticamente el comportamiento de reducción de un volumen para evitar un bucle interminable de acciones de autocrecimiento y autoreducción.

A medida que crece un volumen, es posible que el número máximo de archivos que puede contener se aumente automáticamente. Cuando un volumen se reduce, el número máximo de archivos que puede contener no cambia y un volumen no se puede reducir automáticamente por debajo del tamaño correspondiente a su número máximo actual de archivos. Por este motivo, es posible que no sea posible reducir de forma automática un volumen hasta su tamaño original.

De forma predeterminada, el tamaño máximo que puede crecer un volumen es del 120 % del tamaño en el cual se habilita el crecimiento automático. Si es necesario asegurarse de que el volumen pueda crecer para ser mayor que dicho, debe configurar el tamaño máximo para el volumen según corresponda.

Paso

1. Configure el volumen para que crezca y reduzca su tamaño automáticamente:

```
volume autosize -vserver vs1 vol_name -mode grow_shrink
```

El siguiente comando habilita los cambios de tamaño automáticos para un volumen denominado test2. El volumen se configura para comenzar a reducir cuando está lleno al 60 %. Los valores predeterminados se utilizan para cuándo comenzará a crecer y su tamaño máximo.

```
cluster1::> volume autosize -vserver vs2 test2 -shrink-threshold-percent 60
vol autosize: Flexible volume "vs2:test2" autosize settings UPDATED.

Volume modify successful on volume: test2
```

Requisitos para habilitar la eliminación automática de tinta y de copias de Snapshot

La funcionalidad de autorreducción se puede utilizar con la eliminación automática de copias snapshot si se cumplen determinados requisitos de configuración.

Si desea habilitar la funcionalidad de autorreducción y la eliminación automática de copias snapshot, la configuración debe cumplir los siguientes requisitos:

- ONTAP se debe configurar para intentar aumentar el tamaño del volumen antes de intentar eliminar las copias Snapshot (el `-space-mgmt-try-first` la opción debe estar establecida en `volume_grow`).
- El activador para la eliminación automática de copias de Snapshot debe estar lleno del volumen (el `trigger` el parámetro debe configurarse en `volume`).

Cómo interactúa la funcionalidad de autorreducción con la eliminación de copias snapshot

Dado que la funcionalidad de reducción automática reduce el tamaño de un volumen FlexVol, también puede afectar al eliminación automática de las copias snapshot para volúmenes.

La funcionalidad de autorreducción interactúa con la eliminación automática de copias Snapshot de volumen de las siguientes maneras:

- Si ambos `grow_shrink` El modo autosize y la eliminación automática de copias snapshot se habilitan cuando el tamaño de un volumen reduce, puede activar la eliminación automática de copias snapshot.

Esto es así porque la reserva de Snapshot se basa en un porcentaje del tamaño del volumen (5 % de forma predeterminada), y ese porcentaje ahora se basa en un tamaño de volumen más pequeño. Esto puede provocar que las copias Snapshot se salgan de la reserva y se eliminen automáticamente.

- Si la `grow_shrink` El modo autosize está habilitado y puede eliminar manualmente una copia snapshot; puede que se active una reducción de volumen automática.

Envíe las alertas de ocupación y sobreasignación del volumen de FlexVol en la dirección correspondiente

ONTAP emite mensajes de EMS cuando los volúmenes de FlexVol se están quedando sin espacio, por lo que puede tomar medidas correctivas proporcionando más espacio para el volumen completo. Conocer los tipos de alertas y cómo afrontarlas le ayuda a garantizar la disponibilidad de sus datos.

Cuando un volumen se describe como *Full*, significa que el porcentaje del espacio disponible en el volumen para su uso por parte del sistema de archivos activo (datos de usuario) ha caído por debajo de un umbral (configurable). Cuando un volumen se convierte en *overasignó*, se ha agotado el espacio utilizado por ONTAP para los metadatos y para admitir el acceso a los datos básicos. A veces, el espacio que se reserva normalmente para otros fines se puede utilizar para mantener el volumen en funcionamiento, pero la reserva de espacio o la disponibilidad de los datos pueden estar en riesgo.

La sobreasignación puede ser lógica o física. *Sobreasignación lógica* significa que el espacio reservado para cumplir con los compromisos espaciales futuros, como la reserva espacial, se ha utilizado para otro propósito. *Physical overasignada* significa que el volumen se está quedando sin bloques físicos que usar. Los volúmenes en este estado corren el riesgo de rechazar escrituras, desconectarse o potencialmente provocar una interrupción de controladora.

Un volumen puede estar lleno más de un 100% debido al espacio utilizado o reservado por los metadatos. Sin embargo, una asignación excesiva puede o no sobreasignada a un volumen que esté lleno a más del 100 %. Si existen recursos compartidos a nivel de `qtree` y volumen en el mismo pool FlexVol o SCVMM, los `qtrees` aparecen como directorios en el recurso compartido de FlexVol. Por lo tanto, debe tener cuidado de no eliminarlos accidentalmente.

En la siguiente tabla se describen las alertas de ocupación y sobreasignación de volúmenes, las acciones que se pueden realizar para resolver el problema y los riesgos de no emprender acciones:

| Tipo de alerta | Nivel de EMS | ¿Configurable? | Definición | Formas de abordar | Riesgo si no se toman medidas |
|---------------------------|-------------------|----------------|---|---|---|
| Casi lleno | Depurar | Y | El sistema de archivos ha superado el umbral configurado para esta alerta (el valor predeterminado es 95 %). El porcentaje es el <code>Used Total</code> menos el tamaño de la reserva de Snapshot. | <ul style="list-style-type: none"> • Aumentar el tamaño del volumen • Reducción de los datos de usuario | Todavía no existen riesgos de operaciones de escritura ni disponibilidad de datos. |
| Lleno | Depurar | Y | El sistema de archivos ha superado el umbral definido para esta alerta (el valor predeterminado es 98%). El porcentaje es el <code>Used Total</code> menos el tamaño de la reserva de Snapshot. | <ul style="list-style-type: none"> • Aumentar el tamaño del volumen • Reducción de los datos de usuario | Aún no hay riesgo de sufrir operaciones de escritura ni disponibilidad de datos, pero el volumen se está acercando al estadio en el que podrían estar en riesgo las operaciones de escritura. |
| Sobreasignado lógicamente | Error de servicio | N | Además de que el sistema de archivos está lleno, se agotó el espacio del volumen usado para los metadatos. | <ul style="list-style-type: none"> • Aumentar el tamaño del volumen • Eliminar copias Snapshot • Reducción de los datos de usuario • Deshabilitación de la reserva de espacio para archivos o LUN | Se puede producir un error en las operaciones de escritura en archivos no reservados. |

| Tipo de alerta | Nivel de EMS | ¿Configurable? | Definición | Formas de abordar | Riesgo si no se toman medidas |
|---------------------------|---------------|----------------|--|---|--|
| Sobreasignado físicamente | Error de nodo | N | El volumen se está quedando sin bloques físicos en los que puede escribir. | <ul style="list-style-type: none"> • Aumentar el tamaño del volumen • Eliminar copias Snapshot • Reducción de los datos de usuario | Las operaciones de escritura están en riesgo y la disponibilidad de datos; el volumen puede desconectarse. |

Cada vez que se cruza un umbral para un volumen, ya sea que el porcentaje de ocupación está aumentando o cayendo, se genera un mensaje EMS. Cuando el nivel de llenado del volumen está por debajo de un umbral, A. volume ok Se genera un mensaje EMS.

Envíe las alertas de ocupación y sobreasignación del agregado

ONTAP emite mensajes de EMS cuando los agregados se están quedando sin espacio de modo que puede realizar acciones correctivas proporcionando más espacio para todo el agregado. Conocer los tipos de alertas y cómo puede afrontarlas le ayuda a garantizar la disponibilidad de sus datos.

Cuando un agregado se describe como *Full*, significa que el porcentaje del espacio en el agregado disponible para su uso por los volúmenes ha caído por debajo de un umbral predefinido. Cuando un agregado se convierte en *overasignó*, se ha agotado el espacio utilizado por ONTAP para los metadatos y para admitir el acceso básico a los datos. A veces, el espacio que se suele reservar para otros fines puede utilizarse para mantener el agregado en funcionamiento, pero las garantías de volumen para los volúmenes asociados con el agregado o la disponibilidad de los datos pueden estar en riesgo.

La sobreasignación puede ser lógica o física. *Sobreasignación lógica* significa que el espacio reservado para cumplir con los compromisos espaciales futuros, como las garantías por volumen, se ha utilizado con otro propósito. *Physical overasignada* significa que el agregado se está quedando sin bloques físicos que usar. Los agregados en este estado corren riesgo de rechazar escrituras, desconectarse o potencialmente provocar una interrupción de controladora.

En la siguiente tabla se describen las alertas de ocupación y sobreasignación de agregados, las acciones que puede realizar para resolver el problema y los riesgos de no emprender acciones.

| Tip o de aler ta | Niv el de EM S | ¿Co nfig ura ble ? | Definición | Formas de abordar | Riesgo si no se toman medidas |
|--|---------------------------------|--------------------------------|--|--|---|
| Cas i llen o | Dep urar | N | La cantidad de espacio asignado a los volúmenes, incluidas sus garantías, superó el umbral establecido para esta alerta (95 %). El porcentaje es el <code>Used Total</code> menos el tamaño de la reserva de Snapshot. | <ul style="list-style-type: none"> • Adición de almacenamiento al agregado • Reducir o eliminar volúmenes • Mover volúmenes a otro agregado con más espacio • Eliminar garantías de volumen (establecerlas en <code>none</code>) | Todavía no existen riesgos de operaciones de escritura ni disponibilidad de datos. |
| Lle no | Dep urar | N | El sistema de archivos superó el umbral configurado para esta alerta (98 %). El porcentaje es el <code>Used Total</code> menos el tamaño de la reserva de Snapshot. | <ul style="list-style-type: none"> • Adición de almacenamiento al agregado • Reducir o eliminar volúmenes • Mover volúmenes a otro agregado con más espacio • Eliminar garantías de volumen (establecerlas en <code>none</code>) | Las garantías de volumen para los volúmenes en el agregado pueden estar en riesgo, así como las operaciones de escritura en esos volúmenes. |
| Sob rea sign ado lógica mente | Err or de ser vicio | N | Además del espacio reservado para los volúmenes que está lleno, se ha agotado el espacio del agregado usado para los metadatos. | <ul style="list-style-type: none"> • Adición de almacenamiento al agregado • Reducir o eliminar volúmenes • Mover volúmenes a otro agregado con más espacio • Eliminar garantías de volumen (establecerlas en <code>none</code>) | Las garantías de volumen para los volúmenes del agregado están en riesgo, así como las operaciones de escritura en dichos volúmenes. |

| Tip o de aler ta | Niv el de EM S | ¿Co nfig ura ble ? | Definición | Formas de abordar | Riesgo si no se toman medidas |
|--|-----------------------------|--------------------------------|---|--|--|
| Sob rea sign ado físic am ent e | Err or de nod o | N | El agregado se está quedando sin bloques físicos en los que puede escribir. | <ul style="list-style-type: none"> • Adición de almacenamiento al agregado • Reducir o eliminar volúmenes • Mover volúmenes a otro agregado con más espacio | Las operaciones de escritura en volúmenes del agregado están en riesgo, así como la disponibilidad de datos; el agregado puede desconectarse. En casos extremos, el nodo podría experimentar una interrupción. |

Cada vez que se cruza un umbral para un agregado, ya sea que el porcentaje de ocupación está aumentando o cayendo, se genera un mensaje EMS. Cuando el nivel de llenado del agregado está por debajo de un umbral, una `aggregate ok` Se genera un mensaje EMS.

Consideraciones para establecer la reserva fraccionaria

La reserva fraccionaria, también denominada *LUN overwrite reserve*, le permite desactivar la reserva de sobrescritura para archivos y LUN reservados de espacio en un volumen de FlexVol. Esto puede ayudarle a maximizar el uso del almacenamiento, pero si su entorno se ve afectado negativamente por errores en las operaciones de escritura debido a la falta de espacio, debe comprender los requisitos que impone esta configuración.

La configuración de reserva fraccionaria se expresa como un porcentaje; los únicos valores válidos son 0 y.. 100 porcentaje. La configuración de reserva fraccionaria es un atributo del volumen.

Estableciendo la reserva fraccionaria en 0 aumenta la utilización del almacenamiento. Sin embargo, una aplicación que acceda a los datos del volumen puede sufrir una interrupción del servicio de los datos si el volumen no tiene espacio libre, incluso con la garantía de volumen establecida en `volume`. Sin embargo, con una configuración de volumen y un uso adecuados, se puede minimizar la posibilidad de que falle la escritura. ONTAP proporciona una garantía de escritura «"best effort"» para volúmenes con reserva fraccionaria establecida en 0 cuando se cumplan *all* de los siguientes requisitos:

- La deduplicación no se está utilizando
- La compresión no se está utilizando
- No se utilizan subarchivos FlexClone
- Todos los archivos de FlexClone y LUN de FlexClone están habilitados para la eliminación automática

Esta no es la configuración predeterminada. Debe habilitar de forma explícita la eliminación automática, ya sea en el momento de la creación o modificando el archivo FlexClone o la LUN de FlexClone después de crearla.

- No se están utilizando la descarga de copias ODX y FlexClone

- La garantía de volumen se establece en `volume`
- La reserva de espacio de la LUN o el archivo es `enabled`
- La reserva de copias Snapshot de volumen se establece en `0`
- La eliminación automática de copias Snapshot de volumen es `enabled` con un nivel de compromiso de `destroy`, una lista de destrucción de `lun_clone`, `vol_clone`, `cifs_share`, `file_clone`, `sfsr`, y un disparador de `volume`

Esta configuración también garantiza que los archivos FlexClone y las LUN de FlexClone se eliminen cuando sea necesario.



- Si se cumplen todos los requisitos anteriores, pero la tasa de cambio es alta, en raras ocasiones, la eliminación automática de la copia Snapshot puede quedarse atrás, lo que provoca que el volumen se quede sin espacio.
- Si se cumplen todos los requisitos anteriores y las copias Snapshot no se usan, garantiza que las escrituras de los volúmenes no se queden sin espacio.

Además, tiene la opción de usar la funcionalidad de crecimiento automático de volumen para reducir la probabilidad de que las copias de snapshot del volumen deban eliminarse automáticamente. Si se habilita la funcionalidad de crecimiento automático, se debe supervisar el espacio libre en el agregado asociado. Si el agregado está lo suficientemente lleno como para evitar que el volumen crezca, es probable que se eliminen más copias snapshot a medida que se agota el espacio libre del volumen.

Si no puede satisfacer todos los requisitos de configuración anteriores y es necesario garantizar que el volumen no se quede sin espacio, debe establecer el valor de reserva fraccionaria del volumen en `100`. Esto requiere más espacio libre de antemano, pero garantiza que las operaciones de modificación de datos tendrán éxito incluso cuando las tecnologías enumeradas anteriormente estén en uso.

El valor predeterminado y los valores permitidos para la configuración de reserva fraccionaria dependen de la garantía del volumen:

| Garantía de volumen | Reserva fraccionaria predeterminada | Valores permitidos |
|---------------------|-------------------------------------|--------------------|
| Volumen | 100 | 0, 100 |
| Ninguno | 0 | 0, 100 |

Muestra el uso de archivos o inodo

Los volúmenes FlexVol tienen un número máximo de archivos que pueden contener. Saber cuántos archivos contiene sus volúmenes le ayuda a determinar si necesita aumentar el número de inodos (públicos) de sus volúmenes para evitar que estos puedan alcanzar su límite máximo de archivos.

Acerca de esta tarea

Los inodos públicos pueden ser libres (no están asociados a un archivo) o utilizados (señalan a un archivo). El número de inodos libres de un volumen es el número total de inodos del volumen menos el número de inodos usados (el número de archivos).

Si existen recursos compartidos a nivel de qtree y volumen en el mismo pool FlexVol o SCVMM, los qtrees aparecen como directorios en el recurso compartido de FlexVol. Por lo tanto, debe tener cuidado de no eliminarlos accidentalmente.

Paso

1. Para mostrar el uso de nodos de información de un volumen, introduzca el siguiente comando:

```
volume show -vserver <SVM_name> -volume <volume_name> -fields files
```

Ejemplo

```
cluster1::*> volume show -vserver vs1 -volume vol1 -fields files
Vserver Name: vs1
Files Used (for user-visible data): 98
```

Controle y supervise el rendimiento de I/O de los volúmenes FlexVol mediante la calidad de servicio de almacenamiento

Puede controlar el rendimiento de entrada/salida (I/O) en volúmenes de FlexVol asignando volúmenes a grupos de políticas de calidad de servicio de almacenamiento. Es posible controlar el rendimiento de I/O para garantizar que las cargas de trabajo alcancen objetivos de rendimiento específicos o reducir una carga de trabajo que afecte negativamente a otras cargas de trabajo.

Acerca de esta tarea

Los grupos de directivas aplican un límite máximo de rendimiento (por ejemplo, 100 MB/s). Puede crear un grupo de políticas sin especificar un rendimiento máximo, lo que permite supervisar el rendimiento antes de controlar la carga de trabajo.

También puede asignar SVM, LUN y archivos a los grupos de políticas.

Tenga en cuenta los siguientes requisitos sobre la asignación de un volumen a un grupo de políticas:

- El volumen debe estar contenido por la SVM a la que pertenece el grupo de políticas.

La SVM se especifica al crear el grupo de políticas.

- Si asigna un volumen a un grupo de políticas, no puede asignar la SVM que contiene el volumen ni ningún LUN o archivo secundario a un grupo de políticas.

Para obtener más información acerca de cómo usar la calidad de servicio de almacenamiento, consulte ["Referencia de administración del sistema"](#).

Pasos

1. Utilice la `qos policy-group create` comando para crear un grupo de políticas.
2. Utilice la `volume create` o el `volume modify` con el `-qos-policy-group` parámetro para asignar un volumen a un grupo de políticas.
3. Utilice la `qos statistics` comandos para ver datos de rendimiento.

4. Si es necesario, utilice `qos policy-group modify` comando para ajustar el límite máximo de rendimiento del grupo de políticas.

Eliminar un volumen de FlexVol

Es posible eliminar un volumen de FlexVol que ya no se requiera o que contenga datos dañados.

Lo que necesitará

Ninguna aplicación debe estar accediendo a los datos del volumen que desea eliminar.



Si elimina por error un volumen, consulte el artículo de la base de conocimientos ["Cómo usar la cola de recuperación de volúmenes"](#).

Pasos

1. Si el volumen se montó, desmontarlo:

```
volume unmount -vserver vserver_name -volume volume_name
```

2. Si el volumen forma parte de una relación de SnapMirror, elimine la relación mediante el `snapmirror delete` comando.

3. Si el volumen está en línea, desconecte el volumen:

```
volume offline -vserver vserver_name volume_name
```

4. Elimine el volumen:

```
volume delete -vserver vserver_name volume_name
```

Resultado

Se elimina el volumen, junto con cualquier qtrees y políticas de cuotas asociadas.

Protección contra eliminación accidental de volúmenes

El comportamiento de eliminación de volúmenes predeterminado ayuda a la recuperación de volúmenes de FlexVol eliminados accidentalmente.

1. `volume delete` solicitud contra un volumen que tiene tipo RW o. DP (como se ve en la `volume show` resultado del comando) hace que el volumen se mueva a un estado parcialmente eliminado. De forma predeterminada, se conserva en una cola de recuperación durante al menos 12 horas antes de eliminarse por completo.

Para obtener más información, consulte el artículo de la base de conocimientos ["Cómo usar la cola de recuperación de volúmenes"](#).

Comandos para gestionar volúmenes de FlexVol

Hay comandos específicos para gestionar los volúmenes de FlexVol mediante la interfaz de línea de comandos de ONTAP.

| Si desea... | Se usa este comando... |
|---|---|
| Coloque un volumen en línea | <code>volume online</code> |
| Cambiar el tamaño de un volumen | <code>volume size</code> |
| Determine el agregado asociado de un volumen | <code>volume show</code> |
| Determinar el agregado asociado para todos los volúmenes en una máquina virtual de almacenamiento (SVM) | <code>volume show -vserver -fields aggregate</code> |
| Determine el formato de un volumen | <code>volume show -fields block-type</code> |
| Monte un volumen en otro volumen mediante una unión | <code>volume mount</code> |
| Ponga un volumen en estado restringido | <code>volume restrict</code> |
| Cambiar el nombre de un volumen | <code>volume rename</code> |
| Desconectar un volumen | <code>volume offline</code> |

Consulte la página de manual de cada comando para obtener más información.

Comandos para mostrar información de uso de espacio

Utilice la `storage aggregate` y.. `volume` Comandos para ver cómo se utiliza el espacio en los agregados y volúmenes y en sus copias snapshot.

| Para mostrar información acerca de... | Se usa este comando... |
|--|--|
| Agregados, incluidos detalles sobre los porcentajes de espacio utilizados y disponibles, el tamaño de reserva de Snapshot y otra información de uso de espacio | <code>storage aggregate show storage aggregate show-space -fields snap-size-total,used-including-snapshot-reserve</code> |
| Cómo se usan los discos y los grupos RAID en un agregado y el estado de RAID | <code>storage aggregate show-status</code> |
| La cantidad de espacio en disco que se reclamaría si eliminó una copia de Snapshot específica | <code>volume snapshot compute-reclaimable (avanzado)</code> |
| La cantidad de espacio utilizada por un volumen | <code>volume show -fields size,used,available,percent-used</code> <code>volume show-space</code> |

| Para mostrar información acerca de... | Se usa este comando... |
|---|------------------------------------|
| La cantidad de espacio utilizada por un volumen en el agregado que contiene | <code>volume show-footprint</code> |

Mueva y copie volúmenes

Mueva una información general sobre FlexVol Volume

Puede mover o copiar volúmenes para aprovechar la capacidad, mejorar el rendimiento y cumplir los acuerdos de nivel de servicio.

Saber cómo funciona la transferencia de un volumen de FlexVol le ayuda a determinar si el movimiento de volúmenes cumple los acuerdos de nivel de servicio y a comprender dónde se encuentra un movimiento de volúmenes en el proceso de traslado de volúmenes.

Los volúmenes FlexVol se mueven de un agregado o nodo a otro dentro de la misma máquina virtual de almacenamiento (SVM). Un movimiento de volúmenes no interrumpe el acceso de los clientes durante el movimiento.

El movimiento de un volumen se produce en varias fases:

- Se realiza un nuevo volumen en el agregado de destino.
- Los datos del volumen original se copian al volumen nuevo.

Durante este tiempo, el volumen original está intacto y disponible para que los clientes puedan acceder a él.

- Al final del proceso de transferencia, se bloquea temporalmente el acceso del cliente.

Durante este tiempo, el sistema realiza una replicación final del volumen de origen al volumen de destino, cambia las identidades de los volúmenes de origen y de destino y cambia el volumen de destino al volumen de origen.

- Tras completar la transferencia, el sistema enruta el tráfico de cliente al nuevo volumen de origen y reanuda el acceso del cliente.

El movimiento no provoca interrupciones en el acceso del cliente, porque el tiempo en el que se bloquea el acceso del cliente finaliza antes de que los clientes notan una interrupción y tiempo de espera. De forma predeterminada, el acceso del cliente está bloqueado durante 35 segundos. Si la operación de movimiento de volumen no puede finalizar en el momento en que se deniega el acceso, el sistema cancela esta fase final de la operación de movimiento de volumen y permite el acceso de los clientes. De forma predeterminada, el sistema intenta la fase final tres veces. Después del tercer intento, el sistema espera una hora antes de intentar la secuencia de fase final de nuevo. El sistema ejecuta la fase final de la operación de movimiento de volúmenes hasta que se completa el movimiento de volúmenes.

Consideraciones y recomendaciones al mover volúmenes

El movimiento de un volumen tiene muchas consideraciones y recomendaciones que influyen en el volumen que se está moviendo o la configuración del sistema, por ejemplo, una configuración de MetroCluster. Debe comprender las consideraciones y las recomendaciones asociadas con el movimiento de volúmenes.

Consideraciones y recomendaciones generales

- Si va a actualizar la familia de versiones de un clúster, no mueva un volumen hasta que haya actualizado todos los nodos del clúster.

Esta recomendación impide que intente mover un volumen de una familia de versiones más reciente a una familia de versiones más antigua de forma accidental.

- El volumen de origen debe ser coherente.
- Si asignó uno o varios agregados a la SVM, el agregado de destino debe ser uno de los agregados asignados.
- No podrá mover un volumen a un agregado de CFO trasladado o desde él.
- Si un volumen que contiene LUN no tiene la función NVFAIL habilitada para poder moverlo, el volumen tendrá la función NVFAIL después de moverlo.
- Puede mover un volumen de un agregado de Flash Pool a otro agregado de Flash Pool.
 - También se mueven las políticas de almacenamiento en caché de ese volumen.
 - El movimiento puede afectar al rendimiento del volumen.
- Puede mover volúmenes entre un agregado de Flash Pool y otro que no sea Flash Pool.
 - Si mueve un volumen de un agregado de Flash Pool a uno que no sea Flash Pool, ONTAP muestra un mensaje para advertir que el movimiento puede afectar al rendimiento del volumen y pregunta si desea continuar.
 - Si se mueve un volumen de un agregado que no es Flash Pool a un agregado de Flash Pool, ONTAP asigna el `auto` política de almacenamiento en caché.
- Los volúmenes tienen las protecciones de datos en reposo del agregado en el que residen. Si se mueve un volumen de un agregado que consta de unidades NSE a otro que no lo hace, el volumen ya no tiene la protección de datos en reposo de NSE.

Consideraciones y recomendaciones sobre el volumen FlexClone

- Los volúmenes FlexClone no pueden estar desconectados cuando se muevan.
- Puede mover volúmenes FlexClone de un agregado a otro en el mismo nodo u otro nodo de la misma SVM sin necesidad de iniciar el `vol clone split start` comando.

Al iniciar una operación de movimiento de volúmenes en un volumen FlexClone, el volumen clonado se divide durante el proceso de movimiento hacia otro agregado. Una vez que se ha completado el movimiento del volumen en el volumen clonado, el volumen que se ha movido ya no aparece como clon, sino como un volumen independiente sin ninguna relación de clonado con el volumen principal anterior.

- Las copias snapshot para volúmenes FlexClone no se pierden después de mover un clon.
- Puede mover volúmenes principales FlexClone de un agregado a otro.

Al mover un volumen principal FlexClone, queda un volumen temporal detrás que actúa como volumen principal de todos los volúmenes FlexClone. No se permiten operaciones en el volumen temporal, excepto para desconectarlo o eliminarlo. Una vez que todos los volúmenes FlexClone se dividen o destruyen, se limpia automáticamente el volumen temporal.

- Tras mover un volumen secundario FlexClone, el volumen ya no es un volumen FlexClone.
- Las operaciones de movimiento de FlexClone son mutuamente excluyentes entre las operaciones de copia o división de FlexClone.

- Si hay una operación de división de clones en curso, es posible que se produzca un error en la transferencia de un volumen.

No se debe mover un volumen hasta que se hayan completado las operaciones de separación de clones.

Consideraciones de configuración de MetroCluster

- Durante un movimiento de volúmenes en una configuración MetroCluster, cuando se crea un volumen temporal en el agregado de destino en el clúster de origen, se crea un registro del volumen temporal que corresponde al volumen en el volumen reflejado, pero no asimilado, también se crea un agregado en el clúster superviviente.
- Si se produce una conmutación de MetroCluster antes de la transposición, el volumen de destino tiene un registro y es un volumen temporal (un volumen del tipo TMP).

El trabajo de movimiento se reinicia en el clúster superviviente (recuperación ante desastres), informa de un error y borra todos los elementos relacionados con el movimiento, incluido el volumen temporal. En cualquier caso en el que no se pueda realizar la limpieza correctamente, se genera un EMS para alertar al administrador del sistema de que realice la limpieza necesaria.

- Si una conmutación de MetroCluster se produce después de que se haya iniciado la fase de transición pero antes de que se haya completado el trabajo de movimiento (es decir, el movimiento llegó a una fase en la que puede actualizar el clúster para que apunte al agregado de destino), el trabajo de movimiento se reinicia en el proceso superviviente (recuperación ante desastres). cluster y se ejecuta hasta la finalización.

Todos los elementos relacionados con el traslado se limpian, incluido el volumen temporal (origen original). En cualquier caso en el que no se pueda realizar la limpieza correctamente, se genera un EMS para alertar al administrador del sistema de que realice la limpieza necesaria.

- No se permiten ni devoluciones de MetroCluster forzadas ni forzadas si hay operaciones de movimiento de volúmenes en curso para volúmenes que pertenecen al sitio con switch.

Los interruptores de control no se bloquean cuando las operaciones de movimiento de volúmenes están en curso para los volúmenes locales del sitio superviviente.

- Los interruptores MetroCluster no forzados se bloquean, pero los conmutadores MetroCluster forzados no se bloquean si hay operaciones de movimiento de volúmenes en curso.

Requisito para mover volúmenes en entornos SAN

Antes de mover un volumen que contiene LUN o espacios de nombres, debe cumplir ciertos requisitos.

- Para los volúmenes que contienen una o más LUN, debe tener un mínimo de dos rutas por LUN (LIF) conectadas a cada nodo del clúster.

De este modo, se eliminan los puntos únicos de error y el sistema puede sobrevivir a fallos de componentes.

- Para los volúmenes que contienen espacios de nombres, el clúster debe ejecutar ONTAP 9.6 o una versión posterior.

La transferencia de volúmenes no es compatible con configuraciones de NVMe que ejecuten ONTAP 9.5.

Mover un volumen

Es posible mover un volumen de FlexVol a otro agregado, nodo o ambos dentro de la misma máquina virtual de almacenamiento (SVM) para equilibrar la capacidad de almacenamiento después de determinar que hay un desequilibrio de capacidad de almacenamiento.

Acerca de esta tarea

De forma predeterminada, si la operación de transposición no puede completarse en un plazo de 30 segundos, volverá a intentarlo. Puede ajustar el comportamiento predeterminado mediante la `-cutover-window` y `-cutover-action` parámetros, ambos requieren acceso avanzado a nivel de privilegios. Para obtener más detalles, consulte `volume move start` página de manual.

Pasos

1. Si mueve un reflejo de protección de datos y no ha inicializado la relación de reflejo, inicialice la relación de reflejo con el `snapmirror initialize` comando.

Es necesario inicializar las relaciones de mirroring de protección de datos para poder mover uno de los volúmenes.

2. Determine un agregado al que puede mover el volumen mediante el `volume move target-aggr show` comando.

El agregado que seleccione debe tener espacio suficiente para el volumen; es decir, el tamaño disponible es mayor que el volumen que se está moviendo.

El siguiente ejemplo muestra que el volumen `vs2` se puede mover a cualquiera de los agregados enumerados:

```
cluster1::> volume move target-aggr show -vserver vs2 -volume user_max
Aggregate Name      Available Size      Storage Type
-----
aggr2                467.9GB             hdd
node12a_aggr3        10.34GB             hdd
node12a_aggr2        10.36GB             hdd
node12a_aggr1        10.36GB             hdd
node12a_aggr4        10.36GB             hdd
5 entries were displayed.
```

3. Compruebe que el volumen se puede mover al agregado previsto mediante la `volume move start -perform-validation-only` para ejecutar una comprobación de validación.
4. Mueva el volumen mediante la `volume move start` comando.

El siguiente comando mueve el volumen `user_max` de la SVM `vs2` al agregado `node12a_aggr3`. El movimiento se ejecuta como un proceso en segundo plano.

```
cluster1::> volume move start -vserver vs2 -volume user_max
-destination-aggregate node12a_aggr3
```

5. Determine el estado de la operación de movimiento de volumen mediante el `volume move show` comando.

El siguiente ejemplo muestra el estado de un movimiento de volumen que completó la fase de replicación y se encuentra en la fase de transposición:

```
cluster1::> volume move show
Vserver    Volume      State      Move Phase  Percent-Complete  Time-To-
Complete
-----
vs2        user_max    healthy    cutover     -                  -
```

El movimiento de volumen se completa cuando ya no aparece en la `volume move show` resultado del comando.

Comandos para mover volúmenes

Hay comandos de la ONTAP específicos para gestionar los movimientos de volúmenes.

| Si desea... | Se usa este comando... |
|--|--|
| Anule una operación de movimiento de volumen activa. | <code>volume move abort</code> |
| Muestra el estado de un volumen moviendo de un agregado a otro agregado. | <code>volume move show</code> |
| Empiece a mover un volumen de un agregado a otro. | <code>volume move start</code> |
| Gestione los agregados de destino para mover volúmenes. | <code>volume move target-aggr</code> |
| Activar la transición de un trabajo de movimiento. | <code>volume move trigger-cutover</code> |
| Cambie la cantidad de tiempo en el que se bloquea el acceso del cliente si el valor predeterminado no es adecuado. | <code>volume move start</code> o <code>volume move modify</code> con la <code>-cutover-window</code> parámetro. La <code>volume move modify</code> el comando es un comando avanzado y la <code>-cutover-window</code> es un parámetro avanzado. |

| Si desea... | Se usa este comando... |
|--|--|
| Determine qué hace el sistema si no se puede completar la operación de movimiento de volumen durante el momento en que se bloquea el acceso de los clientes. | <code>volume move start</code> o <code>volume move modify</code> con la <code>-cutover-action</code> parámetro. La <code>volume move modify</code> el comando es un comando avanzado y la <code>-cutover-action</code> es un parámetro avanzado. |

Consulte la página de manual de cada comando para obtener más información.

Métodos para copiar un volumen

El copiado de un volumen crea una copia independiente de un volumen que se puede usar para pruebas y con otros fines. El método que se utiliza para copiar un volumen depende del caso de uso.

El método que se utilice para copiar un volumen depende de si se va a copiar en el mismo agregado o en otro, y si se desean conservar copias Snapshot del volumen original. En la siguiente tabla se enumeran las características de la copia y los métodos utilizados para crear dicha copia.

| Si desea copiar un volumen... | Entonces, el método que usa es... |
|---|---|
| Dentro del mismo agregado, por lo que no se desean copiar copias Snapshot del volumen original. | Creación de un volumen FlexClone del volumen original. |
| En otro agregado, no desea copiar copias Snapshot del volumen original. | Crear un volumen FlexClone del volumen original y, a continuación, mover el volumen a otro agregado mediante el <code>volume move</code> comando. |
| A otro agregado y conservar todas las copias Snapshot del volumen original. | Replicar el volumen original mediante SnapMirror y, a continuación, dividir la relación de SnapMirror para hacer una copia de volumen de lectura/escritura. |

Use volúmenes FlexClone para crear copias eficientes de sus volúmenes de FlexVol

Use volúmenes FlexClone para crear copias eficientes de la descripción general de los volúmenes de FlexVol

Los volúmenes FlexClone son copias puntuales modificables de un volumen FlexVol principal. Los volúmenes FlexClone gestionan el espacio de manera eficiente porque comparten los mismos bloques de datos con sus volúmenes FlexVol principales para los datos comunes. La copia snapshot utilizada para crear un volumen FlexClone también se comparte con el volumen principal.

Puede clonar un volumen FlexClone existente para crear otro volumen FlexClone. También puede crear un clon de un volumen FlexVol que contenga LUN y clones de LUN.

También puede dividir un volumen FlexClone de su volumen principal. A partir de ONTAP 9.4, en el caso de volúmenes sin garantía en sistemas AFF, la operación de división de volúmenes FlexClone comparte los

bloques físicos y no copia los datos. Por lo tanto, la separación de volúmenes FlexClone en sistemas AFF es más rápida que la operación de separación de FlexClone en otros sistemas FAS en ONTAP 9.4 y versiones posteriores.

Puede crear dos tipos de volúmenes FlexClone: Volúmenes FlexClone de lectura y escritura y volúmenes FlexClone de protección de datos. Aunque se puede crear un volumen FlexClone de lectura y escritura de un volumen FlexVol normal, solo se debe utilizar un volumen secundario SnapVault para crear un volumen FlexClone de protección de datos.

Cree un volumen FlexClone

Se puede crear un volumen de FlexClone de protección de datos desde un volumen de destino de SnapMirror o desde un volumen de FlexVol principal que sea un volumen secundario de SnapVault. A partir de ONTAP 9,7, se puede crear un volumen FlexClone a partir de un volumen FlexGroup. Después de crear un volumen FlexClone, no se puede eliminar el volumen principal mientras el volumen FlexClone existe.

Antes de empezar

- Debe instalar la licencia de FlexClone en el clúster. Esta licencia se incluye con "ONTAP One".
- El volumen que desea clonar debe estar en línea.



No se admite la clonación de un volumen como volumen FlexClone en otra SVM en las configuraciones de MetroCluster.

Crear un volumen FlexClone de un FlexVol o FlexGroup

Paso

1. Cree un volumen FlexClone:

```
volume clone create
```



Al crear un volumen FlexClone de lectura y escritura desde el volumen principal de lectura y escritura, no es necesario especificar la copia Snapshot base. ONTAP crea una copia Snapshot si no nombra ninguna copia Snapshot específica que se usará como copia Snapshot base para el clon. Debe especificar la copia snapshot básica para crear un volumen FlexClone cuando el volumen principal sea un volumen de protección de datos.

Ejemplo

- El siguiente comando crea un volumen FlexClone de lectura y escritura vol1_clone a partir del volumen principal vol1:

```
volume clone create -vserver vs0 -flexclone vol1_clone -type RW -parent-volume vol1
```

- El siguiente comando crea una protección de datos FlexClone volume vol_dp_clone del volumen principal dp_vol usando la copia Snapshot básica snap1:

```
volume clone create -vserver vs1 -flexclone vol_dp_clone -type DP -parent-volume dp_vol -parent-snapshot snap1
```

Cree un FlexClone de cualquier tipo de SnapLock

A partir de ONTAP 9.13.1, puede especificar uno de los tres tipos de SnapLock, `compliance`, `enterprise`, `non-snaplock`. Al crear un FlexClone de un volumen RW. De forma predeterminada, se crea un volumen FlexClone con el mismo tipo de SnapLock que el volumen principal. Sin embargo, puede sustituir el valor predeterminado mediante `snaplock-type` Durante la creación del volumen FlexClone.

Con el `non-snaplock` con el `snaplock-type` Puede crear un volumen FlexClone que no es de tipo SnapLock desde un volumen primario de SnapLock para proporcionar un método más rápido para volver a conectar los datos cuando sea necesario.

Más información acerca de "[SnapLock](#)".

Antes de empezar

Debe conocer las siguientes limitaciones de volumen de FlexClone si tienen un tipo de SnapLock diferente al volumen principal.

- Solo se admiten clones de tipo RW. No se admiten los clones de tipo DP con un tipo de SnapLock diferente al volumen principal.
- Los volúmenes con LUN no se pueden clonar utilizando la opción de tipo `snaplock` configurada con un valor distinto de 'no snaplock', porque los volúmenes de SnapLock no admiten LUN.
- No se puede clonar un volumen en un agregado reflejado de MetroCluster con un tipo de SnapLock de cumplimiento de normativas porque los volúmenes de SnapLock Compliance no son compatibles con los agregados reflejados de MetroCluster.
- Los volúmenes de cumplimiento de normativas de SnapLock con conservación legal no se pueden clonar con un tipo de SnapLock diferente. La conservación legal solo se admite en los volúmenes de cumplimiento de normativas de SnapLock.
- La recuperación de desastres de SVM no es compatible con los volúmenes de SnapLock. Se producirá un error al intentar crear un clon SnapLock a partir de un volumen de una SVM que forma parte de una relación de recuperación ante desastres de SVM.
- Las prácticas recomendadas de FabricPool recomiendan que los clones conserven la misma política de organización en niveles que el volumen principal. Sin embargo, un clon de cumplimiento de normativas de SnapLock de un volumen habilitado para FabricPool no puede tener la misma política de organización en niveles que el volumen principal. La política de organización en niveles debe establecerse en `none`. Se intenta crear un clon de cumplimiento de normativas de SnapLock a partir de un elemento principal con una política de organización en niveles distinta de `none` fallará.

Pasos

1. Cree un volumen FlexClone con un tipo de SnapLock: `volume clone create -vserver svm_name -flexclone flexclone_name -type RW [-snaplock-type {non-snaplock|compliance|enterprise}]`

Ejemplo:

```
> volume clone create -vserver vs0 -flexclone voll_clone -type RW  
-snaplock-type enterprise -parent-volume voll
```

Divida un volumen FlexClone de su volumen principal

Puede dividir un volumen FlexClone de su principal para que el clon sea un volumen FlexVol normal.

La operación de división de clones tiene lugar en segundo plano. Se puede acceder a los datos en el clon y en el elemento principal durante la división. A partir de ONTAP 9,4, se mantiene la eficiencia del espacio. El proceso de división solo actualiza los metadatos y requiere una E/S mínima. No se copian bloques de datos.

Acerca de esta tarea

- Durante la operación de división, no se pueden crear nuevas copias snapshot del volumen FlexClone.
- No se puede dividir un volumen FlexClone del volumen principal si pertenece a una relación de protección de datos o forma parte de un reflejo de distribución de cargas.
- Si desconecta el volumen FlexClone mientras la separación está en curso, la operación de división se suspenderá; cuando el volumen FlexClone vuelva a estar en línea, se reanudará la operación de separación.
- Después de la división, tanto el volumen FlexVol principal como el clon requieren toda la asignación de espacio determinada por las garantías de volumen.
- Después de dividir un volumen FlexClone de su principal, no se pueden volver a unir dos.
- A partir de ONTAP 9.4, en el caso de volúmenes sin garantía en sistemas AFF, la operación de división de volúmenes FlexClone comparte los bloques físicos y no copia los datos. Por lo tanto, la división de volúmenes FlexClone en sistemas AFF es más rápida que la operación de división de FlexClone en otros sistemas FAS en ONTAP 9,4 y versiones posteriores. La operación de separación de FlexClone mejorada en sistemas AFF aporta las siguientes ventajas:
 - La eficiencia del almacenamiento se mantiene tras dividir el clon del principal.
 - Las copias Snapshot existentes no se eliminan.
 - La operación es más rápida.
 - El volumen FlexClone puede dividirse desde cualquier punto de la jerarquía de clones.

Antes de empezar

- Debe ser un administrador de clústeres.
- El volumen FlexClone debe estar en línea cuando comience la operación de división.
- El volumen primario debe estar en línea para que la división se complete correctamente.

Pasos

1. Determine la cantidad de espacio libre necesario para completar la operación de división:

```
volume clone show -estimate -vserver vservice_name -flexclone clone_volume_name  
-parent-volume parent_vol_name
```

En el siguiente ejemplo se proporciona información acerca del espacio libre necesario para dividir el volumen FlexClone «clone1» de su volumen principal «vol1»:

```
cluster1::> volume clone show -estimate -vserver vs1 -flexclone clone1  
-parent-volume volume1
```

| | | Split |
|---------|-----------|----------|
| Vserver | FlexClone | Estimate |
| ----- | ----- | ----- |
| vs1 | clone1 | 40.73MB |

2. Compruebe que el agregado que contiene el volumen FlexClone y su principal tiene suficiente espacio:
 - a. Determine la cantidad de espacio libre del agregado que contiene el volumen FlexClone y su principal:

```
storage aggregate show
```

- b. Si el agregado que contiene no tiene suficiente espacio libre disponible, añada almacenamiento al agregado:

```
storage aggregate add-disks
```

3. Inicie la operación de división:

```
volume clone split start -vserver vserver_name -flexclone clone_volume_name
```

El ejemplo siguiente muestra cómo puedes iniciar el proceso para dividir el volumen FlexClone «clone1» de su volumen principal «vol1»:

```
cluster1::> volume clone split start -vserver vs1 -flexclone clone1
```

```
Warning: Are you sure you want to split clone volume clone1 in Vserver  
vs1 ?
```

```
{y|n}: y
```

```
[Job 1617] Job is queued: Split clone1.
```

4. Supervise el estado de la operación de división de FlexClone:

```
volume clone split show -vserver vserver_name -flexclone clone_volume_name
```

En el siguiente ejemplo, se muestra el estado de la operación de división FlexClone en un sistema AFF:

```
cluster1::> volume clone split show -vserver vs1 -flexclone clone1
```

| | | Inodes | | | | |
|----------|-----------|-----------|-------|---------|---------|---------|
| Blocks | | ----- | | | | |
| ----- | | | | | | |
| Vserver | FlexClone | Processed | Total | Scanned | Updated | % Inode |
| % Block | | | | | | |
| Complete | Complete | | | | | |
| vs1 | clone1 | 0 | 0 | 411247 | 153600 | 0 |
| 37 | | | | | | |

5. Compruebe que el volumen de división ya no es un volumen FlexClone:

```
volume show -volume volume_name -fields clone-volume
```

El valor de clone-volume La opción es «`false`» para un volumen que no sea FlexClone.

En el siguiente ejemplo, se muestra cómo se puede verificar si el volumen «clone1» que está dividido de su principal no es un volumen FlexClone.

```
cluster1::> volume show -volume clone1 -fields clone-volume
vserver volume **clone-volume**
----- **-----**
vs1      clone1 **false**
```

Determine el espacio utilizado por un volumen FlexClone

Puede determinar el espacio utilizado por un volumen FlexClone en función de su tamaño nominal y la cantidad de espacio que comparte con el volumen FlexVol principal. Cuando se crea un volumen FlexClone, comparte todos sus datos con su volumen principal. Por lo tanto, aunque el tamaño nominal del volumen FlexVol es el mismo que el tamaño de su principal, utiliza muy poco espacio libre del agregado.

Acerca de esta tarea

El espacio libre utilizado por un volumen FlexClone recién creado es aproximadamente del 0.5 % de su tamaño nominal. Este espacio se utiliza para almacenar los metadatos del volumen FlexClone.

Los nuevos datos escritos en el volumen principal o en el volumen FlexClone no se comparten entre los volúmenes. El aumento de la cantidad de datos nuevos que se escriben en el volumen FlexClone provoca un aumento del espacio que requiere el volumen FlexClone por parte de su agregado que contiene.

Paso

1. Determine el espacio físico real utilizado por el volumen FlexClone mediante el `volume show` comando.

En el ejemplo siguiente se muestra el espacio físico total que utiliza el volumen FlexClone:


```
cluster1::> volume show -vserver vs01 -volume clone_vol1 -fields
size,used,available,
percent-used,physical-used,physical-used-percent
vserver      volume      size  available  used   percent-used  physical-
used         physical-used-percent
-----
vs01         clone_vol1   20MB   18.45MB   564KB   7%            196KB
1%
```

Consideraciones que tener en cuenta para crear un volumen FlexClone a partir de un volumen de origen o de destino de SnapMirror

Se puede crear un volumen FlexClone desde el volumen de origen o de destino en una relación de SnapMirror para volúmenes existente. No obstante, al hacerlo se podría provocar que las operaciones futuras de replicación de SnapMirror no se completasen correctamente.

La replicación puede no funcionar porque al crear el volumen FlexClone, puede bloquear una copia snapshot que utilice SnapMirror. Si esto sucede, SnapMirror detiene la replicación en el volumen de destino hasta que el volumen FlexClone se destruya o se separe de su principal. Existen dos opciones para solucionar este problema:

- Si necesita el volumen FlexClone temporalmente y puede acomodar una parada temporal de la replicación de SnapMirror, puede crear el volumen FlexClone y eliminarlo o dividirlo en su principal cuando sea posible.

La replicación de SnapMirror continúa normalmente cuando el volumen FlexClone se elimina o se divide de su principal.

- Si no se acepta una parada temporal de la replicación de SnapMirror, puede crear una copia snapshot en el volumen de origen de SnapMirror y, a continuación, utilizarla para crear el volumen FlexClone. (Si crea el volumen FlexClone desde el volumen de destino, deberá esperar a que la copia snapshot se replique al volumen de destino de SnapMirror).

Este método de creación de una copia snapshot en el volumen de origen de SnapMirror permite crear el clon sin bloquear una copia snapshot que utilice SnapMirror.

Utilice archivos FlexClone y LUN FlexClone para crear copias eficientes de archivos y LUN

Use los archivos FlexClone y las LUN FlexClone para crear copias eficientes de archivos y LUN de descripción general

Los archivos FlexClone y las LUN de FlexClone son clones que permiten escritura y gestión eficiente del espacio de los archivos principales y las LUN principales, y ayudan a utilizar con eficiencia el espacio del agregado físico. Los archivos FlexClone y las LUN FlexClone solo se admiten para volúmenes FlexVol.

Los archivos FlexClone y las LUN FlexClone utilizan el 0.4 % de su tamaño para almacenar los metadatos. Los clones comparten los bloques de datos de sus archivos principales y las LUN principales y ocupan un espacio de almacenamiento mínimo hasta que los clientes escriben los datos nuevos en el archivo principal o la LUN o en el clon.

Los clientes pueden realizar todas las operaciones de archivos y LUN en las entidades principal y clonado.

Puede utilizar varios métodos para eliminar archivos FlexClone y LUN FlexClone.

Cree un archivo FlexClone o una LUN FlexClone

Puede crear clones de archivos y LUN presentes en los volúmenes FlexVol o FlexClone con gestión eficiente del espacio y con gestión eficiente del tiempo mediante el `volume file clone create` comando.

Lo que necesitará

- Debe instalar la licencia de FlexClone en el clúster. Esta licencia se incluye con "ONTAP One".
- Si se utilizan varios rangos de bloques para la clonación de LUN secundarias o la clonación de archivos secundarios, los números de bloque no deben solaparse.
- Si está creando una subLUN o un subarchivo en volúmenes con compresión adaptativa activada, los rangos de bloques no deben estar mal alineados.

Esto significa que el número de bloque inicial de origen y el número de bloque inicial de destino deben estar alineados o impares.

Acerca de esta tarea

Según los privilegios asignados por el administrador del clúster, un administrador de SVM puede crear archivos FlexClone y LUN FlexClone.

Puede especificar la configuración de eliminación automática para archivos FlexClone y LUN FlexClone al crear y modificar clones. De forma predeterminada, la configuración de eliminación automática está desactivada.

Puede sobrescribir un archivo FlexClone o una LUN FlexClone existente al crear un clon mediante la `volume file clone create` con el `-overwrite-destination` parámetro.

Cuando el nodo alcanza su carga de división máxima, el nodo deja de aceptar temporalmente solicitudes para crear archivos FlexClone y LUN FlexClone, y emite un `EBUSY` mensaje de error. Cuando la carga de división del nodo está por debajo del máximo, el nodo acepta solicitudes para crear archivos FlexClone y LUN FlexClone de nuevo. Debe esperar hasta que el nodo tenga capacidad para crear los clones antes de volver a intentar crear la solicitud.

Pasos

1. Cree un archivo FlexClone o una LUN FlexClone mediante el `volume file clone create` comando.

El siguiente ejemplo muestra cómo puede crear un archivo FlexClone `archivo1_clone` del archivo primario `file1_source` en el volumen `vol1`:

```
cluster1::> volume file clone create -vserver vs0 -volume vol1 -source
-path /file1_source -destination-path /file1_clone
```

Para obtener más información acerca de cómo utilizar este comando, consulte las páginas man.

Información relacionada

["Comandos de ONTAP 9"](#)

Ver la capacidad de nodos para crear y eliminar archivos FlexClone y LUN FlexClone

Puede ver si un nodo tiene capacidad para recibir nuevas solicitudes para crear y eliminar archivos FlexClone y LUN FlexClone al ver la carga de división del nodo. Si se alcanza la carga de división máxima, no se aceptan solicitudes nuevas hasta que la carga dividida caiga por debajo del máximo.

Acerca de esta tarea

Cuando el nodo alcanza su carga dividida máxima, una `EBUSY` se emite un mensaje de error en respuesta a las solicitudes de creación y eliminación. Cuando la carga de división del nodo está por debajo del máximo, el nodo acepta solicitudes para crear y eliminar archivos FlexClone y LUN de nuevo.

Un nodo puede aceptar nuevas solicitudes cuando el campo carga dividida permitida muestra capacidad y la solicitud de creación encaja en la capacidad disponible.

Paso

1. Vea la cantidad de capacidad que tiene un nodo para crear y eliminar archivos FlexClone y LUN FlexClone mediante el `volume file clone split load show` comando.

En el siguiente ejemplo, se muestra la carga dividida en todos los nodos de cluster1. Todos los nodos del clúster tienen capacidad para crear y eliminar archivos FlexClone y LUN FlexClone, como se indica en el campo carga dividida permitida:

```
cluster1::> volume file clone split load show
Node           Max           Current      Token           Allowable
              Split Load Split Load Reserved Load Split Load
-----
node1           15.97TB           0B           100MB           15.97TB
node2           15.97TB           0B           100MB           15.97TB
2 entries were displayed.
```

Vea el ahorro de espacio debido a los archivos FlexClone y las LUN FlexClone

Puede ver el porcentaje de espacio en disco ahorrado por uso compartido de bloques dentro de un volumen que contiene archivos FlexClone y LUN.

Paso

1. Para ver el ahorro de espacio conseguido debido a los archivos de FlexClone y las LUN de FlexClone, escriba el siguiente comando:

```
df -s volname
```

volname Es el nombre del volumen FlexVol.



Si ejecuta el `df -s` Comando en un volumen FlexVol habilitado para la deduplicación, puede ver el espacio ahorrado tanto por la deduplicación como por los archivos FlexClone y las LUN.

Ejemplo

En el siguiente ejemplo, se muestra el ahorro de espacio en un volumen FlexClone test1:

```
systemA> df -s test1
```

| Filesystem | used | saved | %saved | Vserver |
|-------------|------|-------|--------|---------|
| /vol/test1/ | 4828 | 5744 | 54% | vs1 |

Métodos para eliminar archivos FlexClone y LUN FlexClone

Puede utilizar varios métodos para eliminar archivos FlexClone y LUN FlexClone. Comprender qué métodos están disponibles le permite planificar cómo gestionar clones.

Puede utilizar los siguientes métodos para eliminar archivos de FlexClone y LUN de FlexClone:

- Es posible configurar un volumen de FlexVol para eliminar automáticamente clones con la eliminación automática habilitada cuando el espacio libre de un volumen de FlexVol disminuye por debajo de un umbral en particular.
- Puede configurar clientes para eliminar clones mediante el SDK de gestión de NetApp.
- Puede utilizar los clientes para eliminar clones mediante los protocolos NAS y SAN.

El método de eliminación más lento se habilita de forma predeterminada porque este método no utiliza el SDK de gestión de NetApp. Sin embargo, puede configurar el sistema para que utilice el método de eliminación más rápido al eliminar archivos FlexClone mediante el `volume file clone deletion` comandos.

Cómo un volumen de FlexVol puede reclamar espacio libre con la configuración de eliminación automática

Cómo un volumen de FlexVol puede reclamar espacio libre con la información general de configuración de eliminación automática

Puede activar la configuración de eliminación automática de un volumen FlexVol para eliminar automáticamente archivos FlexClone y LUN FlexClone. Al habilitar la eliminación automática, se puede recuperar una cantidad de espacio libre objetivo en el volumen cuando un volumen está casi lleno.

Puede configurar un volumen para que comience a eliminar automáticamente archivos FlexClone y LUN FlexClone cuando el espacio libre en el volumen disminuya por debajo de un valor de umbral determinado y deje de eliminar automáticamente clones cuando se reclame una cantidad de espacio libre objetivo en el volumen. Aunque, no puede especificar el valor de umbral que inicia la eliminación automática de clones, puede especificar si un clon es apto para su eliminación y puede especificar la cantidad de espacio libre objetivo para un volumen.

Un volumen elimina automáticamente los archivos FlexClone y las LUN FlexClone cuando el espacio libre en

el volumen disminuye por debajo de un umbral determinado y cuando se cumplen los siguientes requisitos:

- La función de eliminación automática está habilitada para el volumen que contiene los archivos FlexClone y las LUN FlexClone.

Para habilitar la funcionalidad de eliminación automática para un volumen de FlexVol, se puede usar la `volume snapshot autodelete modify` comando. Debe configurar el `-trigger` parámetro a `volume o. snap_reserve` Para que un volumen elimine automáticamente archivos FlexClone y LUN FlexClone.

- La función de eliminación automática está activada para los archivos de FlexClone y las LUN de FlexClone.

Puede activar la eliminación automática para un archivo FlexClone o una LUN FlexClone mediante el `file clone create` con el `-autodelete` parámetro. Como resultado, puede conservar algunos archivos FlexClone y LUN FlexClone deshabilitando la eliminación automática de los clones y asegurándose de que otras opciones de configuración del volumen no anulen la configuración del clon.

Configurar un volumen FlexVol para que elimine automáticamente archivos FlexClone y LUN FlexClone

Es posible habilitar un volumen FlexVol para eliminar automáticamente archivos de FlexClone y LUN FlexClone con la eliminación automática habilitada cuando el espacio libre en el volumen disminuye por debajo de un umbral en particular.

Lo que necesitará

- El volumen FlexVol debe contener archivos FlexClone y LUN FlexClone, y estar en línea.
- El volumen FlexVol no debe ser un volumen de solo lectura.

Pasos

1. Permita la eliminación automática de archivos de FlexClone y LUN de FlexClone en el volumen de FlexVol mediante el `volume snapshot autodelete modify` comando.

- Para la `-trigger` parámetro, puede especificar `volume o. snap_reserve`.
- Para la `-destroy-list` parámetro, debe especificar siempre `lun_clone, file_clone` independientemente de si desea eliminar solo un tipo de clon.

El siguiente ejemplo muestra cómo puede habilitar `volume vol1` para activar la eliminación automática de archivos FlexClone y LUN de FlexClone para la reclamación de espacio hasta que el 25% del volumen esté compuesto por espacio libre:

```
cluster1::> volume snapshot autodelete modify -vserver vs1 -volume  
vol1 -enabled true -commitment disrupt -trigger volume -target-free  
-space 25 -destroy-list lun_clone,file_clone
```

```
Volume modify successful on volume:vol1
```



Al habilitar la eliminación automática de volúmenes de FlexVol, si establece el valor de `-commitment` parámetro a. `destroy`, Todos los archivos FlexClone y las LUN FlexClone con `-autodelete` parámetro establecido en `true` puede eliminarse cuando el espacio libre en el volumen disminuya por debajo del valor de umbral especificado. Sin embargo, los archivos FlexClone y las LUN FlexClone con el `-autodelete` parámetro establecido en `false` no se eliminará.

2. Compruebe que la eliminación automática de archivos FlexClone y LUN de FlexClone está activada en el volumen de FlexVol mediante el `volume snapshot autodelete show` comando.

El siguiente ejemplo muestra que el volumen `vol1` está activado para la eliminación automática de archivos FlexClone y LUN FlexClone:

```
cluster1::> volume snapshot autodelete show -vserver vs1 -volume vol1

Vserver Name: vs1
Volume Name: vol1
Enabled: true
Commitment: disrupt
Defer Delete: user_created
Delete Order: oldest_first
Defer Delete Prefix: (not specified)
Target Free Space: 25%
Trigger: volume
*Destroy List: lun_clone,file_clone*
Is Constituent Volume: false
```

3. Asegúrese de que la eliminación automática esté habilitada para los archivos de FlexClone y las LUN FlexClone del volumen que desea eliminar siguiendo estos pasos:
 - a. Permitir la eliminación automática de un archivo FlexClone o una LUN FlexClone concretos mediante el `volume file clone autodelete` comando.

Puede forzar la eliminación automática de un archivo FlexClone o una LUN de FlexClone mediante la `volume file clone autodelete` con el `-force` parámetro.

El ejemplo siguiente muestra que la eliminación automática de la LUN de FlexClone `lun1_clone` contenida en el volumen `vol1` está habilitada:

```
cluster1::> volume file clone autodelete -vserver vs1 -clone-path
/vol/vol1/lun1_clone -enabled true
```

Puede activar la eliminación automática cuando crea archivos FlexClone y LUN de FlexClone.

- b. Compruebe que el archivo FlexClone o la LUN de FlexClone están activados para eliminación automática mediante la `volume file clone show-autodelete` comando.

El ejemplo siguiente muestra que la LUN de FlexClone `lun1_clone` está habilitada para eliminación

automática:

```
cluster1::> volume file clone show-autodelete -vserver vs1 -clone
-path vol/vol1/lun1_clone
Vserver Name: vs1
Clone Path: vol/vol1/lun1_clone
**Autodelete Enabled: true**
```

Para obtener más información acerca del uso de los comandos, consulte las páginas man correspondientes.

Evitar que se elimine automáticamente un archivo FlexClone o una LUN de FlexClone específica

Si configura un volumen FlexVol para eliminar automáticamente archivos FlexClone y LUN FlexClone, es posible eliminar cualquier clon que se ajuste a los criterios que especifique. Si tiene archivos FlexClone o LUN FlexClone específicos que desea conservar, puede excluirlos del proceso automático de eliminación de FlexClone.

Lo que necesitará

Debe instalar una licencia de FlexClone. Esta licencia se incluye con ["ONTAP One"](#).

Acerca de esta tarea

Cuando se crea un archivo FlexClone o una LUN de FlexClone, se deshabilita de forma predeterminada la configuración de eliminación automática del clon. Los archivos FlexClone y las LUN FlexClone con eliminación automática desactivada se conservan cuando se configura un volumen FlexVol para eliminar automáticamente los clones para reclamar espacio en el volumen.



Si establece la `commitment` nivel el volumen a `try` o `disrupt`, Puede conservar de forma individual archivos de FlexClone o LUN de FlexClone desactivando la eliminación automática de dichos clones. Sin embargo, si establece la `commitment` nivel el volumen a `destroy` y las listas de destrucción incluyen `lun_clone`, `file_clone`, La configuración de volumen anula la configuración de clon y todos los archivos FlexClone y las LUN FlexClone se pueden eliminar independientemente de la configuración de eliminación automática de los clones.

Pasos

1. Evite que un archivo FlexClone o una LUN de FlexClone específicos se eliminen automáticamente mediante el `volume file clone autodelete` comando.

El ejemplo siguiente muestra cómo puede deshabilitar la eliminación automática para FlexClone LUN `lun1_clone` contenido en `vol1`:

```
cluster1::> volume file clone autodelete -vserver vs1 -volume vol1
-clone-path lun1_clone -enable false
```

No se puede eliminar automáticamente un archivo FlexClone o una LUN FlexClone con la eliminación automática para reclamar espacio en el volumen.

2. Compruebe que la eliminación automática está deshabilitada para el archivo FlexClone o la LUN FlexClone mediante el `volume file clone show-autodelete` comando.

El ejemplo siguiente muestra que la eliminación automática es falsa para la LUN FlexClone `lun1_clone`:

```
cluster1::> volume file clone show-autodelete -vserver vs1 -clone-path
vol/vol1/lun1_clone

Name: vs1
Clone Path: vol/vol1/lun1_clone
Autodelete: false
Enabled: false
```

Comandos para configurar la eliminación de archivos FlexClone

Cuando los clientes eliminan archivos FlexClone sin usar el SDK de gestión de NetApp, puede utilizar el `volume file clone deletion` Comandos para permitir la eliminación más rápida de archivos FlexClone de un volumen de FlexVol. Se utilizan extensiones y un tamaño mínimo de los archivos FlexClone para permitir una eliminación más rápida.

Puede utilizar el `volume file clone deletion` Comandos para especificar una lista de extensiones compatibles y un requisito de tamaño mínimo para archivos FlexClone en un volumen. El método de eliminación más rápido se utiliza únicamente para archivos FlexClone que cumplen con los requisitos. En el caso de los archivos FlexClone que no cumplen con los requisitos, se utiliza el método de eliminación más lento.

Cuando los clientes eliminan archivos FlexClone y LUN FlexClone de un volumen mediante el SDK para facilitar la gestión de NetApp, no se aplican los requisitos de extensión y tamaño porque siempre se utiliza el método de eliminación más rápido.

| Para... | Se usa este comando... |
|---|--|
| Añada una extensión a la lista de extensiones admitidas del volumen | <code>volume file clone deletion add-extension</code> |
| Cambie el tamaño mínimo de los archivos FlexClone que se pueden eliminar del volumen mediante el método de eliminación más rápido | <code>volume file clone deletion modify</code> |
| Quite una extensión de la lista de extensiones compatibles del volumen | <code>volume file clone deletion remove-extension</code> |

| Para... | Se usa este comando... |
|--|--|
| Consulte la lista de extensiones admitida y el tamaño mínimo de los archivos FlexClone que los clientes pueden eliminar del volumen mediante el método de eliminación más rápido | <code>volume file clone deletion show</code> |

Para obtener información detallada sobre estos comandos, consulte la página man correspondiente.

Utilice qtrees para crear particiones de los volúmenes de FlexVol

Use qtrees para crear particiones de la descripción general de los volúmenes de FlexVol

Los qtrees permiten dividir los volúmenes de FlexVol en segmentos más pequeños que puede gestionar individualmente. Puede usar qtrees para gestionar cuotas, estilo de seguridad y bloqueos oportunistas CIFS.

ONTAP crea un qtree predeterminado, denominado *qtree0*, para cada volumen. Si no se colocan datos en un qtree, se encuentran en *qtree0*.

Los nombres de qtree no deben tener más de 64 caracteres.

No se pueden mover los directorios entre qtrees. Solo los archivos se pueden mover entre qtrees.

Si crea recursos compartidos a nivel de qtree y volumen en el mismo pool FlexVol o SCVMM, los qtrees aparecen como directorios en el recurso compartido de FlexVol. Por lo tanto, debe tener cuidado de no eliminarlos accidentalmente.

Obtenga una ruta de unión de qtree

Puede montar un qtree individual obteniendo la ruta de unión o la ruta de espacio de nombres del qtree. La ruta Qtree que se muestra con el comando de la CLI `qtree show -instance` tiene el formato `/vol/<volume_name>/<qtree_name>`. Sin embargo, esta ruta no hace referencia a la ruta de unión o la ruta de espacio de nombres del qtree.

Acerca de esta tarea

Debe conocer la ruta de unión del volumen para obtener la ruta de unión o la ruta de espacio de nombres del qtree.

Paso

1. Utilice la `vserver volume junction-path` comando para obtener la ruta de unión de un volumen.

En el siguiente ejemplo, se muestra la ruta de unión del volumen denominado vol1 ubicado en la máquina virtual de almacenamiento (SVM) denominada vs0:

```
cluster1::> volume show -volume vol1 -vserver vs0 -fields junction-path  
  
-----  
  
vs0 vol1 /vol1
```

En la salida anterior, la ruta de unión del volumen es /vol1. Como los qtrees siempre están anclados en el volumen, será la ruta de unión o la ruta de espacio de nombres del qtree /vol1/qtree1.

Restricciones en el nombre de qtree

Los nombres de qtree no pueden tener más de 64 caracteres. Además, el uso de algunos caracteres especiales en los nombres de qtree, como comas y espacios, puede ocasionar problemas con otras funcionalidades y debería evitarse.

["Obtenga más información sobre el comportamiento y las restricciones de la CLI al crear nombres de archivos".](#)

Convertir un directorio en un qtree

Convertir un directorio en una información general para qtree

Si tiene un directorio en la raíz de un volumen FlexVol que desea convertir en un qtree, debe migrar los datos del directorio a un nuevo qtree con el mismo nombre usando la aplicación cliente.

Acerca de esta tarea

Los pasos que se deben seguir para convertir un directorio en un qtree dependen del cliente que se use. El siguiente proceso describe las tareas generales que debe realizar:

Pasos

1. Cambie el nombre del directorio que se va a convertir en qtree.
2. Cree un nuevo qtree con el nombre de directorio original.
3. Utilice la aplicación cliente para mover el contenido del directorio al nuevo qtree.
4. Elimine el directorio ahora vacío.



No puede eliminar un directorio si está asociado a un recurso compartido de CIFS existente.

Convertir un directorio a un qtree mediante un cliente Windows

Para convertir un directorio en un qtree y utilizar un cliente Windows, debe cambiar el nombre del directorio, crear un qtree en el sistema de almacenamiento y mover el contenido del directorio al qtree.

Acerca de esta tarea

Debe utilizar el Explorador de Windows para este procedimiento. No se puede utilizar la interfaz de línea de

comandos de Windows ni el entorno de símbolo del sistema de dos.

Pasos

1. Abra el Explorador de Windows.
2. Haga clic en la representación de carpeta del directorio que desea cambiar.



El directorio debe residir en la raíz del volumen que lo contiene.

3. En el menú **Archivo**, seleccione **Cambiar nombre** para dar a este directorio un nombre diferente.
4. En el sistema de almacenamiento, utilice `volume qtree create` comando para crear un qtree nuevo con el nombre original del directorio.
5. En el Explorador de Windows, abra la carpeta de directorio cuyo nombre ha cambiado y seleccione los archivos que contiene.
6. Arrastre estos archivos a la representación de carpetas del nuevo qtree.



Cuanto más subcarpetas contenga la carpeta que esté moviendo, más tiempo durará la operación de movimiento.

7. En el menú **Archivo**, seleccione **Eliminar** para eliminar la carpeta de directorio ahora vacía cuyo nombre ha cambiado.

Convertir un directorio a un qtree mediante un cliente UNIX

Para convertir un directorio en un qtree de UNIX, debe cambiar el nombre del directorio, crear un qtree en el sistema de almacenamiento y mover el contenido del directorio al qtree.

Pasos

1. Abra una ventana de cliente UNIX.
2. Utilice la `mv` comando para cambiar el nombre del directorio.

```
client: mv /n/user1/vol1/dir1 /n/user1/vol1/olddir
```

3. Desde el sistema de almacenamiento, utilice `volume qtree create` comando para crear un qtree con el nombre original.

```
system1: volume qtree create /n/user1/vol1/dir1
```

4. Desde el cliente, utilice la `mv` comando para mover el contenido del directorio antiguo al qtree.



Cuanto más subdirectorios contenga un directorio que se esté moviendo, más tiempo tardará la operación de movimiento.

```
client: mv /n/user1/vol1/olddir/* /n/user1/vol1/dir1
```

5. Utilice la `rmdir` comando para eliminar el directorio antiguo, ahora vacío.

```
client: rmdir /n/user1/vol1/olddir
```

Después de terminar

Dependiendo de cómo implemente el cliente UNIX `mv` es posible que no se conserven la propiedad del archivo y los permisos. Si esto ocurre, actualice los propietarios y permisos de los archivos a sus valores anteriores.

Comandos para gestionar y configurar qtrees

Puede gestionar y configurar qtrees mediante comandos ONTAP específicos.

| Si desea... | Se usa este comando... |
|--|--|
| Cree un qtree | <code>volume qtree create</code> |
| Mostrar una lista filtrada de qtrees | <code>volume qtree show</code> |
| Eliminar un qtree | <code>volume qtree delete</code> <div> El comando <code>Qtree volume qtree delete</code> fallará a menos que el qtree esté vacío o el <code>-force true</code> se agrega el indicador.</div> |
| Modificar los permisos UNIX de un qtree | <code>volume qtree modify -unix-permissions</code> |
| Modifique la configuración de los bloqueos oportunistas CIFS de un qtree | <code>volume qtree oplocks</code> |
| Modificar la configuración de seguridad de un qtree | <code>volume qtree security</code> |
| Cambie el nombre a un qtree | <code>volume qtree rename</code> |
| Mostrar las estadísticas de un qtree | <code>volume qtree statistics</code> |
| Restablecer las estadísticas de un qtree | <code>volume qtree statistics -reset</code> |



La `volume rehost` el comando puede provocar errores en otras operaciones administrativas simultáneas dirigidas a ese volumen.

Generación de informes sobre el espacio lógico y cumplimiento para volúmenes

Información general sobre la generación de informes y el cumplimiento de requisitos de espacio lógico para volúmenes

A partir de ONTAP 9.4, puede permitir que se muestre a los usuarios el espacio lógico utilizado en un volumen y la cantidad de espacio de almacenamiento restante. A partir de ONTAP 9.5, puede limitar la cantidad de espacio lógico que consumen los usuarios.

La generación de informes y la aplicación de espacio lógico están deshabilitadas de forma predeterminada.

Los siguientes tipos de volumen admiten la generación de informes y la aplicación de espacio lógico.

| Tipo de volumen | ¿Se admite la generación de informes de espacio? | ¿Se admite la aplicación de espacio? |
|------------------------------------|---|--------------------------------------|
| Volúmenes de FlexVol | Sí, a partir de ONTAP 9.4 | Sí, a partir de ONTAP 9.5 |
| Volúmenes de destino de SnapMirror | Sí, a partir de ONTAP 9.8 | Sí, a partir de ONTAP 9.13.1 |
| Volúmenes de FlexGroup | Sí, a partir de ONTAP 9.9.1 | Sí, a partir de ONTAP 9.9.1 |
| Volúmenes de FlexCache | La configuración de origen se utiliza en la caché | No aplicable |

Qué muestra la generación de informes de espacio lógico

Cuando se habilita el informe de espacio lógico en un volumen, el sistema puede mostrar la cantidad de espacio lógico usado y disponible además del espacio total en un volumen. Además, los usuarios de sistemas cliente Linux y Windows pueden ver el espacio disponible y el utilizado lógico en lugar de los físicos utilizados y el espacio disponible físico.

Definiciones:

- El espacio físico hace referencia a los bloques físicos de almacenamiento disponibles o utilizados en el volumen.
- El espacio lógico hace referencia al espacio utilizable de un volumen.
- El espacio lógico utilizado es el espacio físico utilizado y el ahorro derivado de las funciones de eficiencia del almacenamiento (como la deduplicación y la compresión) que se han configurado.

A partir de ONTAP 9.5, puede habilitar el cumplimiento del espacio lógico junto con los informes de espacio.

Cuando está habilitada, la generación de informes de espacio lógico muestra los siguientes parámetros con el `volume show` comando:

| Parámetro | Significado |
|------------------------------------|---|
| <code>-logical-used</code> | Muestra información solo sobre el volumen o los volúmenes que tienen el tamaño lógico usado especificado. Este valor incluye todo el espacio ahorrado por las funciones de eficiencia del almacenamiento junto con el espacio físicamente utilizado. Esto no incluye la reserva de Snapshot pero sí considera el derrame de Snapshot. |
| <code>-logical-used-by-afs</code> | Muestra información solo sobre los volúmenes con el tamaño lógico especificado que utiliza el sistema de archivos activo. Este valor difiere del <code>-logical-used</code> Valor por la cantidad de derrame de instantánea que supera la reserva de Snapshot. |
| <code>-logical-available</code> | Cuando solo se activa la generación de informes de espacio lógico, solo se muestra el espacio físico disponible. Cuando la generación de informes de espacio y la aplicación están habilitadas, se muestra la cantidad de espacio libre disponible actualmente, y considera el espacio ahorrado por las funciones de eficiencia del almacenamiento como se está utilizando. Esto no incluye la reserva de Snapshot. |
| <code>-logical-used-percent</code> | <p>Muestra el porcentaje del actual <code>-logical-used</code> Valor con el tamaño aprovisionado, excluida la reserva de Snapshot del volumen.</p> <p>Este valor puede ser superior al 100%, porque el <code>-logical-used-by-afs</code> el valor incluye ahorros de eficiencia en el volumen. La <code>-logical-used-by-afs</code> El valor de un volumen no incluye el derrame de instantáneas como espacio usado. La <code>-physical-used</code> El valor de un volumen incluye el derrame de instantáneas como espacio utilizado.</p> |
| <code>-used</code> | Muestra la cantidad de espacio ocupado por los datos de usuario y los metadatos del sistema de archivos. Difiere de <code>physical-used</code> espacio por la suma del espacio que se reserva para futuras escrituras y el espacio que se ahorra mediante la eficiencia del almacenamiento del agregado. Incluye el exceso de copias de Snapshot (la cantidad de espacio mediante la que las copias Snapshot superan la reserva de Snapshot). No incluye la reserva de Snapshot. |

Al habilitar la generación de informes sobre el espacio lógico en la CLI, también se pueden mostrar los valores de espacio lógico usado (%) y espacio lógico en System Manager

Los sistemas cliente ven el espacio lógico mostrado como espacio "usado" en las siguientes pantallas del sistema:

- **Salida df** en sistemas Linux
- Detalles de espacio en Propiedades usando el Explorador de Windows en sistemas Windows.



Si la generación de informes sobre el espacio lógico está habilitada sin aplicar el espacio lógico, el total mostrado en los sistemas cliente puede ser mayor que el espacio aprovisionado.

¿Qué hace el cumplimiento del espacio lógico

Cuando se habilita la aplicación de espacio lógico en ONTAP 9.5 y versiones posteriores, ONTAP cuenta los bloques lógicos utilizados en un volumen para determinar la cantidad de espacio que aún está disponible en ese volumen. Si no hay espacio disponible en un volumen, el sistema devuelve un mensaje de error de ENOSPC (sin espacio).

La aplicación del espacio lógico garantiza que se notifique a los usuarios cuando un volumen está lleno o casi lleno. La aplicación lógica del espacio devuelve tres tipos de alertas para informarle acerca del espacio disponible en un volumen:

- `Monitor.vol.full.inc.sav`: Esta alerta se activa cuando se ha utilizado el 98% del espacio lógico en el volumen.
- `Monitor.vol.nearFull.inc.sav`: Esta alerta se activa cuando se ha utilizado el 95% del espacio lógico del volumen.
- `Vol.log.overalloc.inc.sav`: Esta alerta se activa cuando el espacio lógico utilizado en el volumen es mayor que el tamaño total del volumen.

Esta alerta indica que añadir al tamaño del volumen puede no crear espacio disponible, ya que dicho espacio ya estará consumido por bloques lógicos asignados en exceso.



El total (espacio lógico) debe ser igual al espacio aprovisionado, excepto la reserva de Snapshot del volumen con cumplimiento del espacio lógico.

Para obtener más información, consulte ["Configurar volúmenes para que proporcionen automáticamente más espacio cuando estén llenos"](#)

Habilite la generación de informes y la ejecución de espacio lógico

A partir de ONTAP 9.4, se puede habilitar la generación de informes de espacio lógico. A partir de la versión 9.5, puede habilitar el cumplimiento del espacio lógico, o bien la generación de informes y la aplicación juntos.

Acerca de esta tarea

Además de habilitar la generación de informes y la aplicación de espacio lógico en un nivel de volumen individual, puede habilitarlos a nivel de SVM para cada volumen que admita la funcionalidad. Si habilita las funciones de espacio lógico para toda la SVM, también puede deshabilitarlas para volúmenes individuales.

A partir de ONTAP 9.8, si se habilita la generación de informes de espacio lógico en un volumen de origen de SnapMirror, se habilita automáticamente en el volumen de destino después de la transferencia.

A partir de ONTAP 9.13.1, si la opción de aplicación se habilita en un volumen de origen de SnapMirror, el destino informará del consumo de espacio lógico y respetará su aplicación, lo que permitirá mejorar la planificación de la capacidad.



Si su versión de ONTAP es anterior a ONTAP 9.13.1, debe comprender que, aunque la configuración de aplicación se transfiere al volumen de destino de SnapMirror, el volumen de destino no admite la aplicación. Como resultado, el destino informará sobre el consumo de espacio lógico pero no respetará su cumplimiento.

Más información acerca de ["Compatibilidad de versiones de ONTAP para informes sobre el espacio lógico"](#).

Opciones

- Habilitar la generación de informes de espacio lógico para un volumen:

```
volume modify -vserver svm_name -volume volume_name -size volume_size -is  
-space-reporting-logical true
```

- Habilitar el cumplimiento de espacio lógico para un volumen:

```
volume modify -vserver svm_name -volume volume_name -size volume_size -is  
-space-enforcement-logical true
```

- Habilite la generación de informes y la aplicación de espacio lógico en un volumen:

```
volume modify -vserver svm_name -volume volume_name -size volume_size -is  
-space-reporting-logical true -is-space-enforcement-logical true
```

- Habilite la generación de informes o el cumplimiento de espacio lógico para una nueva SVM:

```
vserver create -vserver _svm_name_ -rootvolume root-_volume_name_ -rootvolume  
-security-style unix -data-services {desired-data-services} [-is-space-  
reporting-logical true] [-is-space-enforcement-logical true]
```

- Habilite la generación de informes o el cumplimiento de espacio lógico para una SVM existente:

```
vserver modify -vserver _svm_name_ {desired-data-services} [-is-space-  
reporting-logical true] [-is-space-enforcement-logical true]
```

Gestione los límites de capacidad de SVM

A partir de ONTAP 9.13.1, puede establecer una capacidad máxima para una máquina virtual de almacenamiento (SVM). También puede configurar alertas cuando la SVM se acerca a un nivel de umbral de capacidad.

Acerca de esta tarea

La capacidad de un SVM se calcula como la suma de FlexVols, Volúmenes FlexGroup, FlexClones y volúmenes de FlexCache. El cálculo de la capacidad afecta al volumen aunque estén restringidos, sin conexión o en la cola de recuperación después de la eliminación. Si hay volúmenes configurados con el crecimiento automático, el valor máximo de tamaño automático del volumen se calculará en el tamaño de la SVM; sin un crecimiento automático, se calculará el tamaño real del volumen.

La siguiente tabla captura cómo `autosize-mode` los parámetros afectan al cálculo de capacidad.

| | |
|--|--|
| <code>autosize-mode off</code> | El parámetro SIZE se utilizará para el cálculo |
| <code>autosize-mode grow</code> | La <code>max-autosize</code> el parámetro se utilizará para el cálculo |
| <code>autosize-mode grow-shrink</code> | La <code>max-autosize</code> el parámetro se utilizará para el cálculo |

Antes de empezar

- Para establecer un límite de las máquinas virtuales de almacenamiento, debe ser un administrador del

clúster.

- No pueden configurarse límites de almacenamiento para ninguna SVM que contenga volúmenes de protección de datos, volúmenes en una relación de SnapMirror o en una configuración de MetroCluster.
- Al migrar una SVM, la SVM de origen no puede tener un límite de almacenamiento habilitado. Para completar la operación de migración, desactive el límite de almacenamiento en el origen y, a continuación, complete la migración.
- La capacidad de la SVM es distinta de [cuotas](#). Las cuotas no pueden superar el tamaño máximo.
- No es posible establecer un límite de almacenamiento cuando haya otras operaciones en curso en la SVM. Utilice la `job show vservser svm_name` comando para ver trabajos existentes. Intente ejecutar el comando de nuevo cuando haya terminado algún trabajo.

Impacto en la capacidad

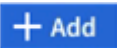
Cuando se alcanza el límite de capacidad, las operaciones siguientes fallarán:

- Creación de LUN, espacio de nombres o volumen
- Clonado de LUN, espacio de nombres o volumen
- Modificar un LUN, espacio de nombres o volumen
- Aumentando el tamaño de LUN, espacio de nombres o volumen
- Expansión de LUN, espacio de nombres o volumen
- Realojamiento de LUN, espacio de nombres o volumen

Establezca un límite de capacidad en una SVM nueva

System Manager

Pasos

1. Seleccione **Almacenamiento > VM de almacenamiento**.
2. Seleccione  Para crear la SVM.
3. Asigne un nombre a la SVM y seleccione un **Protocolo de acceso**.
4. En **Storage VM settings**, seleccione **Enable Maximum Capacity limit**.

Proporcione un tamaño de capacidad máximo para la SVM.

5. Seleccione **Guardar**.

CLI

Pasos

1. Cree la SVM. Para establecer un límite de almacenamiento, proporcione un `storage-limit` valor. Para configurar una alerta de umbral para el límite de almacenamiento, proporcione un valor de porcentaje para `-storage-limit-threshold-alert`.

```
vserver create -vserver vserver_name -aggregate aggregate_name -rootvolume root_volume_name -rootvolume-security-style {unix|ntfs|mixed} -storage -limit value [GiB|TiB] -storage-limit-threshold-alert percentage [-ipSPACE IPspace_name] [-language <language>] [-snapshot-policy snapshot_policy_name] [-quota-policy quota_policy_name] [-comment comment]
```

Si no proporciona valor de umbral, de forma predeterminada, se activará una alerta cuando la SVM se encuentre en un 90 % de su capacidad. Para deshabilitar la alerta de umbral, proporcione un valor de cero.

2. Confirme que la SVM se ha creado correctamente:

```
vserver show -vserver vserver_name
```

3. Si desea deshabilitar el límite de almacenamiento, modifique la SVM con `-storage-limit` parámetro definido en cero:

```
vserver modify -vserver vserver_name -storage-limit 0
```


Establezca o modifique un límite de capacidad en una SVM existente

Es posible establecer un límite de capacidad y una alerta de umbral en una SVM existente o deshabilitar un límite de capacidad.

Una vez que se configura el límite de capacidad, no se puede modificar el límite a un valor inferior a la capacidad asignada actualmente.

System Manager

Pasos

1. Seleccione **Almacenamiento > VM de almacenamiento**.
2. Seleccione la SVM que desea modificar. Junto al nombre de la SVM, seleccione  Luego **Editar**.
3. Para habilitar un límite de capacidad, seleccione la casilla situada junto a **Activar límite de capacidad**. Introduzca un valor para **Capacidad máxima** y un valor de porcentaje para **Umbral de alerta**.

Si desea desactivar el límite de capacidad, desmarque la casilla situada junto a **Habilitar límite de capacidad**.

4. Seleccione **Guardar**.

CLI

Pasos

1. En el clúster que aloja la SVM, emita el `vserver modify` comando. Proporcione un valor numérico para `-storage-limit` y un valor porcentual para `-storage-limit-threshold-alert`.

```
vserver modify -vserver vserver_name -storage-limit value [GiB|TiB]
-storage-limit-threshold-alert percentage
```

Si no se proporciona el valor de umbral, tendrá una alerta predeterminada al 90 % de capacidad. Para deshabilitar la alerta de umbral, proporcione un valor de cero.

2. Si desea deshabilitar el límite de almacenamiento, modifique la SVM con `-storage-limit` establecer en cero:

```
vserver modify -vserver vserver_name -storage-limit 0
```

Alcanzar los límites de capacidad

Cuando alcance la capacidad máxima o el umbral de alerta, puede consultar el `vserver.storage.threshold` Mensajes EMS o utilice la página **Insights** en System Manager para obtener información sobre posibles acciones. Las posibles soluciones incluyen:

- Edite los límites de capacidad máxima de SVM
- Purgado de la cola de recuperación de volúmenes para liberar espacio
- Elimine la snapshot para proporcionar espacio para el volumen

Información adicional

- [Mediciones de capacidad en System Manager](#)
- [Supervise la capacidad en System Manager](#)

Utilice cuotas para restringir o realizar un seguimiento del uso de los recursos

Descripción general del proceso de cuotas

Proceso de cuotas

Las cuotas proporcionan una forma de restringir o realizar un seguimiento del espacio en disco y del número de archivos que usan los usuarios, grupos o qtrees. Las cuotas se aplican a un volumen o qtree de FlexVol concreto.

Las cuotas pueden ser suaves o duras. Las cuotas blandas hacen que ONTAP envíe una notificación cuando se superen los límites especificados y las cuotas rígidas evitan que una operación de escritura tenga éxito cuando se superen los límites especificados.

Cuando ONTAP recibe una solicitud de un usuario o grupo de usuarios para escribir en un volumen de FlexVol, comprueba si se activan las cuotas en ese volumen para el usuario o el grupo de usuarios y determina lo siguiente:

- Si se alcanzará el límite rígido

En caso afirmativo, la operación de escritura falla cuando se alcanza el límite rígido y se envía la notificación de cuota dura.

- Si se incumplido el límite blando

Si la respuesta es sí, la operación de escritura se realiza correctamente cuando se cumple el límite de software y se envía la notificación de cuota de software.

- Si una operación de escritura no superará el límite de software

Si la respuesta es sí, la operación de escritura es correcta y no se envía ninguna notificación.

Diferencias entre cuotas duras, blandas y umbrales

Las cuotas rígidas impiden las operaciones mientras que las cuotas blandas activan las notificaciones.

Las cuotas estrictas imponen un límite duro a los recursos del sistema; cualquier operación que pueda resultar en superar el límite falla. Los siguientes ajustes crean cuotas rígidas:

- Parámetro límite de discos
- Parámetro límite de archivos

Las cuotas suaves envían un mensaje de advertencia cuando el uso de recursos alcanza un cierto nivel, pero no afectan a las operaciones de acceso a datos, por lo que puede tomar las acciones apropiadas antes de que se supere la cuota. Los siguientes ajustes crean cuotas programables:

- Umbral del parámetro Disk Limit
- Parámetro límite de disco duro
- Parámetro límite de archivos de software

Las cuotas de umbral y de disco duro permiten a los administradores recibir más de una notificación sobre una cuota. Normalmente, los administradores establecen el umbral del límite de disco en un valor que es sólo ligeramente inferior al límite de disco, de modo que el umbral proporciona una "advertencia final" antes de que las escrituras empiecen a fallar.

Acerca de las notificaciones de cuotas

Las notificaciones de cuota son mensajes que se envían al sistema de gestión de eventos (EMS) y también se configuran como capturas SNMP.

Las notificaciones se envían en respuesta a los siguientes eventos:

- Se alcanza una cuota dura; en otras palabras, se intenta superarla
- Se supera una cuota suave
- Ya no se supera una cuota blanda

Los umbrales son ligeramente diferentes de los de otras cuotas blandas. Los umbrales desencadenan notificaciones sólo cuando se superan, no cuando ya no se superan.

Las notificaciones de cuota fija se pueden configurar mediante el comando `volume quota modify`. Puede desactivarlas completamente y puede cambiar su frecuencia, por ejemplo, para evitar el envío de mensajes redundantes.

Las notificaciones de cuotas blandas no se pueden configurar porque es poco probable que generen mensajes redundantes y su único propósito es la notificación.

En la siguiente tabla se enumeran los eventos que las cuotas envían al sistema EMS:

| Cuando se produce esto... | Este evento se envía al EMS... |
|---|--|
| Se alcanza un límite duro en una cuota de árbol | <code>wafl.quota.qtree.exceeded</code> |
| Se alcanza un límite rígido en una cuota de usuario en el volumen | <code>wafl.quota.user.exceeded</code> (Para un usuario UNIX) <code>wafl.quota.user.exceeded.win</code> (Para un usuario de Windows) |
| Se alcanza un límite rígido en una cuota de usuario en un qtree | <code>wafl.quota.userQtree.exceeded</code> (Para un usuario UNIX) <code>wafl.quota.userQtree.exceeded.win</code> (Para un usuario de Windows) |
| Un límite duro se alcanza en una cuota de grupo en el volumen | <code>wafl.quota.group.exceeded</code> |
| Un límite duro se alcanza en una cuota de grupo en un qtree | <code>wafl.quota.groupQtree.exceeded</code> |
| Se supera un límite suave, incluido un umbral | <code>quota.softlimit.exceeded</code> |
| Ya no se supera un límite suave | <code>quota.softlimit.normal</code> |

En la tabla siguiente se enumeran las capturas SNMP que generan las cuotas:

| Cuando se produce esto... | Esta captura SNMP se envía... |
|---|-----------------------------------|
| Se alcanza un límite rígido | QuotaExceeded |
| Se supera un límite suave, incluido un umbral | QuotaExceeded y softQuotaExceeded |
| Ya no se supera un límite suave | QuotaNormal y softQuotaNormal |



Las notificaciones contienen números de ID de qtree en lugar de nombres de qtree. Es posible correlacionar los nombres de qtree con números de ID mediante el `volume qtree show -id` comando.

Por qué se usan cuotas

Puede utilizar las cuotas para limitar el uso de recursos en volúmenes de FlexVol, para proporcionar una notificación cuando el uso de los recursos alcanza niveles específicos o para realizar un seguimiento del uso de los recursos.

Se especifica una cuota por los siguientes motivos:

- Para limitar la cantidad de espacio en disco o el número de archivos que puede utilizar un usuario o grupo, o que puede contener un qtree
- Para realizar el seguimiento de la cantidad de espacio en disco o del número de archivos que usan los usuarios, un grupo o un qtree, sin fijar un límite
- Para advertir a los usuarios cuando su uso de disco o uso de archivo es alto

Utilice cuotas predeterminadas, explícitas, derivadas y de seguimiento para gestionar el uso del disco de la forma más eficaz.

Qué son las reglas de cuotas, las políticas de cuotas y las cuotas

Las cuotas se definen en reglas de cuotas específicas de los volúmenes de FlexVol. Estas reglas de cuota se recogen en una política de cuotas de una máquina virtual de almacenamiento (SVM) y, a continuación, se activan en cada volumen del SVM.

Una regla de cuota siempre es específica de un volumen. Las reglas de cuota no tienen efecto hasta que se activan las cuotas en el volumen definido en la regla de cuota.

Una política de cuota es una colección de reglas de cuota para todos los volúmenes de una SVM. Las políticas de cuotas no se comparten entre las SVM. Una SVM puede tener hasta cinco políticas de cuota, lo que le permite tener copias de backup de políticas de cuotas. Se asigna una política de cuota a una SVM en cualquier momento.

Una cuota es la restricción real que ONTAP impone o el seguimiento real que ONTAP realiza. Una regla de cuota siempre da como resultado al menos una cuota y podría dar lugar a muchas cuotas derivadas adicionales. La lista completa de cuotas forzadas sólo es visible en los informes de cuotas.

La activación es el proceso de activación de ONTAP para crear cuotas impuestas a partir del conjunto actual de reglas de cuotas en la política de cuotas asignada. La activación se produce volumen por volumen. La primera activación de cuotas en un volumen se denomina inicialización. Las activaciones posteriores se

denominan reinicialización o cambio de tamaño, según el alcance de los cambios.




Cuando se inicializa o cambia el tamaño de las cuotas en un volumen, se activan las reglas de cuota en la política de cuotas que está actualmente asignada a la SVM.

Tipos y objetivos de cuota

Las cuotas tienen un tipo: Pueden ser usuario, grupo o árbol. Los destinos de cuota especifican el usuario, el grupo o el qtree para los que se aplican los límites de cuota.

En la siguiente tabla se enumeran los tipos de objetivos de cuota, los tipos de cuotas a los que está asociado cada destino de cuota y cómo se representa cada destino de cuota:

| Destino de cuota | Tipo de cuota | Cómo se representa el destino | Notas |
|------------------|--|--|---|
| usuario | cuota de usuario | Nombre de usuario UNIX UID Un archivo o directorio cuyo UID coincida con el usuario Nombre de usuario de Windows en formato anterior a Windows 2000 SID de Windows Un archivo o directorio con una ACL propiedad del SID del usuario | Pueden aplicarse cuotas de usuario para un volumen o un qtree concreto. |
| grupo | cuota de grupo | Nombre UNIX GID de grupo Un archivo o directorio cuyo GID coincida con el grupo | Las cuotas de grupo se pueden aplicar para un volumen o un qtree específicos.  ONTAP no aplica cuotas de grupos basadas en los ID de Windows. |
| qtree | cuota de árbol | nombre del qtree | Las cuotas de árbol se aplican a un volumen concreto y no afectan a los qtrees de otros volúmenes. |
| "" | cuota de usuario quotagroup cuota de árbol | Comillas dobles ("") | Un destino de cuota de "" indica una cuota <i>default</i> . Para cuotas predeterminadas, el tipo de cuota está determinado por el valor del campo de tipo. |

Tipos especiales de cuotas

Cómo funcionan las cuotas predeterminadas

Puede utilizar cuotas predeterminadas para aplicar una cuota a todas las instancias de un determinado tipo de cuota. Por ejemplo, una cuota de usuario predeterminada afecta a todos los usuarios del sistema para el volumen o qtree de FlexVol especificado. Además, las cuotas predeterminadas le permiten modificar fácilmente sus cuotas.

Puede utilizar cuotas predeterminadas para aplicar automáticamente un límite a un gran conjunto de destinos de cuota sin tener que crear cuotas independientes para cada destino. Por ejemplo, si desea limitar la mayoría de los usuarios a 10 GB de espacio en disco, puede especificar una cuota de usuario predeterminada de 10 GB de espacio en disco en lugar de crear una cuota para cada usuario. Si tiene usuarios específicos para los que desea aplicar un límite diferente, puede crear cuotas explícitas para esos usuarios. (Cuotas explícitas --cuotas con un destino o lista de destinos específicos—anulan las cuotas predeterminadas.)

Además, las cuotas predeterminadas le permiten utilizar el cambio de tamaño en lugar de la reinicialización cuando desea que los cambios de cuota surtan efecto. Por ejemplo, si se agrega una cuota de usuario explícita a un volumen que ya tiene una cuota de usuario predeterminada, se puede activar la nueva cuota mediante el cambio de tamaño.

Las cuotas predeterminadas se pueden aplicar a los tres tipos de destino de cuota (usuarios, grupos y qtrees).

Las cuotas predeterminadas no tienen necesariamente límites especificados; una cuota predeterminada puede ser una cuota de seguimiento.

Una cuota se indica mediante un destino que es una cadena vacía ("") o un asterisco (*), según el contexto:

- Cuando se crea una cuota mediante `volume quota policy rule create` comando, establecer el `-target` el parámetro de una cadena vacía ("") crea una cuota predeterminada.
- En la `volume quota policy rule create` comando, el `-qtree` parámetro especifica el nombre del qtree al que se aplica la regla de cuota. Este parámetro no se aplica a las reglas de tipo de árbol. Para las reglas de tipo de usuario o grupo en el nivel de volumen, este parámetro debe contener "".
- En el resultado del `volume quota policy rule show` comando, aparece una cuota predeterminada con una cadena vacía ("") como destino.
- En el resultado del `volume quota report` Comando, aparece una cuota predeterminada con un asterisco (*) como ID y especificador de cuota.

Ejemplo de cuota de usuario predeterminada

La siguiente regla de cuota utiliza una cuota de usuario predeterminada para aplicar un límite de 50 MB a cada usuario para vol1:


```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "" -qtree "" -disk-limit 50m

cluster1::> volume quota policy rule show -vserver vs0 -volume vol1
```

| | | | | | | | |
|--------------|--------|-------|-----------------|-------|-------|--------------|-------|
| Vserver: vs0 | | | Policy: default | | | Volume: vol1 | |
| | | | | | Soft | | Soft |
| | | | User | Disk | Disk | Files | Files |
| Type | Target | Qtree | Mapping | Limit | Limit | Limit | Limit |
| Threshold | | | | | | | |
| ----- | ----- | ----- | ----- | ----- | ----- | ----- | ----- |
| ----- | ----- | | | | | | |
| user | "" | "" | off | 50MB | - | - | - |
| - | | | | | | | |

Si algún usuario del sistema introduce un comando que haría que los datos del usuario tomaran más de 50 MB en vol1 (por ejemplo, escribir en un archivo desde un editor), el comando falla.

Cómo se utilizan cuotas explícitas

Puede utilizar cuotas explícitas para especificar una cuota para un destino de cuota específico o para anular una cuota predeterminada para un destino específico.

Una cuota explícita especifica un límite para un usuario, grupo o qtree concreto. Una cuota explícita reemplaza cualquier cuota predeterminada que esté en vigor para el mismo destino.

Cuando agrega una cuota de usuario explícita para un usuario que tiene una cuota de usuario derivada, debe utilizar la misma configuración de asignación de usuario que la cuota de usuario predeterminada. De lo contrario, al cambiar el tamaño de las cuotas, se rechaza la cuota de usuario explícita porque se considera una cuota nueva.

Las cuotas explícitas solo afectan a las cuotas predeterminadas al mismo nivel (volumen o qtree). Por ejemplo, una cuota de usuario explícita para un qtree no afecta a la cuota de usuario predeterminada del volumen en el que contiene dicho qtree. Sin embargo, la cuota de usuario explícita para el qtree anula (sustituye los límites definidos por) la cuota de usuario predeterminada para ese qtree.

Ejemplos de cuotas explícitas

Las siguientes reglas de cuota definen una cuota de usuario predeterminada que limita todos los usuarios de vol1 a 50MB de espacio. Sin embargo, a un usuario, jsmith, se le permite 80MB GB de espacio, debido a la cuota explícita (que se muestra en **negrita**):

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "" -qtree "" -disk-limit 50m

cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "jsmith" -qtree "" -disk-limit 80m

cluster1::> volume quota policy rule show -vserver vs0 -volume vol1
```

| Vserver: vs0 | | | Policy: default | | | Volume: vol1 | |
|--------------|--------|-------|-----------------|------------|-----------------|--------------|------------------|
| Type | Target | Qtree | User Mapping | Disk Limit | Soft Disk Limit | Files Limit | Soft Files Limit |
| user | "" | "" | off | 50MB | - | - | - |
| user | jsmith | "" | off | 80MB | - | - | - |

La siguiente regla de cuota restringe el usuario especificado, representado por cuatro ID, a 550MB GB de espacio en disco y a 10.000 GB en el volumen vol1:

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "
jsmith,corp\jsmith,engineering\john smith,S-1-5-32-544" -qtree "" -disk
-limit 550m -file-limit 10000

cluster1::> volume quota policy rule show -vserver vs0 -volume vol1
```

| Vserver: vs0 | | | Policy: default | | | Volume: vol1 | |
|--------------|--|-------|-----------------|------------|-----------------|--------------|------------------|
| Type | Target | Qtree | User Mapping | Disk Limit | Soft Disk Limit | Files Limit | Soft Files Limit |
| user | "jsmith,corp\jsmith,engineering\john smith,S-1-5-32-544" | "" | off | 550MB | - | 10000 | - |

La siguiente regla de cuota restringe el grupo ENG1 a 150MB GB de espacio en disco y un número ilimitado de archivos en el qtree proj1:

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol2
-policy-name default -type group -target "eng1" -qtree "proj1" -disk-limit
150m
```

```
cluster1::> volume quota policy rule show -vserver vs0 -volume vol2
```

| | | | | | | | |
|--------------|--------|-------|-----------------|-------|-------|--------------|-------|
| Vserver: vs0 | | | Policy: default | | | Volume: vol2 | |
| | | | | | Soft | | Soft |
| | | | User | Disk | Disk | Files | Files |
| Type | Target | Qtree | Mapping | Limit | Limit | Limit | Limit |
| Threshold | | | | | | | |
| ----- | ----- | ----- | ----- | ----- | ----- | ----- | ----- |
| ----- | | | | | | | |
| group | eng1 | proj1 | off | 150MB | - | - | - |
| - | | | | | | | |

La siguiente regla de cuota restringe el qtree de proj1 TB del volumen vol2 a 750MB GB de espacio en disco y archivos 75.000 GB:

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol2
-policy-name default -type tree -target "proj1" -disk-limit 750m -file
-limit 75000
```

```
cluster1::> volume quota policy rule show -vserver vs0 -volume vol2
```

| | | | | | | | |
|--------------|--------|-------|-----------------|-------|-------|--------------|-------|
| Vserver: vs0 | | | Policy: default | | | Volume: vol2 | |
| | | | | | Soft | | Soft |
| | | | User | Disk | Disk | Files | Files |
| Type | Target | Qtree | Mapping | Limit | Limit | Limit | Limit |
| Threshold | | | | | | | |
| ----- | ----- | ----- | ----- | ----- | ----- | ----- | ----- |
| ----- | | | | | | | |
| tree | proj1 | "" | - | 750MB | - | 75000 | - |
| - | | | | | | | |

Cómo funcionan las cuotas derivadas

Una cuota impuesta como resultado de una cuota predeterminada, en lugar de una cuota explícita (una cuota con un objetivo específico), se denomina cuota derivada_.

El número y la ubicación de las cuotas derivadas dependen del tipo de cuota:

- Una cuota de árbol predeterminada de un volumen crea cuotas de árbol predeterminadas derivadas para cada qtree del volumen.
- Una cuota de usuario o de grupo predeterminada crea una cuota de usuario o grupo derivada para cada

usuario o grupo al que pertenece un archivo en el mismo nivel (volumen o qtree).

- Una cuota de usuario o de grupo predeterminada en un volumen crea una cuota de usuario o grupos predeterminada derivada en cada qtree que también tiene una cuota de árbol.

La configuración (incluidos los límites y la asignación de usuarios) de las cuotas derivadas es la misma que la configuración de las cuotas predeterminadas correspondientes. Por ejemplo, una cuota de árbol predeterminada con un límite de disco de 20 GB en un volumen crea cuotas de árbol derivadas con límites de disco de 20 GB en los qtrees del volumen. Si una cuota predeterminada es una cuota de seguimiento (sin límites), las cuotas derivadas también realizan un seguimiento de las cuotas.

Para ver las cuotas derivadas, puede generar un informe de cuotas. En el informe, un usuario derivado o cuota de grupo se indica mediante un especificador de cuota que está en blanco o un asterisco (*). Sin embargo, una cuota de árbol derivada tiene un especificador de cuota; para identificar una cuota de árbol derivada, debe buscar una cuota de árbol predeterminada en el volumen con los mismos límites.

Las cuotas explícitas interactúan con las cuotas derivadas de las siguientes formas:

- Las cuotas derivadas no se crean si ya existe una cuota explícita para el mismo destino.
- Si existe una cuota derivada al crear una cuota explícita para un destino, puede activar la cuota explícita cambiando el tamaño en lugar de tener que realizar una inicialización completa de la cuota.

Cómo se utilizan las cuotas de seguimiento

El seguimiento de las cuotas genera informes de uso de disco y archivo y no limita el uso de recursos. Cuando se utilizan las cuotas de seguimiento, la modificación de los valores de cuota resulta menos disruptiva, ya que puede cambiar el tamaño de las cuotas en lugar de desactivarlas y volver a ponerlas.

Para crear una cuota de seguimiento, se omiten los parámetros límite de disco y límite de archivos. Esto indica a ONTAP que supervise el uso de discos y archivos para ese destino a ese nivel (volumen o qtree) sin imponer límites. Las cuotas de seguimiento se indican en la salida de `show` comandos y el informe de cuotas con un guión ("-") para todos los límites. ONTAP crea cuotas de seguimiento automáticamente cuando utiliza la interfaz de usuario de System Manager para crear cuotas explícitas (cuotas con destinos específicos). Cuando se utiliza la CLI, el administrador de almacenamiento crea cuotas de seguimiento además de las cuotas explícitas.

También puede especificar una cuota de seguimiento *default*, que se aplica a todas las instancias del destino. Las cuotas de seguimiento predeterminadas le permiten realizar un seguimiento del uso de todas las instancias de un tipo de cuota (por ejemplo, todos los qtrees o todos los usuarios). Además, le permiten utilizar el cambio de tamaño en lugar de la reinicialización cuando desea que los cambios de cuota surtan efecto.

Ejemplos

El resultado de una regla de seguimiento muestra las cuotas vigentes para un qtree, usuario y grupo, como se muestra en el siguiente ejemplo de una regla de seguimiento a nivel de volumen:

| Vserver: vs0 | | | Policy: default | | | Volume: fv1 | | |
|--------------|--------|-------|-----------------|-------|--------------|-------------|---------------|-----------|
| Type | Target | Qtree | User | Disk | Soft Disk | Files | Soft Files | Threshold |
| | | | Mapping | Limit | Limit | Limit | Limit | |
| ----- | ----- | ----- | ----- | ----- | ----- | ----- | ----- | ----- |
| tree | "" | "" | - | - | - | - | - | - |
| user | "" | "" | off | - | - | - | - | - |
| group | "" | "" | - | - | - | - | - | - |

Cómo se aplican las cuotas

Al comprender cómo se aplican las cuotas, puede configurar cuotas y establecer los límites esperados.

Cada vez que se intenta crear un archivo o escribir datos en un archivo de un volumen de FlexVol con cuotas habilitadas, se comprueban los límites de cuotas antes del avance de la operación. Si la operación supera el límite de disco o el límite de archivos, se impedirá la operación.

Los límites de cuota se comprueban en el siguiente orden:

1. La cuota de árbol para ese qtree (esta comprobación no es relevante si el archivo se está creando o escribiendo en qtree0).
2. La cuota de usuario del usuario al que pertenece el archivo en el volumen
3. La cuota de grupo del grupo al que pertenece el archivo en el volumen
4. La cuota de usuario del usuario al que pertenece el archivo en el qtree (esta comprobación no es relevante si el archivo se crea o se escribe en qtree0).
5. La cuota de grupo del grupo al que pertenece el archivo en el qtree (esta comprobación no es relevante si el archivo se crea o se escribe en qtree0).

Puede que la cuota con el límite más pequeño no sea la que se supere primero. Por ejemplo, si una cuota de usuario para el volumen vol1 es 100 GB, Además, la cuota de usuario para el segundo qtree que contiene el volumen vol1 es de 20 GB. Se podría llegar al límite de volumen primero si ese usuario ya ha escrito más de 80 GB de datos en el volumen vol1 (pero fuera del segundo trimestre del qtree).

Consideraciones a tener en cuenta para asignar políticas de cuota

Una política de cuota es un grupo de las reglas de cuota para todos los volúmenes de FlexVol de una SVM. Debe tener en cuenta ciertas consideraciones al asignar las políticas de cuota.

- Una SVM tiene una política de cuotas asignada en cualquier momento. Cuando se crea una SVM, se crea una política de cuota vacía y se asigna a la SVM. Esta política de cuota predeterminada tiene el nombre "default" a menos que se especifique otro nombre cuando se crea la SVM.
- Un SVM puede tener hasta cinco políticas de cuotas. Si un SVM tiene cinco políticas de cuotas, no se puede crear una nueva política de cuotas para la SVM hasta que se elimine una política de cuotas existente.

- Cuando necesite crear una regla de cuota o cambiar reglas de cuota para una política de cuota, puede elegir cualquiera de los siguientes enfoques:
 - Si está trabajando en una política de cuota que está asignada a una SVM, no necesita asignar la política de cuota a la SVM.
 - Si está trabajando en una política de cuota sin asignar y luego asigna la política de cuota al SVM, debe tener un backup de la política de cuota a la que puede revertir si es necesario.

Por ejemplo, puede realizar una copia de la política de cuotas asignada, cambiar la copia, asignar la copia a la SVM y cambiar el nombre de la política de cuotas original.

- Puede cambiar el nombre de una política de cuotas incluso aunque se asigne a la SVM.

Cómo funcionan las cuotas con usuarios y grupos

Información general sobre cómo funcionan las cuotas con usuarios y grupos

Cuando se especifica un usuario o grupo como destino de una cuota, los límites impuestos por esa cuota se aplican a ese usuario o grupo. Sin embargo, algunos grupos especiales y usuarios se gestionan de forma diferente. Existen diferentes formas de especificar ID para los usuarios, según su entorno.

Cómo se especifican usuarios UNIX para las cuotas

Puede especificar un usuario UNIX para una cuota utilizando uno de tres formatos: El nombre de usuario, el UID o un archivo o directorio propiedad del usuario.

Para especificar un usuario UNIX para una cuota, puede utilizar uno de los siguientes formatos:

- El nombre de usuario, como jsmith.



No puede utilizar un nombre de usuario UNIX para especificar una cuota si ese nombre incluye una barra invertida (\) o un signo @. Esto se debe a que ONTAP trata los nombres que contienen estos caracteres como nombres de Windows.

- El UID, como 20.
- La ruta de un archivo o directorio que pertenezca a ese usuario, de manera que el UID del archivo coincida con el usuario.



Si especifica un nombre de archivo o directorio, debe seleccionar un archivo o directorio que durará tanto como la cuenta de usuario permanezca en el sistema.

La especificación de un nombre de archivo o directorio para el UID no hace que ONTAP aplique una cuota a ese archivo o directorio.

Cómo se especifican usuarios de Windows para las cuotas

Puede especificar un usuario de Windows para una cuota utilizando uno de tres formatos: El nombre de Windows en formato anterior a Windows 2000, el SID o un archivo o directorio propiedad del SID del usuario.

Para especificar un usuario de Windows para una cuota, puede utilizar uno de los siguientes formatos:

- El nombre de Windows en formato anterior a Windows 2000.
- El identificador de seguridad (SID), tal como muestra Windows en formato de texto, como S-1-5-32-544.
- Nombre de un archivo o directorio que tiene una ACL propiedad del SID de ese usuario.



Si especifica un nombre de archivo o directorio, debe seleccionar un archivo o directorio que durará tanto como la cuenta de usuario permanezca en el sistema.

Para que ONTAP obtenga el SID de la ACL, la ACL debe ser válida.

Si el archivo o directorio existe en un qtree de estilo UNIX o si el sistema de almacenamiento utiliza el modo UNIX para la autenticación de usuarios, ONTAP aplica la cuota de usuario al usuario cuyo **UID**, no SID, coincide con el del archivo o directorio.

La especificación de un nombre de archivo o directorio para identificar a un usuario para una cuota no hace que ONTAP aplique una cuota a ese archivo o directorio.

Cómo crean cuotas derivadas las cuotas de usuario y de grupo predeterminadas

Cuando se crean cuotas predeterminadas de usuarios o grupos, las cuotas de usuarios o grupos correspondientes se crean automáticamente para cada usuario o grupo al que pertenecen archivos en el mismo nivel.

Las cuotas de usuarios y grupos derivadas se crean de las siguientes formas:

- Una cuota de usuario predeterminada en un volumen de FlexVol crea cuotas de usuario derivadas para cada usuario al que pertenece un archivo en cualquier parte del volumen.
- Una cuota de usuario predeterminada en un qtree crea cuotas de usuario derivadas para cada usuario al que pertenece un archivo en el qtree.
- Una cuota de grupo predeterminada en un volumen FlexVol crea cuotas de grupo derivadas para cada grupo al que pertenece un archivo en cualquier parte del volumen.
- Una cuota de grupo predeterminada en un qtree crea cuotas de grupo derivadas para cada grupo al que pertenece un archivo en el qtree.

Si un usuario o grupo no posee archivos en el nivel de una cuota de grupo o de usuario predeterminada, no se crean cuotas derivadas para el usuario o grupo. Por ejemplo, si se crea una cuota de usuario predeterminada para el proyecto de qtree 1 y el jsmith de usuario es propietario de archivos en un qtree diferente, no se crea ninguna cuota de usuario derivada para jsmith.

Las cuotas derivadas tienen la misma configuración que las cuotas predeterminadas, incluidos los límites y la asignación de usuarios. Por ejemplo, si una cuota de usuario predeterminada tiene un límite de disco de 50 MB y tiene activada la asignación de usuarios, todas las cuotas derivadas resultantes también tienen un límite de disco de 50 MB y la asignación de usuarios activada.

Sin embargo, no existen límites en las cuotas derivadas para tres usuarios y grupos especiales. Si los siguientes usuarios y grupos poseen archivos en el nivel de una cuota de grupo o de usuario predeterminada, se crea una cuota derivada con la misma configuración de asignación de usuario que la cuota de grupo o usuario predeterminada, pero sólo es una cuota de seguimiento (sin límites):

- Usuario raíz UNIX (UID 0)

- Grupo raíz UNIX (GID 0)
- Grupo BUILTIN\Administradores de Windows

Puesto que se realiza un seguimiento de las cuotas para los grupos de Windows como cuotas de usuario, una cuota derivada para este grupo es una cuota de usuario derivada de una cuota de usuario predeterminada, no de una cuota de grupo predeterminada.

Ejemplo de cuotas de usuario derivadas

Si tiene un volumen en el que tres usuarios (archivos root, jsmith y bob) son propios y crea una cuota de usuario predeterminada en el volumen, ONTAP crea automáticamente tres cuotas de usuario derivadas. Por lo tanto, después de reiniciar las cuotas en el volumen, aparecen cuatro nuevas cuotas en el informe de cuotas:

```
cluster1::> volume quota report
Vserver: vs1
```

| Volume | Tree | Type | ID | ----Disk---- | | ----Files----- | | Quota |
|-----------|-------|-------|--------|--------------|-------|----------------|-------|-------|
| | | | | Used | Limit | Used | Limit | |
| Specifier | | | | | | | | |
| ----- | ----- | ----- | ----- | ----- | ----- | ----- | ----- | |
| vol1 | | user | * | 0B | 50MB | 0 | - | * |
| vol1 | | user | root | 5B | - | 1 | - | |
| vol1 | | user | jsmith | 30B | 50MB | 10 | - | * |
| vol1 | | user | bob | 40B | 50MB | 15 | - | * |

4 entries were displayed.

La primera línea nueva es la cuota de usuario predeterminada que ha creado, que puede identificarse con el asterisco (*) como ID. Las otras líneas nuevas son las cuotas de usuario derivadas. Las cuotas derivadas para jsmith y bob tienen el mismo límite de disco de 50 MB que la cuota predeterminada. La cuota derivada para el usuario raíz es una cuota de seguimiento sin límites.

Cómo se aplican las cuotas al usuario raíz

El usuario raíz (UID=0) de los clientes UNIX está sujeto a cuotas de árbol, pero no a cuotas de usuario o cuotas de grupo. Esto permite que el usuario raíz realice acciones en nombre de otros usuarios que de otro modo serían evitados por una cuota.

Cuando root realiza un cambio de propiedad de archivos o directorios u otras operaciones (como UNIX `chown` Comando) en nombre de un usuario con menos privilegios, ONTAP comprueba las cuotas según el nuevo propietario, pero no informa de errores ni detiene la operación, incluso si se exceden las restricciones de cuota rígida del nuevo propietario. Esto puede ser útil cuando una acción administrativa, como la recuperación de datos perdidos, resulta en exceder temporalmente las cuotas.



Sin embargo, una vez realizada la transferencia de propiedad, un sistema cliente informará de un error de espacio en disco si el usuario intenta asignar más espacio en disco mientras se supera la cuota.

Cómo funcionan las cuotas con grupos especiales de Windows

Las cuotas se aplican al grupo Everyone y al grupo BUILTIN\Administrators de forma diferente que a otros grupos de Windows.

En la siguiente lista se describe lo que ocurre si el destino de cuota es un identificador de grupo especial de Windows:

- Si el destino de cuota es el grupo Everyone, un archivo cuyo ACL muestra que el propietario es todos se cuenta bajo el SID para todos.
- Si el destino de cuota es BUILTIN\Administrators, la entrada se considera una cuota de usuario, sólo para el seguimiento.

No puede imponer restricciones a BUILTIN\Administrators.

Si un miembro de BUILTIN\Administrators crea un archivo, éste es propiedad de BUILTIN\Administrators y se cuenta bajo el SID de BUILTIN\Administrators, no el SID personal del usuario.



ONTAP no admite cuotas de grupos basadas en los ID de grupos de Windows. Si especifica un identificador de grupo de Windows como destino de cuota, la cuota se considera una cuota de usuario.

Cómo se aplican las cuotas a los usuarios con múltiples ID

Un usuario puede estar representado por varios ID. Puede configurar una única cuota de usuario para dicho usuario especificando una lista de ID como destino de cuota. Un archivo que pertenece a cualquiera de estos ID está sujeto a la restricción de la cuota de usuario.

Supongamos que un usuario tiene el UID de UNIX 20 y los Id corp\john_smith de Windows y engineering\jsmith. Para este usuario, puede especificar una cuota en la que el destino de cuota sea una lista de UID e Id. De Windows. Cuando este usuario escribe en el sistema de almacenamiento, se aplica la cuota especificada, independientemente de si la escritura se origina en UID 20, corp\john_smith o engineering\jsmith.



Las reglas de cuota independientes se consideran destinos independientes, incluso si los ID pertenecen al mismo usuario. Por ejemplo, para el mismo usuario puede especificar una cuota que limite el UID 20 a 1 GB de espacio en disco y otra cuota que limita corp\john_smith a 2 GB de espacio en disco, aunque ambos ID representen al mismo usuario. ONTAP aplica cuotas a UID 20 y corp\john_smith por separado.

En este caso, no se aplican límites a engineering\jsmith, aunque se aplican límites a los demás ID utilizados por el mismo usuario.

Cómo ONTAP determina los ID de usuario en un entorno mixto

Si tiene usuarios que acceden al almacenamiento de ONTAP desde clientes Windows y UNIX, se utiliza la seguridad de Windows y UNIX para determinar la propiedad de los archivos. Hay varios factores que determinan si ONTAP usa un identificador de UNIX o Windows al aplicar cuotas de usuario.

Si el estilo de seguridad del volumen qtree o FlexVol que contiene el archivo es solo NTFS o sólo UNIX, el estilo de seguridad determina el tipo de ID utilizado al aplicar cuotas de usuario. Para qtrees con estilo de seguridad mixto, el tipo de ID utilizado viene determinado por si el archivo tiene una ACL.

En la tabla siguiente se resume el tipo de ID que se utiliza:

| Estilo de seguridad | ACL | Sin ACL |
|---------------------|---------------|---------------|
| UNIX | ID DE UNIX | ID DE UNIX |
| Mixto | ID de Windows | ID DE UNIX |
| NTFS | ID de Windows | ID de Windows |

Cómo funcionan las cuotas con múltiples usuarios

Cuando se colocan varios usuarios en el mismo destino de cuota, los límites de cuota definidos por esa cuota no se aplican a cada usuario individual; en este caso, los límites de cuota se comparten entre todos los usuarios incluidos en el destino de cuota.

A diferencia de lo que ocurre con los comandos de gestión de objetos, como volúmenes y qtrees, no se puede cambiar el nombre de un destino de cuota, incluida una cuota de varios usuarios. Esto significa que una vez definida una cuota de varios usuarios, no se pueden modificar los usuarios en el destino de cuota y no se pueden agregar usuarios a un destino ni quitar usuarios de un destino. Si desea agregar o quitar un usuario de una cuota de varios usuarios, debe eliminarse la cuota que contiene ese usuario y definir una nueva regla de cuota con el conjunto de usuarios del destino.



Si combina cuotas de usuario independientes en una cuota de múltiples usuarios, puede activar el cambio mediante el cambio de tamaño de las cuotas. Sin embargo, si desea quitar usuarios de un destino de cuota con varios usuarios o agregar usuarios a un destino que ya tiene varios usuarios, debe reiniciar las cuotas antes de que el cambio surta efecto.

Ejemplo de más de un usuario en una regla de cuota

En el siguiente ejemplo, hay dos usuarios en la entrada de cuota. Los dos usuarios pueden utilizar hasta 80MB de espacio combinado. Si uno usa 75MB, entonces el otro solo puede usar 5MB.

```
cluster1::> volume quota policy rule create -vserver vs0 -volume voll
-policy-name default -type user -target "jsmith,chen" -qtree "" -disk
-limit 80m

cluster1::> volume quota policy rule show -vserver vs0 -volume voll
```

| | | | | | | | |
|--------------|---------------|-------|-----------------|-------|--------------|-------|-------|
| Vserver: vs0 | | | Policy: default | | Volume: voll | | |
| | | | | | Soft | | Soft |
| | | | User | Disk | Disk | Files | Files |
| Type | Target | Qtree | Mapping | Limit | Limit | Limit | Limit |
| Threshold | | | | | | | |
| ----- | ----- | ----- | ----- | ----- | ----- | ----- | ----- |
| ----- | | | | | | | |
| user | "jsmith,chen" | "" | off | 80MB | - | - | - |
| - | | | | | | | |

Cómo se vinculan los nombres de las cuotas de UNIX y Windows

En un entorno mixto, los usuarios pueden iniciar sesión como usuarios de Windows o como usuarios de UNIX. Puede configurar cuotas para reconocer que el identificador de UNIX y el identificador de Windows de un usuario representan al mismo usuario.

Las cuotas para el nombre de usuario de Windows se asignan a un nombre de usuario de UNIX, o viceversa, cuando se cumplen las dos condiciones siguientes:

- La `user-mapping` el parámetro se establece en "on" en la regla de cuota para el usuario.
- Los nombres de usuario se asignaron con el `vserver name-mapping` comandos.

Cuando un nombre de UNIX y Windows se asignan conjuntamente, se tratan como la misma persona para determinar el uso de cuotas.

Cómo funcionan las cuotas con qtrees

Puede crear cuotas con un qtree como destino; estas cuotas se denominan *tree Quotas*. También puede crear cuotas de usuario y de grupo para un qtree concreto. Además, las cuotas de un volumen FlexVol a veces son heredadas por los qtrees que contiene ese volumen.

Cómo funcionan las cuotas de árbol

Descripción general de cómo funcionan las cuotas de árbol

Puede crear una cuota con un qtree como destino para limitar el tamaño del qtree de destino. Estas cuotas también se denominan *tree Quotas*.

Cuando se aplica una cuota a un qtree, el resultado es similar a una partición de disco, excepto que se puede cambiar el tamaño máximo del qtree en cualquier momento si se cambia la cuota. Cuando se aplica una cuota de árbol, ONTAP limita el espacio en disco y el número de archivos en el qtree, independientemente de sus

propietarios. Ningún usuario, incluidos root y miembros del grupo BUILTIN\Administrators, puede escribir en el qtree si la operación de escritura hace que se supere la cuota de árbol.



El tamaño de la cuota no garantiza ninguna cantidad específica de espacio disponible. El tamaño de la cuota puede ser mayor que la cantidad de espacio libre disponible para el qtree. Puede utilizar el `volume quota report` comando para determinar la cantidad real de espacio disponible en el qtree.

Cómo funcionan las cuotas de usuario y de grupo con qtrees

Las cuotas de árbol limitan el tamaño general del qtree. Para evitar que usuarios o grupos individuales consuman todo el qtree, debe especificar una cuota de usuario o de grupo para ese qtree.

Ejemplo de cuota de usuario en un qtree

Supongamos que tiene las siguientes reglas de cuota:

```
cluster1::> volume quota policy rule show -vserver vs0 -volume vol1
```

| Vserver: vs0 | | | Policy: default | | | Volume: vol1 | |
|--------------|--------|-------|-----------------|------------|-----------------|--------------|------------------|
| Type | Target | Qtree | User Mapping | Disk Limit | Soft Disk Limit | Files Limit | Soft Files Limit |
| user | "" | "" | off | 50MB | - | - | - |
| user | jsmith | "" | off | 80MB | - | - | - |

Observarás que un determinado usuario, kjones, está ocupando demasiado espacio en un qtree crítico, proj1, que reside en vol1. Puede restringir el espacio de este usuario agregando la siguiente regla de cuota:

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "kjones" -qtree "proj1" -disk
-limit 20m -threshold 15m
```

```
cluster1::> volume quota policy rule show -vserver vs0 -volume vol1
```

| Vserver: vs0 | | | Policy: default | | Volume: vol1 | | |
|--------------|--------|-------|-----------------|------------|-----------------|-------------|------------------|
| Type | Target | Qtree | User Mapping | Disk Limit | Soft Disk Limit | Files Limit | Soft Files Limit |
| user | "" | "" | off | 50MB | - | - | - |
| 45MB | | | | | | | |
| user | jsmith | "" | off | 80MB | - | - | - |
| 75MB | | | | | | | |
| user | kjones | proj1 | off | 20MB | - | - | - |
| 15MB | | | | | | | |

Cómo crean las cuotas de árbol predeterminadas en un volumen FlexVol las cuotas de árbol derivadas

Cuando se crea una cuota de árbol predeterminada en un volumen de FlexVol, las cuotas de árbol derivadas correspondientes se crean automáticamente para cada qtree de ese volumen.

Estas cuotas de árbol derivadas tienen los mismos límites que la cuota de árbol predeterminada. Si no existen cuotas adicionales, los límites tienen los siguientes efectos:

- Los usuarios pueden utilizar tanto espacio en un qtree como se asignan para todo el volumen (siempre y cuando no hayan superado el límite del volumen utilizando el espacio en la raíz u otro qtree).
- Cada uno de los qtrees puede crecer para consumir el volumen completo.

La existencia de una cuota de árbol predeterminada en un volumen sigue afectando a todos los qtrees nuevos que se agregan al volumen. Cada vez que se crea un qtree nuevo, también se crea una cuota de árbol derivada.

Al igual que todas las cuotas derivadas, las cuotas de árbol derivadas muestran los siguientes comportamientos:

- Sólo se crean si el destino no tiene una cuota explícita.
- Aparecen en los informes de cuotas pero no aparecen cuando se muestran las reglas de cuota con `volume quota policy rule show` comando.

Ejemplo de cuotas de árbol derivadas

Tiene un volumen con tres qtrees (proyecto 1, proyecto 2 y proyecto 3) y la única cuota de árbol es una cuota explícita en el qtree del proyecto 1 que limita su tamaño de disco a 10 GB. Si crea una cuota de árbol predeterminada en el volumen y reinicializa cuotas en el volumen, el informe de cuota ahora contiene cuatro

cuotas de árbol:

| Volume Specifier | Tree | Type | ID | ----Disk---- | | ----Files----- | | Quota |
|---------------------|-------|-------|-------|--------------|-------|----------------|-------|-------|
| | | | | Used | Limit | Used | Limit | |
| ----- | ----- | ----- | ----- | ----- | ----- | ----- | ----- | |
| ----- | | | | | | | | |
| vol1 | proj1 | tree | 1 | 0B | 10GB | 1 | - | proj1 |
| vol1 | | tree | * | 0B | 20GB | 0 | - | * |
| vol1 | proj2 | tree | 2 | 0B | 20GB | 1 | - | proj2 |
| vol1 | proj3 | tree | 3 | 0B | 20GB | 1 | - | proj3 |
| ... | | | | | | | | |

La primera línea muestra la cuota explícita original en el qtree del proyecto 1. Esta cuota permanece sin cambios.

La segunda línea muestra la nueva cuota de árbol predeterminada en el volumen. El especificador de cuota asterisco (*) indica que es una cuota predeterminada. Esta cuota es el resultado de la regla de cuota que ha creado.

Las dos últimas líneas muestran nuevas cuotas de árboles derivadas para los qtrees proj2 y proy3. ONTAP creó automáticamente estas cuotas como resultado de la cuota de árbol predeterminada en el volumen. Estas cuotas de árbol derivadas tienen el mismo límite de disco de 20 GB que la cuota de árbol predeterminada del volumen. ONTAP no creó una cuota de árbol derivada para el qtree del proyecto 1 porque el qtree del proyecto 1 ya tenía una cuota explícita.

Las cuotas de usuario predeterminadas de un volumen de FlexVol afectan a las cuotas de los qtrees de ese volumen

Si se define una cuota de usuario predeterminada para un volumen de FlexVol, se crea automáticamente una cuota de usuario predeterminada para cada qtree contenido en ese volumen para el que existe una cuota de árbol explícita o derivada.

Si ya existe una cuota de usuario predeterminada en el qtree, no se verá afectada cuando se crea la cuota de usuario predeterminada en el volumen.

Las cuotas de usuario predeterminadas que se crean automáticamente en los qtrees tienen los mismos límites que la cuota de usuario predeterminada que se crea para el volumen.

Una cuota de usuario explícita para un qtree anula (sustituye los límites aplicados por) la cuota de usuario predeterminada creada automáticamente, del mismo modo que anula una cuota de usuario predeterminada en ese qtree que creó un administrador.

Cómo afectan los cambios de qtree a las cuotas

Información general sobre cómo afectan los cambios en los qtrees

Cuando se elimina, se cambia el nombre o se cambia el estilo de seguridad de un qtree, las cuotas aplicadas por ONTAP podrían cambiar en función de las cuotas actuales que se estén aplicando.

Cómo eliminar un qtree afecta a las cuotas de árbol

Cuando se elimina un qtree, ONTAP ya no aplica todas las cuotas aplicables a ese qtree, ya sean explícitas o derivadas.

Si persisten las reglas de cuota depende del lugar donde se elimine el qtree:

- Si elimina un qtree mediante ONTAP, las reglas de cuota de ese qtree se eliminan automáticamente, incluidas las reglas de cuota de árbol y cualquier regla de cuota de usuario y de grupo configurada para ese qtree.
- Si elimina un qtree mediante el cliente CIFS o NFS, debe eliminar cualquier regla de cuota para ese qtree para evitar que se produzcan errores al reiniciar las cuotas. Si crea un qtree nuevo con el mismo nombre que el que eliminó, las reglas de cuota existentes no se aplicarán al nuevo qtree hasta que se reinicien las cuotas.

Cómo afecta el cambio de nombre a un qtree a las cuotas

Cuando se cambia el nombre de un qtree mediante ONTAP, las reglas de cuota de ese qtree se actualizan automáticamente. Si cambia el nombre de un qtree mediante el cliente CIFS o NFS, debe actualizar las reglas de cuota de ese qtree.



Si cambia el nombre de un qtree mediante su cliente CIFS o NFS y no actualiza las reglas de cuota para ese qtree con el nuevo nombre antes de que se reinicien las cuotas, las cuotas no se aplicarán al qtree y las cuotas explícitas para el qtree-- incluir las cuotas de árbol y las cuotas de usuario o grupo para el qtree, podría convertirse en cuotas derivadas.

Cómo cambiar el estilo de seguridad de un qtree afecta a las cuotas de usuario

Puede aplicar listas de control de acceso (ACL) en qtrees utilizando NTFS o estilos de seguridad mixtos, pero no utilizando el estilo de seguridad UNIX. Por lo tanto, cambiar el estilo de seguridad de un qtree puede afectar a cómo se calculan las cuotas. Siempre debe reiniciar las cuotas después de cambiar el estilo de seguridad de un qtree.

Si cambia el estilo de seguridad de un qtree de NTFS o mixto a UNIX, se ignoran todas las ACL de los archivos en ese qtree y el uso del archivo se cobra por los ID de usuario de UNIX.

Si cambia el estilo de seguridad de un qtree de UNIX a uno mixto o NTFS, se vuelven visibles las ACL ocultas anteriormente. Además, cualquier ACL que se ignoraron vuelve a ser efectiva y se ignora la información de usuario de NFS. Si no había ninguna ACL antes, la información de NFS se sigue utilizando en el cálculo de la cuota.



Para asegurarse de que los usos de la cuota para los usuarios de UNIX y Windows se calculen correctamente después de cambiar el estilo de seguridad de un qtree, debe reiniciar las cuotas del volumen que contiene ese qtree.

Ejemplo

En el siguiente ejemplo, se muestra cómo un cambio en el estilo de seguridad de un qtree concreto se traduce en que se carga a otro usuario por el uso de un archivo en el qtree concreto.

Supongamos que la seguridad NTFS está en vigor en el qtree A, y una ACL da al usuario de Windows corp\joe la propiedad de un archivo de 5 MB. User corp\joe se carga con 5 MB de uso de espacio en disco

para el qtree A.

Ahora se cambia el estilo De seguridad Del qtree A de NTFS a UNIX. Una vez reinicializadas las cuotas, el usuario de Windows corp\joe ya no se carga para este archivo; en su lugar, el usuario UNIX correspondiente al UID del archivo se carga para el archivo. El UID podría ser un usuario UNIX asignado a corp\joe o al usuario raíz.

Cómo se activan las cuotas

Descripción general de cómo se activan las cuotas

Las nuevas cuotas y los cambios en las cuotas no surten efecto hasta que se activen. Saber cómo funciona la activación de cuotas puede ayudarle a gestionar las cuotas de forma menos disruptiva.

Es posible activar cuotas en el nivel de volumen.

Las cuotas se activan mediante *inicializando* (activándolas) o *redimensionamiento*. La desactivación de cuotas y su activación se denomina reinicialización.

La duración del proceso de activación y su impacto en la aplicación de las cuotas depende del tipo de activación:

- El proceso de inicialización incluye dos partes: A `quota on` trabajo y un análisis de cuota del sistema de archivos completo del volumen. La exploración comienza después de la `quota on` el trabajo se completa correctamente. El análisis de cuotas puede tardar algún tiempo; cuantos más archivos tenga el volumen, más tiempo tardará. Hasta que finalice la exploración, la activación de cuota no se completa y las cuotas no se aplican.
- El proceso de cambio de tamaño solo implica un `quota resize` trabajo. El cambio de tamaño requiere menos tiempo que una inicialización de cuota porque no implica una exploración de cuota. Durante el proceso de cambio de tamaño, las cuotas se siguen aplicando.

De forma predeterminada, la `quota on` y.. `quota resize` los trabajos se ejecutan en segundo plano, lo que permite utilizar otros comandos al mismo tiempo.

Los errores y advertencias del proceso de activación se envían al sistema de administración de eventos. Si utiliza la `-foreground` con el `volume quota on` o `volume quota resize` comandos, el comando no devuelve hasta que el trabajo se completa; esto es útil si se está reinicializando desde un script. Para mostrar más adelante los errores y advertencias, puede utilizar la `volume quota show` con el `-instance` parámetro.

La activación de la cuota permanece en paradas y reinicios. El proceso de activación de cuotas no afecta a la disponibilidad de los datos del sistema de almacenamiento.

Cuando se puede utilizar el cambio de tamaño

Puesto que el cambio de tamaño de la cuota es más rápido que la inicialización de la cuota, debe utilizar el cambio de tamaño siempre que sea posible. Sin embargo, el cambio de tamaño sólo funciona para ciertos tipos de cambios de cuota.

Puede cambiar el tamaño de las cuotas al realizar los siguientes tipos de cambios en las reglas de cuota:

- Cambiar una cuota existente.

Por ejemplo, cambiar los límites de una cuota existente.

- Agregar una cuota para un destino de cuota para el que existe una cuota predeterminada o una cuota de seguimiento predeterminada.
- Eliminación de una cuota para la que se especifica una entrada de cuota predeterminada o de cuota de seguimiento predeterminada.
- Combinar cuotas de usuario separadas en una cuota para varios usuarios.



Después de realizar cambios extensos de cuotas, debe realizar una reinicialización completa para garantizar que todos los cambios surtan efecto.



Si intenta cambiar el tamaño y no todos los cambios de cuota se pueden incorporar mediante una operación de cambio de tamaño, ONTAP emitirá una advertencia. Puede determinar a partir del informe de cuotas si su sistema de almacenamiento está realizando un seguimiento del uso del disco para un usuario, grupo o qtree concreto. Si ve una cuota en el informe de cuotas, significa que el sistema de almacenamiento está realizando un seguimiento del espacio en disco y del número de archivos que pertenecen al destino de cuota.

Ejemplo de cambios en las cuotas que se pueden hacer efectivos mediante el cambio de tamaño

Algunos cambios en las reglas de cuota se pueden hacer efectivos mediante el cambio de tamaño. Considere las siguientes cuotas:

| #Quota | Target | type | disk | files | thold | sdisk | sfile |
|--------|--------|-----------------|------|-------|-------|-------|-------|
| #----- | ---- | ---- | ---- | ----- | ----- | ----- | ----- |
| * | | user@/vol/vol2 | 50M | 15K | | | |
| * | | group@/vol/vol2 | 750M | 85K | | | |
| * | | tree@/vol/vol2 | - | - | | | |
| jdoe | | user@/vol/vol2/ | 100M | 75K | | | |
| kbuck | | user@/vol/vol2/ | 100M | 75K | | | |

Supongamos que realiza los siguientes cambios:

- Aumente el número de archivos para el destino de usuario predeterminado.
- Agregue una nueva cuota de usuario para un nuevo usuario, boris, que necesita más límite de disco que la cuota de usuario predeterminada.
- Eliminar la entrada explícita de cuota del usuario kbuck; el nuevo usuario necesita ahora sólo los límites de cuota predeterminados.

Estos cambios tienen como resultado las siguientes cuotas:

| #Quota | Target | type | disk | files | thold | sdisk | sfile |
|--------|--------|-----------------|------|-------|-------|-------|-------|
| #----- | ----- | ---- | ---- | ----- | ----- | ----- | ----- |
| * | | user@/vol/vol2 | 50M | 25K | | | |
| * | | group@/vol/vol2 | 750M | 85K | | | |
| * | | tree@/vol/vol2 | - | - | | | |
| jdoe | | user@/vol/vol2/ | 100M | 75K | | | |
| boris | | user@/vol/vol2/ | 100M | 75K | | | |

El cambio de tamaño activa todos estos cambios; no es necesaria una reinicialización completa de la cuota.

Cuando se requiere una reinicialización completa de la cuota

Aunque el cambio de tamaño de las cuotas es más rápido, debe volver a inicializar todas las cuotas si realiza algunos cambios pequeños o extensos en las cuotas.

Es necesaria una reinicialización completa de la cuota en las siguientes circunstancias:

- Se crea una cuota para un destino que no ha tenido previamente una cuota (ni una cuota explícita ni una derivada de una cuota por defecto).
- Se cambia el estilo de seguridad de un qtree de UNIX a mixto o NTFS.
- Se cambia el estilo de seguridad de un qtree de NTFS o mixto a UNIX.
- Se quitan usuarios de un destino de cuota con varios usuarios o se agregan usuarios a un destino que ya tiene varios usuarios.
- Usted realiza cambios extensos en sus cuotas.

Ejemplo de cambios de cuotas que requieren inicialización

Supongamos que tiene un volumen que contiene tres qtrees y las únicas cuotas en el volumen son tres cuotas de árbol explícitas. Decide realizar los siguientes cambios:

- Agregue un qtree nuevo y cree una nueva cuota de árbol para él.
- Añada una cuota de usuario predeterminada para el volumen.

Ambos cambios requieren una inicialización de cuota completa. El redimensionamiento no hace que las cuotas sean efectivas.

Cómo se puede ver la información de cuota

Cómo se puede ver la información general de la cuota

Puede utilizar los informes de cuotas para ver detalles como la configuración de reglas y políticas de cuota, cuotas aplicadas y configuradas, y errores que se producen durante el cambio de tamaño y la reinicialización de cuotas.

La visualización de la información de cuota es útil en situaciones como las siguientes:

- Configurar cuotas, por ejemplo, para configurar cuotas y verificar las configuraciones
- Respondiendo a las notificaciones de que pronto se alcanzarán los límites de espacio en disco o de archivos o que se hayan alcanzado

- Responder a las solicitudes de más espacio

Cómo se puede utilizar el informe de cuotas para ver qué cuotas están en vigor

Debido a las diversas formas en que interactúan las cuotas, hay más cuotas en vigor que sólo las que se han creado explícitamente. Para ver qué cuotas están en vigor, puede ver el informe de cuotas.

Los siguientes ejemplos muestran informes de cuotas para los diferentes tipos de cuotas aplicadas en un volumen de FlexVol vol1 y un qtree de ese volumen:

Ejemplo que no tiene ninguna cuota de usuario especificada para el qtree

En este ejemplo, hay un qtree, q1, que está contenido por el volumen vol1. El administrador ha creado tres cuotas:

- Límite de cuota de árbol por defecto en vol1 de 400MB
- Un límite de cuota de usuario predeterminado en vol1 de 100MB
- Un límite de cuota de usuario explícito en vol1 de 200MB para el usuario jsmith

Las reglas de cuota para estas cuotas son similares al siguiente ejemplo:

```
cluster1::*> volume quota policy rule show -vserver vs1 -volume vol1
```

| Vserver: vs1 | | | Policy: default | | | Volume: vol1 | |
|--------------|--------|-------|-----------------|------------|-----------------|--------------|------------------|
| Type | Target | Qtree | User Mapping | Disk Limit | Soft Disk Limit | Files Limit | Soft Files Limit |
| Threshold | | | | | | | |
| tree | "" | "" | - | 400MB | - | - | - |
| - | | | | | | | |
| user | "" | "" | off | 100MB | - | - | - |
| - | | | | | | | |
| user | jsmith | "" | off | 200MB | - | - | - |
| - | | | | | | | |

El informe de cuotas de estas cuotas es similar al siguiente ejemplo:

```
cluster1::> volume quota report
Vserver: vs1
```

| Volume | Tree | Type | ID | ----Disk---- | | ----Files----- | | Quota |
|-----------|-------|-------|--------|--------------|-------|----------------|-------|--------|
| | | | | Used | Limit | Used | Limit | |
| Specifier | | | | | | | | |
| ----- | ----- | ----- | ----- | ----- | ----- | ----- | ----- | |
| vol1 | - | tree | * | 0B | 400MB | 0 | - | * |
| vol1 | - | user | * | 0B | 100MB | 0 | - | * |
| vol1 | - | user | jsmith | 150B | 200MB | 7 | - | jsmith |
| vol1 | q1 | tree | 1 | 0B | 400MB | 6 | - | q1 |
| vol1 | q1 | user | * | 0B | 100MB | 0 | - | |
| vol1 | q1 | user | jsmith | 0B | 100MB | 5 | - | |
| vol1 | - | user | root | 0B | 0MB | 1 | - | |
| vol1 | q1 | user | root | 0B | 0MB | 8 | - | |

Las tres primeras líneas del informe de cuotas muestran las tres cuotas especificadas por el administrador. Puesto que dos de estas cuotas son cuotas predeterminadas, ONTAP crea automáticamente cuotas derivadas.

La cuarta línea muestra la cuota de árbol derivada de la cuota de árbol predeterminada para cada qtree en vol1 (en este ejemplo, sólo q1).

La quinta línea muestra la cuota de usuario predeterminada que se crea para el qtree como resultado de la existencia de la cuota de usuario predeterminada en el volumen y en la cuota de qtree.

La sexta línea muestra la cuota de usuario derivada que se crea para jsmith en el qtree porque hay una cuota de usuario predeterminada para el qtree (línea 5) y el jsmith de usuario es propietario de archivos en ese qtree. Tenga en cuenta que el límite aplicado al usuario jsmith en el qtree Q1 no está determinado por el límite explícito de cuota de usuario (200MB). Esto se debe a que el límite de cuota de usuario explícito está en el volumen, por lo que no afecta los límites del qtree. En su lugar, el límite de cuota de usuario derivado para el qtree se determina con la cuota de usuario predeterminada para el qtree (100MB).

Las dos últimas líneas muestran más cuotas de usuario que se derivan de las cuotas de usuario predeterminadas en el volumen y en el qtree. Se creó una cuota de usuario derivada para el usuario raíz tanto en el volumen como en el qtree porque el usuario raíz era propietario de los archivos tanto del volumen como del qtree. Puesto que el usuario root recibe un tratamiento especial en términos de cuotas, sus cuotas derivadas sólo realizan un seguimiento de las cuotas.

Ejemplo con cuotas de usuario especificadas para el qtree

Este ejemplo es similar al anterior, salvo que el administrador haya añadido dos cuotas al qtree.

Aún hay un volumen, vol1, y un qtree, el primer trimestre. El administrador ha creado las siguientes cuotas:

- Límite de cuota de árbol por defecto en vol1 de 400MB
- Un límite de cuota de usuario predeterminado en vol1 de 100MB
- Un límite de cuota de usuario explícito en vol1 para el usuario jsmith de 200MB
- Un límite de cuota de usuario predeterminado en el qtree Q1 de 50MB

- Un límite explícito de cuota de usuario en el qtree Q1 para el usuario jsmith de 75MB

Las reglas de cuota para estas cuotas son las siguientes:

```
cluster1::> volume quota policy rule show -vserver vs1 -volume vol1
```

| Vserver: vs1 | | | Policy: default | | Volume: vol1 | | |
|--------------|--------|-------|-----------------|------------|-----------------|-------------|------------------|
| Type | Target | Qtree | User Mapping | Disk Limit | Soft Disk Limit | Files Limit | Soft Files Limit |
| tree | "" | "" | - | 400MB | - | - | - |
| user | "" | "" | off | 100MB | - | - | - |
| user | "" | q1 | off | 50MB | - | - | - |
| user | jsmith | "" | off | 200MB | - | - | - |
| user | jsmith | q1 | off | 75MB | - | - | - |

El informe de cuotas de estas cuotas tiene este aspecto:

```
cluster1::> volume quota report
```

| Volume | Tree | Type | ID | ----Disk---- | | ----Files---- | | Quota |
|-----------|------|------|--------|--------------|-------|---------------|-------|--------|
| Specifier | | | | Used | Limit | Used | Limit | |
| vol1 | - | tree | * | 0B | 400MB | 0 | - | * |
| vol1 | - | user | * | 0B | 100MB | 0 | - | * |
| vol1 | - | user | jsmith | 2000B | 200MB | 7 | - | jsmith |
| vol1 | q1 | user | * | 0B | 50MB | 0 | - | * |
| vol1 | q1 | user | jsmith | 0B | 75MB | 5 | - | jsmith |
| vol1 | q1 | tree | 1 | 0B | 400MB | 6 | - | q1 |
| vol1 | - | user | root | 0B | 0MB | 2 | - | |
| vol1 | q1 | user | root | 0B | 0MB | 1 | - | |

Las cinco primeras líneas del informe de cuotas muestran las cinco cuotas creadas por el administrador. Puesto que algunas de estas cuotas son cuotas predeterminadas, ONTAP crea automáticamente cuotas derivadas.

La sexta línea muestra la cuota de árbol derivada de la cuota de árbol predeterminada para cada qtree en vol1 (en este ejemplo, sólo q1).

Las últimas dos líneas muestran las cuotas de usuario que se derivan de las cuotas de usuario predeterminadas en el volumen y en el qtree. Se creó una cuota de usuario derivada para el usuario raíz tanto en el volumen como en el qtree porque el usuario raíz era propietario de los archivos tanto del volumen como del qtree. Puesto que el usuario root recibe un tratamiento especial en términos de cuotas, sus cuotas derivadas sólo realizan un seguimiento de las cuotas.

No se han creado otras cuotas predeterminadas ni cuotas derivadas por los siguientes motivos:

- No se creó una cuota de usuario derivada para el usuario jsmith aunque el usuario tenga archivos tanto en el volumen como en el qtree, ya que el usuario ya tiene cuotas explícitas en ambos niveles.
- No se crearon cuotas de usuario derivadas para otros usuarios, ya que ningún otro usuario posee archivos, ya sea en el volumen o en el qtree.
- La cuota de usuario predeterminada del volumen no creó una cuota de usuario predeterminada en el qtree porque el qtree ya tenía una cuota de usuario predeterminada.

El motivo por el que las cuotas impuestas difieren de las cuotas configuradas

Las cuotas forzadas difieren de las configuradas porque las cuotas derivadas se aplican sin ser configuradas, pero las cuotas configuradas se aplican sólo después de inicializarse correctamente. La comprensión de estas diferencias puede ayudarle a comparar las cuotas impuestas que se muestran en los informes de cuotas con las cuotas configuradas.

Las cuotas forzadas, que aparecen en los informes de cuotas, pueden diferir de las reglas de cuota configuradas por los siguientes motivos:

- Las cuotas derivadas se aplican sin estar configuradas como reglas de cuota; ONTAP crea cuotas derivadas automáticamente en respuesta a las cuotas predeterminadas.
- Es posible que las cuotas no se hayan reinicializado en un volumen después de configurar las reglas de cuota.
- Es posible que se hayan producido errores cuando se inicializaron las cuotas en un volumen.

Utilice el informe de cuotas para determinar qué cuotas limitan las escrituras en un archivo específico

Puede usar el comando `volume quota report` con una ruta de archivo específica para determinar qué límites de cuota afectan a las operaciones de escritura en un archivo. Esto puede ayudarle a entender qué cuota está impidiendo una operación de escritura.

Paso

1. El comando `volume quota report` se utiliza con el parámetro `-path`.

Ejemplo de visualización de cuotas que afectan a un archivo específico

En el siguiente ejemplo, se muestran el comando y el resultado para determinar qué cuotas están vigentes para las escrituras en el archivo 1, que reside en el primer trimestre de qtree del volumen FlexVol vol2:

```
cluster1:> volume quota report -vserver vs0 -volume vol2 -path
/vol/vol2/q1/file1
Virtual Server: vs0
```

| Volume Specifier | Tree | Type | ID | ----Disk---- | | ----Files----- | | Quota |
|---------------------|------|-------|-------------|--------------|-------|----------------|-------|-------|
| | | | | Used | Limit | Used | Limit | |
| vol2 | q1 | tree | jsmith | 1MB | 100MB | 2 | 10000 | q1 |
| vol2 | q1 | group | eng | 1MB | 700MB | 2 | 70000 | |
| vol2 | | group | eng | 1MB | 700MB | 6 | 70000 | * |
| vol2 | | user | corp\jsmith | 1MB | 50MB | 1 | - | * |
| vol2 | q1 | user | corp\jsmith | 1MB | 50MB | 1 | - | |

5 entries were displayed.

Comandos para mostrar información acerca de las cuotas

Puede utilizar comandos para mostrar un informe de cuotas que contenga cuotas forzadas y uso de recursos, mostrar información sobre el estado y los errores de las cuotas, o sobre las políticas de cuotas y las reglas de cuota.



Los siguientes comandos solo se pueden ejecutar en volúmenes de FlexVol.

| Si desea... | Se usa este comando... |
|--|--|
| Ver información sobre cuotas forzadas | <code>volume quota report</code> |
| Ver el uso de recursos (espacio en disco y número de archivos) de los destinos de cuota | <code>volume quota report</code> |
| Determine qué límites de cuota se ven afectados cuando se permite la escritura en un archivo | <code>volume quota report</code> con la <code>-path</code> parámetro |
| Muestra el estado de la cuota, por ejemplo on, off, y. initializing | <code>volume quota show</code> |
| Ver información sobre el registro de mensajes de cuota | <code>volume quota show</code> con la <code>-logmsg</code> parámetro |
| Errores de vista que se producen durante la inicialización y el cambio de tamaño de la cuota | <code>volume quota show</code> con la <code>-instance</code> parámetro |
| Ver información acerca de las políticas de cuotas | <code>volume quota policy show</code> |

| Si desea... | Se usa este comando... |
|---|---|
| Ver información acerca de las reglas de cuota | <code>volume quota policy rule show</code> |
| Ver el nombre de la normativa de cuotas que se asigna a una máquina virtual de almacenamiento (SVM, antes denominada Vserver) | <code>vserver show</code> con la <code>-instance</code> parámetro |

Consulte la página de manual de cada comando para obtener más información.

Cuándo se deben usar los comandos `show` de la regla de política de cuota de volumen y los comandos `volume quota report`

Aunque ambos comandos muestran información acerca de las cuotas, el `volume quota policy rule show` muestra rápidamente las reglas de cuota configuradas mientras `volume quota report` comando, que consume más tiempo y recursos, muestra las cuotas forzadas y el uso de recursos.

La `volume quota policy rule show` el comando es útil con los siguientes fines:

- Compruebe la configuración de las reglas de cuota antes de activarlas

Este comando muestra todas las reglas de cuota configuradas independientemente de si se han inicializado o cambiado el tamaño de las cuotas.

- Vea rápidamente las reglas de cuotas sin afectar a los recursos del sistema

Como no muestra el uso de disco y archivo, este comando no consume tanto recursos como un informe de cuota.

- Muestra las reglas de cuotas en una política de cuotas que no está asignada a la SVM.

La `volume quota report` el comando es útil con los siguientes fines:

- Ver cuotas forzadas, incluidas las cuotas derivadas
- Vea el espacio en disco y el número de archivos utilizados por cada cuota en efecto, incluidos los destinos afectados por las cuotas derivadas

(Para las cuotas predeterminadas, el uso aparece como "0" porque se realiza un seguimiento del uso con respecto a la cuota derivada resultante).

- Determine qué límites de cuota afectan al momento en que se permitirá la escritura en un archivo

Añada el `-path` parámetro de la `volume quota report` comando.



El informe de cuotas es una operación que requiere muchos recursos. Si la ejecuta en muchos volúmenes de FlexVol en el clúster, es posible que tarde mucho tiempo en completarse. Una forma más eficaz sería ver el informe de cuotas de un volumen concreto de una SVM.

Diferencia de uso de espacio mostrada por un informe de cuotas y una descripción general del cliente UNIX

El valor del espacio en disco usado que se muestra en un informe de cuota para un volumen o qtree de FlexVol puede ser diferente del valor que muestra un cliente UNIX para el mismo volumen o qtree. La diferencia en los valores de uso se debe a la diferencia en los métodos seguidos por el informe de cuotas y los comandos UNIX para calcular los bloques de datos en el volumen o qtree.

Por ejemplo, si un volumen contiene un archivo con bloques de datos vacíos (en los que no se escriben los datos), el informe de cuota del volumen no cuenta los bloques de datos vacíos al informar el uso de espacio. Sin embargo, cuando el volumen está montado en un cliente UNIX y el archivo se muestra como el resultado del `ls` command, los bloques de datos vacíos también se incluyen en el uso de espacio. Por lo tanto, la `ls` el comando muestra un tamaño de archivo más alto en comparación con el uso de espacio mostrado por el informe de cuotas.

Del mismo modo, los valores de uso de espacio que se muestran en un informe de cuotas también pueden diferir de los valores que se muestran como resultado de comandos UNIX como `df` y `du`.

Cómo un informe de cuotas tiene en cuenta el espacio en disco y el uso de archivos

La cantidad de archivos usados y la cantidad de espacio en disco especificada en un informe de cuota de un volumen de FlexVol o un qtree dependen del recuento de bloques de datos usados que corresponden a cada nodo de información del volumen o del qtree.

El recuento de bloques incluye los bloques directos e indirectos utilizados para los archivos normales y de secuencias. Los bloques utilizados para directorios, listas de control de acceso (ACL), directorios de flujo y archivos de metadatos no se contabilizan en el informe de cuotas. En el caso de archivos dispersos de UNIX, los bloques de datos vacíos no se incluyen en el informe de cuotas.

El subsistema de cuota está diseñado para considerar e incluir sólo los aspectos controlables por el usuario del sistema de archivos. Los directorios, las ACL y el espacio de instantáneas son ejemplos de espacio excluido de los cálculos de cuotas. Las cuotas se utilizan para imponer límites, no garantías, y sólo funcionan en el sistema de archivos activo. La contabilidad de cuotas no cuenta con ciertas construcciones del sistema de archivos, ni tiene en cuenta la eficiencia del almacenamiento (como la compresión o la deduplicación).

Cómo el comando `ls` tiene en cuenta el uso de espacio

Cuando utilice la `ls` Comando para ver el contenido de un volumen FlexVol montado en un cliente UNIX, los tamaños de archivo mostrados en la salida pueden ser inferiores o superiores al uso de espacio mostrado en el informe de cuota del volumen según el tipo de bloques de datos para el archivo.

El resultado del `ls` el comando muestra sólo el tamaño de un archivo y no incluye los bloques indirectos utilizados por el archivo. Los bloques vacíos del archivo también se incluyen en el resultado del comando.

Por lo tanto, si un archivo no tiene bloques vacíos, el tamaño que muestra el `ls` el comando puede ser inferior al uso de disco especificado por un informe de cuotas debido a la inclusión de bloques indirectos en el informe de cuotas. A la inversa, si el archivo tiene bloques vacíos, entonces el tamaño que muestra el `ls` el comando puede ser superior al uso del disco especificado por el informe de cuotas.

El resultado del `ls` el comando muestra sólo el tamaño de un archivo y no incluye los bloques indirectos utilizados por el archivo. Los bloques vacíos del archivo también se incluyen en el resultado del comando.

Ejemplo de la diferencia entre el uso de espacio contabilizado por el comando `ls` y un informe de cuota

En el siguiente informe de cuotas se muestra un límite de 10 MB para un primer trimestre de `qtree`:

| Volume | Tree | Type | ID | ----Disk---- | | ----Files----- | | Quota |
|-----------|-------|-------|-------|--------------|-------|----------------|-------|-------|
| | | | | Used | Limit | Used | Limit | |
| Specifier | | | | | | | | |
| ----- | ----- | ----- | ----- | ----- | ----- | ----- | ----- | |
| ----- | | | | | | | | |
| voll | q1 | tree | user1 | 10MB | 10MB | 1 | - | q1 |
| ... | | | | | | | | |

Un archivo presente en el mismo `qtree` puede tener un tamaño que supere el límite de cuota cuando se vea desde un cliente UNIX utilizando el `ls` comando, como se muestra en el siguiente ejemplo:

```
[user1@lin-sys1 q1]$ ls -lh
-rwxr-xr-x  1 user1 nfsuser  **27M** Apr 09  2013 file1
```

Cómo el comando `df` tiene en cuenta el tamaño del archivo

La manera en que en `df` el comando informa de que el uso de espacio depende de dos condiciones: si las cuotas están habilitadas o deshabilitadas en el volumen que contiene el `qtree` y si se realiza un seguimiento del uso de cuotas en el `qtree`.

Cuando se habilitan las cuotas para el volumen que contiene el `qtree` y el uso de cuotas dentro del `qtree`, se realiza un seguimiento del uso de espacio informado en la `df` el comando es igual al valor especificado por el informe de cuota. En esta situación, el uso de cuotas excluye los bloques utilizados por directorios, ACL, directorios de flujo y archivos de metadatos.

Cuando las cuotas no están habilitadas en el volumen o cuando el `qtree` no tiene configurada una regla de cuota, el uso de espacio informado incluye bloques utilizados por directorios, ACL, directorios de flujo y archivos de metadatos para todo el volumen, incluidos otros `qtrees` dentro del volumen. En esta situación, el uso de espacio notificado por la `df` el comando es mayor que el valor esperado que se informa cuando se realiza el seguimiento de las cuotas.

Cuando ejecute el `df` comando desde el punto de montaje de un `qtree` para el que se realiza el seguimiento del uso de cuotas, el resultado del comando muestra el mismo uso de espacio que el valor especificado en el informe de cuotas. En la mayoría de los casos, cuando la regla de cuota de árbol tiene un límite de disco duro, el tamaño total registrado por la `df` el comando es igual al límite de disco y el espacio disponible es igual a la diferencia entre el límite de disco de cuota y el uso de cuota.

Sin embargo, en algunos casos, el espacio disponible notificado por el `df` el comando puede ser igual al espacio disponible en todo el volumen. Esto puede suceder cuando no hay un límite de disco duro configurado para el `qtree`. A partir de ONTAP 9.9.1, también puede ocurrir cuando el espacio disponible en el conjunto del volumen es menor que el espacio de cuota de árbol restante. Cuando se produce cualquiera de estas

condiciones, el tamaño total notificado por `df` El comando es un número sintetizado igual a la cuota utilizada en el `qtree` más el espacio disponible en el volumen FlexVol.



Este tamaño total no es ni el límite de disco de `qtree` ni el tamaño configurado en el volumen. También puede variar en función de la actividad de escritura en otros `qtrees` o en la actividad de eficiencia del almacenamiento en segundo plano.

Ejemplo de uso de espacio que cuenta la `df` y un informe de cuotas

El siguiente informe de cuotas muestra un límite de disco de 1 GB para el `qtree` `alice`, 2 GB para el `qtree` `bob` y sin límite para el proyecto de `Qtree`.1:

```
C1_vsim1::> quota report -vserver vs0
Vserver: vs0
```

| Volume | Tree | Type | ID | ----Disk---- | | ----Files----- | | Quota |
|----------|----------|------|----|--------------|-------|----------------|-------|-------|
| | | | | Used | Limit | Used | Limit | |
| ----- | | | | | | | | |
| vol2 | alice | tree | 1 | 502.0MB | 1GB | 2 | - | alice |
| vol2 | bob | tree | 2 | 1003MB | 2GB | 2 | - | bob |
| vol2 | project1 | tree | 3 | 200.8MB | - | 2 | - | |
| project1 | | | | | | | | |
| vol2 | | tree | * | 0B | - | 0 | - | * |

4 entries were displayed.

En el siguiente ejemplo, el resultado del `df` En `qtrees` `alice` y `bob` informan del mismo espacio utilizado que el informe de cuotas y del mismo tamaño total (en términos de un millón de bloques) que el límite de discos. Esto se debe a que las reglas de cuota de los `qtrees` `alice` y `bob` tienen un límite de disco definido y el espacio disponible del volumen (1211 MB) es mayor que el espacio restante de la cuota de árbol para el `qtree` `alice` (523 MB) y el `qtree` `bob` (1045 MB).

```
linux-client1 [~]$ df -m /mnt/vol2/alice
Filesystem          1M-blocks  Used Available Use% Mounted on
172.21.76.153:/vol2    1024    502      523  50% /mnt/vol2

linux-client1 [~]$ df -m /mnt/vol2/bob
Filesystem          1M-blocks  Used Available Use% Mounted on
172.21.76.153:/vol2    2048   1004     1045  50% /mnt/vol2
```

En el siguiente ejemplo, el resultado del `df` El comando en el proyecto `Qtree` informa del mismo espacio usado que el informe de cuotas, pero el tamaño total se sintetiza agregando el espacio disponible en el volumen en su conjunto (1211 MB) al uso de la cuota del proyecto `qtree` 1 (201 MB) para dar un total de 1412 MB. Esto se debe a que la regla de cuota para el proyecto de `qtree` 1 no tiene ningún límite de disco.

```
linux-client1 [~]$ df -m /mnt/vol2/project1
Filesystem            1M-blocks  Used Available Use% Mounted on
172.21.76.153:/vol2      1412    201      1211  15% /mnt/vol2
```

El siguiente ejemplo muestra cómo el resultado del `df` el comando en el volumen en su conjunto informa del mismo espacio disponible que el `project1`.



```
linux-client1 [~]$ df -m /mnt/vol2
Filesystem            1M-blocks  Used Available Use% Mounted on
172.21.76.153:/vol2      2919  1709      1211  59% /mnt/vol2
```

Cómo el comando `du` tiene en cuenta el uso del espacio

Cuando ejecute el `du` Comando para comprobar el uso del espacio en disco de un volumen de `qtree` o `FlexVol` montado en un cliente UNIX, puede que el valor de uso sea superior al valor que se muestra en un informe de cuota para el `qtree` o volumen.

El resultado del `du` el comando contiene el uso de espacio combinado de todos los archivos a través del árbol de directorios que comienza en el nivel del directorio en el que se emite el comando. Porque el valor de uso que muestra `du` el comando también incluye los bloques de datos de los directorios, es superior al valor mostrado por un informe de cuota.

Ejemplo de la diferencia entre el uso de espacio contabilizado por el comando `du` y un informe de cuota

En el siguiente informe de cuotas se muestra un límite de 10 MB para un primer trimestre de `qtree`:

| Volume Specifier | Tree | Type | ID | ----Disk---- | | ----Files----- | | Quota |
|---------------------|-------|-------|-------|--------------|-------|----------------|-------|-------|
| | | | | Used | Limit | Used | Limit | |
| ----- | ----- | ----- | ----- | ----- | ----- | ----- | ----- | |
| vol1 | q1 | tree | user1 | 10MB | 10MB | 1 | - | q1 |
| ... | | | | | | | | |

En el siguiente ejemplo, el uso de espacio en disco como resultado del `du` el comando muestra un valor mayor que supera el límite de cuota:

```
[user1@lin-sys1 q1]$ du -sh
**11M**      q1
```

Ejemplos de configuración de cuotas

Estos ejemplos le ayudan a comprender cómo configurar cuotas y leer informes de

cuotas.

Para los siguientes ejemplos, supongamos que tiene un sistema de almacenamiento que incluye una SVM, vs1, con un volumen, vol1. Para comenzar a configurar cuotas, debe crear una nueva política de cuotas para la SVM con el siguiente comando:

```
cluster1::>volume quota policy create -vserver vs1 -policy-name
quota_policy_vs1_1
```

Dado que la política de cuota es nueva, se la asigna a la SVM:

```
cluster1::>vserver modify -vserver vs1 -quota-policy quota_policy_vs1_1
```

Ejemplo 1: Cuota de usuario predeterminada

Usted decide imponer un límite duro de 50 MB para cada usuario en vol1:

```
cluster1::>volume quota policy rule create -vserver vs1 -policy-name
quota_policy_vs1_1 -volume vol1 -type user -target "" -disk-limit 50MB
-qtrees ""
```

Para activar la nueva regla, se inicializan las cuotas en el volumen:

```
cluster1::>volume quota on -vserver vs1 -volume vol1 -foreground
```

Para ver el informe de cuotas, escriba el siguiente comando:

```
cluster1::>volume quota report
```

El informe de cuotas resultante es similar al siguiente informe:

| | | | | | | | | |
|--------------|-------|-------|--------|--------------|-------|----------------|-------|-------|
| Vserver: vs1 | | | | | | | | |
| | | | | ----Disk---- | | ----Files----- | | Quota |
| Volume | Tree | Type | ID | Used | Limit | Used | Limit | |
| Specifier | | | | | | | | |
| ----- | ----- | ----- | ----- | ----- | ----- | ----- | ----- | |
| ----- | | | | | | | | |
| vol1 | | user | * | 0B | 50MB | 0 | - | * |
| vol1 | | user | jsmith | 49MB | 50MB | 37 | - | * |
| vol1 | | user | root | 0B | - | 1 | - | |

La primera línea muestra la cuota de usuario predeterminada que ha creado, incluido el límite de discos. Al igual que todas las cuotas predeterminadas, esta cuota de usuario predeterminada no muestra información

acerca del uso de discos o archivos. Además de la cuota que se creó, aparecen otras dos cuotas: Una cuota para cada usuario que actualmente posee archivos en vol1. Estas cuotas adicionales son cuotas de usuario que se derivan automáticamente de la cuota de usuario predeterminada. La cuota de usuario derivada para el jsmith de usuario tiene el mismo límite de disco de 50 MB que la cuota de usuario predeterminada. La cuota de usuario derivada para el usuario raíz es una cuota de seguimiento (sin límites).

Si algún usuario del sistema (distinto del usuario root) intenta realizar una acción que utilizaría más de 50 MB en vol1 (por ejemplo, escribir en un archivo desde un editor), la acción falla.

Ejemplo 2: Cuota de usuario explícita que anula una cuota de usuario predeterminada

Si tiene que proporcionar más espacio en el volumen vol1 al usuario jsmith, introduzca el siguiente comando:

```
cluster1::>volume quota policy rule create -vserver vs1 -policy-name
quota_policy_vs1_1 -volume vol1 -type user -target jsmith -disk-limit 80MB
-qtrees ""
```

Se trata de una cuota de usuario explícita, ya que el usuario aparece explícitamente como destino de la regla de cuota.

Se trata de un cambio en un límite de cuota existente, ya que cambia el límite de disco de la cuota de usuario derivada para el jsmith de usuario del volumen. Por lo tanto, no es necesario que se reinicien las cuotas en el volumen para activar el cambio.

Para cambiar el tamaño de las cuotas:

```
cluster1::>volume quota resize -vserver vs1 -volume vol1 -foreground
```

Las cuotas permanecen vigentes mientras cambia el tamaño, y el proceso de cambio de tamaño es breve.

El informe de cuotas resultante es similar al siguiente informe:

```
cluster1::> volume quota report
Vserver: vs1
```

| Volume | Tree | Type | ID | ----Disk---- | | ----Files---- | | Quota |
|-----------|-------|-------|--------|--------------|-------|---------------|-------|--------|
| | | | | Used | Limit | Used | Limit | |
| Specifier | | | | | | | | |
| ----- | ----- | ----- | ----- | ----- | ----- | ----- | ----- | |
| vol1 | | user | * | 0B | 50MB | 0 | - | * |
| vol1 | | user | jsmith | 50MB | 80MB | 37 | - | jsmith |
| vol1 | | user | root | 0B | - | 1 | - | |

3 entries were displayed.

La segunda línea muestra ahora un límite de disco de 80 MB y un especificador de cuota de jsmith.

Por lo tanto, jsmith puede utilizar hasta 80 MB de espacio en vol1, aunque todos los demás usuarios todavía están limitados a 50 MB.

Ejemplo 3: Umbrales

Supongamos que desea recibir una notificación cuando los usuarios alcanzan los 5 MB de sus límites de disco. Para crear un umbral de 45 MB para todos los usuarios y un umbral de 75 MB para jsmith, se cambian las reglas de cuota existentes:

```
cluster1::>volume quota policy rule modify -vserver vs1 -policy
quota_policy_vs1_1 -volume voll -type user -target "" -qtree "" -threshold
45MB
cluster1::>volume quota policy rule modify -vserver vs1 -policy
quota_policy_vs1_1 -volume voll -type user -target jsmith -qtree ""
-threshold 75MB
```

Dado que se modifican los tamaños de las reglas existentes, se cambia el tamaño de las cuotas en el volumen para activar los cambios. Espere hasta que termine el proceso de cambio de tamaño.

Para ver el informe de cuotas con umbrales, agregue `-thresholds` parámetro de la `volume quota report` comando:

```
cluster1::>volume quota report -thresholds
Vserver: vs1
```

| Volume | Tree | Type | ID | ----Disk---- | | ----Files----- | | Quota |
|-----------|-------|-------|--------|--------------|----------------|----------------|-------|--------|
| | | | | Used | Limit | Used | Limit | |
| | | | | (Thold) | | | | |
| Specifier | | | | | | | | |
| ----- | ----- | ----- | ----- | ----- | ----- | ----- | ----- | |
| voll | | user | * | 0B | 50MB (45MB) | 0 | - | * |
| voll | | user | jsmith | 59MB | 80MB (75MB) | 55 | - | jsmith |
| voll | | user | root | 0B | - (-) | 1 | - | |

3 entries were displayed.

Los umbrales aparecen entre paréntesis en la columna Disk Limit.

Ejemplo 4: Cuotas de qtrees

Supongamos que necesita particionar un poco de espacio para dos proyectos. Puede crear dos qtrees, llamados `projo1` y `proja2`, para alojar esos proyectos dentro del `voll1`.

Actualmente, los usuarios pueden usar tanto espacio en un qtree como se asignan para todo el volumen (siempre y cuando no superen el límite del volumen utilizando el espacio en la raíz u otro qtree). Además, cada uno de los qtrees puede crecer para consumir el volumen completo. Si desea asegurarse de que ninguno de los qtrees supere los 20 GB, puede crear una cuota de árbol predeterminada en el volumen:

```
cluster1:>>volume quota policy rule create -vserver vs1 -policy-name
quota_policy_vs1_1 -volume voll -type tree -target "" -disk-limit 20GB
```

Observe que el tipo correcto es *tree*, no *Qtree*.

Como se trata de una cuota nueva, no se puede activar cambiando el tamaño. Las cuotas se reinician en el volumen:

```
cluster1:>>volume quota off -vserver vs1 -volume voll
cluster1:>>volume quota on -vserver vs1 -volume voll -foreground
```



Debe asegurarse de esperar unos cinco minutos antes de volver a activar las cuotas en cada volumen afectado, ya que intenta activarlos casi inmediatamente después de ejecutar el `volume quota off` el comando puede generar errores. Como alternativa, es posible ejecutar los comandos para volver a inicializar las cuotas de un volumen desde el nodo que contiene el volumen en particular.

Las cuotas no se aplican durante el proceso de reinicialización, lo que lleva más tiempo que el proceso de redimensionamiento.

Cuando se muestra un informe de cuotas, tiene varias líneas nuevas: Algunas líneas son para las cuotas de árbol y algunas líneas para las cuotas de usuario derivadas.

Las siguientes líneas nuevas son para las cuotas de árbol:

| Volume | Tree | Type | ID | ----Disk---- | ----Files----- | Quota | |
|-----------|-------|-------|-------|--------------|----------------|-------|---------|
| Specifier | | | | Used | Limit | Used | Limit |
| ----- | ----- | ----- | ----- | ----- | ----- | ----- | ----- |
| ... | | | | | | | |
| voll | | tree | * | 0B | 20GB | 0 | - * |
| voll | proj1 | tree | 1 | 0B | 20GB | 1 | - proj1 |
| voll | proj2 | tree | 2 | 0B | 20GB | 1 | - proj2 |
| ... | | | | | | | |

La cuota de árbol predeterminada que ha creado aparece en la primera línea nueva, que tiene un asterisco (*) en la columna ID. En respuesta a la cuota de árbol predeterminada de un volumen, ONTAP crea automáticamente cuotas de árbol derivadas para cada qtree del volumen. Estos se muestran en las líneas en las que aparecen el proyecto 1 y el proyecto 2 en la columna árbol.

Las siguientes líneas nuevas son para cuotas de usuario derivadas:

| Volume Specifier | Tree | Type | ID | ----Disk---- | | ----Files----- | | Quota |
|---------------------|-------|-------|-------|--------------|-------|----------------|-------|-------|
| | | | | Used | Limit | Used | Limit | |
| ----- | ----- | ----- | ----- | ----- | ----- | ----- | ----- | |
| ----- | | | | | | | | |
| ... | | | | | | | | |
| vol1 | proj1 | user | * | 0B | 50MB | 0 | - | |
| vol1 | proj1 | user | root | 0B | - | 1 | - | |
| vol1 | proj2 | user | * | 0B | 50MB | 0 | - | |
| vol1 | proj2 | user | root | 0B | - | 1 | - | |
| ... | | | | | | | | |

Las cuotas de usuario predeterminadas de un volumen se heredan automáticamente para todos los qtrees que contiene ese volumen, si se habilitan las cuotas para qtrees. Al añadir la primera cuota de qtree, se han habilitado cuotas en qtrees. Por lo tanto, se crearon cuotas de usuario predeterminadas derivadas para cada qtree. Se muestran en las líneas donde el ID es un asterisco (*).

Como el usuario raíz es el propietario de un archivo, cuando se crearon cuotas de usuario predeterminadas para cada uno de los qtrees, también se crearon cuotas de seguimiento especiales para el usuario raíz de cada uno de los qtrees. Estos se muestran en las líneas en las que el ID es raíz.

Ejemplo 5: Cuota de usuario en un qtree

Decide limitar a los usuarios a menos espacio en el qtree del proyecto 1 del que consiguen en el volumen como un todo. Desea evitar que utilicen más de 10 MB en el qtree del proyecto 1. Por lo tanto, debe crear una cuota de usuario predeterminada para el qtree:

```
cluster1::>volume quota policy rule create -vserver vs1 -policy-name
quota_policy_vs1_1 -volume vol1 -type user -target "" -disk-limit 10MB
-qtrees proj1
```

Se trata de un cambio en una cuota existente, ya que cambia la cuota de usuario predeterminada para el qtree proj1 que se derivó de la cuota de usuario predeterminada del volumen. Por lo tanto, puede activar el cambio cambiando el tamaño de las cuotas. Una vez completado el proceso de cambio de tamaño, puede ver el informe de cuotas.

En el informe de cuotas se muestra la siguiente línea nueva que muestra la nueva cuota de usuario explícita para el qtree:

| Volume Specifier | Tree | Type | ID | ----Disk---- | | ----Files----- | | Quota |
|---------------------|-------|-------|-------|--------------|-------|----------------|-------|-------|
| | | | | Used | Limit | Used | Limit | |
| ----- | ----- | ----- | ----- | ----- | ----- | ----- | ----- | |
| ----- | | | | | | | | |
| vol1 | proj1 | user | * | 0B | 10MB | 0 | - | * |

Sin embargo, se está impidiendo al usuario jsmith escribir más datos en el qtree proj1 porque la cuota que

creó para anular la cuota de usuario predeterminada (para proporcionar más espacio) se encontraba en el volumen. Tal como se ha añadido una cuota de usuario predeterminada en el qtree proj1, se está aplicando esa cuota y se limita todo el espacio del usuario en ese qtree, incluido jsmith. Para proporcionar más espacio al jsmith de usuario, se debe añadir una regla de cuota de usuario explícita para el qtree con un límite de disco de 80 MB para anular la regla de cuota de usuario predeterminada para el qtree:

```
cluster1::>volume quota policy rule create -vserver vs1 -policy-name
quota_policy_vs1_1 -volume voll1 -type user -target jsmith -disk-limit 80MB
-qtree proj1
```

Como se trata de una cuota explícita para la que ya existe una cuota predeterminada, se activa el cambio mediante el cambio de tamaño de las cuotas. Una vez completado el proceso de cambio de tamaño, se muestra un informe de cuota.

En el informe de cuotas aparece la siguiente línea nueva:

| Volume Specifier | Tree | Type | ID | ----Disk---- | | ----Files----- | | Quota |
|---------------------|-------|------|--------|--------------|-------|----------------|-------|--------|
| | | | | Used | Limit | Used | Limit | |
| | | | | Specifier | | | | |
| | | | | ----- | ----- | ----- | ----- | |
| voll1 | proj1 | user | jsmith | 61MB | 80MB | 57 | - | jsmith |

El informe final sobre cuotas es similar al siguiente informe:

```
cluster1::>volume quota report
Vserver: vs1

Volume  Tree      Type  ID      ----Disk----  ----Files-----  Quota
Specifier
-----
voll1      tree      *      0B      20GB      0      -      *
voll1      user      *      0B      50MB      0      -      *
voll1      user      jsmith 70MB     80MB     65     -      jsmith
voll1      proj1     tree    1      0B      20GB     1      -      proj1
voll1      proj1     user    *      0B      10MB     0      -      *
voll1      proj1     user    root   0B      -        1      -      -
voll1      proj2     tree    2      0B      20GB     1      -      proj2
voll1      proj2     user    *      0B      50MB     0      -      -
voll1      proj2     user    root   0B      -        1      -      -
voll1      proj2     user    root   0B      -        3      -      -
voll1      proj1     user    jsmith 61MB     80MB     57     -      jsmith
11 entries were displayed.
```

El jsmith de usuario debe cumplir los siguientes límites de cuota para escribir en un archivo de proj1:

1. La cuota de árbol para el qtree del proyecto 1.
2. La cuota de usuario en el qtree del proyecto 1.
3. La cuota de usuario en el volumen.

Configurar cuotas en un SVM

Para configurar cuotas en una nueva máquina virtual de almacenamiento (SVM, antes conocida como Vserver), debe crear una política de cuotas, agregar reglas de política de cuotas a la política, asignar la política a la SVM e inicializar cuotas en cada volumen FlexVol de la SVM.

Pasos

1. Introduzca el comando `vserver show -instance` Para mostrar el nombre de la política de cuotas predeterminada que se creó automáticamente al crear la SVM.

Si no se especificó un nombre cuando se creó la SVM, el nombre es "predeterminado". Puede utilizar el `vserver quota policy rename` para asignar un nombre a la directiva predeterminada.



También puede crear una nueva directiva con el `volume quota policy create` comando.

2. Utilice la `volume quota policy rule create` Comando para crear *any* de las siguientes reglas de cuota para cada volumen de la SVM:
 - Reglas de cuota predeterminadas para todos los usuarios
 - Reglas de cuota explícitas para usuarios específicos
 - Reglas de cuota predeterminadas para todos los grupos
 - Reglas explícitas de cuotas para grupos específicos
 - Reglas de cuota predeterminadas para todos los qtrees
 - Reglas de cuota explícitas para qtrees específicos
3. Utilice la `volume quota policy rule show` comando para comprobar que las reglas de cuota están configuradas correctamente.
4. Si está trabajando en una nueva directiva, utilice la `vserver modify` Comando para asignar la nueva política a la SVM.
5. Utilice la `volume quota on` Comando para inicializar las cuotas de cada volumen en la SVM.

Puede supervisar el proceso de inicialización de las siguientes maneras:

- Cuando utilice la `volume quota on` puede agregar el `-foreground` parámetro para ejecutar la cuota en el trabajo en primer plano. (De forma predeterminada, el trabajo se ejecuta en segundo plano).

Cuando el trabajo se ejecuta en segundo plano, puede supervisar su progreso mediante el `job show` comando.

- Puede utilizar el `volume quota show` comando para supervisar el estado de inicialización de la

cuota.

6. Utilice la `volume quota show -instance` comando para comprobar si hay errores de inicialización, como reglas de cuota que no se han podido inicializar.
7. Utilice la `volume quota report` comando para mostrar un informe de cuotas de forma que pueda garantizar que las cuotas forzadas se ajustan a sus expectativas.

Modificar (o redimensionar) los límites de cuota

Cuando se realizan cambios en el tamaño de las cuotas existentes, se puede cambiar el tamaño de las cuotas en todos los volúmenes afectados, lo que es más rápido que reinicializar las cuotas en esos volúmenes.

Acerca de esta tarea

Tiene una máquina virtual de almacenamiento (SVM, anteriormente conocida como Vserver) con cuotas forzadas y desea cambiar los límites de tamaño de las cuotas existentes o añadir o eliminar cuotas para destinos que ya tienen cuotas derivadas.

Pasos

1. Utilice la `vserver show` con el `-instance` El parámetro para determinar el nombre de la política actualmente asignada a la SVM.
2. Modifique las reglas de cuota realizando cualquiera de las siguientes acciones:
 - Utilice la `volume quota policy rule modify` para modificar los límites de disco o archivo de las reglas de cuota existentes.
 - Utilice la `volume quota policy rule create` comando para crear reglas de cuota explícitas para destinos (usuarios, grupos o qtrees) que actualmente tienen cuotas derivadas.
 - Utilice la `volume quota policy rule delete` comando para eliminar reglas de cuota explícitas para destinos (usuarios, grupos o qtrees) que también tienen cuotas predeterminadas.
3. Utilice la `volume quota policy rule show` comando para comprobar que las reglas de cuota están configuradas correctamente.
4. Utilice la `volume quota resize` comando en cada volumen donde se han modificado las cuotas para activar los cambios en cada volumen.

Puede supervisar el proceso de cambio de tamaño de una de las siguientes formas:

- Cuando utilice la `volume quota resize` puede agregar el `-foreground` parámetro para ejecutar el trabajo de cambio de tamaño en primer plano. (De forma predeterminada, el trabajo se ejecuta en segundo plano).

Cuando el trabajo se ejecuta en segundo plano, puede supervisar su progreso mediante el `job show` comando.

- Puede utilizar el `volume quota show` comando para supervisar el tamaño del estado.

5. Utilice la `volume quota show -instance` comando para comprobar si hay errores de cambio de tamaño como, por ejemplo, reglas de cuota que no se han podido cambiar de tamaño.

En particular, compruebe si hay errores de «nueva definición», que se producen cuando se cambia el tamaño de las cuotas después de agregar una cuota explícita para un destino que no tiene ya una cuota derivada.

6. Utilice la `volume quota report` comando para mostrar un informe de cuotas de forma que pueda garantizar que las cuotas forzadas se ajustan a sus requisitos.

Reinicializar las cuotas después de realizar cambios extensos

Cuando se realizan cambios extensos en las cuotas existentes; por ejemplo, al agregar o eliminar cuotas para los destinos que no tienen cuotas forzadas, se deben realizar los cambios y volver a inicializar cuotas en todos los volúmenes afectados.

Acerca de esta tarea

Tiene una máquina virtual de almacenamiento (SVM) con cuotas forzadas y desea realizar cambios que requieran una reinicialización completa de las cuotas.

Pasos

1. Utilice la `vserver show` con el `-instance` El parámetro para determinar el nombre de la política actualmente asignada a la SVM.
2. Modifique las reglas de cuota realizando cualquiera de las siguientes acciones:

| Si desea... | Realice lo siguiente... |
|--|---|
| Crear nuevas reglas de cuota | Utilice la <code>volume quota policy rule create</code> comando |
| Modifique la configuración de las reglas de cuota existentes | Utilice la <code>volume quota policy rule modify</code> comando |
| Eliminar reglas de cuota existentes | Utilice la <code>volume quota policy rule delete</code> comando |

3. Utilice la `volume quota policy rule show` comando para comprobar que las reglas de cuota están configuradas correctamente.
4. Vuelva a inicializar las cuotas en cada volumen en el que haya modificado las cuotas desactivando las cuotas y, a continuación, activando las cuotas para dichos volúmenes.
 - a. Utilice la `volume quota off` comando en cada volumen afectado para desactivar las cuotas de ese volumen.
 - b. Utilice la `volume quota on` comando en cada volumen afectado para activar cuotas en ese volumen.



Debe asegurarse de esperar unos cinco minutos antes de volver a activar las cuotas en cada volumen afectado, ya que intenta activarlos casi inmediatamente después de ejecutar el `volume quota off` el comando puede generar errores.

Como alternativa, es posible ejecutar los comandos para volver a inicializar las cuotas de un volumen desde el nodo que contiene el volumen en particular.

Puede supervisar el proceso de inicialización de cualquiera de las siguientes maneras:

- Cuando utilice la `volume quota on` puede agregar el `-foreground` parámetro para ejecutar la cuota en el trabajo en primer plano. (De forma predeterminada, el trabajo se ejecuta en segundo

plano).

Cuando el trabajo se ejecuta en segundo plano, puede supervisar su progreso mediante el `job show` comando.

- Puede utilizar el `volume quota show` comando para supervisar el estado de inicialización de la cuota.
5. Utilice la `volume quota show -instance` comando para comprobar si hay errores de inicialización, como reglas de cuota que no se han podido inicializar.
 6. Utilice la `volume quota report` comando para mostrar un informe de cuotas de forma que pueda garantizar que las cuotas forzadas se ajustan a sus expectativas.

Comandos para gestionar reglas de cuota y directivas de cuota

Puede utilizar el `volume quota policy rule` comandos para configurar las reglas de cuota y utilizar `volume quota policy` comandos y algunos `vserver` comandos para configurar las directivas de cuota.



Los siguientes comandos solo se pueden ejecutar en volúmenes de FlexVol.

Comandos para administrar reglas de cuota

| Si desea... | Se usa este comando... |
|--|--|
| Cree una nueva regla de cuota | <code>volume quota policy rule create</code> |
| Eliminar una regla de cuota existente | <code>volume quota policy rule delete</code> |
| Modifique una regla de cuota existente | <code>volume quota policy rule modify</code> |
| Muestra información acerca de las reglas de cuota configuradas | <code>volume quota policy rule show</code> |

Comandos para gestionar políticas de cuotas

| Si desea... | Se usa este comando... |
|--|---|
| Duplique una política de cuota y las reglas de cuota que contiene | <code>volume quota policy copy</code> |
| Cree una nueva política de cuota en blanco | <code>volume quota policy create</code> |
| Eliminar una política de cuotas existente que no está asignada actualmente a una máquina virtual de almacenamiento (SVM) | <code>volume quota policy delete</code> |
| Cambiar el nombre de una política de cuota | <code>volume quota policy rename</code> |

| Si desea... | Se usa este comando... |
|---|---|
| Mostrar información sobre las políticas de cuota | <code>volume quota policy show</code> |
| Asigne una política de cuotas a una SVM | <code>vserver modify -quota-policy policy_name</code> |
| Muestre el nombre de la política de cuotas asignada a una SVM | <code>vserver show</code> |

Consulte ["Referencia de comandos de la ONTAP"](#) para cada comando para obtener más información.

Comandos para activar y modificar cuotas

Puede utilizar el `volume quota` comandos para cambiar el estado de las cuotas y configurar el registro de mensajes de las cuotas.

| Si desea... | Se usa este comando... |
|---|----------------------------------|
| Activar las cuotas (también llamadas <i>inicializando</i> ellas) | <code>volume quota on</code> |
| Cambiar el tamaño de las cuotas existentes | <code>volume quota resize</code> |
| Desactivar cuotas | <code>volume quota off</code> |
| Cambie el registro de mensajes de cuotas, active las cuotas, desactive las cuotas o cambie el tamaño de las cuotas existentes | <code>volume quota modify</code> |

Consulte la página de manual de cada comando para obtener más información.

Use la deduplicación, la compresión y la compactación de datos para aumentar la eficiencia del almacenamiento

Utilice la deduplicación, la compresión y la compactación de datos para aumentar la información general de la eficiencia del almacenamiento

Puede ejecutar la deduplicación, la compresión y la compactación de datos de forma conjunta o de forma independiente para lograr un ahorro de espacio óptimo en un volumen de FlexVol. La deduplicación elimina los bloques de datos duplicados. La compresión de datos comprime los bloques de datos para reducir la cantidad de almacenamiento físico necesaria. La compactación de datos almacena más datos en menos espacio para aumentar la eficiencia del almacenamiento.



A partir de ONTAP 9.2, todas las funciones de eficiencia del almacenamiento en línea, como la deduplicación inline y la compresión inline, se habilitan de forma predeterminada en los volúmenes AFF.

Active la deduplicación en un volumen

Puede activar la deduplicación en un volumen de FlexVol para obtener eficiencia del almacenamiento. Puede habilitar la deduplicación postprocesamiento en todos los volúmenes y la deduplicación inline en los volúmenes que residen en agregados de AFF o Flash Pool.

Si desea habilitar la deduplicación en línea en otros tipos de volúmenes, consulte el artículo de la base de conocimientos "[Cómo habilitar la deduplicación en línea de volúmenes en agregados que no son AFF \(All Flash FAS\)](#)".

Lo que necesitará

En un volumen FlexVol, debe haber verificado que hay espacio libre suficiente para los metadatos de la deduplicación en volúmenes y agregados. Los metadatos de la deduplicación requieren una cantidad mínima de espacio libre en el agregado. Esta cantidad equivale al 3 % de la cantidad total de datos físicos de todos los volúmenes FlexVol o componentes de datos deduplicados en el agregado. Cada uno de los volúmenes de FlexVol o componente de datos debe tener el 4% del total de datos físicos en espacio libre, para un total del 7%.



A partir de ONTAP 9.2, la deduplicación inline está habilitada de forma predeterminada en los sistemas AFF.

Opciones

- Utilice la `volume efficiency on` comando para habilitar la deduplicación postprocesamiento.

El siguiente comando habilita la deduplicación postprocesamiento en el volumen VolA:

```
volume efficiency on -vserver vs1 -volume VolA
```

- Utilice la `volume efficiency on` comando seguido de `volume efficiency modify` con el `-inline-deduplication` opción establecida en `true` para habilitar tanto la deduplicación postprocesamiento como la deduplicación en línea.

Los siguientes comandos permiten la deduplicación postprocesamiento y la deduplicación inline en el volumen VolA:

```
volume efficiency on -vserver vs1 -volume VolA
```

```
volume efficiency modify -vserver vs1 -volume VolA -inline-dedupe true
```

- Utilice la `volume efficiency on` comando seguido de `volume efficiency modify` con el `-inline-deduplication` opción establecida en `true` y la `-policy` opción establecida en `inline-only` para habilitar solo la deduplicación inline.

Los siguientes comandos permiten solo la deduplicación en línea en el volumen VolA:

```
volume efficiency on -vserver vs1 -volume VolA
```



```
volume efficiency modify -vserver vs1 -volume VolA -policy inline-only -inline
-dedupe true
```

Después de terminar

Compruebe que la configuración haya cambiado viendo la configuración de eficiencia del volumen:

```
volume efficiency show -instance
```

Desactivar la deduplicación en un volumen

Puede deshabilitar la deduplicación postprocesamiento y la deduplicación en línea de forma independiente en un volumen.

Lo que necesitará

Detenga cualquier operación de eficiencia de volumen que esté activa actualmente en el volumen: `volume efficiency stop`

Acerca de esta tarea

Si ha habilitado la compresión de datos en el volumen, ejecute el `volume efficiency off` el comando deshabilita la compresión de datos.

Opciones

- Utilice la `volume efficiency off` comando para deshabilitar tanto la deduplicación postprocesamiento como la deduplicación en línea.

El siguiente comando deshabilita la deduplicación postprocesamiento y la deduplicación en línea en el volumen Vola:

```
volume efficiency off -vserver vs1 -volume VolA
```

- Utilice la `volume efficiency modify` con el `-policy` opción establecida en `inline only` para deshabilitar la deduplicación postprocesamiento, pero la deduplicación en línea sigue estando habilitada.

El siguiente comando deshabilita la deduplicación postprocesamiento, pero la deduplicación inline permanece habilitada en el volumen Vola:

```
volume efficiency modify -vserver vs1 -volume VolA -policy inline-only
```

- Utilice la `volume efficiency modify` con el `-inline-deduplication` opción establecida en `false` para deshabilitar solo la deduplicación inline.

El siguiente comando deshabilita solo la deduplicación en línea en el volumen Vola:

```
volume efficiency modify -vserver vs1 -volume VolA -inline-deduplication false
```

Gestione la deduplicación automática en segundo plano a nivel de volumen en sistemas AFF

A partir de la versión 9.3 de ONTAP, es posible gestionar la deduplicación en segundo plano en el nivel de volumen para ejecutarlos automáticamente con un valor predefinido `auto` Política de AFF. No se requiere ninguna configuración manual de los programas. La `auto` la normativa realiza una deduplicación continua en segundo plano.

La `auto` la política se establece para todos los volúmenes nuevos y para todos los volúmenes actualizados que no se configuraron manualmente para la deduplicación en segundo plano. Puede cambiar la política a `default` o cualquier otra directiva para deshabilitar la función.

Si un volumen cambia de un sistema distinto a AFF a un sistema AFF, el `auto` la política está habilitada en el nodo de destino de manera predeterminada. Si un volumen se mueve de un nodo AFF a otro no AFF, el `auto` la política del nodo de destino se reemplaza por la `inline-only` política de forma predeterminada.

En AFF, el sistema supervisa todos los volúmenes que tienen el `auto` política y despriorización del volumen que tenga menos ahorro o que tenga sobrescrituras frecuentes. Los volúmenes con prioridad desprioritarios ya no participan en la deduplicación automática en segundo plano. El registro de cambios en volúmenes desprioritarios está deshabilitado y se truncan los metadatos del volumen.

Los usuarios pueden promover el volumen sin prioridad para reparticipar en una deduplicación automática en segundo plano mediante el `volume efficiency promote` comando disponible en el nivel de privilegio avanzado.

Gestione la deduplicación inline a nivel de agregado en sistemas AFF

La deduplicación a nivel de agregado elimina los bloques duplicados en los volúmenes que pertenecen al mismo agregado. A partir de ONTAP 9.2, puede realizar deduplicación a nivel de agregado en línea en sistemas AFF. La función está habilitada de forma predeterminada en todos los volúmenes nuevos y en todos los volúmenes actualizados en los que se haya activado la deduplicación en línea del volumen.

Acerca de esta tarea

La operación de deduplicación elimina los bloques duplicados antes de que se escriban los datos en el disco. Solo volúmenes con `space guarantee` establezca en `none` puede participar en la deduplicación en línea de nivel de agregado. Esta es la configuración predeterminada en sistemas AFF.



La deduplicación en línea a nivel de agregado se denomina en ocasiones deduplicación en línea entre volúmenes.

Paso

- 1. Gestione la deduplicación inline a nivel de agregado en los sistemas AFF:

| Si desea... | Utilice este comando |
|--|---|
| Habilite la deduplicación inline a nivel de agregado | <code>volume efficiency modify -vserver vserver_name -volume vol_name -cross -volume-inline-dedupe true</code> |
| Desactive la deduplicación en línea en el nivel del agregado | <code>volume efficiency modify -vserver vserver_name -volume vol_name -cross -volume-inline-dedupe false</code> |
| Muestra el estado de deduplicación en línea en el nivel del agregado | <code>volume efficiency config -volume vol_name</code> |

Ejemplos

El siguiente comando muestra el estado de deduplicación en línea en el nivel del agregado:

```
wfit-8020-03-04::> volume efficiency config -volume choke0_wfit_8020_03_0
Vserver:                                vs0
Volume:                                choke0_wfit_8020_03_0
Schedule:                               -
Policy:                                 choke_VE_policy
Compression:                            true
Inline Compression:                      true
Inline Dedupe:                           true
Data Compaction:                         true
Cross Volume Inline Deduplication:       false
```

Gestione la deduplicación en segundo plano a nivel agregado en sistemas AFF

La deduplicación a nivel de agregado elimina los bloques duplicados en los volúmenes que pertenecen al mismo agregado. A partir de ONTAP 9.3, puede realizar deduplicación a nivel de agregado en segundo plano en sistemas AFF. La función está habilitada de forma predeterminada en todos los volúmenes nuevos y en todos los volúmenes actualizados en los que se haya activado la deduplicación en segundo plano de los volúmenes.

Acerca de esta tarea

La operación se activa automáticamente cuando se completa un porcentaje lo suficientemente grande del registro de cambios. No hay ninguna programación o política asociada con la operación.

A partir de ONTAP 9.4, los usuarios de AFF también pueden ejecutar el análisis de deduplicación en el nivel agregado para eliminar los duplicados de los datos existentes en los volúmenes del agregado. Puede utilizar el `storage aggregate efficiency cross-volume-dedupe start` con el `-scan-old-data=true` opción para iniciar el escáner:

```
cluster-1::> storage aggregate efficiency cross-volume-dedupe start
-aggregate aggr1 -scan-old-data true
```

El análisis de la deduplicación puede requerir mucho tiempo. Se recomienda ejecutar la operación en horas de menor actividad.



La deduplicación en segundo plano a nivel de agregado se denomina en ocasiones deduplicación en segundo plano entre volúmenes.

Paso

1. Gestione la deduplicación en segundo plano a nivel agregado en los sistemas AFF:

| Si desea... | Utilice este comando |
|--|--|
| Habilite la deduplicación en segundo plano a nivel del agregado | <code>volume efficiency modify -vserver <vserver_name> -volume <vol_name> -cross-volume-background-dedupe true</code> |
| Desactive la deduplicación en segundo plano en el nivel del agregado | <code>volume efficiency modify -vserver <vserver_name> -volume <vol_name> -cross-volume-background-dedupe false</code> |
| Muestra el estado de deduplicación en segundo plano en el nivel del agregado | <code>aggregate efficiency cross-volume-dedupe show</code> |

Descripción general de la eficiencia del almacenamiento en la que la temperatura es importante

ONTAP ofrece ventajas en eficiencia del almacenamiento sensible a la temperatura; para ello, evalúa la frecuencia con la que se accede a los datos del volumen y asigna esa frecuencia al grado de compresión aplicado a esos datos. En el caso de los datos inactivos a los que se accede con poca frecuencia, se comprimen los bloques de datos más grandes, y en el caso de los datos activos, a los que se accede con frecuencia y se sobrescriben con mayor frecuencia, se comprimen los bloques de datos más pequeños, lo que hace que el proceso sea más eficiente.

La eficiencia del almacenamiento sensible a la temperatura (TSSE) se introduce en ONTAP 9,8 y se activa automáticamente en los volúmenes AFF con Thin Provisioning recientemente creados. Se puede habilitar la eficiencia del almacenamiento sensible a la temperatura en volúmenes AFF existentes y en volúmenes de DP que no sean AFF con Thin-Provisioning.

Introducción de los modos «predeterminado» y «eficiente»

A partir de ONTAP 9.10.1, se introducen dos modos de eficiencia de almacenamiento a nivel de volumen solo para sistemas AFF, *default* y *efficient*. Los dos modos proporcionan una opción entre compresión de archivo (predeterminado), que es el modo predeterminado cuando se crean nuevos volúmenes AFF, o la eficiencia del almacenamiento sensible a la temperatura (eficiente), que permite una eficiencia del almacenamiento sensible a la temperatura. Con ONTAP 9.10.1, ["debe definirse explícitamente la eficacia del almacenamiento sensible a la temperatura"](#) para activar la compresión adaptativa automática. Sin embargo, otras funciones de eficiencia del almacenamiento, como la compactación de datos, la programación de deduplicación automática, la deduplicación inline, la deduplicación inline entre volúmenes y la deduplicación en segundo plano entre volúmenes, están habilitadas de forma predeterminada en las plataformas de AFF, tanto en los modos predeterminados como eficientes.

Los dos modos de eficiencia del almacenamiento (predeterminado y eficiente) son compatibles con los agregados habilitados para FabricPool y con todos los tipos de políticas de organización en niveles.

La eficiencia del almacenamiento sensible a la temperatura habilitada en plataformas C-Series

La eficiencia del almacenamiento sensible a la temperatura se activa de forma predeterminada en las plataformas AFF C-Series y cuando se migran volúmenes de una plataforma no TSSE a una plataforma C-Series habilitada para TSSE mediante Volume Move o SnapMirror con las siguientes versiones instaladas en el destino:

- ONTAP 9.12.1P4 y versiones posteriores
- ONTAP 9.13.1 y versiones posteriores

Para obtener más información, consulte ["Comportamiento de la eficiencia del almacenamiento con movimiento de volúmenes y operaciones de SnapMirror"](#).

En el caso de los volúmenes existentes, la eficiencia del almacenamiento sensible a la temperatura no se habilita automáticamente; sin embargo, sí puede ["modifique el modo de eficiencia del almacenamiento"](#) manualmente para cambiar al modo eficiente.



Una vez que cambia el modo de eficiencia del almacenamiento a Eficiencia, no se puede volver a cambiar.

Eficiencia del almacenamiento mejorada con paquetes secuenciales de bloques físicos contiguos

A partir de ONTAP 9.13.1, la eficiencia del almacenamiento sensible a la temperatura añade paquetes secuenciales de bloques físicos contiguos para mejorar aún más la eficiencia del almacenamiento. Los volúmenes con eficiencia del almacenamiento sensible a la temperatura habilitada tienen habilitado automáticamente el empaquetado secuencial al actualizar los sistemas a ONTAP 9.13.1. Una vez activado el empaquetado secuencial, debe hacerlo ["volver a copiar manualmente los datos existentes"](#).

Consideraciones de renovación

Cuando se actualiza a ONTAP 9.10.1 y versiones posteriores, se asigna a los volúmenes existentes un modo de eficiencia del almacenamiento según el tipo de compresión actualmente habilitado en los volúmenes. Durante una actualización, se asigna el modo predeterminado a los volúmenes con compresión habilitada y se asigna el modo eficiente a los volúmenes con eficiencia de almacenamiento sensible a la temperatura habilitada. Si la compresión no está habilitada, el modo de eficiencia del almacenamiento sigue vacío.

Comportamiento de la eficiencia del almacenamiento con movimiento de volúmenes y operaciones de SnapMirror

La forma en que la eficiencia del almacenamiento se comporta de un volumen cuando se ejecuta un movimiento de volúmenes o una operación de SnapMirror y lo que sucede cuando se realiza una interrupción de SnapMirror y se habilita manualmente la eficiencia del almacenamiento sensible a la temperatura depende del tipo de eficiencia del volumen de origen.

En la siguiente tabla se describe el comportamiento de un volumen de origen y de destino cuando se ejecuta un movimiento de volúmenes o una operación de SnapMirror con diferentes tipos de eficiencia del almacenamiento, así como el comportamiento cuando se habilita manualmente la eficiencia del almacenamiento sensible a la temperatura (TSSE).

| Eficiencia del volumen de origen | Comportamiento predeterminado del volumen de destino | | | Comportamiento predeterminado después de habilitar manualmente TSSE (tras la interrupción de SnapMirror) | | |
|----------------------------------|--|--------------------------|-------------------------------|--|--------------------------|-------------------------------|
| | * Tipo de eficiencia de almacena miento* | Nuevas escrituras | * Compresión de datos fríos * | * Tipo de eficiencia de almacena miento* | Nuevas escrituras | * Compresión de datos fríos * |
| | | | | | | |

| | | | | | | |
|--|--|--|--|--|---|--|
| Sin eficiencia de almacenamiento (probablemente FAS) | Compresión de archivos | La compresión de archivos se intenta en línea en los datos recién escritos | Sin compresión de datos inactivos; los datos permanecen tal cual | TSSE con algoritmo de exploración de datos fríos como ZSTD | La compresión en línea de 8K se intenta en formato TSSE | <p>Datos comprimidos de archivo: N/A</p> <p>Datos descomprimidos: Se intentó una compresión de 32K después de los días límite</p> <p>Datos recién escritos: 32K intento de compresión después de los días de umbral cumplidos</p> |
| Sin eficiencia de almacenamiento (probablemente FAS) | Compresión de archivos en plataformas C-Series utilizando ONTAP 9.11.1P10 o ONTAP 9.12.1P3 | Sin compresión de datos inactivos compatible con TSSE | Datos comprimidos de archivo: N/A | TSSE con algoritmo de exploración de datos fríos como ZSTD | Compresión en línea de 8K Kb | <p>Datos comprimidos de archivo: N/A</p> <p>Datos descomprimidos: Se intentó una compresión de 32K después de los días límite</p> <p>Datos recién escritos: 32K intento de compresión después de los días de umbral cumplidos</p> |
| Sin eficiencia de almacenamiento (probablemente FAS) | TSSE en plataformas C-Series que utilizan ONTAP 9.12.1P4 y versiones posteriores, o ONTAP 9.13.1 y versiones posteriores | La compresión en línea de 8K se intenta en formato TSSE | <p>Datos comprimidos de archivo: N/A</p> <p>Datos descomprimidos: Se intentó una compresión de 32K después de los días límite</p> <p>Datos recién escritos: 32K intento de compresión después de los días de umbral cumplidos</p> | TSSE con algoritmo de exploración de datos fríos como ZSTD | La compresión en línea de 8K se intenta en formato TSSE | <p>Datos comprimidos de archivo: N/A</p> <p>Datos descomprimidos: Se intentó una compresión de 32K después de los días límite</p> <p>Datos recién escritos: 32K intento de compresión después de los días de umbral cumplidos</p> |

| | | | | | | |
|---------------------------------|---|--|---|---|---|--|
| Grupo de compresión de archivos | Igual que la fuente | La compresión de archivos se intenta en línea en los datos recién escritos | Sin compresión de datos inactivos; los datos permanecen tal cual | TSSE con algoritmo de exploración de datos fríos como ZSTD | La compresión en línea de 8K se intenta en formato TSSE | Datos comprimidos de archivo: No comprimidos Datos descomprimidos: Se intenta realizar la compresión 32K después de los días límite Datos recién escritos: La compresión 32K se intenta después de los días de umbral cumplidos |
| Exploración de datos fríos TSSE | TSSE usando el mismo algoritmo de compresión que el volumen de origen (LZOPro→LZOPro y ZSTD→ZSTD) | Se ha intentado realizar una compresión en línea de 8K MB en formato TSSE | La compresión 32K se intentó con LzoPro después de que se alcanzara la frialdad basada en días de umbral tanto en los datos existentes como en los datos recién escritos. | TSSE está activado. NOTA: El algoritmo de exploración de datos fríos de LZOPro se puede cambiar a ZSTD. | La compresión en línea de 8K se intenta en formato TSSE | La compresión de 32K MB se intenta una vez que se alcanza el umbral de frío tanto en los datos existentes como en los datos recién escritos. |

Configure el modo de eficiencia del almacenamiento durante la creación de un volumen


A partir de ONTAP 9.10.1, puede establecer el modo de eficiencia del almacenamiento al crear un nuevo volumen de AFF. Uso del parámetro `-storage-efficiency-mode`, puede especificar si el volumen utiliza el modo eficaz o el modo de rendimiento predeterminado. Los dos modos proporcionan una opción entre compresión de archivo (predeterminado), que es el modo predeterminado cuando se crean nuevos volúmenes AFF, o eficiencia del almacenamiento sensible a la temperatura (eficiente), que permite la eficiencia del almacenamiento sensible a la temperatura. La `-storage-efficiency-mode` No se admite el parámetro en volúmenes sin AFF ni en volúmenes de protección de datos.

Pasos

Puede realizar esta tarea mediante ONTAP System Manager o la interfaz de línea de comandos de ONTAP.

System Manager

A partir de ONTAP 9.10.1, se puede usar System Manager para permitir una mayor eficiencia de almacenamiento con la función de eficiencia del almacenamiento sensible a la temperatura. La eficiencia del almacenamiento basada en el rendimiento está habilitada de forma predeterminada.

1. Haga clic en **almacenamiento > volúmenes**.
2. Busque el volumen en el que desea habilitar o deshabilitar la eficiencia del almacenamiento y haga clic en .
3. Haga clic en **Editar > Volúmenes** y desplácese a **Eficiencia de almacenamiento**.
4. Seleccione **Activar mayor eficiencia de almacenamiento**.

CLI

Crear un nuevo volumen mediante el modo eficiente

Para establecer el modo de eficiencia de almacenamiento sensible a la temperatura al crear un nuevo volumen, puede utilizar el `-storage-efficiency-mode` parámetro con el valor `efficient`.

1. Cree un nuevo volumen con el modo de eficiencia habilitado:

```
volume create -vserver <vserver name> -volume <volume name> -aggregate  
<aggregate name> -size <volume size> -storage-efficiency-mode efficient
```

```
volume create -vserver vs1 -volume aff_vol1 -aggregate aff_aggr1  
-storage-efficiency-mode efficient -size 10g
```

Cree un nuevo volumen mediante el modo de rendimiento

El modo de rendimiento se establece de forma predeterminada cuando se crean nuevos volúmenes AFF con eficiencia del almacenamiento. Aunque no es obligatorio, puede utilizar opcionalmente el `default` valor con la `-storage-efficiency-mode` Parámetro cuando se crea un nuevo volumen de AFF.

1. Cree un nuevo volumen usando el modo de eficiencia del almacenamiento del rendimiento, «predeterminado»:

```
volume create -vserver <vserver name> -volume <volume name> -aggregate  
<aggregate name> -size <volume size> -storage-efficiency-mode default
```

```
volume create -vserver vs1 -volume aff_vol1 -aggregate aff_aggr1 -storage  
-efficiency-mode default -size 10g
```

Cambie el umbral de compresión de datos inactivos del volumen

Puede cambiar la frecuencia con la que ONTAP realiza un análisis de datos fríos modificando el umbral de frío en los volúmenes mediante la eficiencia del almacenamiento sensible a la temperatura.

Antes de empezar

Debe ser administrador de clústeres o de SVM y utilizar el nivel de privilegios avanzado de interfaz de línea de

comandos de ONTAP.

Acerca de esta tarea

El umbral de frialdad puede ser de 1 a 60 días. El umbral predeterminado es de 14 días.

Pasos

1. Establezca el nivel de privilegio:

```
set -privilege advanced
```

2. Modificar la compresión de datos inactivos en un volumen:

```
volume efficiency inactive-data-compression modify -vserver <vserver_name>  
-volume <volume_name> -threshold-days <integer>
```

Consulte la página de manual para obtener información adicional acerca de ["modificar la compresión de datos inactivos"](#).

Comprobar el modo de eficiencia del volumen

Puede utilizar el `volume-efficiency-show` Comando en un volumen de AFF para comprobar si la eficiencia está establecida y ver el modo de eficiencia actual.

Paso

1. Compruebe el modo de eficiencia en un volumen:

```
volume efficiency show -vserver <vserver name> -volume <volume name> -fields  
storage-efficiency-mode
```

Cambiar el modo de eficiencia del volumen

A partir de ONTAP 9.10.1, se introducen dos modos de eficiencia de almacenamiento a nivel de volumen solo para sistemas AFF, *default* y *efficient*. Los dos modos proporcionan una opción entre compresión de archivo (predeterminado), que es el modo predeterminado cuando se crean nuevos volúmenes AFF, o la eficiencia del almacenamiento sensible a la temperatura (eficiente), que permite una eficiencia del almacenamiento sensible a la temperatura. Puede utilizar el `volume efficiency modify` Comando para cambiar el modo de eficiencia del almacenamiento definido en un volumen AFF. Puede cambiar el modo desde `default` para `efficient` también puede establecer un modo de eficiencia cuando todavía no esté configurada la eficiencia del volumen.

Pasos

1. Cambie el modo de eficiencia de volumen:

```
volume efficiency modify -vserver <vserver name> -volume <volume name>  
-storage-efficiency-mode <default|efficient>
```

Vea el ahorro en huella de volumen con o sin eficiencia de almacenamiento sensible a la temperatura

A partir de ONTAP 9.11.1, puede utilizar el `volume show-footprint` comando para ver el ahorro de huella física en los volúmenes "Habilitado con eficiencia de almacenamiento sensible a la temperatura (TSSE)". A partir de ONTAP 9.13.1, puede usar el mismo comando para ver el ahorro de espacio físico en los volúmenes que no están habilitados con TSSE.

Paso

- 1. Vea el ahorro de la huella de volumen:

```
volume show-footprint
```

Salida de ejemplo con TSSE activado

| | | | |
|---------------------------|----------------------------|-------|--|
| Vserver | : vs0 | | |
| Volume | : vol_tsse_75_per_compress | | |
| Feature | Used | Used% | |
| ----- | ----- | ----- | |
| Volume Data Footprint | 10.15GB | 13% | |
| Volume Guarantee | 0B | 0% | |
| Flexible Volume Metadata | 64.25MB | 0% | |
| Delayed Frees | 235.0MB | 0% | |
| File Operation Metadata | 4KB | 0% | |
| Total Footprint | 10.45GB | 13% | |
| Footprint Data Reduction | 6.85GB | 9% | |
| Auto Adaptive Compression | 6.85GB | 9% | |
| Effective Total Footprint | 3.59GB | 5% | |

Salida de ejemplo sin TSSE activado

```
Vserver : vs0
Volume  : vol_file_cg_75_per_compress
```

| Feature | Used | Used% |
|------------------------------|------------|--------|
| ----- | ----- | ----- |
| Volume Data Footprint | 5.19GB | 7% |
| Volume Guarantee | 0B | 0% |
| Flexible Volume Metadata | 32.12MB | 0% |
| Delayed Frees | 90.17MB | 0% |
| File Operation Metadata | 4KB | 0% |
| Total Footprint | 5.31GB | 7% |
| Footprint Data Reduction | 1.05GB | 1% |
| Data Compaction | 1.05GB | 1% |
| Effective Total Footprint | 4.26GB | 5% |

Activar la compresión de datos en un volumen

Puede habilitar la compresión de datos en un volumen de FlexVol para lograr el ahorro de espacio mediante el `volume efficiency modify` comando. También puede asignar un tipo de compresión al volumen si no desea usar el tipo de compresión predeterminado.

Lo que necesitará

Debe haber habilitado la deduplicación en el volumen.



- La deduplicación solo tiene que estar activada y no es necesario estar en ejecución en el volumen.
- El escáner de compresión se debe utilizar para comprimir los datos existentes en los volúmenes presentes en las plataformas AFF.

"Activación de la deduplicación en un volumen"

Acerca de esta tarea

- En agregados de HDD y agregados de Flash Pool, puede habilitar la compresión en línea y de postprocesamiento o solo la compresión de postprocesamiento en un volumen.

Si está habilitando ambos, debe habilitar la compresión de postprocesamiento en el volumen antes de habilitar la compresión en línea.

- En las plataformas AFF, solo es compatible la compresión inline.

Antes de habilitar la compresión inline, debe habilitar la compresión de postprocesamiento en el volumen. Sin embargo, como la compresión de postprocesamiento no es compatible con las plataformas AFF, no se realiza ninguna compresión de postprocesamiento en esos volúmenes y se genera un mensaje EMS para

informarle de que se ha saltado la compresión de postprocesamiento.

- La eficiencia del almacenamiento sensible a la temperatura se introduce en ONTAP 9.8. Con esta función, la eficiencia del almacenamiento se aplica en función de si los datos están activos o inactivos. En el caso de los datos inactivos, los bloques de datos más grandes se comprimen y, para los datos activos, que se sobrescriben con mayor frecuencia, los bloques de datos más pequeños se comprimen, lo que hace que el proceso sea más eficiente. La eficiencia del almacenamiento sensible a la temperatura se habilita automáticamente en los volúmenes de AFF con aprovisionamiento ligero recién creados.
- El tipo de compresión se asigna automáticamente en función de la plataforma del agregado:

| Plataforma/agregados | Tipo de compresión |
|-------------------------|-----------------------|
| AFF | Compresión adaptativa |
| Agregados de Flash Pool | Compresión adaptativa |
| Agregados de HDD | Compresión secundaria |

Opciones

- Utilice la `volume efficiency modify` comando para habilitar la compresión de datos con el tipo de compresión predeterminado.

El siguiente comando habilita la compresión de postprocesamiento en el volumen Vola de SVM vs1:

```
volume efficiency modify -vserver vs1 -volume VolA -compression true
```

El siguiente comando habilita el postprocesamiento y la compresión en línea en el volumen Vola de SVM vs1:

```
volume efficiency modify -vserver vs1 -volume VolA -compression true -inline  
-compression true
```

- Utilice la `volume efficiency modify` comando en el nivel de privilegio avanzado para habilitar la compresión de datos con un tipo de compresión específico.
 - a. Utilice la `set -privilege advanced` comando para cambiar el nivel de privilegio a avanzado.
 - b. Utilice la `volume efficiency modify` comando para asignar un tipo de compresión a un volumen.

El siguiente comando habilita la compresión de postprocesamiento y asigna el tipo de compresión adaptativa al volumen Vola de la SVM vs1:

```
volume efficiency modify -vserver vs1 -volume VolA -compression true  
-compression-type adaptive
```

El siguiente comando habilita la compresión en línea y de postprocesamiento, y asigna el tipo de compresión adaptativa al volumen Vola de SVM vs1:

```
volume efficiency modify -vserver vs1 -volume VolA -compression true  
-compression-type adaptive -inline-compression true
```

- a. Utilice la `set -privilege admin` comando para cambiar el nivel de privilegio a admin.

Cambie entre la compresión secundaria y la compresión adaptativa

Puede cambiar entre la compresión secundaria y la compresión adaptativa en función de la cantidad de lecturas de datos. Es preferible realizar la compresión adaptativa cuando hay un gran volumen de lecturas aleatorias en el sistema y se requiere un mayor rendimiento. Se recomienda la compresión secundaria cuando los datos se escriben de forma secuencial y se requieren mayores ahorros en la compresión.

Acerca de esta tarea

El tipo de compresión predeterminado se selecciona según los agregados y la plataforma.

Pasos

1. Deshabilite la compresión de datos en el volumen:

```
volume efficiency modify
```

El siguiente comando inhabilita la compresión de datos en el volumen vol1:

```
volume efficiency modify -compression false -inline-compression false -volume vol1
```

2. Cambie al nivel de privilegio avanzado:

```
set -privilege advanced
```

3. Descomprimir los datos comprimidos:

```
volume efficiency undo
```

El siguiente comando descomprime los datos comprimidos en el volumen vol1:

```
volume efficiency undo -vserver vs1 -volume vol1 -compression true
```



Debe verificar que dispone de espacio suficiente en el volumen para acomodar los datos descomprimidos.

4. Verificar que el estado de la operación está inactivo:

```
volume efficiency show
```

El siguiente comando muestra el estado de una operación de eficiencia en el volumen vol1:

```
volume efficiency show -vserver vs1 -volume vol1
```

5. Habilite la compresión de datos y, a continuación, establezca el tipo de compresión:

```
volume efficiency modify
```

El siguiente comando habilita la compresión de datos y establece el tipo de compresión como compresión secundaria en el volumen vol1:

```
volume efficiency modify -vserver vs1 -volume vol1 -compression true
```

`-compression-type secondary`



Este paso solo habilita la compresión secundaria en el volumen, mientras que los datos del volumen no se comprimen.

- Para comprimir los datos existentes en sistemas AFF, debe ejecutar el análisis de compresión en segundo plano.
- Para comprimir los datos existentes en agregados de Flash Pool o agregados de HDD, debe ejecutar la compresión en segundo plano.

6. Cambie al nivel de privilegio de administrador:

```
set -privilege admin
```

7. Opcional: Habilitar la compresión en línea:

```
volume efficiency modify
```

El siguiente comando habilita la compresión en línea en el volumen vol1:

```
volume efficiency modify -vserver vs1 -volume voll -inline-compression true
```

Desactivar la compresión de datos en un volumen

Puede deshabilitar la compresión de datos en un volumen mediante el `volume efficiency modify` comando.

Acerca de esta tarea

Si desea deshabilitar la compresión de postprocesamiento, primero debe deshabilitar la compresión en línea en el volumen.

Pasos

1. Detenga cualquier operación de eficiencia de volumen que esté activa actualmente en el volumen:

```
volume efficiency stop
```

2. Desactivar la compresión de datos:

```
volume efficiency modify
```

Los datos comprimidos existentes seguirán comprimidos en el volumen. Solo las nuevas escrituras que entran en el volumen no se comprimen.

Ejemplos

El siguiente comando desactiva la compresión en línea en el volumen Vola:

```
volume efficiency modify -vserver vs1 -volume VolA -inline-compression false
```

El siguiente comando deshabilita la compresión de postprocesamiento y la compresión en línea en el volumen Vola:

```
volume efficiency modify -vserver vs1 -volume VolA -compression false -inline  
-compression false
```

Gestione la compactación de datos inline para sistemas AFF

Puede controlar la compactación de datos inline en sistemas AFF a nivel de volumen mediante el `volume efficiency modify` comando. La compactación de datos está habilitada de forma predeterminada para todos los volúmenes de los sistemas AFF.

Lo que necesitará

La compactación de datos requiere que se establezca la garantía de espacio de volumen en `none`. Este es el valor predeterminado para los sistemas AFF.



La garantía de espacio predeterminada en volúmenes de protección de datos sin AFF se ha establecido en `none`.

Pasos

1. Para verificar la configuración de garantía de espacio del volumen:

```
volume show -vserver vserver_name -volume volume_name -fields space-guarantee
```

2. Para habilitar la compactación de datos:

```
volume efficiency modify -vserver vserver_name -volume volume_name -data  
-compaction true
```

3. Para deshabilitar la compactación de datos:

```
volume efficiency modify -vserver vserver_name -volume volume_name -data  
-compaction false
```

4. Para mostrar el estado de compactación de datos:

```
volume efficiency show -instance
```

Ejemplos

```
cluster1::> volume efficiency modify -vserver vs1 -volume vol1 -data-compaction  
true cluster1::> volume efficiency modify -vserver vs1 -volume vol1 -data  
-compaction false
```

Habilite la compactación de datos inline para sistemas de FAS

Puede controlar la compactación de datos inline en sistemas FAS con agregados de Flash Pool (híbridos) o agregados de HDD a nivel de volumen o de agregado mediante el `volume efficiency` comando shell del clúster. La compactación de datos está deshabilitada de forma predeterminada para los sistemas FAS.

Acercas de esta tarea

Si habilita la compactación de datos en el nivel de agregado, la compactación de datos está habilitada en cualquier nuevo volumen que se cree con una garantía de espacio de volumen de `none` en el agregado. Al

habilitar la compactación de datos en un volumen en un agregado de HDD, se utilizan recursos de CPU adicionales.

Pasos

- 1. Cambie al nivel de privilegio avanzado:
`set -privilege advanced`
- 2. Compruebe el estado de compactación de datos de los volúmenes y los agregados del nodo deseado:
`volume efficiency show -volume volume_name +`
- 3. Habilite la compactación de datos en el volumen:
`volume efficiency modify -volume volume_name -data-compaction true`



Si se establece la compactación de datos en `false` para un agregado o un volumen, la compactación falla. Habilitar la compactación no compacta los datos existentes; solo se compactan las nuevas escrituras en el sistema. La `volume efficiency start` El comando contiene más información acerca de cómo compactar los datos existentes (en ONTAP 9.1 y posteriores).
["Comandos de ONTAP 9"](#)

- 4. Consulte las estadísticas de compactación:
`volume efficiency show -volume volume_name`

La eficiencia del almacenamiento inline habilitada de forma predeterminada en los sistemas AFF

Las funciones de eficiencia del almacenamiento están habilitadas de forma predeterminada en todos los volúmenes nuevos creados en los sistemas AFF. A partir de ONTAP 9.2, todas las funciones de eficiencia del almacenamiento en línea están habilitadas de forma predeterminada en todos los volúmenes existentes y creados recientemente en todos los sistemas AFF.

Las funciones de eficiencia del almacenamiento incluyen deduplicación en línea, deduplicación en línea entre volúmenes y compresión inline, y se habilitan de forma predeterminada en los sistemas AFF, como se muestra en la tabla.



El comportamiento de la compactación de datos en volúmenes AFF no cambia en ONTAP 9.2, ya que ya está habilitado de forma predeterminada.

| Condiciones de volumen | Funciones de eficiencia del almacenamiento habilitadas de forma predeterminada en ONTAP 9.2 | | |
|--|---|--|---------------------|
| | Deduplicación en línea | Deduplicación en línea entre volúmenes | Compresión en línea |
| Actualización del clúster a 9.2 | Sí | Sí | Sí |
| Transición de ONTAP 7-Mode a Clustered ONTAP | Sí | Sí | Sí |

| Condiciones de volumen | Funciones de eficiencia del almacenamiento habilitadas de forma predeterminada en ONTAP 9.2 | | |
|---|---|----|----|
| Movimiento de volúmenes | Sí | Sí | Sí |
| Volúmenes aprovisionados con thick-Provisioning | Sí | No | Sí |
| Volúmenes cifrados | Sí | No | Sí |

Las siguientes excepciones se aplican a una o varias funciones de eficiencia del almacenamiento inline:

- Solo los volúmenes de lectura y escritura pueden admitir la habilitación de la eficiencia de almacenamiento en línea predeterminada.
- Los volúmenes con ahorro de compresión se omiten la habilitación de la compresión inline.
- Se omite el hecho de habilitar la compresión inline en los volúmenes con la deduplicación postprocesamiento activada.
- En los volúmenes en los que está desactivada la eficiencia del volumen, el sistema anula la configuración de la política de eficiencia del volumen existente y lo establece para habilitar la política de solo línea.

Permite la visualización de la eficiencia del almacenamiento

Utilice la `storage aggregate show-efficiency` comando para mostrar información sobre la eficiencia del almacenamiento de todos los agregados del sistema.

La `storage aggregate show-efficiency` el comando tiene tres vistas diferentes que se pueden invocar pasando opciones de comando.

Vista predeterminada

La vista predeterminada muestra la relación general de cada uno de los agregados.

```
cluster1::> storage aggregate show-efficiency
```

Vista detallada

Invoque la vista detallada con el `-details` opción de comando. Esta vista muestra lo siguiente:

- Tasa de eficiencia general para cada uno de los agregados.
- La proporción general sin copias Snapshot.
- División de ratio para las siguientes tecnologías de eficiencia: Deduplicación de volúmenes, compresión de volúmenes, copias Snapshot, clones, compactación de datos, y la deduplicación inline de agregados.

```
cluster1::> storage aggregate show-efficiency -details
```

Vista avanzada

La vista avanzada es similar a la vista detallada y muestra detalles utilizados tanto lógicos como físicos.

Este comando se debe ejecutar en el nivel de privilegios avanzados. Cambie a privilegios avanzados mediante el `set -privilege advanced` comando.

El símbolo del sistema cambia a `cluster::*>`.

```
cluster1::> set -privilege advanced
```

Invoque la vista avanzada con `-advanced` opción de comando.

```
cluster1::*> storage aggregate show-efficiency -advanced
```

Para ver las relaciones de un único agregado, invoque individualmente el `-aggregate aggregate_name` comando. Este comando puede ejecutarse en el nivel admin, como también en el nivel de privilegios avanzados.

```
cluster1::> storage aggregate show-efficiency -aggregate aggr1
```

Cree una política de eficiencia de volúmenes para ejecutar operaciones de eficiencia

Cree una política de eficiencia de volúmenes para ejecutar operaciones de eficiencia

Puede crear una política de eficiencia de volúmenes para ejecutar deduplicación o compresión de datos seguida de la deduplicación en un volumen durante un periodo específico y especificar la programación de tareas con la `volume efficiency policy create` comando.

Antes de empezar

Debe haber creado una programación de cron con el `job schedule cron create` comando. Para obtener más información acerca de la administración de las programaciones de cron, consulte ["Referencia de administración del sistema"](#).

Acerca de esta tarea

Un administrador de SVM con roles predefinidos predeterminados no puede gestionar las políticas de deduplicación. Sin embargo, el administrador de clúster puede modificar los privilegios asignados a un administrador de SVM usando cualquier rol personalizado. Para obtener más información sobre las capacidades de administrador de SVM, consulte ["Autenticación de administrador y RBAC"](#).



Puede ejecutar operaciones de deduplicación o compresión de datos en un momento programado, o bien crear una programación con una duración específica, o bien especificar un porcentaje de umbral, que espera a que los nuevos datos superen el umbral y, a continuación, active la operación de deduplicación o compresión de datos. Este valor de umbral es el porcentaje de la cantidad total de bloques utilizados en el volumen. Por ejemplo, si se establece el valor del umbral en un volumen en un 20% cuando el número total de bloques usados en el volumen es del 50%, la deduplicación o la compresión de datos se activan automáticamente cuando se escriben nuevos datos en el volumen en un 10% (el 20% de los bloques 50% utilizados). Si es necesario, puede obtener el número total de bloques utilizados en `df` resultado del comando.

Pasos

1. Utilice la `volume efficiency policy create` comando para crear una política de eficiencia de volumen.

Ejemplos

El siguiente comando crea una política de eficiencia del volumen llamada pol1 que activa una operación de eficiencia diaria:

```
volume efficiency policy create -vserver vs1 -policy pol1 -schedule daily
```

El siguiente comando crea una política de eficiencia de volumen llamada pol2 que activa una operación de eficiencia cuando el porcentaje de umbral alcanza el 20 %:

```
volume efficiency policy create -vserver vs1 -policy pol2 -type threshold -start -threshold-percent 20%
```

Asignar una política de eficiencia de volumen a un volumen

Puede asignar una política de eficiencia a un volumen para ejecutar operaciones de deduplicación o compresión de datos mediante la `volume efficiency modify` comando.

Acerca de esta tarea

Si se asigna una política de eficiencia a un volumen secundario SnapVault, solo se tiene en cuenta el atributo de prioridad de eficiencia del volumen al ejecutar operaciones de eficiencia del volumen. Las programaciones de tareas se ignoran y la operación de deduplicación se ejecuta cuando se realizan actualizaciones incrementales en el volumen secundario de SnapVault.

Paso

1. Utilice la `volume efficiency modify` comando para asignar una política a un volumen.

Ejemplo

El siguiente comando asigna la política de eficiencia del volumen llamada `new_policy` con el volumen `Vola`:

```
volume efficiency modify -vserver vs1 -volume VolA -policy new_policy
```

Modificar una política de eficiencia de volúmenes

Puede modificar una política de eficiencia de volúmenes para ejecutar la deduplicación y la compresión de datos durante otro periodo o cambiar la programación de tareas con la `volume efficiency policy modify` comando.

Paso

1. Utilice la `volume efficiency policy modify` comando para modificar una política de eficiencia de volúmenes.

Ejemplos

El siguiente comando modifica la directiva de eficiencia de volumen denominada `policy1` para que se ejecute cada hora:

```
volume efficiency policy modify -vserver vs1 -policy policy1 -schedule hourly
```

El siguiente comando modifica una política de eficiencia del volumen llamada `pol2` al umbral 30 %:

```
volume efficiency policy modify -vserver vs1 -policy pol1 -type threshold -start
```

`-threshold-percent 30%`

Vea una política de eficiencia de volumen

Puede ver el nombre, la programación, la duración y la descripción de la política de eficiencia del volumen mediante la `volume efficiency policy show` comando.

Acerca de esta tarea

Cuando ejecute el `volume efficiency policy show` desde el alcance del clúster, las políticas de ámbito del clúster no se muestran. Sin embargo, puede ver las políticas de ámbito del clúster en el contexto de máquinas virtuales de almacenamiento (SVM).

Paso

1. Utilice la `volume efficiency policy show` comando para ver información acerca de una política de eficiencia de volúmenes.

El resultado depende de los parámetros que se especifiquen. Para obtener más información sobre cómo mostrar la vista detallada y otros parámetros, consulte la página man de este comando.

Ejemplos

El siguiente comando muestra información acerca de las políticas creadas para la SVM vs1: `volume efficiency policy show -vserver vs1`

El siguiente comando muestra las políticas para las que la duración se establece como 10 horas: `volume efficiency policy show -duration 10`

Desasociar una política de eficiencia de volumen de un volumen

Es posible desasociar una política de eficiencia de volumen de un volumen para detener la ejecución de todas las operaciones de deduplicación y compresión de datos adicionales basadas en la programación en el volumen. Una vez que se desasociar una política de eficiencia de volumen, debe activarse manualmente.

Paso

1. Utilice la `volume efficiency modify` comando para desasociar una política de eficiencia de un volumen.

Ejemplo

El siguiente comando desasocia la política de eficiencia del volumen de Vola: `volume efficiency modify -vserver vs1 -volume VolA -policy -`

Eliminar una política de eficiencia de volumen

Una política de eficiencia de volumen se puede eliminar mediante la `volume efficiency policy delete` comando.

Lo que necesitará

Debe haberse asegurado de que la política que desea eliminar no está asociada a ningún volumen.



No puede eliminar la directiva de eficiencia predefinida *inline-only* ni la directiva de eficacia predefinida *default*.

Paso

1. Utilice la `volume efficiency policy delete` comando para eliminar una política de eficiencia de volumen.

Ejemplo

El siguiente comando elimina una directiva de eficiencia de volumen denominada `policy 1`: `volume efficiency policy delete -vserver vs1 -policy policy1`

Gestione manualmente operaciones de eficiencia de volúmenes

Información general manual sobre las operaciones de eficiencia del volumen de gestiona

Puede gestionar la forma en que se ejecutan las operaciones de eficiencia en un volumen ejecutando manualmente las operaciones de eficiencia.

También puede controlar cómo se ejecutan las operaciones de eficiencia en función de las siguientes condiciones:

- Utilice puntos de control o no
- Ejecute operaciones de eficiencia en datos existentes o solo datos nuevos
- Detenga las operaciones de eficiencia si es necesario

Puede utilizar el `volume efficiency show` comando con `schedule` como valor para `-fields` opción para ver la programación asignada a los volúmenes.

Ejecute operaciones de eficiencia manualmente

Puede ejecutar operaciones de eficiencia manualmente en un volumen mediante el `volume efficiency start` comando.

Lo que necesitará

Según la operación de eficiencia que desee ejecutar manualmente, debe tener activada la deduplicación o tanto la compresión de datos como la deduplicación en un volumen.

Acerca de esta tarea

Cuando se activa la eficiencia de almacenamiento sensible a la temperatura en un volumen, se ejecuta inicialmente la deduplicación y, a continuación, la compresión de datos.

La deduplicación es un proceso en segundo plano que consume recursos del sistema mientras se está ejecutando. Si los datos no cambian con frecuencia en un volumen, es mejor ejecutar la deduplicación con menos frecuencia. Varias operaciones de deduplicación simultáneas que se ejecutan en un sistema de almacenamiento, generan un mayor consumo de recursos del sistema.

Puede ejecutar un máximo de ocho operaciones simultáneas de deduplicación o compresión de datos por nodo. Si se programa alguna operación de mayor eficiencia, las operaciones se pondrán en cola.

A partir de ONTAP 9.13.1, si la eficiencia de almacenamiento sensible a la temperatura está habilitada en un volumen, puede ejecutar la eficiencia del volumen en los datos existentes para aprovechar el empaquetado

secuencial y mejorar aún más la eficiencia del almacenamiento.

Ejecute la eficiencia manualmente

Paso

1. Inicie la operación de eficiencia en un volumen: `volume efficiency start`

Ejemplo

El siguiente comando le permite iniciar manualmente solo la deduplicación o la deduplicación seguidas de la compresión lógica y la compresión de contenedores en Vola del volumen

```
volume efficiency start -vserver vs1 -volume VolA
```

Volver a comprimir datos existentes

Para aprovechar el paquete de datos secuencial introducido en ONTAP 9.13.1 en volúmenes con eficiencia de almacenamiento sensible a la temperatura habilitada, puede volver a montar los datos existentes. Para utilizar este comando, debe estar en modo de privilegio avanzado.

Paso

1. Establezca el nivel de privilegio: `set -privilege advanced`
2. Volver a comprimir datos existentes: `volume efficiency inactive-data-compression start -vserver vserver_name -volume volume_name -scan-mode extended_recompression`

Ejemplo

```
volume efficiency inactive-data-compression start -vserver vs1 -volume  
voll1 -scan-mode extended_recompression
```

Utilice puntos de control para reanudar el funcionamiento de la eficacia

Los puntos de control se utilizan internamente para registrar el proceso de ejecución de una operación de eficacia. Cuando se detiene una operación de eficiencia por cualquier motivo (como la detención del sistema, la interrupción del sistema, el reinicio o el fallo de la última operación de eficiencia) y existen datos de punto de comprobación, la operación de eficiencia puede reanudarse desde el archivo de punto de comprobación más reciente.

Se ha creado un punto de comprobación:

- en cada etapa o subetapa de la operación
- cuando ejecute el `sis stop` comando
- cuando caduque la duración

Reanudar una operación de eficiencia detenida

Si una operación de eficiencia se detiene debido a una interrupción del sistema o un reinicio, puede reanudar la operación de eficiencia desde el mismo punto utilizando el `volume efficiency start` comando con la opción punto de comprobación. Esto ayuda a ahorrar tiempo y recursos al no tener que reiniciar la operación de eficiencia desde el principio.

Acerca de esta tarea

Si solo habilitó la deduplicación en el volumen, la deduplicación se ejecutará en los datos. Si ha activado tanto la deduplicación como la compresión de datos en un volumen, la compresión de datos se ejecuta primero, seguida de la deduplicación.

Puede ver los detalles del punto de control de un volumen mediante `volume efficiency show` comando.

De forma predeterminada, las operaciones de eficiencia se reanudan desde los puntos de control. Sin embargo, si un punto de control corresponde a una operación de eficiencia anterior (la fase cuando la `volume efficiency start` el comando `-scan-old-data` se ejecuta) tiene más de 24 horas y, a continuación, la operación de eficiencia no se reanuda automáticamente desde el punto de comprobación anterior. En este caso, la operación de eficiencia comienza desde el principio. Sin embargo, si sabe que no se han producido cambios significativos en el volumen desde la última exploración, puede forzar la continuación del punto de comprobación anterior utilizando la `-use-checkpoint` opción.

Paso

1. Utilice la `volume efficiency start` con el `-use-checkpoint` opción para reanudar una operación de eficiencia.

El siguiente comando le permite reanudar una operación de eficiencia en los nuevos datos del volumen Vola:

```
volume efficiency start -vserver vs1 -volume VolA -use-checkpoint true
```

El siguiente comando permite reanudar una operación de eficiencia en los datos existentes en el volumen Vola:

```
volume efficiency start -vserver vs1 -volume VolA -scan-old-data true -use-checkpoint true
```

Ejecute operaciones de eficiencia manualmente en datos existentes

Puede ejecutar las operaciones de eficiencia manualmente en los datos que hay en volúmenes de eficiencia del almacenamiento sin sensibilidad a la temperatura antes de habilitar la deduplicación, la compresión de datos o la compactación de datos con versiones de ONTAP anteriores a ONTAP 9.8. Puede ejecutar estas operaciones mediante la `volume efficiency start -scan-old-data` comando.

Acerca de esta tarea

La `-compression` opción no funciona con `-scan-old-data` en volúmenes de eficiencia de almacenamiento sensibles a la temperatura. La compresión de datos inactiva se ejecuta automáticamente en

los datos previos para los volúmenes de eficiencia del almacenamiento sensibles a la temperatura en ONTAP 9.8 y versiones posteriores.

Si solo activa la deduplicación en un volumen, la deduplicación se ejecuta en los datos. Si habilita la deduplicación, la compresión de datos y la compactación de datos en un volumen, primero se ejecuta la compresión de datos, seguida de la deduplicación y la compactación de datos.

Al ejecutar la compresión de datos en los datos existentes, de forma predeterminada, la operación de compresión de datos omite los bloques de datos compartidos por la deduplicación y los bloques de datos que quedan bloqueados por las copias Snapshot. Si decide ejecutar compresión de datos en bloques compartidos, la optimización se desactiva y se captura la información de huella digital para compartirla de nuevo. Es posible cambiar el comportamiento predeterminado de la compresión de datos al comprimir los datos existentes.

Puede ejecutar un máximo de ocho operaciones de deduplicación, compresión de datos o compactación de datos simultáneamente por nodo. Las operaciones restantes se ponen en cola.



La compresión de postprocesamiento no se ejecuta en plataformas AFF. Se genera un mensaje de EMS para informarle de que esta operación se ha omitido.

Paso

1. Utilice la `volume efficiency start -scan-old-data` comando para ejecutar manualmente la deduplicación, la compresión o la compactación de datos en los datos existentes.

El siguiente comando permite ejecutar estas operaciones manualmente en los datos existentes en el volumen Vola:

```
volume efficiency start -vserver vs1 -volume VolA -scan-old-data true [-compression | -dedupe | -compaction ] true
```

Gestione las operaciones de eficiencia de volúmenes mediante programaciones

Ejecute operaciones de eficiencia en función de la cantidad de datos nuevos escritos

Es posible modificar la programación de las operaciones de eficiencia para ejecutar la deduplicación o la compresión de datos cuando la cantidad de bloques nuevos escritos en el volumen después de que la operación de eficiencia anterior (realizada manualmente o programada) supere un porcentaje de umbral especificado.

Acerca de esta tarea

Si la `schedule` opción establecida en `auto`, la operación de eficacia programada se ejecuta cuando la cantidad de datos nuevos supera el porcentaje especificado. El valor del umbral predeterminado es de 20 %. Este valor de umbral es el porcentaje del número total de bloques ya procesados por la operación de eficiencia.

Paso

1. Utilice la `volume efficiency modify` con el `auto@num` opción para modificar el valor del porcentaje del umbral.

`num` es un número de dos dígitos para especificar el porcentaje.

Ejemplo

El siguiente comando modifica el valor del porcentaje del umbral al 30 % para el volumen Vola:

```
volume efficiency modify -vserver vs1 -volume -VolA -schedule auto@30
```

Ejecute las operaciones de eficiencia mediante programación

Puede modificar la programación de la deduplicación o la operación de compresión de datos en un volumen mediante el `volume efficiency modify` comando. Las opciones de configuración de una política de eficiencia de programación y volumen se excluyen mutuamente.

Paso

1. Utilice la `volume efficiency modify` comando para modificar la programación de las operaciones de deduplicación o compresión de datos en un volumen.

Ejemplos

El siguiente comando modifica la programación de las operaciones de eficiencia para que Vola se ejecute a las 11 p. m., de lunes a viernes:

```
volume efficiency modify -vserver vs1 -volume VolA -schedule mon-fri@23
```

Supervisar operaciones de eficiencia del volumen

Ver el estado y las operaciones de eficiencia

Puede ver si la deduplicación o la compresión de datos están habilitadas en un volumen. También puede ver el estado, la condición, el tipo de compresión y el progreso de las operaciones de eficiencia de un volumen mediante el `volume efficiency show` comando.

Ver el estado de la eficiencia

Paso

1. Vea el estado de una operación de eficiencia en un volumen: `volume efficiency show`

El siguiente comando muestra el estado de una operación de eficiencia en el volumen Vola al que se le ha asignado el tipo de compresión adaptativa:

```
volume efficiency show -instance -vserver vs1 -volume VolA
```

Si la operación de eficiencia está activada en el volumen de Vola y la operación está inactiva, puede ver lo siguiente en el resultado del sistema:

```
cluster1::> volume efficiency show -vserver vs1 -volume VolA
```

```
Vserver Name: vs1  
Volume Name: VolA  
Volume Path: /vol/VolA  
State: Enabled  
Status: Idle  
Progress: Idle for 00:03:20
```

Determine si los volúmenes contienen datos agrupados secuencialmente

Es posible mostrar una lista de los volúmenes que tienen habilitado el empaquetado secuencial, por ejemplo, cuando necesite revertir a una versión de ONTAP anterior a 9.13.1. Para utilizar este comando, debe estar en modo de privilegio avanzado.

Paso

1. Establezca el nivel de privilegio: `set -privilege advanced`
2. Enumera los volúmenes que tienen el empaquetado secuencial activado: 'Eficiencia del volumen show -extended-auto-adaptive-compression true'

Ver el ahorro de espacio eficiente

Puede ver la cantidad de ahorro de espacio que se consigue mediante la deduplicación y la compresión de datos en un volumen mediante la `volume show` comando.

Acerca de esta tarea

El ahorro de espacio de las copias Snapshot no se incluye al calcular el ahorro de espacio conseguido en un volumen. El uso de la deduplicación no afecta a las cuotas de volumen. Las cuotas se notifican en el nivel lógico y permanecen sin cambios.

Paso

1. Utilice la `volume show` comando para ver el ahorro de espacio que se consigue en un volumen mediante la deduplicación y la compresión de datos.

Ejemplo

El siguiente comando le permite ver el ahorro de espacio conseguido usando la deduplicación y la compresión de datos en el volumen VolA: `volume show -vserver vs1 -volume VolA`

```
cluster1::> volume show -vserver vs1 -volume VolA

Vserver Name: vs1
Volume Name: VolA

...

    Space Saved by Storage Efficiency: 115812B
Percentage Saved by Storage Efficiency: 97%
    Space Saved by Deduplication: 13728B
Percentage Saved by Deduplication: 81%
    Space Shared by Deduplication: 1028B
    Space Saved by Compression: 102084B
Percentage Space Saved by Compression: 97%

...
```

Ver las estadísticas de eficiencia de un volumen de FlexVol

Puede ver los detalles de las operaciones de eficiencia que se ejecutan en un volumen de FlexVol mediante el `volume efficiency stat` comando.

Paso

1. Utilice la `volume efficiency stat` Comando para ver las estadísticas de las operaciones de eficiencia en un volumen de FlexVol.

Ejemplo

El siguiente comando le permite ver las estadísticas de las operaciones de eficiencia en el volumen VolA:
`volume efficiency stat -vserver vs1 -volume VolA`

```
cluster1::> volume efficiency stat -vserver vs1 -volume VolA

Vserver Name: vs1
Volume Name: VolA
Volume Path: /vol/VolA
Inline Compression Attempts: 0
```

Detenga las operaciones de eficiencia del volumen

Puede detener una operación de deduplicación o compresión de postprocesamiento mediante el `volume efficiency stop` comando. Este comando genera automáticamente un punto de comprobación.

Paso

1. Utilice la `volume efficiency stop` comando para detener una deduplicación activa o una operación de compresión de postprocesamiento.

Si especifica el `-all` se cancelan las operaciones de eficiencia activas y en cola.

Ejemplos

El siguiente comando detiene la operación de deduplicación o compresión de postprocesamiento que está activa en este momento en el volumen VolA:

```
volume efficiency stop -vserver vs1 -volume VolA
```

El siguiente comando aborta tanto la deduplicación activa como la cola, como las operaciones de compresión de postprocesamiento en el volumen VolA:

```
volume efficiency stop -vserver vs1 -volume VolA -all true
```

Información sobre cómo eliminar el ahorro de espacio de un volumen

Puede optar por eliminar el ahorro de espacio obtenido mediante la ejecución de operaciones de eficiencia en un volumen, pero debe tener el espacio suficiente para dar cabida a la reversión.

Consulte estos artículos de la base de conocimientos:

- ["Cómo observar ahorros de espacio gracias a la deduplicación, la compresión y la compactación en ONTAP 9"](#)
- ["Cómo deshacer los ahorros en eficiencia del almacenamiento en ONTAP"](#)

Vuelva a alojar un volumen de una SVM a otra

Vuelva a alojar un volumen de una SVM a otra información general de SVM

El realojamiento de volúmenes le permite reasignar volúmenes NAS o SAN de una máquina virtual de almacenamiento (SVM, antes denominada Vserver) a otra SVM sin necesidad de realizar una copia SnapMirror. Los procedimientos de realojamiento de volúmenes dependen del tipo de protocolo y el tipo de volumen. El realojamiento de volúmenes es una operación disruptiva para el acceso a datos y la gestión de volúmenes.

Antes de empezar

Se deben cumplir varias condiciones para poder volver a alojar un volumen de una SVM a otra:

- El volumen debe estar en línea.
- Protocolos: SAN o NAS

Para el protocolo NAS, el volumen debe estar desmontado.

- Si el volumen está en una relación de SnapMirror, debe eliminarse o romperse la relación antes de volver a alojar el volumen.

Es posible volver a sincronizar la relación de SnapMirror una vez que la operación de realojamiento del volumen.

Vuelva a alojar los volúmenes SMB

Es posible volver a alojar volúmenes que sirven datos mediante el protocolo SMB. Después de volver a alojar el volumen CIFS, para seguir accediendo a los datos a través del protocolo SMB, debe configurar manualmente las políticas y las reglas asociadas.

Acerca de esta tarea

- El realojamiento es una operación disruptiva.
- Si la operación de realojamiento falla, es posible que deba volver a configurar las políticas de volumen y las reglas asociadas en el volumen de origen.
- Si la SVM de origen y los dominios de Active Directory de destino difieren, es posible que se pierda acceso a los objetos del volumen.
- A partir de ONTAP 9,8, se admite el realojamiento de un volumen con cifrado de volúmenes de NetApp (NVE). Si se usa un gestor de claves incorporado, los metadatos cifrados se modificarán durante la operación de nuevo alojamiento. Los datos de usuario no se modifican.

Si se utiliza ONTAP 9,8 o temprano, se debe descifrar el volumen antes de realizar la operación de rehost.

- Cuando la SVM de origen cuenta con usuarios y grupos locales, los permisos para los archivos y directorios (ACL) que se establecen ya no serán efectivos después de la operación de realojamiento de volumen.

Lo mismo se aplica a las ACL de auditoría (SACL).

- Tras la operación de realojamiento, se pierden las siguientes políticas de volumen, reglas de política y configuraciones en el volumen de origen y se deben volver a configurar manualmente en el volumen hospedado:
 - Políticas de exportación de volúmenes y qtrees
 - Directivas de antivirus
 - Política de eficiencia de volúmenes
 - Políticas de calidad de servicio (QoS)
 - Políticas de Snapshot
 - Reglas de cuotas
 - reglas y políticas de exportación de configuración de ns-switch y servicios de nombres
 - ID de usuario y de grupo

Antes de empezar

- El volumen debe estar en línea.
- No se deben ejecutar las operaciones de gestión de volúmenes, como el movimiento de volúmenes o el movimiento de LUN.
- Se debe detener el acceso a los datos al volumen que se está realojando.
- La configuración de los servicios de nombres y ns-switch de la SVM objetivo debe configurarse para admitir el acceso a los datos del volumen de realojamiento.
- La SVM de origen y la SVM de destino deben tener el mismo dominio de Active Directory y realmDNS.
- El ID de usuario y el ID de grupo del volumen deben estar disponibles en la SVM objetivo o cambiarse en el volumen de host.



Si se configuran usuarios y grupos locales y si hay archivos y directorios en ese volumen con permisos establecidos para esos usuarios o grupos, estos permisos ya no serán efectivos.

Pasos

1. Registre información sobre los recursos compartidos CIFS para evitar la pérdida de información sobre los recursos compartidos CIFS en caso de que falle la operación de realojamiento del volumen.
2. Desmonte el volumen del volumen principal:

```
volume unmount
```

3. Cambie al nivel de privilegio avanzado:

```
set -privilege advanced
```

4. Vuelva a alojar el volumen en la SVM de destino:

```
volume rehost -vserver source_svm -volume vol_name -destination-vserver  
destination_svm
```

5. Monte el volumen en la ruta de unión adecuada en la SVM de destino:

```
volume mount
```

6. Crear recursos compartidos de CIFS para el volumen realojado:

```
vserver cifs share create
```

7. Si los dominios DNS difieren entre la SVM de origen y la SVM de destino, cree nuevos usuarios y grupos.
8. Actualice el cliente CIFS con las nuevas LIF de SVM de destino y la ruta de unión al volumen realojado.

Después de terminar

Es necesario volver a configurar manualmente las políticas y las reglas asociadas en el volumen realojado.

["Configuración de SMB"](#)

["Configuración de varios protocolos de SMB y NFS"](#)

Vuelva a alojar volúmenes NFS

Puede volver a alojar volúmenes que sirven datos mediante el protocolo NFS. Después de volver a alojar los volúmenes NFS, para seguir accediendo a los datos mediante el protocolo NFS, debe asociar el volumen con la política de exportación de la SVM de host y configurar manualmente las políticas y las reglas asociadas.

Acerca de esta tarea

- El realojamiento es una operación disruptiva.
- Si la operación de realojamiento falla, es posible que deba volver a configurar las políticas de volumen y las reglas asociadas en el volumen de origen.
- A partir de ONTAP 9,8, se admite el realojamiento de un volumen con cifrado de volúmenes de NetApp

(NVE). Si se usa un gestor de claves incorporado, los metadatos cifrados se modificarán durante la operación de nuevo alojamiento. Los datos de usuario no se modifican.

Si se utiliza ONTAP 9,8 o temprano, se debe descifrar el volumen antes de realizar la operación de rehost.

- Tras la operación de realojamiento, se pierden las siguientes políticas de volumen, reglas de política y configuraciones en el volumen de origen y se deben volver a configurar manualmente en el volumen hospedado:
 - Políticas de exportación de volúmenes y qtrees
 - Directivas de antivirus
 - Política de eficiencia de volúmenes
 - Políticas de calidad de servicio (QoS)
 - Políticas de Snapshot
 - Reglas de cuotas
 - reglas y políticas de exportación de configuración de ns-switch y servicios de nombres
 - ID de usuario y de grupo

Antes de empezar

- El volumen debe estar en línea.
- No se deben ejecutar las operaciones de gestión de volúmenes, como movimientos de volúmenes o movimientos de LUN.
- Se debe detener el acceso a los datos al volumen que se está realojando.
- La configuración de los servicios de nombres y ns-switch de la SVM objetivo debe configurarse para admitir el acceso a los datos del volumen de realojamiento.
- El ID de usuario y el ID de grupo del volumen deben estar disponibles en la SVM objetivo o cambiarse en el volumen de host.

Pasos

1. Registrar información sobre las políticas de exportación de NFS para evitar la pérdida de información sobre las políticas de NFS en caso de que se produzca un error en la operación de realojamiento del volumen.
2. Desmonte el volumen del volumen principal:

```
volume unmount
```

3. Cambie al nivel de privilegio avanzado:

```
set -privilege advanced
```

4. Vuelva a alojar el volumen en la SVM de destino:

```
volume rehost -vserver source_svm -volume volume_name -destination-vserver  
destination_svm
```

La política de exportación predeterminada de la SVM de destino se aplica al volumen realojado.

5. Cree la política de exportación:

```
vserver export-policy create
```

6. Actualice la política de exportación del volumen realojado a una política de exportación definida por el usuario:

```
volume modify
```

7. Monte el volumen en la ruta de unión adecuada en la SVM de destino:

```
volume mount
```

8. Compruebe que el servicio NFS está en ejecución en la SVM de destino.
9. Reanude el acceso NFS al volumen que se realoja.
10. Actualice las credenciales del cliente NFS y las configuraciones de LIF para reflejar las LIF de SVM de destino.

Esto se debe a que la ruta de acceso al volumen (LIF y ruta de unión) ha sufrido cambios.

Después de terminar

Es necesario volver a configurar manualmente las políticas y las reglas asociadas en el volumen realojado.

["Configuración de NFS"](#)

Vuelva a alojar volúmenes SAN

Puede volver a alojar volúmenes que tienen LUN asignadas. Después de volver a crear el iGroup en la SVM de destino, el realojamiento de volúmenes puede reasignar automáticamente el volumen en la misma SVM.

Acerca de esta tarea

- El realojamiento es una operación disruptiva.
- Si la operación de realojamiento falla, es posible que deba volver a configurar las políticas de volumen y las reglas asociadas en el volumen de origen.
- A partir de ONTAP 9,8, se admite el realojamiento de un volumen con cifrado de volúmenes de NetApp (NVE). Si se usa un gestor de claves incorporado, los metadatos cifrados se modificarán durante la operación de nuevo alojamiento. Los datos de usuario no se modifican.

Si se utiliza ONTAP 9,8 o temprano, se debe descifrar el volumen antes de realizar la operación de rehost.

- Tras la operación de realojamiento, se pierden las siguientes políticas de volumen, reglas de política y configuraciones en el volumen de origen y se deben reconfigurar manualmente en el volumen realojado:
 - Directivas de antivirus
 - Política de eficiencia de volúmenes
 - Políticas de calidad de servicio (QoS)
 - Políticas de Snapshot
 - reglas y políticas de exportación de configuración de ns-switch y servicios de nombres
 - ID de usuario y de grupo

Antes de empezar

- El volumen debe estar en línea.
- No se deben ejecutar las operaciones de gestión de volúmenes, como movimientos de volúmenes o movimientos de LUN.
- No debe haber operaciones de I/O activas en los volúmenes o las LUN.
- Debe haber verificado que la SVM de destino no tiene un igroup con el mismo nombre, sino iniciadores diferentes.

Si el igroup tiene el mismo nombre, debe haber cambiado el nombre del igroup en una de las SVM (origen o destino).

- Debe haber habilitado el `force-unmap-luns` opción.
 - El valor predeterminado de `force-unmap-luns` la opción es `false`.
 - Cuando se establece el, no se muestra ningún mensaje de advertencia o confirmación `force-unmap-luns` opción a. `true`.

Pasos

1. Registre la información de asignación de LUN en el volumen objetivo:

```
lun mapping show volume volume vserver source_svm
```

Este es un paso preventivo para evitar perder información sobre la asignación de LUN en caso de que se produzca un error en el rehost del volumen.

2. Elimine los iGroups asociados al volumen objetivo.
3. Vuelva a alojar el volumen de destino a la SVM de destino:

```
volume rehost -vserver source_svm -volume volume_name -destination-vserver destination_svm
```

4. Asigne las LUN del volumen objetivo a los iGroups adecuados.
 - El realojamiento de volúmenes mantiene las LUN en el volumen de destino; sin embargo, las LUN permanecen sin asignar.
 - Utilice el conjunto de puertos de SVM de destino al asignar las LUN.
 - Si la `auto-remap-luns` opción establecida en `true`, Las LUN se asignan automáticamente después de realojar.

Vuelva a alojar volúmenes en una relación de SnapMirror

Es posible volver a alojar volúmenes en una relación de SnapMirror.

Acerca de esta tarea

- El realojamiento es una operación disruptiva.
- Si la operación de realojamiento falla, es posible que deba volver a configurar las políticas de volumen y las reglas asociadas en el volumen de origen.
- Tras la operación de realojamiento, se pierden las siguientes políticas de volumen, reglas de política y configuraciones en el volumen de origen y se deben reconfigurar manualmente en el volumen realojado:
 - Políticas de exportación de volúmenes y qtrees

- Directivas de antivirus
- Política de eficiencia de volúmenes
- Políticas de calidad de servicio (QoS)
- Políticas de Snapshot
- Reglas de cuotas
- reglas y políticas de exportación de configuración de ns-switch y servicios de nombres
- ID de usuario y de grupo

Antes de empezar

- El volumen debe estar en línea.
- No se deben ejecutar las operaciones de gestión de volúmenes, como movimientos de volúmenes o movimientos de LUN.
- Se debe detener el acceso a los datos al volumen que se está realojando.
- La configuración de los servicios de nombres y ns-switch de la SVM objetivo debe configurarse para admitir el acceso a los datos del volumen de realojamiento.
- El ID de usuario y el ID de grupo del volumen deben estar disponibles en la SVM objetivo o cambiarse en el volumen de host.

Pasos

1. Registre el tipo de relación SnapMirror:

```
snapmirror show
```

Este es un paso preventivo para evitar perder información sobre el tipo de relación SnapMirror en caso de que se produzca un error en el rehost del volumen.

2. En el clúster de destino, elimine la relación SnapMirror:

```
snapmirror delete
```

No debe interrumpir la relación de SnapMirror; de lo contrario, la funcionalidad de protección de datos del volumen de destino se pierde y la relación no se puede restablecer después de la operación de realojamiento.

3. En el clúster de origen, quite la información sobre relaciones de SnapMirror:

```
snapmirror release relationship-info-only true
```

Ajuste de `relationship-info-only` parámetro a `true` Elimina la información de relaciones de origen sin eliminar las copias Snapshot.

4. Cambie al nivel de privilegio avanzado:

```
set -privilege advanced
```

5. Vuelva a alojar el volumen en la SVM de destino:

```
volume rehost -vserver source_svm -volume vol_name -destination-vserver destination_svm
```

6. Si no hay ninguna relación entre iguales de SVM, cree la relación entre iguales de SVM entre la SVM de origen y la SVM de destino:

```
vserver peer create
```

7. Cree la relación de SnapMirror entre el volumen de origen y el de destino:

```
snapmirror create
```

Debe ejecutar el `snapmirror create` Comando desde la SVM que aloja el volumen de DP. El volumen realojado puede ser el origen o el destino de la relación de SnapMirror.

8. Resincronice la relación SnapMirror.

Funciones que no admiten la realojamiento de volúmenes

Hay ciertas funciones que no admiten la realojamiento de volúmenes.

Las siguientes funciones no admiten la realojamiento de volúmenes:

- DR DE SVM
- Configuraciones de MetroCluster



También no se admite la clonado de un volumen como volumen FlexClone en otra máquina virtual de almacenamiento (SVM) en las configuraciones de MetroCluster.

- Volúmenes de SnapLock
- Volúmenes de cifrado de volúmenes de NetApp (NVE) (en versiones de ONTAP anteriores a 9,8)

En las versiones de ONTAP anteriores a 9,8, debe anular el cifrado del volumen antes de volver a alojarlo. Las claves de cifrado de volúmenes dependen de las claves de SVM. Si se mueve un volumen a otra SVM y está habilitada la configuración de claves multitenant en la SVM de origen o de destino, las claves de SVM y el volumen no coincidirán.

A partir de ONTAP 9,8, se puede realojar un volumen con NVE.

- Volúmenes de FlexGroup
- Clonar volúmenes

Límites de almacenamiento

Hay límites para los objetos de almacenamiento que debe tener en cuenta a la hora de planificar y gestionar su arquitectura de almacenamiento.

Los límites a menudo dependen de la plataforma. Consulte la "[Hardware Universe de NetApp](#)" para conocer los límites de su configuración específica. Consulte [\[hwu\]](#) Para obtener instrucciones sobre cómo identificar la información adecuada para la configuración de ONTAP.

Los límites se enumeran en las siguientes secciones:

- [\[vollimits\]](#)

- [\[flexclone\]](#)

Los límites de almacenamiento para Cloud Volumes ONTAP se documentan en la ["Notas de la versión de Cloud Volumes ONTAP"](#).

Límites de volumen

| Objeto de almacenamiento | Límite | Almacenamiento nativo | Cabinas de almacenamiento |
|---|---|---|--|
| LUN de matriz | Tamaño mínimo del volumen raíz | N.A. | Depende del modelo |
| Archivos | Tamaño máximo | Dependiente de la versión ² | Dependiente de la versión ² |
| Máximo por volumen ⁴ | Depende del tamaño del volumen, hasta 2 mil millones de dólares | Depende del tamaño del volumen, hasta 2 mil millones de dólares | Volúmenes FlexClone |
| Profundidad de clon jerárquico ⁵ | 499 | 499 | Volúmenes FlexVol |
| Máximo por nodo 1 | Depende del modelo | Depende del modelo | Máximo por nodo por SVM ⁶ |
| Depende del modelo | Depende del modelo | Tamaño mínimo | 20 MB |
| 20 MB | Tamaño máximo 1 | Depende del modelo | Depende del modelo |
| Volúmenes FlexVol para cargas de trabajo primarias | Máximo por nodo ³ | Depende del modelo | Depende del modelo |
| Volúmenes raíz FlexVol | Tamaño mínimo 1 | Depende del modelo | Depende del modelo |
| LUN | Máximo por nodo ⁶ | Depende del modelo | Depende del modelo |
| Máximo por grupo ⁶ | Depende del modelo | Depende del modelo | Máximo por volumen 6 |
| Depende del modelo | Depende del modelo | Tamaño máximo | Dependiente de la versión ² |
| Dependiente de la versión ² | Qtrees | Máximo por volumen FlexVol | 4,995 |
| 4,995 | Copias Snapshot | Máximo por volumen ⁷ | 255/1023 |

| Objeto de almacenamiento | Límite | Almacenamiento nativo | Cabinas de almacenamiento |
|--------------------------|--|-----------------------------|---------------------------|
| 255/1023 | Volúmenes | Máximo por clúster para NAS | 12.000 |
| 12.000 | Máximo por clúster con protocolos SAN configurados | Depende del modelo | Depende del modelo |

Notas:

1. En ONTAP 9.3 y versiones anteriores, un volumen puede contener hasta 255 copias snapshot. A partir de la versión 9.4 de ONTAP, un volumen puede contener hasta 1023 copias snapshot.
2. Comenzando con ONTAP 9.12.1P2, el límite es 128 TB. En ONTAP 9.11.1 y versiones anteriores, el límite es de 16 TB.
3. A partir de ONTAP 9,7, el número máximo admitido de volúmenes FlexVol en plataformas AFF con al menos 128 GB de memoria se ha aumentado hasta 2.500 volúmenes FlexVol por nodo.

Para obtener información específica sobre la plataforma y detalles de soporte más recientes, consulte ["Hardware Universe"](#).

4. 2 mil millones = 2×10^9
5. La profundidad máxima de una jerarquía anidada de volúmenes FlexClone que se pueden crear a partir de un único volumen de FlexVol.
6. Este límite se aplica solo en entornos SAN.

"CONFIGURACIÓN DE SAN"

7. Puede utilizar una puesta en marcha en cascada de SnapMirror para aumentar este límite.

Límites de archivos y LUN de FlexClone

| Límite | Almacenamiento nativo | Cabinas de almacenamiento |
|--|-----------------------|---------------------------|
| Máximo por archivo o LUN 1 | 32.767 | 32.767 |
| Máximo total de datos compartidos por volumen FlexVol | 640 TB | 640 TB |

Nota:

1. Si intenta crear más de 32,767 clones, ONTAP crea automáticamente una nueva copia física del archivo principal o LUN.

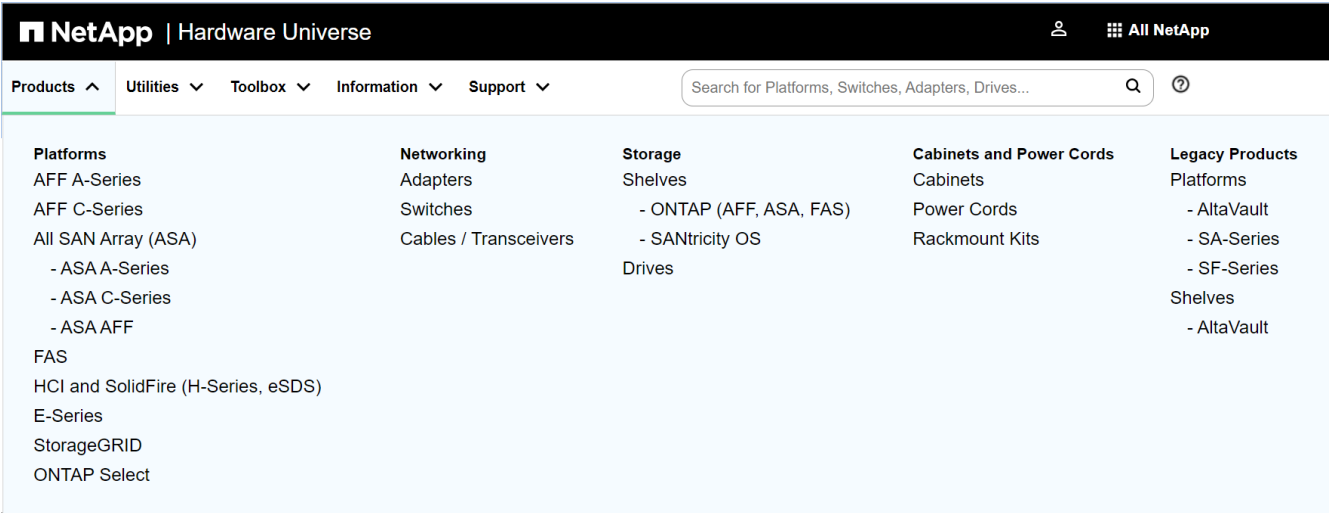
Este límite puede ser menor para volúmenes FlexVol que utilizan deduplicación.

Desplácese por NetApp Hardware Universe

Para encontrar límites específicos de la plataforma y dependientes del modelo, consulte la ["Hardware Universe de NetApp"](#).

Pasos

- 1. En el menú desplegable **Productos**, seleccione su configuración de hardware.



- 2. Seleccione la plataforma.

☒ **Start with Platforms** ☐ **Start with OS** [Help](#)

☐ **Show EOA Platforms**

☒ **Display Platform Configurations**

Filter Platforms

☒ AFF C-Series

☒ AFF C250

☐ AFF C250 Single Chassis HA Pair

☐ AFF C250 Single Chassis HA Pair 100V

☐ AFF C250 4-Node MetroCluster IP

☐ AFF C250 8-Node MetroCluster IP

☒ AFF C400

☐ AFF C400 Single Chassis HA Pair, Ethernet Bundle

☐ AFF C400 Single Chassis HA Pair, FC Bundle

☐ AFF C400 4-Node MetroCluster IP, Ethernet Bundle

☐ AFF C400 4-Node MetroCluster IP, FC Bundle

☐ AFF C400 8-Node MetroCluster IP, Ethernet Bundle

☐ AFF C400 8-Node MetroCluster IP, FC Bundle

☒ AFF C800

☐ AFF C800 Single Chassis HA Pair

☐ AFF C800 4-Node MetroCluster IP

3. Seleccione la versión apropiada de ONTAP y luego **Mostrar resultados**.

783

Start with Platforms

Start with OS

Help

☐ Show EOA Platforms

☒ Display Platform Configurations

Filter Platforms

AFF C-Series

☐ AFF C250

☐ AFF C250 Single Chassis HA Pair

☐ AFF C250 Single Chassis HA Pair 100V

☐ AFF C250 4-Node MetroCluster IP

☐ AFF C250 8-Node MetroCluster IP

☐ AFF C400

☐ AFF C400 Single Chassis HA Pair, Ethernet Bundle

☐ AFF C400 Single Chassis HA Pair, FC Bundle

☐ AFF C400 4-Node MetroCluster IP, Ethernet Bundle

☐ AFF C400 4-Node MetroCluster IP, FC Bundle

☐ AFF C400 8-Node MetroCluster IP, Ethernet Bundle

☐ AFF C400 8-Node MetroCluster IP, FC Bundle

☒ AFF C800

☒ AFF C800 Single Chassis HA Pair

☒ AFF C800 4-Node MetroCluster IP

☒ AFF C800 8-Node MetroCluster IP

Clear

Filter by OS Status :

☐ Show All
 ☒ Hide EOVS
 ☐ Hide Obsolete

Show OS :

☒ Support at least one of the platform selected

☐ Support all the platform selected

☐ Show all

DataONTAP

9.14.1

☐ Release Candidate

☐ 9.14.1RC1

9.13.1

☒ General Availability

☒ 9.13.1

☐ Patch Release

☐ 9.13.1P6

☐ 9.13.1P4

☐ 9.13.1P3

☐ 9.13.1P2

☐ 9.13.1P1

9.12.1

☐ Patch Release

☐ 9.12.1P10

☐ 9.12.1P9

☐ 9.12.1P8

Clear

Note: AFF C190 model information is in the AFF A-Series product category

Preference ▾ **Show Results**

Información relacionada

["Busque las notas de la versión de Cloud Volumes ONTAP"](#)

Combinaciones de configuración recomendadas de volúmenes y archivos o LUN

Información general de las combinaciones de configuración de volúmenes y archivos o LUN recomendadas

Existen combinaciones específicas de configuraciones de volumen y archivo de FlexVol o LUN que puede utilizar, en función de sus requisitos de aplicación y administración. Comprender los beneficios y los costos de estas combinaciones puede ayudarlo a determinar la combinación adecuada de configuración de volúmenes y LUN para su entorno.

Se recomiendan las siguientes combinaciones de configuración de volúmenes y LUN:

- Archivos reservados de espacio o LUN con aprovisionamiento de volumen grueso
- Archivos sin espacio reservado o LUN con thin provisioning de volumen
- Archivos reservados de espacio o LUN con aprovisionamiento de volumen grueso

Puede utilizar thin provisioning SCSI en sus LUN junto con cualquiera de estas combinaciones de configuración.

Archivos reservados de espacio o LUN con aprovisionamiento de volumen grueso

Beneficios:

- Se garantizan todas las operaciones de escritura en los archivos con espacio reservado; no se producen errores debido a la falta de espacio.
- No existen restricciones sobre las tecnologías de eficiencia del almacenamiento y protección de datos en el volumen.

Costos y limitaciones:

- Debe reservar espacio suficiente desde el agregado hacia delante para admitir el volumen considerablemente aprovisionado.
- El espacio es igual al doble del tamaño de la LUN se asigna desde el volumen en el momento de creación de la LUN.

Archivos sin espacio reservado o LUN con thin provisioning de volumen

Beneficios:

- No existen restricciones sobre las tecnologías de eficiencia del almacenamiento y protección de datos en el volumen.
- El espacio se asigna solo como se utiliza.

Costos y restricciones:

- No se garantizan las operaciones de escritura; pueden fallar si el volumen se queda sin espacio libre.
- Debe gestionar eficazmente el espacio libre del agregado para evitar que el agregado se quede sin espacio libre.

Archivos reservados de espacio o LUN con aprovisionamiento de volumen grueso

Beneficios:

Se reserva menos espacio inicial que para el aprovisionamiento de volúmenes gruesos y se ofrece una garantía de escritura de mejor esfuerzo.

Costos y restricciones:

- Las operaciones de escritura pueden fallar con esta opción.

Puede mitigar este riesgo equilibrando correctamente el espacio libre en el volumen frente a la volatilidad de los datos.

- No puede confiar en la retención de objetos de protección de datos como copias Snapshot, archivos FlexClone y LUN.

- No se pueden utilizar funcionalidades de eficiencia del almacenamiento con uso compartido de bloques de ONTAP que no se pueden eliminar automáticamente, incluida la deduplicación, la compresión y la descarga ODX/copia.

Determinar la combinación correcta de configuración de volumen y LUN para su entorno

Responder a algunas preguntas básicas acerca de su entorno puede ayudarle a determinar la mejor configuración de LUN y volumen FlexVol para su entorno.

Acerca de esta tarea

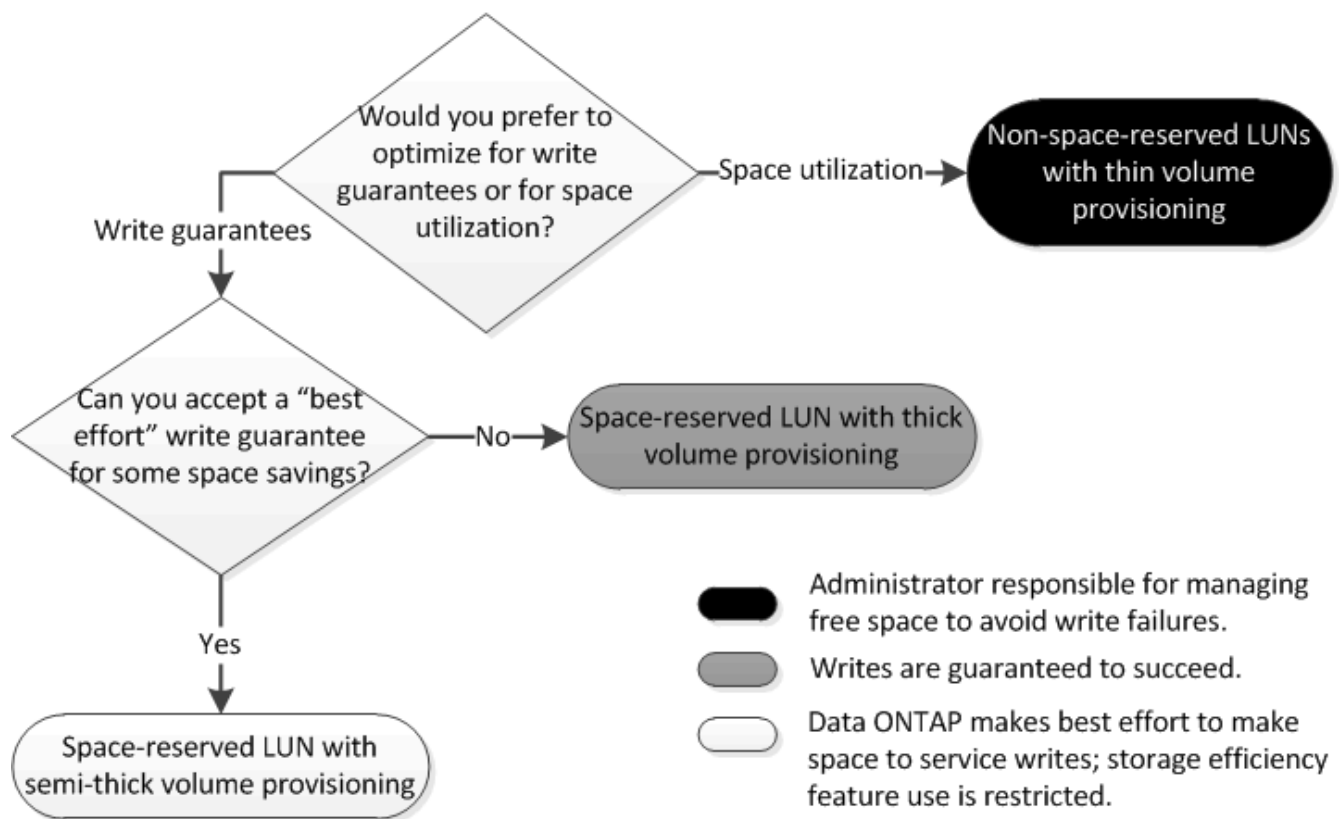
Puede optimizar su configuración de LUN y volúmenes para un uso máximo del almacenamiento o para la seguridad de garantías de escritura. En función de sus requisitos de utilización del almacenamiento y su capacidad para supervisar y reponer espacio libre rápidamente, debe determinar el volumen de FlexVol y los volúmenes LUN adecuados para su instalación.



No es necesario un volumen separado para cada LUN.

Paso

1. Use el siguiente árbol de decisiones para determinar la mejor combinación de configuración de volumen y LUN para su entorno:



Opción de configuración para archivos reservados espacio o LUN con volúmenes aprovisionados con thick-Provisioning

Esta combinación de configuración de volumen y archivo de FlexVol o LUN ofrece la capacidad de utilizar tecnologías de eficiencia del almacenamiento y no le requiere supervisar de forma activa el espacio libre, ya que se asigna suficiente espacio de

antemano.

Las siguientes opciones de configuración son necesarias para configurar un archivo o LUN con espacio reservado en un volumen mediante el aprovisionamiento grueso:

| Ajuste del volumen | Valor |
|------------------------------------|--|
| Garantizado | Volumen |
| Reserva fraccionaria | 100 |
| Reserva de Snapshot | Cualquiera |
| Eliminación automática de Snapshot | Opcional |
| Crecimiento automático | Opcional; si está habilitado, el espacio libre del agregado debe supervisarse de forma activa. |

| Configuración de archivo o LUN | Valor |
|--------------------------------|----------|
| Reserva de espacio | Activado |

Configuración para archivos que no estén reservados espacio o LUN con volúmenes con thin provisioning

Esta combinación de configuración de volumen y archivo FlexVol o LUN requiere la cantidad más pequeña de almacenamiento que se asigne de antemano, pero requiere la gestión activa del espacio libre para evitar errores debido a la falta de espacio.

Los siguientes ajustes de configuración son necesarios para configurar un LUN o archivos sin espacio reservado en un volumen con thin provisioning:

| Ajuste del volumen | Valor |
|------------------------------------|------------|
| Garantizado | Ninguno |
| Reserva fraccionaria | 0 |
| Reserva de Snapshot | Cualquiera |
| Eliminación automática de Snapshot | Opcional |
| Crecimiento automático | Opcional |

| Configuración de archivo o LUN | Valor |
|--------------------------------|---------------|
| Reserva de espacio | Deshabilitado |

Consideraciones adicionales

Cuando el volumen o el agregado se queda sin espacio, se puede producir un error en las operaciones de escritura en el archivo o la LUN.

Si no desea supervisar activamente el espacio libre tanto del volumen como del agregado, debe habilitar la fila automática para el volumen y establecer el tamaño máximo para el volumen en el tamaño del agregado. En esta configuración, se debe supervisar el espacio libre del agregado de forma activa, pero no es necesario supervisar el espacio libre del volumen.

Configuración para archivos reservados espacio o LUN con aprovisionamiento de volúmenes semigruesos

Esta combinación de configuración de volumen y archivo o LUN de FlexVol requiere que haya menos almacenamiento que la combinación completamente aprovisionada, pero impone restricciones sobre las tecnologías de eficiencia que se pueden utilizar para el volumen. Las sobrescrituras se realizan de acuerdo con el mejor esfuerzo posible para esta combinación de configuración.

Las siguientes opciones de configuración son necesarias para configurar un LUN con reserva de espacio en un volumen mediante el aprovisionamiento semi-grueso:

| Ajuste del volumen | Valor |
|------------------------------------|---|
| Garantizado | Volumen |
| Reserva fraccionaria | 0 |
| Reserva de Snapshot | 0 |
| Eliminación automática de Snapshot | Activado, con un nivel de compromiso de destrucción, una lista de destrucción que incluye todos los objetos, el activador establecido en volumen y todos los LUN y archivos FlexClone habilitados para la eliminación automática. |
| Crecimiento automático | Opcional; si está habilitado, el espacio libre del agregado debe supervisarse de forma activa. |

| Configuración de archivo o LUN | Valor |
|--------------------------------|----------|
| Reserva de espacio | Activado |

Restricciones tecnológicas

No se pueden usar las siguientes tecnologías de eficiencia del almacenamiento de volumen para esta combinación de configuración:

- Compresión
- Deduplicación

- Descarga de copias ODX y FlexClone
- LUN y archivos de FlexClone no marcados para eliminación automática (clones activos)
- Subarchivos FlexClone
- ODX/descarga de copias

Consideraciones adicionales

Al emplear esta combinación de configuración deben tenerse en cuenta los siguientes hechos:

- Cuando el volumen que admite que la LUN se ejecuta con poco espacio, se destruyen los datos de protección (LUN y archivos de FlexClone, copias Snapshot).
- Es posible que se agote el tiempo de espera de las operaciones de escritura y se produzca un error en ellas cuando el volumen se queda sin espacio libre.

De forma predeterminada, la compresión se habilita para las plataformas AFF. Debe deshabilitar explícitamente la compresión en cualquier volumen para el que desee utilizar aprovisionamiento de media en una plataforma AFF.

Precauciones y consideraciones para cambiar la capacidad del archivo o directorio

Consideraciones que tener en cuenta para cambiar el número máximo de archivos permitidos en un volumen FlexVol

Los volúmenes FlexVol tienen un número máximo de archivos que pueden contener. Es posible cambiar la cantidad máxima de archivos de un volumen, pero antes de hacerlo, se debe comprender cómo afecta este cambio al volumen.

Si los datos requieren un gran número de archivos o directorios muy grandes, puede ampliar la capacidad de archivos o directorios de ONTAP. Sin embargo, debe comprender las limitaciones y advertencias a la hora de hacerlo antes de continuar.

El número de archivos que puede contener un volumen está determinado por la cantidad de inodos que tiene. Un *inode* es una estructura de datos que contiene información acerca de los archivos. Los volúmenes tienen inodos tanto privados como públicos. Los inodos públicos se utilizan para archivos visibles para el usuario; los inodos privados se utilizan para archivos que ONTAP utiliza internamente. Solo se puede cambiar el número máximo de inodos públicos de un volumen. No puede afectar el número de inodos privados.

ONTAP establece automáticamente el número máximo de inodos públicos de un volumen recién creado en función del tamaño del volumen: 1 inodo por 32 KB de tamaño del volumen. Cuando aumenta el tamaño de un volumen, ya sea directamente por un administrador o de forma automática por medio de ONTAP mediante la función de dimensionamiento automático, ONTAP también aumenta (si es necesario) el número máximo de inodos públicos, de modo que hay al menos 1 inodo por cada 32 KB de tamaño de volumen. Hasta que el volumen alcance aproximadamente 680 GB.

En versiones de ONTAP anteriores a 9.13.1, aumentar el volumen a más de 680 GB no da como resultado automáticamente más inodos, ya que ONTAP no crea automáticamente más de 22.369.621 inodos. Si necesita más archivos que el número predeterminado para cualquier volumen de tamaño, puede usar el comando `volume modify` para aumentar la cantidad máxima de inodos del volumen.

A partir de ONTAP 9.13.1, el número máximo de inodos sigue creciendo de modo que hay un inodo por 32 KB de espacio de volumen incluso si el volumen es mayor que 680 GB. Este crecimiento continúa hasta que el volumen alcanza el inodo máximo de 2.147.483.632.

También puede disminuir el número máximo de inodos públicos. Al disminuir el número de inodos públicos, *not* cambia la cantidad de espacio asignado a inodes, pero reduce la cantidad máxima de espacio que puede consumir el archivo de inodo público. Una vez asignado espacio para inodos, el volumen no volverá nunca a devolverlo. Por lo tanto, la reducción del número máximo de inodos por debajo del número de inodos asignados actualmente no devuelve el espacio utilizado por los inodos asignados.

Más información

- [Muestra el uso de archivos o inodo](#)

Precauciones para aumentar el tamaño máximo de directorio para volúmenes de FlexVol

Puede aumentar el tamaño máximo de directorio predeterminado para un volumen de FlexVol específico mediante el `-maxdir-size` opción de `volume modify` comando, pero hacerlo puede afectar al rendimiento del sistema. Consulte el artículo de la base de conocimientos "[¿Qué es maxdirsize?](#)".

Para obtener más información acerca de los tamaños máximos de directorio dependientes del modelo de los volúmenes FlexVol, visite "[Hardware Universe de NetApp](#)".

Reglas que rigen los volúmenes raíz del nodo y los agregados raíz

El volumen raíz de un nodo contiene directorios y archivos especiales para ese nodo. El agregado raíz contiene el volumen raíz. Algunas reglas rigen el volumen raíz y el agregado raíz de un nodo.

El volumen raíz de un nodo es un volumen FlexVol que se instala de fábrica o mediante el software de configuración. Está reservado para los archivos del sistema, los archivos de registro y los archivos de núcleo. El nombre del directorio es `/mroot`, a la que sólo se puede acceder a través del shell del sistema mediante el soporte técnico. El tamaño mínimo para el volumen raíz de un nodo depende del modelo de plataforma.

- Las siguientes reglas rigen el volumen raíz del nodo:
 - A menos que el soporte técnico le indique que lo haga, no modifique la configuración ni el contenido del volumen raíz.
 - No almacenar datos de usuario en el volumen raíz.

El almacenamiento de datos de usuario en el volumen raíz aumenta el tiempo de devolución del almacenamiento entre nodos de un par de alta disponibilidad.

- Puede mover el volumen raíz a otro agregado.

["Reubicación de volúmenes raíz en nuevos agregados"](#)

- El agregado raíz está dedicado únicamente al volumen raíz del nodo.

ONTAP impide la creación de otros volúmenes en el agregado raíz.

["Hardware Universe de NetApp"](#)

Reubique los volúmenes raíz en nuevos agregados

El procedimiento de reemplazo raíz migra el agregado raíz actual a otro conjunto de

discos sin interrupciones.

Acerca de esta tarea

Puede cambiar la ubicación del volumen raíz a un nuevo agregado en las siguientes situaciones:

- Cuando los agregados raíz no se encuentran en el disco que prefiere
- Cuando desee reorganizar los discos conectados al nodo
- Cuando realice el reemplazo de una bandeja de bandejas de discos EOS

Pasos

1. Reubicar el agregado raíz:

```
system node migrate-root -node node_name -disklist disk_list -raid-type  
raid_type
```

- **-nodo**

Especifica el nodo que posee el agregado raíz que desea migrar.

- **-disklist**

Especifica la lista de discos en los que se creará el nuevo agregado raíz. Todos los discos deben ser repuestos y ser propiedad del mismo nodo. El número mínimo de discos necesario depende del tipo de RAID.

- **-raid-type**

Especifica el tipo de RAID del agregado raíz. El valor predeterminado es `raid-dp`. Este es el único tipo admitido en el modo avanzado.

2. Supervise el progreso del trabajo:

```
job show -id jobid -instance
```

Resultados

Si todas las comprobaciones previas se realizan correctamente, el comando inicia un trabajo de reemplazo de volumen raíz y sale del mismo.

Funciones compatibles con archivos FlexClone y LUN FlexClone

Funciones compatibles con archivos FlexClone y LUN FlexClone

Los archivos FlexClone y las LUN de FlexClone funcionan con diferentes funciones de ONTAP, como la deduplicación, las copias snapshot, las cuotas y SnapMirror para volúmenes.

Las siguientes funciones son compatibles con archivos FlexClone y LUN FlexClone:

- Deduplicación
- Copias Snapshot
- Listas de control de acceso

- Cuotas
- Volúmenes FlexClone
- NDMP
- SnapMirror para volúmenes
- La `volume move` comando
- Reserva de espacio
- Configuración de ALTA DISPONIBILIDAD

Cómo funciona la deduplicación con archivos FlexClone y LUN FlexClone

Puede utilizar de manera eficiente el espacio de almacenamiento físico de los bloques de datos creando un archivo FlexClone o una LUN FlexClone del archivo principal y la LUN principal en un volumen habilitado para la deduplicación.

La deduplicación también utiliza el mecanismo de uso compartido de bloques utilizado por archivos y LUN FlexClone. Puede maximizar el ahorro de espacio en un volumen de FlexVol activando la deduplicación en el volumen y, a continuación, clonando el volumen en el que se ha activado la deduplicación.



Al ejecutar el `sis undo` Comando en un volumen habilitado para la deduplicación, no puede crear archivos FlexClone ni LUN FlexClone de los archivos principales ni las LUN principales que residen en dicho volumen.

Cómo funcionan las copias snapshot con archivos FlexClone y LUN FlexClone

Puede crear archivos FlexClone y LUN FlexClone a partir de una copia snapshot existente de los archivos principales y LUN principales contenidos en un volumen FlexVol.

Sin embargo, no puede eliminar manualmente una copia snapshot desde la que se crean los archivos FlexClone o las LUN FlexClone hasta que finalice el proceso de uso compartido de bloques entre las entidades principal y clonado. La copia Snapshot permanece bloqueada hasta que se completa el proceso de uso compartido de bloques, lo que se produce en segundo plano. Por lo tanto, cuando se intenta eliminar una copia Snapshot bloqueada, el sistema muestra un mensaje en el que se le solicita volver a intentar la operación después de un tiempo. En esta situación, si desea eliminar manualmente la copia de Snapshot particular, debe seguir reintentando la operación de eliminación para que la copia de Snapshot se elimine una vez que se haya completado el uso compartido de bloque.

Cómo funcionan las listas de control de acceso con los archivos FlexClone y las LUN FlexClone

Los archivos FlexClone y las LUN FlexClone heredan las listas de control de acceso de sus LUN y archivos principales.

Si los archivos principales contienen secuencias de Windows NT, los archivos FlexClone heredan también la información de la secuencia. Sin embargo, los archivos principales que contienen más de seis flujos no se pueden clonar.

Cómo funcionan las cuotas con los archivos FlexClone y las LUN FlexClone

Los límites de cuota se aplican al tamaño lógico total de los archivos FlexClone o las

LUN FlexClone. Las operaciones de clonado no fallan en el uso compartido de bloques, incluso si provoca que las cuotas superen.

Al crear un archivo FlexClone o LUN de FlexClone, las cuotas no reconocen ningún ahorro de espacio. Por ejemplo, si crea un archivo FlexClone de un archivo principal de 10 GB, solo utiliza 10 GB de espacio físico, pero la utilización de cuota se registra como 20 GB (10 GB para el archivo principal y 10 GB para el archivo FlexClone).

Si la creación de un archivo o un LUN FlexClone hace que se supere la cuota de usuario o grupo, la operación de clonado se complete correctamente siempre que el volumen FlexVol tenga suficiente espacio para contener los metadatos del clon. Sin embargo, la cuota para ese usuario o grupo está suscrita en exceso.

Funcionamiento de los volúmenes FlexClone con archivos FlexClone y LUN FlexClone

Puede crear un volumen FlexClone de un volumen FlexVol que tenga tanto un archivo FlexClone como una LUN FlexClone y su archivo principal o LUN.

Los archivos FlexClone o las LUN FlexClone y sus archivos principales o las LUN presentes en el volumen FlexClone siguen compartiendo los bloques del mismo modo que en el volumen FlexVol principal. De hecho, todas las entidades FlexClone y sus padres comparten los mismos bloques de datos físicos subyacentes, lo que minimiza el uso de espacio en disco físico.

Si el volumen FlexClone está dividido desde el volumen principal, los archivos FlexClone o las LUN FlexClone y sus archivos principales o LUN dejan de compartir los bloques del clon del volumen FlexClone. A partir de entonces, existen como archivos o LUN independientes. Esto significa que el clon del volumen usa más espacio que antes de la operación de división.

Cómo funciona NDMP con archivos FlexClone y LUN FlexClone

NDMP funciona a nivel lógico con archivos FlexClone y LUN FlexClone. Se realiza un backup de todos los archivos FlexClone o LUN como archivos o LUN independientes.

Cuando utiliza servicios NDMP para realizar backup de un volumen qtree o FlexVol que contiene archivos FlexClone o LUN FlexClone, no se conserva el uso compartido de bloques entre entidades principales y clones, y se realiza un backup de las entidades clonadas en cinta como archivos o LUN independientes. Se pierde el ahorro de espacio. Por lo tanto, la cinta de la que realiza la copia de seguridad debe tener espacio suficiente para almacenar la cantidad ampliada de datos. Al restaurar, todos los archivos FlexClone y las LUN FlexClone se restauran como archivos físicos y LUN independientes. Puede activar la deduplicación en el volumen para restaurar las ventajas de uso compartido de bloques.



Cuando se crean archivos FlexClone y LUN FlexClone a partir de una copia Snapshot existente de un volumen FlexVol, no se puede realizar un backup del volumen a cinta hasta que se complete el proceso de uso compartido de bloques, que sucede en segundo plano. Si utiliza NDMP en el volumen cuando el proceso de uso compartido de bloques está en curso, el sistema muestra un mensaje que le pide que vuelva a intentar la operación después de un tiempo. En tal caso, debe seguir volviendo a intentar la operación de copia de seguridad de cinta para que tenga éxito una vez que se haya completado el uso compartido del bloque.

Cómo funciona SnapMirror para volúmenes con archivos FlexClone y LUN FlexClone

SnapMirror para volúmenes utilizado con archivos FlexClone y LUN de FlexClone ayuda a mantener el ahorro de espacio, ya que las entidades clonadas solo se replican una

vez.

Si un volumen FlexVol es un origen de SnapMirror para volúmenes y contiene archivos FlexClone o LUN FlexClone, SnapMirror para volúmenes transfiere solo el bloque físico compartido y una pequeña cantidad de metadatos al destino de SnapMirror para volúmenes. El destino almacena sólo una copia del bloque físico y este bloque se comparte entre las entidades principal y clonada. Por tanto, el volumen de destino es una copia exacta del volumen de origen y todos los archivos o LUN clonados del volumen de destino comparten el mismo bloque físico.

Cómo afecta el movimiento de volúmenes a los archivos FlexClone y las LUN de FlexClone

Durante la fase de transición de una operación de movimiento de volúmenes, no se pueden crear archivos FlexClone ni LUN FlexClone de un volumen FlexVol.

Cómo funciona la reserva de espacio con los archivos FlexClone y las LUN FlexClone

De forma predeterminada, los archivos FlexClone y las LUN FlexClone heredan el atributo de reserva de espacio del archivo principal y la LUN principal. Sin embargo, puede crear archivos FlexClone y LUN FlexClone con la reserva de espacio deshabilitada desde un archivo principal y una LUN principal con la reserva de espacio habilitada si el volumen FlexVol carece de espacio.

Si el volumen FlexVol no contiene espacio suficiente para crear un archivo FlexClone o una LUN FlexClone con la misma reserva de espacio que la del principal, se produce un error en la operación de clonado.

Cómo funciona una configuración de alta disponibilidad con archivos FlexClone y LUN FlexClone

Las operaciones con archivos FlexClone y LUN FlexClone se admiten en una configuración de alta disponibilidad.

En un par de alta disponibilidad, no se pueden crear archivos FlexClone o LUN FlexClone en el partner mientras la operación de toma de control o devolución está en curso. Todas las operaciones de uso compartido de bloques pendientes en el partner se reanudan una vez completada la operación de toma de control o devolución.

Aprovisione almacenamiento NAS para sistemas de archivos de gran tamaño con volúmenes FlexGroup

Un volumen FlexGroup es un contenedor NAS escalable que ofrece alto rendimiento junto con la distribución automática de la carga. Los volúmenes FlexGroup proporcionan una enorme capacidad (en petabytes), que supera considerablemente los límites de los volúmenes FlexVol, sin añadir gastos generales de gestión.

Los temas de esta sección muestran la forma de gestionar volúmenes de FlexGroup con System Manager en ONTAP 9.7 y versiones posteriores. Si utiliza la versión clásica de System Manager (disponible solo en ONTAP 9.7 y versiones anteriores), consulte este tema:

- ["Cree volúmenes de FlexGroup"](#)

A partir de ONTAP 9.9.1, se admiten relaciones de ventilador de SnapMirror de dos o más volúmenes

FlexGroup, con un máximo de ocho patas de ventilador. System Manager no admite relaciones de volúmenes de FlexGroup en cascada de SnapMirror.

ONTAP selecciona automáticamente los niveles locales necesarios para crear el volumen FlexGroup.

A partir de ONTAP 9.8, cuando se aprovisiona el almacenamiento, la calidad de servicio se habilita de forma predeterminada. Puede deshabilitar la calidad de servicio o seleccionar una política de calidad de servicio personalizada durante el proceso de aprovisionamiento o más adelante.

Pasos

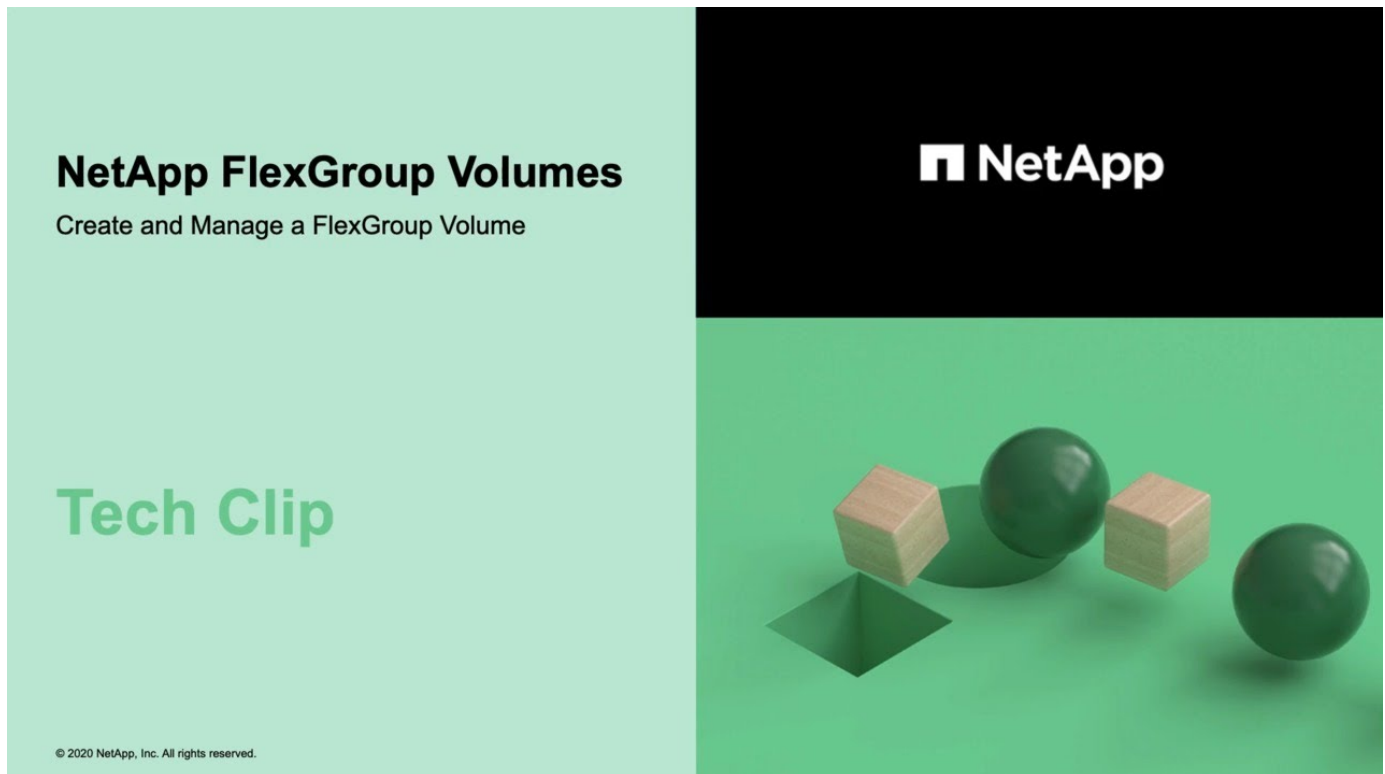
1. Haga clic en **almacenamiento > volúmenes**.
2. Haga clic en **Agregar**.
3. Haga clic en **más opciones** y seleccione **distribuir datos de volumen en el clúster**.



Si está ejecutando ONTAP 9,8 o posterior y desea deshabilitar QoS o elegir una política de QoS personalizada, haga clic en **Más opciones** y, a continuación, en **Almacenamiento y optimización**, seleccione **Nivel de servicio de rendimiento**.

Vídeos

Cree y gestione un volumen de FlexGroup



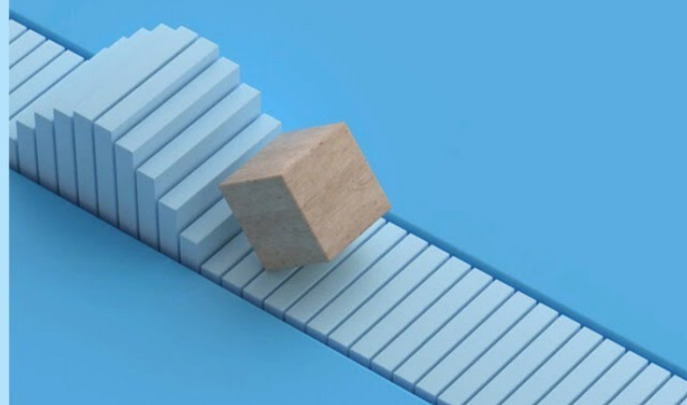
Volúmenes FlexGroup: Haga más con menos

NetApp FlexGroup Volumes

Do More with Less

Use Case

© 2020 NetApp, Inc. All rights reserved.



Gestión de volúmenes de FlexGroup con interfaz de línea de comandos

Información general de gestión de volúmenes de FlexGroup con la interfaz de línea de comandos

Puede configurar, gestionar y proteger volúmenes de FlexGroup para garantizar la escalabilidad y el rendimiento. Un volumen FlexGroup es un volumen de escalado horizontal que ofrece alto rendimiento junto con la distribución automática de la carga.

Puede configurar los volúmenes FlexGroup si se cumplen las siguientes condiciones:

- Utiliza ONTAP 9,1 o una versión posterior.
- Desea utilizar NFSv4.x, NFSv3, SMB 2.0 o SMB 2.1.
- Desea usar la interfaz de línea de comandos (CLI) de ONTAP, no System Manager ni una herramienta de secuencias de comandos automatizada.

Puede encontrar más detalles acerca de la sintaxis de comandos en la ayuda de la CLI y en las páginas manuales de ONTAP.

En System Manager, se encuentra disponible un subconjunto importante de la funcionalidad de FlexGroup.

- Quiere utilizar las prácticas recomendadas, no explorar todas las opciones disponibles.
- Tiene privilegios de administrador de clúster, no de administrador de SVM.



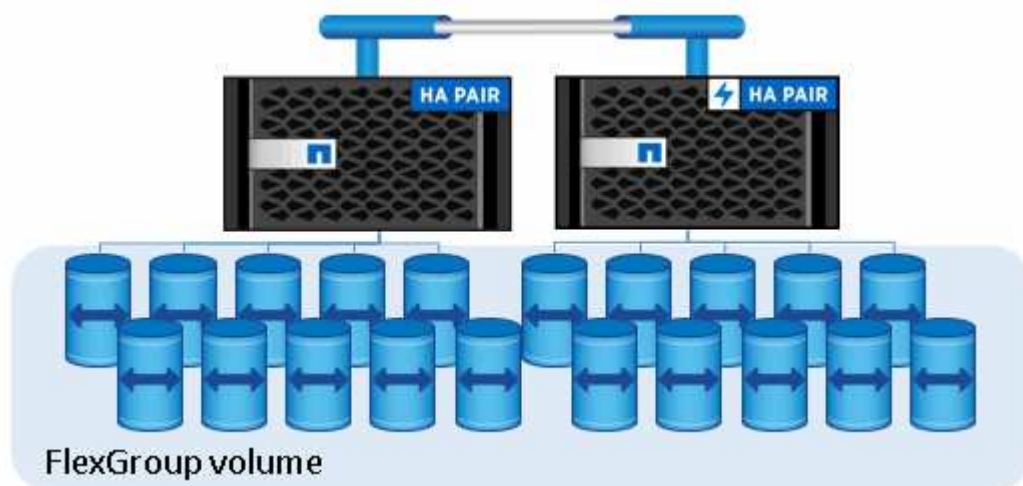
A partir de ONTAP 9,5, las instancias de FlexGroup reemplazan a los Infinite Volume, que no son compatibles con ONTAP 9,5 o versiones posteriores.

Información relacionada

La información conceptual sobre los volúmenes de FlexVol se aplica a los volúmenes de FlexGroup. La información sobre FlexVol Volumes y la tecnología ONTAP está disponible en la biblioteca de referencia de ONTAP y en los informes técnicos (TRS).

Qué es un volumen FlexGroup

Un volumen FlexGroup es un contenedor NAS de escalado horizontal que proporciona un alto rendimiento junto con la distribución de la carga y la escalabilidad automáticas. Un volumen FlexGroup consta de varios componentes que comparten el tráfico de forma automática y transparente. *Constituents* son los volúmenes FlexVol subyacentes que componen un volumen FlexGroup.



Los volúmenes de FlexGroup ofrecen los siguientes beneficios:

- Alta escalabilidad

El tamaño máximo de un volumen FlexGroup en ONTAP 9.1 y versiones posteriores es de 20 PB, con 400 000 millones de archivos en un clúster de 10 nodos.

- Altas prestaciones

Los volúmenes de FlexGroup pueden utilizar los recursos del clúster para servir cargas de trabajo que tienen un alto rendimiento y una baja latencia.

- Gestión simplificada

Un volumen FlexGroup es un único contenedor de espacio de nombres que se puede gestionar de manera similar a los volúmenes FlexVol.

Configuraciones para volúmenes de FlexGroup admitidas y no compatibles

Debe conocer las funciones de ONTAP que son compatibles y no están admitidas con

FlexGroup Volumes en ONTAP 9.

Funciones compatibles a partir de ONTAP 9.14.1

- Etiquetado de copias de Snapshot: Compatibilidad para crear, modificar y eliminar etiquetas de copias de Snapshot (etiquetas de SnapMirror y comentarios) para copias Snapshot de los volúmenes de FlexGroup con el `volume snapshot` comando.

Funciones compatibles a partir de ONTAP 9.13.1

- Protección autónoma contra ransomware (ARP) para volúmenes FlexGroup, incluida la siguiente funcionalidad admitida:
 - FlexGroup amplía las operaciones: Un nuevo componente hereda los atributos de protección autónoma frente a ransomware.
 - Conversiones de FlexVol a FlexGroup: Es posible convertir FlexVols con protección autónoma contra ransomware activa.
 - Reequilibrio de FlexGroup: La protección autónoma frente a ransomware se admite durante operaciones de reequilibrio disruptivas y no disruptivas.
- Programe una sola operación de reequilibrio de FlexGroup.
- Relaciones de expansión de SnapMirror con DR de SVM en volúmenes de FlexGroup. Admite fanout a ocho sitios.

Funciones compatibles a partir de ONTAP 9.12.1

- Reequilibrado de FlexGroup
- SnapLock para SnapVault
- La recuperación ante desastres de FabricPool, FlexGroup y SVM funciona conjuntamente. (En las versiones anteriores a ONTAP 9.12.1, dos de estas funciones funcionaban juntas, pero no las tres de manera conjunta).
- El componente del volumen de FlexGroup aumenta hasta un máximo de 300 TB en las plataformas AFF y FAS cuando se usa ONTAP 9.12.1 P2 y versiones posteriores.

Funciones compatibles a partir de ONTAP 9.11.1

- Volúmenes de SnapLock

SnapLock no admite las siguientes funciones con los volúmenes de FlexGroup:

- Conservación legal
- Retención basada en eventos
- SnapLock para SnapVault

Puede configurar SnapLock en el nivel de FlexGroup. No se puede configurar SnapLock a nivel de componente.

Qué es SnapLock

- Eliminación del directorio asíncrono de cliente

[Gestione los derechos de cliente para eliminar directorios rápidamente](#)

Funciones compatibles desde ONTAP 9.10.1

- Convierta volúmenes FlexVol en volúmenes FlexGroup en un origen SVM-DR

[Convierta un volumen FlexVol en un volumen FlexGroup dentro de una relación SVM-DR](#)

- Compatibilidad de FlexClone de Recuperación de desastres de SVM para volúmenes de FlexGroup

[Más información sobre la creación de volúmenes FlexClone.](#)

Funciones compatibles a partir de ONTAP 9.9.1

- Recuperación ante desastres de SVM

No se admite la clonado de un volumen FlexGroup que forma parte de una relación SVM-DR.

- SnapMirror tiene relaciones de fanout de 2 o más (A a B, A C), con un máximo de 8 patas de fanout.

[Consideraciones que tener en cuenta para crear relaciones de SnapMirror en cascada y fanout para FlexGroups](#)

- Relaciones en cascada de SnapMirror con hasta dos niveles (De A a B a C)

[Consideraciones que tener en cuenta para crear relaciones de SnapMirror en cascada y fanout para FlexGroups](#)

Funciones compatibles desde ONTAP 9.8

- Restaurar un solo archivo desde un almacén de SnapMirror de FlexGroup o desde un destino UDP
 - Restore puede ser de un volumen FlexGroup de cualquier geometría a un volumen FlexGroup de cualquier geometría
 - Solo se admite un archivo por operación de restauración
- Conversión de volúmenes en sistemas de 7-mode a volúmenes de FlexGroup

Para obtener más información, vea el artículo de la base de conocimientos ["Cómo convertir un FlexVol en FlexGroup que se ha realizado la transición"](#).

- NFSv4,2
- Eliminación asíncrona de archivos y directorios
- Análisis de sistemas de archivos (FSA)
- FlexGroup como almacén de datos de VMware vSphere
- Compatibilidad adicional para backups en cinta y restauraciones con NDMP, incluidas las siguientes funciones:
 - Extensión de backup reinicializable de NDMP (RBE) y extensión de gestión de Snapshot (SSME)
 - Las variables de entorno EXCLUYEN y MULTI_SUBTREE_NAMES admiten copias de seguridad de FlexGroup
 - Introducción de la variable de entorno IGNORE_CTIME_MTIME para las copias de seguridad de FlexGroup
 - Recuperación de archivos individuales en un FlexGroup mediante el mensaje

nfmp_SNAP_RECOVER, que forma parte de la extensión 0x2050

Las sesiones de volcado y restauración se cancelan durante una actualización o reversión.

Funciones compatibles a partir de ONTAP 9,7

- Volumen FlexClone
- NFSv4 y NFSv4,1
- PNFs
- Backup y restauración a cinta mediante NDMP

Debe tener en cuenta los siguientes puntos para compatibilidad con NDMP en los volúmenes de FlexGroup:

- El mensaje NDMP_SNAP_RECOVER de la clase de extensión 0x2050 solo se puede utilizar para recuperar un volumen FlexGroup completo.

No se pueden recuperar archivos individuales en un volumen FlexGroup.

- La extensión de backup (RBE) NDMP restartable no se admite en los volúmenes de FlexGroup.
- Las variables de entorno EXCLUDE y MULTI_SUBTREE_NAMES no son compatibles con los volúmenes FlexGroup.
- La `ndmpcopy` Se admite el comando para la transferencia de datos entre los volúmenes de FlexVol y FlexGroup.

Si se revierte de Data ONTAP 9.7 a una versión anterior, la información de transferencia incremental de las transferencias anteriores no se conserva y, por lo tanto, se debe realizar una copia básica después de revertir.

- API de VMware vStorage para integración de cabinas (VAAI)
- Conversión de un volumen de FlexVol a un volumen de FlexGroup
- Volúmenes FlexGroup como volúmenes de origen de FlexCache

Funciones compatibles a partir de ONTAP 9,6

- Recursos compartidos de SMB disponibles de forma continua
- Configuraciones de MetroCluster
- Cambiar el nombre de un volumen FlexGroup (`volume rename` comando)
- Reducir o reducir el tamaño de un volumen de FlexGroup (`volume size` comando)
- Tamaño elástico
- Cifrado de agregados de NetApp (NAE)
- Cloud Volumes ONTAP

Funciones compatibles a partir de ONTAP 9,5

- Descarga de copias ODX
- Protección de acceso al nivel de almacenamiento
- Mejoras en las notificaciones de cambio para recursos compartidos de SMB

Las notificaciones de cambios se envían para los cambios realizados en el directorio principal en el que `changenotify` se establece la propiedad y para los cambios realizados en todos los subdirectorios de ese directorio principal.

- FabricPool
- Cumplimiento de cuotas
- Estadísticas de Qtree
- Calidad de servicio adaptativa para archivos en volúmenes de FlexGroup
- FlexCache (solo caché; FlexGroup como origen admitido en ONTAP 9.7)

Funciones compatibles a partir de ONTAP 9,4

- FPolicy
- Auditoría de archivos
- Piso de rendimiento (QoS mín.) y QoS adaptativo para volúmenes de FlexGroup
- Techo de rendimiento (QoS máx.) y piso de rendimiento (QoS mín.) para archivos en volúmenes FlexGroup

Utilice la `volume file modify` Comando para gestionar el grupo de políticas de calidad de servicio asociado a un archivo.

- Límites SnapMirror relajados
- SMB 3.x multicanal

Funciones compatibles a partir de ONTAP 9,3

- Configuración de antivirus
- Notificaciones de cambios para recursos compartidos de SMB

Las notificaciones se envían sólo para los cambios realizados en el directorio principal en el que `changenotify` la propiedad está establecida. Las notificaciones de cambio no se envían para los cambios realizados en los subdirectorios del directorio principal.

- Qtrees
- Techo de rendimiento (QoS máx.)
- Expandir el volumen de FlexGroup de origen y el volumen de FlexGroup de destino en una relación de SnapMirror
- Backup y restauración de SnapVault
- Relaciones de protección de datos unificadas
- Opción de autotrecimiento y autorreducción
- El recuento de nodos de información se contemplado en la ingesta

Función compatible a partir de ONTAP 9.2

- Cifrado de volúmenes
- Deduplicación inline de agregados (deduplicación entre volúmenes)

- Cifrado de volúmenes de NetApp (NVE)

Funciones compatibles a partir de ONTAP 9.1

Los volúmenes de FlexGroup se introdujeron en ONTAP 9.1, con compatibilidad con varias funciones de ONTAP.

- Tecnología SnapMirror
- Copias Snapshot
- Active IQ
- Compresión adaptativa inline
- Deduplicación en línea
- Compactación de datos inline
- AFF
- Informes de cuotas
- Tecnología Snapshot de NetApp
- Software SnapRestore (nivel FlexGroup)
- Agregados híbridos
- Movimiento de un componente o un volumen miembro
- Deduplicación postprocesamiento
- Tecnología RAID-TEC de NetApp
- Punto de coherencia por agregado
- El uso compartido de FlexGroup con volumen FlexVol en la misma SVM

Configuraciones no admitidas en ONTAP 9

| Protocolos no compatibles | Funciones de protección de datos no compatibles | Otras funciones ONTAP no admitidas |
|---|---|--|
| <ul style="list-style-type: none"> • PNFs (ONTAP 9.0 a 9.6) • SMB 1.0 • Conmutación por error transparente de SMB (ONTAP 9.0 a 9.5) • SAN | <ul style="list-style-type: none"> • Volúmenes de SnapLock (ONTAP 9.10.1 y versiones anteriores) • SMTape • SnapMirror sincrónico • DR de SVM con volúmenes de FlexGroup que contienen FabricPool | <ul style="list-style-type: none"> • Servicio de copia de volúmenes redundantes (VSS) remoto • Movilidad de datos de SVM |

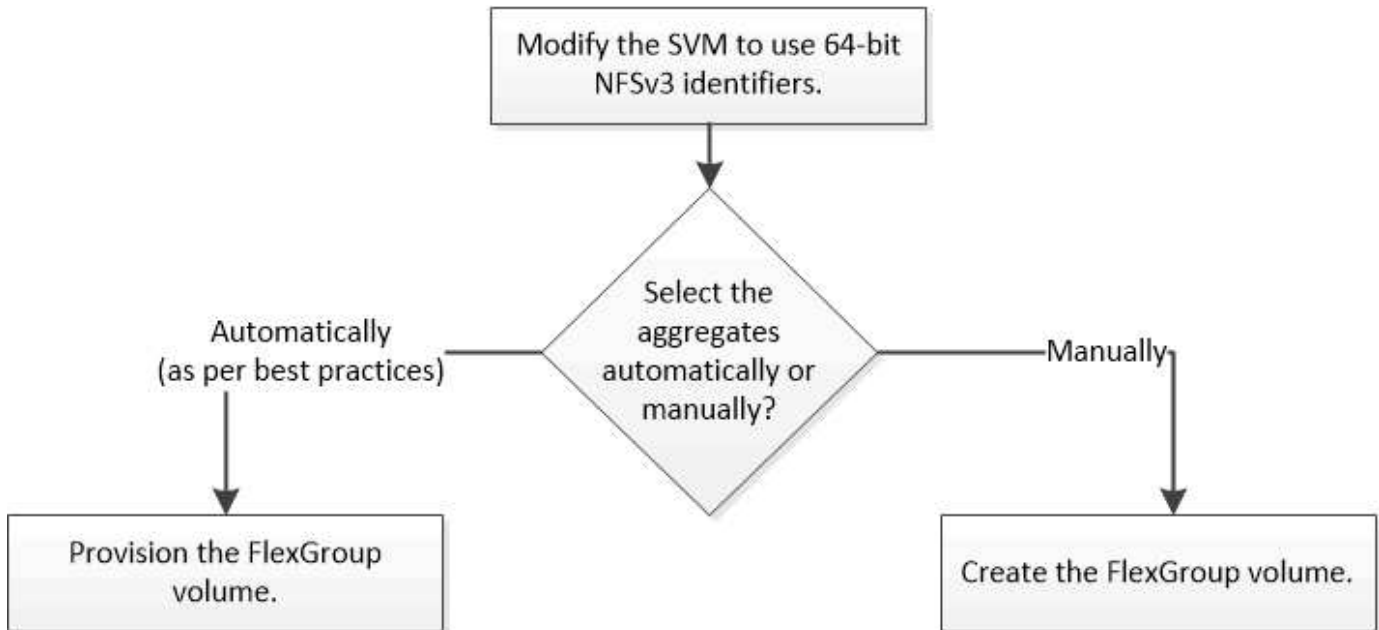
Información relacionada

["Centro de documentación de ONTAP 9"](#)

Configuración de volúmenes de FlexGroup

Flujo de trabajo de configuración del volumen FlexGroup

Puede aprovisionar un volumen de FlexGroup donde ONTAP selecciona automáticamente los agregados según las prácticas recomendadas para un rendimiento óptimo, o bien crear un volumen de FlexGroup seleccionando manualmente los agregados y configurándolo para el acceso a los datos.



Lo que necesitará

Debe haber creado la SVM con NFS y SMB añadidos a la lista de protocolos permitidos para la SVM.

Acerca de esta tarea

Es posible aprovisionar automáticamente un volumen de FlexGroup solo en clústeres con cuatro nodos o menos. En los clústeres con más de cuatro nodos, debe crear un volumen FlexGroup de forma manual.

Habilite los identificadores de NFSv3 de 64 bits en una SVM

Para admitir el número alto de archivos de los volúmenes de FlexGroup y evitar las colisiones de ID de archivo, debe habilitar los identificadores de archivo de 64 bits en la SVM donde se debe crear el volumen de FlexGroup.

Pasos

1. Inicie sesión en el nivel de privilegio avanzado: `set -privilege advanced`
2. Modifique la SVM para utilizar los ID de archivo y los ID de SO NFSv3 de 64 bits: `vserver nfs modify -vserver svm_name -v3-64bit-identifiers enabled`

```
cluster1::*> vserver nfs modify -vserver vs0 -v3-64bit-identifiers
enabled

Warning: You are attempting to increase the number of bits used for
NFSv3
        FSIIDs and File IDs from 32 to 64 on Vserver "vs0". This could
        result in older client software no longer working with the
volumes
        owned by Vserver "vs0".
Do you want to continue? {y|n}: y

Warning: Based on the changes you are making to the NFS server on
Vserver
        "vs0", it is highly recommended that you remount all NFSv3
clients
        connected to it after the command completes.
Do you want to continue? {y|n}: y
```

Después de terminar

Todos los clientes deben volver a montarse. Esto es necesario porque cambian los ID del sistema de archivos y es posible que los clientes reciban mensajes obsoletos al intentar realizar operaciones NFS.

Aprovisionar automáticamente un volumen FlexGroup

Puede aprovisionar automáticamente un volumen de FlexGroup. ONTAP crea y configura un volumen de FlexGroup seleccionando automáticamente los agregados. Los agregados se seleccionan según las prácticas recomendadas para un rendimiento óptimo.

Lo que necesitará

Cada nodo del clúster debe tener al menos un agregado.



Para crear un volumen de FlexGroup para FabricPool en ONTAP 9.5, cada nodo debe tener al menos un agregado que sea FabricPool.


Acerca de esta tarea

ONTAP selecciona dos agregados con la mayor cantidad de espacio útil de cada nodo para crear el volumen FlexGroup. Si no hay dos agregados disponibles, ONTAP selecciona un agregado por nodo para crear el volumen FlexGroup.

Pasos

1. Aprovisione el volumen FlexGroup:

| Si está usando... | Se usa este comando... |
|-------------------|------------------------|
| | |

| | |
|-----------------------|--|
| ONTAP 9,2 o posterior | <pre>volume create -vserver svm_name -volume fg_vol_name -auto-provision-as flexgroup -size fg_size [-encrypt true] [-qos-policy-group qos_policy_group_name] [-support- tiering true]</pre> <p>A partir de ONTAP 9.5, se pueden crear volúmenes de FlexGroup para FabricPool. Para aprovisionar automáticamente un volumen de FlexGroup en FabricPool, debe configurar el <code>-support-tiering</code> parámetro a <code>true</code>. La garantía de volumen siempre debe configurarse en <code>none</code> Para FabricPool. También puede especificar la política de organización en niveles y el período de refrigeración mínimo del volumen de FlexGroup.</p> <p>"Gestión de discos y agregados"</p> <p>A partir de ONTAP 9.3, puede especificar un techo de rendimiento (QoS máx.) para los volúmenes FlexGroup, que limita los recursos de rendimiento que puede consumir el volumen FlexGroup. A partir de ONTAP 9.4, se pueden especificar pisos de rendimiento (calidad de servicio mínima) y calidad de servicio adaptativa para los volúmenes FlexGroup.</p> <p>"Gestión del rendimiento"</p> <p>A partir de ONTAP 9.2, puede configurar el <code>-encrypt</code> parámetro a <code>true</code> Si desea habilitar el cifrado en el volumen de FlexGroup. Para crear un volumen cifrado, debe haber instalado la licencia de cifrado de volúmenes y el gestor de claves.</p> <div data-bbox="873 1402 928 1461">  </div> <div data-bbox="987 1350 1432 1518"> <p>Debe habilitar el cifrado en volúmenes de FlexGroup en el momento de su creación. No puede habilitar el cifrado en volúmenes de FlexGroup existentes.</p> </div> <p>"Cifrado de datos en reposo"</p> |
| ONTAP 9,1 | <pre>volume flexgroup deploy -vserver svm_name -size fg_size</pre> |

La `size` El parámetro especifica el tamaño del volumen FlexGroup en KB, MB, GB, TB o PB.

El ejemplo siguiente muestra cómo aprovisionar un volumen FlexGroup de tamaño 400 TB en ONTAP 9.2:

```
cluster-1::> volume create -vserver vs0 -volume fg -auto-provision-as
flexgroup -size 400TB
Warning: The FlexGroup "fg" will be created with the following number of
constituents of size 25TB: 16.
The constituents will be created on the following aggregates:
aggr1,aggr2
Do you want to continue? {y|n}: y
[Job 34] Job succeeded: Successful
```

El siguiente ejemplo muestra cómo crear un grupo de políticas de calidad de servicio para techo de rendimiento y cómo se aplica a un volumen de FlexGroup:

```
cluster1::> qos policy-group create -policy group pg-vs1 -vserver vs1
-max-throughput 5000iops
```

```
cluster-1::> volume create -vserver vs0 -volume fg -auto-provision-as
flexgroup -size 400TB -qos-policy-group pg-vs1
Warning: The FlexGroup "fg" will be created with the following number of
constituents of size 25TB: 16.
The constituents will be created on the following aggregates:
aggr1,aggr2
Do you want to continue? {y|n}: y
[Job 34] Job succeeded: Successful
```

El ejemplo siguiente muestra cómo aprovisionar un volumen FlexGroup de tamaño 400 TB en agregados en FabricPool en ONTAP 9.5:

```
cluster-1::> volume create -vserver vs0 -volume fg -auto-provision-as
flexgroup -size 400TB -support-tiering true -tiering-policy auto
Warning: The FlexGroup "fg" will be created with the following number of
constituents of size 25TB: 16.
The constituents will be created on the following aggregates:
aggr1,aggr2
Do you want to continue? {y|n}: y
[Job 34] Job succeeded: Successful
```

El volumen FlexGroup se crea con ocho componentes en cada nodo del clúster. Los componentes se distribuyen por igual entre los dos agregados de mayor tamaño de cada nodo.

De manera predeterminada, se crea el volumen FlexGroup con la `volume` Configuración de garantía de espacio excepto en sistemas AFF. Para los sistemas AFF, el volumen FlexGroup se crea de forma predeterminada con la `none` garantía de espacio.

2. Monte el volumen FlexGroup en una ruta de unión: `volume mount -vserver vs0 -volume fg2 -junction-path /fg2`

```
cluster1::> volume mount -vserver vs0 -volume fg2 -junction-path /fg2
```

Después de terminar

Debe montar el volumen FlexGroup desde el cliente.

Si ejecuta ONTAP 9.6 o una versión anterior y si la máquina virtual de almacenamiento (SVM) tiene configuradas NFSv3 y NFSv4, es posible que se produzca un error en el montaje del volumen FlexGroup del cliente. En estos casos, debe especificar explícitamente la versión de NFS al montar el volumen de FlexGroup desde el cliente.

```
# mount -t nfs -o vers=3 192.53.19.64:/fg2 /mnt/fg2
# ls /mnt/fg2
file1  file2
```

Cree un volumen de FlexGroup

Puede crear un volumen de FlexGroup seleccionando manualmente los agregados en los que debe crearse el volumen de FlexGroup y especificando el número de componentes en cada agregado.

Acerca de esta tarea

Debe tener en cuenta el espacio requerido en los agregados para crear un volumen de FlexGroup.

Debe tener en cuenta las siguientes directrices al crear un volumen de FlexGroup para obtener los mejores resultados de rendimiento con un volumen de FlexGroup:

- Un volumen de FlexGroup debe abarcar únicamente agregados que utilicen sistemas de hardware idénticos.

El uso de sistemas de hardware idénticos ayuda a proporcionar un rendimiento previsible en todo el volumen de FlexGroup.

- Un volumen FlexGroup debe abarcar agregados con el mismo tipo de disco y la misma configuración de grupo RAID.

Para lograr un rendimiento consistente, debe asegurarse de que todos los agregados estén compuestos por SSD, todos los HDD o todos los agregados híbridos. Además, los agregados deben tener la misma cantidad de unidades y de grupos RAID en el volumen FlexGroup.

- Un volumen de FlexGroup puede abarcar partes de un clúster.

No es necesario configurar un volumen FlexGroup para abarcar todo el clúster, pero al hacerlo se puede sacar mayor partido a los recursos de hardware disponibles.

- Al crear un volumen de FlexGroup, es mejor que los agregados en los que se ha puesto en marcha el volumen FlexGroup tengan las siguientes características:

- Debe haber aproximadamente la misma cantidad de espacio libre en varios agregados, sobre todo cuando se utiliza thin provisioning.
- Se debe reservar aproximadamente el 3 % del espacio libre para los metadatos del agregado después de crear el volumen de FlexGroup.
- Para los sistemas FAS, se recomienda tener dos agregados por nodo y, para los sistemas AFF, debe tener un agregado por nodo para el volumen FlexGroup.
- Para cada volumen de FlexGroup, debe crear al menos ocho componentes que se distribuyan en dos o más agregados en los sistemas de FAS, y en uno o más agregados en los sistemas de AFF.

Antes de empezar

- A partir de ONTAP 9.13.1, se pueden crear volúmenes con análisis de capacidad y seguimiento de actividades habilitados. Para activar la capacidad o el seguimiento de actividades, emita el `volume create` comando con `-analytics-state 0`. `-activity-tracking-state` establezca en `on`.

Para obtener más información sobre el análisis de capacidad y el seguimiento de actividades, consulte [Active File System Analytics](#).

Pasos

1. Cree el volumen de FlexGroup: `volume create -vserver svm_name -volume flexgroup_name -aggr-list aggr1,aggr2,.. -aggr-list-multiplier constituents_per_aggr -size fg_size [-encrypt true] [-qos-policy-group qos_policy_group_name]`

- La `-aggr-list` El parámetro especifica la lista de agregados que se usarán para los componentes de volumen de FlexGroup.

Cada entrada de la lista crea un componente en el agregado especificado. Puede especificar un agregado varias veces para que se creen varios componentes en el agregado.

Para obtener un rendimiento coherente en todo el volumen FlexGroup, todos los agregados deben usar las mismas configuraciones de tipo de disco y grupo RAID.

- La `-aggr-list-multiplier` parámetro especifica la cantidad de veces que se debe iterar sobre los agregados que se enumeran con el `-aggr-list` Parámetro cuando se crea un volumen de FlexGroup.

El valor predeterminado de `-aggr-list-multiplier` el parámetro es 4.

- La `size` El parámetro especifica el tamaño del volumen FlexGroup en KB, MB, GB, TB o PB.
- A partir de ONTAP 9.5, puede crear volúmenes de FlexGroup para FabricPool, que utilizan solo todos los agregados de SSD.

Para crear un volumen de FlexGroup para FabricPool, todos los agregados especificados con el `-aggr-list` El parámetro debe ser FabricPool. La garantía de volumen siempre debe configurarse en `none` Para FabricPool. También puede especificar la política de organización en niveles y el período de refrigeración mínimo del volumen de FlexGroup.

Gestión de discos y agregados

- A partir de ONTAP 9.4, se pueden especificar pisos de rendimiento (calidad de servicio mínima) y calidad de servicio adaptativa para los volúmenes FlexGroup.

"Gestión del rendimiento"

- A partir de ONTAP 9.3, puede especificar un techo de rendimiento (QoS máx.) para los volúmenes FlexGroup, que limita los recursos de rendimiento que puede consumir el volumen FlexGroup.
- A partir de ONTAP 9.2, puede configurar el `-encrypt` parámetro a `true` Si desea habilitar el cifrado en el volumen de FlexGroup.

Para crear un volumen cifrado, debe haber instalado la licencia de cifrado de volúmenes y el gestor de claves.



Debe habilitar el cifrado en volúmenes de FlexGroup en el momento de su creación. No puede habilitar el cifrado en volúmenes de FlexGroup existentes.

"Cifrado de datos en reposo"

```
cluster-1::> volume create -vserver vs0 -volume fg2 -aggr-list  
aggr1,aggr2,aggr3,aggr1 -aggr-list-multiplier 2 -size 500TB
```

```
Warning: A FlexGroup "fg2" will be created with the following number of  
constituents of size 62.50TB: 8.
```

```
Do you want to continue? {y|n}: y
```

```
[Job 43] Job succeeded: Successful
```

En el ejemplo anterior, si desea crear el volumen FlexGroup para FabricPool, todas las agrupaciones (aggr1, aggr2 y aggr3) deben ser agrupaciones en FabricPool. Monte el volumen FlexGroup en una ruta de unión:

```
volume mount -vserver vs0 -volume fg2 -junction-path /fg
```

```
cluster1::> volume mount -vserver vs0 -volume fg2 -junction-path /fg
```

Después de terminar

Debe montar el volumen FlexGroup desde el cliente.

Si ejecuta ONTAP 9.6 o una versión anterior y si la máquina virtual de almacenamiento (SVM) tiene configuradas NFSv3 y NFSv4, es posible que se produzca un error en el montaje del volumen FlexGroup del cliente. En estos casos, debe especificar explícitamente la versión de NFS al montar el volumen de FlexGroup desde el cliente.

```
# mount -t nfs -o vers=3 192.53.19.64:/fg /mnt/fg2  
# ls /mnt/fg2  
file1  file2
```

Información relacionada

["Informe técnico de NetApp 4571: Prácticas recomendadas y guía de implementación de FlexGroup de NetApp"](#)

Gestione volúmenes FlexGroup

Supervise el uso de espacio de un volumen FlexGroup

Puede ver un volumen de FlexGroup y sus componentes, y supervisar el espacio que usa el volumen de FlexGroup.

Acerca de esta tarea

A partir de ONTAP 9.6, se admite el ajuste de tamaño elástico. ONTAP crece automáticamente un componente de un volumen FlexGroup si se está quedando sin espacio reduciendo cualquier otro componente del volumen FlexGroup que tenga espacio libre en una cantidad equivalente. El ajuste de tamaño elástico evita los errores por falta de espacio que se generan debido a que uno o varios volúmenes constituyentes de FlexGroup se están quedando sin espacio.



A partir de ONTAP 9.9.1, la generación de informes y la aplicación de espacio lógico también están disponibles para los volúmenes FlexGroup. Para obtener más información, consulte ["Generación de informes sobre el espacio lógico y cumplimiento para volúmenes"](#).

Paso

1. Vea el espacio utilizado por el volumen de FlexGroup y sus componentes: `volume show -vserver vs1 -volume-style-extended flexgroup vs1 -volume-style-extended [flexgroup | flexgroup-constituent]`

```
cluster-2::> volume show -vserver vs1 -volume-style-extended flexgroup
Vserver   Volume      Aggregate    State    Type    Size
Available Used%
-----
vs1       fg1         -            online   RW      500GB
207.5GB   56%
```

```
ccluster-2::> volume show -vserver vs1 -volume-style-extended flexgroup-
constituent
```

| Vserver | Volume | Aggregate | State | Type | Size |
|-----------|-----------|-----------|--------|-------|---------|
| Available | Used% | | | | |
| ----- | ----- | ----- | ----- | ----- | ----- |
| ----- | ----- | | | | |
| vs1 | fg1__0001 | aggr3 | online | RW | 31.25GB |
| 12.97GB | 56% | | | | |
| vs1 | fg1__0002 | aggr1 | online | RW | 31.25GB |
| 12.98GB | 56% | | | | |
| vs1 | fg1__0003 | aggr1 | online | RW | 31.25GB |
| 13.00GB | 56% | | | | |
| vs1 | fg1__0004 | aggr3 | online | RW | 31.25GB |
| 12.88GB | 56% | | | | |
| vs1 | fg1__0005 | aggr1 | online | RW | 31.25GB |
| 13.00GB | 56% | | | | |
| vs1 | fg1__0006 | aggr3 | online | RW | 31.25GB |
| 12.97GB | 56% | | | | |
| vs1 | fg1__0007 | aggr1 | online | RW | 31.25GB |
| 13.01GB | 56% | | | | |
| vs1 | fg1__0008 | aggr1 | online | RW | 31.25GB |
| 13.01GB | 56% | | | | |
| vs1 | fg1__0009 | aggr3 | online | RW | 31.25GB |
| 12.88GB | 56% | | | | |
| vs1 | fg1__0010 | aggr1 | online | RW | 31.25GB |
| 13.01GB | 56% | | | | |
| vs1 | fg1__0011 | aggr3 | online | RW | 31.25GB |
| 12.97GB | 56% | | | | |
| vs1 | fg1__0012 | aggr1 | online | RW | 31.25GB |
| 13.01GB | 56% | | | | |
| vs1 | fg1__0013 | aggr3 | online | RW | 31.25GB |
| 12.95GB | 56% | | | | |
| vs1 | fg1__0014 | aggr3 | online | RW | 31.25GB |
| 12.97GB | 56% | | | | |
| vs1 | fg1__0015 | aggr3 | online | RW | 31.25GB |
| 12.88GB | 56% | | | | |
| vs1 | fg1__0016 | aggr1 | online | RW | 31.25GB |
| 13.01GB | 56% | | | | |

16 entries were displayed.

Se puede usar el espacio disponible y el porcentaje de espacio utilizado para supervisar el uso de espacio del volumen FlexGroup.

Aumente el tamaño de un volumen de FlexGroup

Puede aumentar el tamaño de un volumen de FlexGroup mediante la adición de más capacidad a los componentes existentes del volumen FlexGroup o la expansión del volumen de FlexGroup con nuevos componentes.

Lo que necesitará

Debe haber suficiente espacio disponible en los agregados.

Acerca de esta tarea

Si desea añadir más espacio, puede aumentar el tamaño colectivo del volumen FlexGroup. Al aumentar el tamaño de un volumen de FlexGroup, se redimensionan los componentes existentes del volumen de FlexGroup.

Si desea mejorar el rendimiento, puede ampliar el volumen de FlexGroup. Quizás sería conveniente expandir un volumen de FlexGroup y añadir nuevos componentes en las siguientes situaciones:

- Se han agregado nuevos nodos al clúster.
- Se han creado nuevos agregados en los nodos existentes.
- Los componentes existentes del volumen FlexGroup han alcanzado el tamaño máximo de FlexVol para el hardware y, por lo tanto, no se puede cambiar el tamaño del volumen FlexGroup.

En las versiones anteriores a ONTAP 9.3, no se deben expandir los volúmenes de FlexGroup después de establecer una relación de SnapMirror. Si expande el volumen FlexGroup de origen después de interrumpir la relación de SnapMirror en las versiones anteriores a ONTAP 9.3, debe volver a realizar una transferencia de referencia al volumen de FlexGroup de destino. A partir de ONTAP 9.3, puede ampliar los volúmenes de FlexGroup que se encuentren en una relación de SnapMirror.

Paso

1. Aumente el tamaño del volumen FlexGroup aumentando la capacidad o el rendimiento del volumen FlexGroup, según sea necesario:

| Si desea aumentar el... | Realice lo siguiente... |
|------------------------------------|--|
| La capacidad del volumen FlexGroup | <div>Cambie el tamaño de los componentes del volumen FlexGroup:</div> <div><pre>volume modify -vserver vserver_name -volume fg_name -size new_size</pre></div> |

| | |
|-------------------------------------|---|
| Rendimiento en el volumen FlexGroup | <p>Expanda el volumen de FlexGroup añadiendo nuevos componentes:</p> <pre>volume expand -vserver vservers_name -volume fg_name -aggr-list aggregate name,... [-aggr-list-multiplier constituents_per_aggr]</pre> <p>El valor predeterminado de <code>-aggr-list</code> <code>-multiplier</code> el parámetro es 1.</p> <p>Para ampliar un volumen de FlexGroup para FabricPool en ONTAP 9.5, todos los agregados nuevos que se usan deben ser FabricPool.</p> |
|-------------------------------------|---|

Siempre que sea posible, debe aumentar la capacidad de un volumen FlexGroup. Si debe expandir un volumen de FlexGroup, debe añadir componentes en los mismos múltiplos que los componentes del volumen de FlexGroup existente para garantizar un rendimiento constante. Por ejemplo, si el volumen FlexGroup existente tiene 16 componentes y ocho componentes por nodo, puede ampliar el volumen FlexGroup existente en 8 o 16 componentes.

Ejemplos

Ejemplo de aumento de la capacidad de los componentes existentes

El siguiente ejemplo muestra cómo añadir espacio de 20 TB a un volumen de FlexGroup Volx:

```
cluster1::> volume modify -vserver svm1 -volume volX -size +20TB
```

Si el volumen FlexGroup tiene 16 componentes, el espacio de cada componente aumenta en 1.25 TB.

Ejemplo de mejora del rendimiento mediante la adición de nuevos componentes

El siguiente ejemplo muestra cómo añadir dos componentes más al volumen Volx de FlexGroup:

```
cluster1::> volume expand -vserver vs1 -volume volX -aggr-list aggr1,aggr2
```

El tamaño de los nuevos constituyentes es el mismo que el de los componentes existentes.

Reduzca el tamaño de un volumen de FlexGroup

A partir de ONTAP 9.6, puede cambiar el tamaño de un volumen FlexGroup a un valor inferior al tamaño actual para liberar el espacio no utilizado del volumen. Cuando se reduce el tamaño de un volumen de FlexGroup, ONTAP cambia automáticamente el tamaño de todos los componentes de FlexGroup.

Paso

1. Compruebe el tamaño actual del volumen de FlexGroup: "Volume size -vserver *vserver_NAME* -volume *fg_NAME*"

2. Reduzca el tamaño del volumen de FlexGroup: `volume size -vserver vservice_name -volume fg_name new_size`

Al especificar el nuevo tamaño, se puede especificar un valor inferior al tamaño actual o un valor negativo mediante el signo menos (-) por el que se reduce el tamaño actual del volumen FlexGroup.



Si se habilita la reducción automática para el volumen (`volume autosize` comando), el valor mínimo de autosize se establece en el nuevo tamaño del volumen.

En el siguiente ejemplo, se muestra el tamaño de volumen actual del volumen de FlexGroup denominado Volx y se cambia el tamaño del volumen a 10 TB:

```
cluster1::> volume size -vserver svm1 -volume volX
(volume size)
vol size: FlexGroup volume 'svm1:volX' has size 15TB.

cluster1::> volume size -vserver svm1 -volume volX 10TB
(volume size)
vol size: FlexGroup volume 'svm1:volX' size set to 10TB.
```

En el siguiente ejemplo, se muestra el tamaño actual del volumen del volumen FlexGroup denominado Volx y se reduce el tamaño del volumen en 5 TB:

```
cluster1::> volume size -vserver svm1 -volume volX
(volume size)
vol size: FlexGroup volume 'svm1:volX' has size 15TB.

cluster1::> volume size -vserver svm1 -volume volX -5TB
(volume size)
vol size: FlexGroup volume 'svm1:volX' size set to 10TB.
```

Configure los volúmenes de FlexGroup para que aumenten y reduzcan su tamaño automáticamente

A partir de ONTAP 9.3, se pueden configurar los volúmenes de FlexGroup para que crezcan y se reduzcan automáticamente en función de la cantidad de espacio que necesiten actualmente.

Lo que necesitará

El volumen FlexGroup debe estar en línea.

Acerca de esta tarea

los volúmenes de FlexGroup se pueden ajustar de forma automática en dos modos:

- Aumente automáticamente el tamaño del volumen (`grow` modo)

El crecimiento automático ayuda a evitar que un volumen de FlexGroup se quede sin espacio si el

agregado puede suministrar más espacio. Puede configurar el tamaño máximo del volumen. El aumento se activa automáticamente en función de la cantidad de datos que se escriben en el volumen en relación con la cantidad actual de espacio usado y todos los umbrales establecidos.

De forma predeterminada, el tamaño máximo que puede crecer un volumen es del 120 % del tamaño en el cual se habilita el crecimiento automático. Si es necesario asegurarse de que el volumen pueda crecer para ser mayor que dicho, debe configurar el tamaño máximo para el volumen según corresponda.

- Reduzca el tamaño del volumen automáticamente (`grow_shrink` modo)

La reducción automática evita que un volumen sea mayor de lo necesario y libera espacio en el agregado para que lo usen otros volúmenes.

La autoreducción sólo se puede utilizar en combinación con el crecimiento automático para satisfacer las cambiantes demandas de espacio y no está disponible solo. Cuando se habilita la función de reducción automática, ONTAP gestiona automáticamente el comportamiento de reducción de un volumen para evitar un bucle interminable de acciones de autocrecimiento y autoreducción.

A medida que crece un volumen, es posible que el número máximo de archivos que puede contener se aumente automáticamente. Cuando un volumen se reduce, el número máximo de archivos que puede contener no cambia y un volumen no se puede reducir automáticamente por debajo del tamaño correspondiente a su número máximo actual de archivos. Por este motivo, es posible que no sea posible reducir de forma automática un volumen hasta su tamaño original.

Paso

1. Configure el volumen para que crezca y reduzca su tamaño automáticamente: `volume autosize -vserver vs_server_name -volume vol_name -mode [grow | grow_shrink]`

También se puede especificar el tamaño máximo, el tamaño mínimo y los umbrales para aumentar o reducir el volumen.

El siguiente comando habilita cambios de tamaño automáticos para un volumen denominado `fg1`. El volumen está configurado para crecer hasta alcanzar un tamaño máximo de 5 TB cuando está lleno al 70 %.

```
cluster1::> volume autosize -volume fg1 -mode grow -maximum-size 5TB
-grow-threshold-percent 70
vol autosize: volume "vs_src:fg1" autosize settings UPDATED.
```

Elimine directorios rápidamente en el clúster

A partir de ONTAP 9.8, puede utilizar la funcionalidad *FAST-directory delete* de baja latencia para eliminar directorios de recursos compartidos de clientes de Linux y Windows de forma asíncrona (es decir, en segundo plano). Los administradores de clústeres y SVM pueden realizar operaciones de eliminación asíncrona tanto en volúmenes FlexVol como en volúmenes FlexGroup.

Si utiliza una versión de ONTAP anterior a ONTAP 9.11.1, debe ser un administrador de clústeres o un administrador de SVM con el modo de privilegios avanzado.

A partir de ONTAP 9.11.1, un administrador de almacenamiento puede otorgar derechos en un volumen para que los clientes NFS y SMB puedan realizar operaciones de eliminación asíncrona. Para obtener más información, consulte ["Gestione los derechos de cliente para eliminar directorios rápidamente"](#).

A partir de ONTAP 9.8, puede utilizar la funcionalidad de eliminación rápida de directorios mediante la interfaz de línea de comandos de ONTAP. A partir de ONTAP 9.9.1, se puede usar esta funcionalidad con System Manager. Para obtener más información acerca de este proceso, consulte ["Adopte medidas correctivas basadas en análisis"](#).

System Manager

1. Haga clic en **almacenamiento > volúmenes** y, a continuación, en **Explorador**.

Al pasar el ratón sobre un archivo o carpeta, aparece la opción para eliminar. Sólo puede eliminar un objeto cada vez.



Cuando se eliminan directorios y archivos, los nuevos valores de capacidad de almacenamiento no se muestran inmediatamente.

CLI

Utilice la CLI para realizar una eliminación rápida de directorios

1. Entre en el modo de privilegio avanzado:

```
-privilege advance
```

2. Elimine directorios en un volumen FlexVol o FlexGroup:

```
volume file async-delete start -vserver vserver_name -volume volume_name  
-path file_path -throttle throttle
```

El valor mínimo del acelerador es 10, el máximo es 100,000 y el valor predeterminado es 5000.

En el ejemplo siguiente se elimina el directorio denominado d2, que se encuentra en el directorio denominado d1.

```
cluster::*>volume file async-delete start -vserver vs1 -volume voll  
-path d1/d2
```

3. Compruebe que el directorio se ha eliminado:

```
event log show
```

En el siguiente ejemplo se muestra el resultado del registro de eventos cuando el directorio se elimina correctamente.

```
cluster-cli::*> event log show  
Time                               Node                               Severity   Event  
-----  
MM/DD/YYYY 00:11:11  cluster-vsim      INFORMATIONAL  
asyncDelete.message.success: Async delete job on path d1/d2 of  
volume (MSID: 2162149232) was completed.
```

Cancelar un trabajo de eliminación de directorio

1. Entre en el modo de privilegio avanzado:

```
set -privilege advanced
```

2. Compruebe que la eliminación del directorio está en curso:

```
volume file async-delete show
```

Si se muestra la SVM, el volumen, el JobID y la ruta de acceso del directorio, puede cancelarla.

3. Cancelar el directorio de eliminación:

```
volume file async-delete cancel -vserver SVM_name -volume volume_name  
-jobid job_id
```

Gestione los derechos de cliente para eliminar directorios rápidamente

A partir de ONTAP 9.11.1, los administradores de almacenamiento pueden conceder derechos en un volumen para que los clientes de NFS y SMB puedan realizar personalmente operaciones de eliminación de directorios iniciales de baja latencia. Cuando se habilita la eliminación asíncrona en el clúster, los usuarios del cliente Linux pueden utilizar el `mv` Los usuarios del comando y del cliente Windows pueden utilizar el `rename` comando para eliminar rápidamente un directorio en el volumen especificado, moviéndolo a un directorio oculto que, de forma predeterminada, se denomina `.ontaptrashbin`.

Habilite la eliminación de directorio asíncrono de cliente

Pasos

1. En la CLI del clúster, introduzca el modo de privilegio avanzado: `-privilege advance`
2. Habilite la eliminación asíncrona del cliente y, si lo desea, proporcione un nombre alternativo para el directorio trashbin:

```
volume file async-delete client enable volume volname vserver vserverName  
trashbinname name
```

Ejemplo que utiliza el nombre de papelera predeterminado:

```
cluster1::*> volume file async-delete client enable -volume v1 -vserver  
vs0
```

```
Info: Async directory delete from the client has been enabled on volume  
"v1" in  
Vserver "vs0".
```

Ejemplo que especifica un nombre de papelera alternativo:

```
cluster1::*> volume file async-delete client enable -volume test
-trashbin .ntaptrash -vserver vs1

Success: Async directory delete from the client is enabled on volume
"v1" in
      Vserver "vs0".
```

3. Compruebe que la eliminación asíncrona del cliente esté habilitada:

```
volume file async-delete client show
```

Ejemplo:

```
cluster1::*> volume file async-delete client show

Vserver Volume      async-delete client TrashBinName
-----
vs1         vol1         Enabled         .ntaptrash
vs2         vol2         Disabled        -

2 entries were displayed.
```

Deshabilite la eliminación del directorio asíncrono del cliente

Pasos

1. En la interfaz de línea de comandos del clúster, deshabilite el directorio asronous del cliente delete:

```
volume file async-delete client disable volume volname vserver vserverName
```

Ejemplo:

```
cluster1::*> volume file async-delete client disable -volume vol1
-vserver vs1

      Success: Asynchronous directory delete client disabled
successfully on volume.
```

2. Compruebe que la eliminación asíncrona del cliente está deshabilitada:

```
volume file async-delete client show
```

Ejemplo:

```
cluster1::*> volume file async-delete client show
```

| Vserver | Volume | async-delete client | TrashBinName |
|---------|--------|---------------------|--------------|
| vs1 | vol1 | Disabled | - |
| vs2 | vol2 | Disabled | - |

```
2 entries were displayed.
```

Crear qtrees con volúmenes de FlexGroup

A partir de ONTAP 9.3, se pueden crear qtrees con los volúmenes de FlexGroup. Los qtrees permiten dividir los volúmenes de FlexGroup en segmentos más pequeños que puede gestionar individualmente.

Acerca de esta tarea

- Si desea revertir a ONTAP 9.2 o una versión anterior y si ha creado uno o más qtrees en el volumen FlexGroup o ha modificado los atributos (estilo de seguridad y bloqueos oportunistas SMB) del qtree predeterminado, Debe eliminar todos los qtrees no predeterminados y, a continuación, deshabilitar la funcionalidad Qtree de cada volumen de FlexGroup antes de revertir a ONTAP 9.2 o anterior.

["Deshabilite la funcionalidad Qtree en volúmenes FlexGroup antes de revertir"](#)

- Si el volumen de FlexGroup de origen tiene qtrees en una relación de SnapMirror, el clúster de destino debe ejecutar ONTAP 9.3 o una versión posterior (una versión del software ONTAP que admite qtrees).
- A partir de la versión 9.5 de ONTAP, se admiten las estadísticas de qtree para volúmenes FlexGroup.

Pasos

1. Cree un qtree en el volumen de FlexGroup: `volume qtree create -vserver vs1 -volume fg1 -qtree qtree1`

Puede especificar de forma opcional el estilo de seguridad, los bloqueos oportunistas SMB, los permisos de UNIX y la política de exportación del qtree.

```
cluster1::*> volume qtree create -vserver vs0 -volume fg1 -qtree qtree1  
-security-style mixed
```

Información relacionada

["Gestión de almacenamiento lógico"](#)

Utilice cuotas para volúmenes de FlexGroup

En ONTAP 9.4 y versiones anteriores, puede aplicar reglas de cuotas a volúmenes de FlexGroup solo con fines de creación de informes, pero no con el fin de aplicar límites de cuotas. A partir de ONTAP 9.5, es posible aplicar límites a las reglas de cuota que se aplican a los volúmenes de FlexGroup.

Acerca de esta tarea

- A partir de ONTAP 9.5, se pueden especificar cuotas de límite rígidas, suaves y de umbrales para volúmenes de FlexGroup.

Puede especificar estos límites para restringir la cantidad de espacio, el número de archivos que puede crear un usuario, un grupo o un qtree específico, o ambos. Los límites de cuota generan mensajes de advertencia en las siguientes situaciones:

- Cuando el uso supera un límite de software configurado, ONTAP emite un mensaje de advertencia, pero aún se permite más tráfico.

Si el uso vuelve a caer por debajo del límite de software configurado, se emite un mensaje de borrado.

- Cuando el uso supera un límite de umbral configurado, ONTAP emite un segundo mensaje de advertencia.

No se emite ningún mensaje administrativo completamente claro cuando el uso cae más tarde por debajo de un límite de umbral configurado.

- Si el uso alcanza un límite rígido configurado, ONTAP evita un mayor consumo de recursos al rechazar el tráfico.
- En ONTAP 9.5, no se pueden crear ni activar reglas de cuota en el volumen FlexGroup de destino de una relación de SnapMirror.
- Durante la inicialización de las cuotas, las cuotas no se aplican y no hay notificaciones de cuotas violadas tras la inicialización de las cuotas.


Para comprobar si se han violado las cuotas durante la inicialización de cuotas, puede utilizar la `volume quota report` comando.

Tipos y objetivos de cuota

Las cuotas tienen un tipo: Pueden ser usuario, grupo o árbol. Los destinos de cuota especifican el usuario, el grupo o el qtree para los que se aplican los límites de cuota.

En la siguiente tabla se enumeran los tipos de objetivos de cuota, los tipos de cuotas a los que está asociado cada destino de cuota y cómo se representa cada destino de cuota:

| Destino de cuota | Tipo de cuota | Cómo se representa el destino | Notas |
|------------------|------------------|--|--|
| usuario | cuota de usuario | Nombre de usuario UNIX UID Nombre de usuario de Windows en formato anterior a Windows 2000 SID de Windows | Pueden aplicarse cuotas de usuario para un volumen o un qtree concreto. |

| | | | |
|-------|--|--------------------------|---|
| grupo | cuota de grupo | Nombre UNIX GID de grupo | <p>Las cuotas de grupo se pueden aplicar para un volumen o un qtree específicos.</p> <div>  <p>ONTAP no aplica cuotas de grupos basadas en los ID de Windows.</p> </div> |
| qtree | cuota de árbol | nombre del qtree | Las cuotas de árbol se aplican a un volumen concreto y no afectan a los qtrees de otros volúmenes. |
| "" | cuota de usuario quotagroup cuota de árbol | Comillas dobles ("") | Un destino de cuota de "" indica una cuota <i>default</i> . Para cuotas predeterminadas, el tipo de cuota está determinado por el valor del campo de tipo. |

Comportamiento de los volúmenes FlexGroup cuando se superan los límites de cuota

A partir de ONTAP 9.5, se admiten límites de cuotas en los volúmenes FlexGroup. Existen algunas diferencias en la forma en que se aplican los límites de cuotas en un volumen de FlexGroup en comparación con un volumen de FlexVol.

Los volúmenes FlexGroup pueden mostrar los siguientes comportamientos cuando se superan los límites de cuota:

- Es posible que el espacio y el uso de archivos en un volumen FlexGroup alcancen hasta un 5 % más elevados que el límite duro configurado antes de que se aplique el límite de cuota rechazando más tráfico.

Para proporcionar el mejor rendimiento, ONTAP puede permitir que el consumo de espacio supere el límite duro configurado con un margen pequeño antes de que comience el cumplimiento de la cuota. Este consumo de espacio adicional no supera el 5 por ciento de los límites duros configurados, 1 GB o 65536 archivos, lo que sea más bajo.

- Una vez alcanzado el límite de cuota, si un usuario o administrador elimina algunos archivos o directorios de modo que el uso de la cuota esté ahora por debajo del límite, la operación de archivo que consume cuotas posterior podría reanudarse con un retraso (puede tardar hasta 5 segundos en reanudarse).
- Cuando el uso total de espacio y archivos de un volumen FlexGroup supera los límites de cuota configurados, es posible que se produzca un ligero retraso en el registro de un mensaje de registro de eventos.
- Puede que se produzcan errores de «sin espacio» si algunos componentes del volumen FlexGroup se

llenen, pero no se alcanzan los límites de las cuotas.

- Las operaciones, como cambiar el nombre de un archivo o un directorio, o mover archivos entre qtrees, en destinos de cuota, para los que se configuran los límites estrictos de cuotas, pueden tardar más en comparación con operaciones similares en volúmenes FlexVol.

Ejemplos de cumplimiento de cuotas para volúmenes FlexGroup

Puede utilizar los ejemplos para comprender cómo configurar cuotas con límites en ONTAP 9.5 y versiones posteriores.

Ejemplo 1: Aplicación de una regla de cuota con límites de disco

1. Debe crear una regla de política de cuota de tipo `user` con un límite alcanzable de discos duros y uno de discos duros.

```
cluster1::> volume quota policy rule create -vserver vs0 -policy-name
default -volume FG -type user -target "" -qtree "" -disk-limit 1T -soft
-disk-limit 800G
```

2. Puede ver la regla de política de cuota:

```
cluster1::> volume quota policy rule show -vserver vs0 -policy-name
default -volume FG
```

| Vserver: vs0 | | | Policy: default | | Volume: FG | | |
|--------------|--------|-------|-----------------|------------|-----------------|-------------|------------------|
| Type | Target | Qtree | User Mapping | Disk Limit | Soft Disk Limit | Files Limit | Soft Files Limit |
| Threshold | | | | | | | |
| ----- | ----- | ----- | ----- | ----- | ----- | ----- | ----- |
| ----- | | | | | | | |
| user | "" | "" | off | 1TB | 800GB | - | - |
| - | | | | | | | |

3. Para activar la nueva regla de cuota, se inicializan las cuotas en el volumen:

```
cluster1::> volume quota on -vserver vs0 -volume FG -foreground true
[Job 49] Job succeeded: Successful
```

4. Se puede ver la información de uso del disco y de uso de archivos del volumen FlexGroup mediante el informe de cuotas.

```
cluster1::> volume quota report -vserver vs0 -volume FG
Vserver: vs0
```

| Volume Specifier | Tree | Type | ID | ----Disk---- | | ----Files----- | | Quota |
|------------------|------|------|------|--------------|-------|----------------|-------|-------|
| | | | | Used | Limit | Used | Limit | |
| FG | | user | root | 50GB | - | 1 | - | |
| FG | | user | * | 800GB | 1TB | 0 | - | * |

2 entries were displayed.

Una vez alcanzado el límite del disco duro, el destino de la regla de política de cuota (usuario, en este caso) se bloquea para que no se escriban más datos en los archivos.

Ejemplo 2: Aplicación de una regla de cuota para varios usuarios

1. Debe crear una regla de política de cuota de tipo `user`, Donde se especifican varios usuarios en el destino de cuota (usuarios UNIX, usuarios SMB o una combinación de ambos) y donde la regla tiene tanto un límite de disco duro como un límite de disco duro alcanzable.

```
cluster1::> quota policy rule create -vserver vs0 -policy-name default
-volume FG -type user -target "rdavis,ABCCORP\RobertDavis" -qtree ""
-disk-limit 1TB -soft-disk-limit 800GB
```

2. Puede ver la regla de política de cuota:

```
cluster1::> quota policy rule show -vserver vs0 -policy-name default
-volume FG
```

| Vserver: vs0 | | | Policy: default | | | Volume: FG | |
|--------------|------------------------------|-------|-----------------|------------|-----------------|-------------|------------------|
| Type | Target | Qtree | User Mapping | Disk Limit | Soft Disk Limit | Files Limit | Soft Files Limit |
| user | "rdavis,ABCCORP\RobertDavis" | "" | off | 1TB | 800GB | - | - |

3. Para activar la nueva regla de cuota, se inicializan las cuotas en el volumen:


```
cluster1::> volume quota on -vserver vs0 -volume FG -foreground true
[Job 49] Job succeeded: Successful
```

4. Puede comprobar que el estado de la cuota está activo:

```
cluster1::> volume quota show -vserver vs0 -volume FG
Vserver Name: vs0
Volume Name: FG
Quota State: on
Scan Status: -
Logging Messages: on
Logging Interval: 1h
Sub Quota Status: none
Last Quota Error Message: -
Collection of Quota Errors: -
```

5. Se puede ver la información de uso del disco y de uso de archivos del volumen FlexGroup mediante el informe de cuotas.

```
cluster1::> quota report -vserver vs0 -volume FG
Vserver: vs0
```

| Volume | Tree | Type | ID | -----Disk----- | -----Files----- | Quota | |
|----------------------------|-------|-------|----------------------------|----------------|-----------------|-------|-------|
| Specifier | | | | Used | Limit | Used | Limit |
| ----- | ----- | ----- | ----- | ----- | ----- | ----- | ----- |
| FG | | user | rdavis,ABCCORP\RobertDavis | 0B | 1TB | 0 | - |
| rdavis,ABCCORP\RobertDavis | | | | | | | |

El límite de cuota se comparte entre todos los usuarios enumerados en el destino de cuota.

Una vez alcanzado el límite del disco duro, los usuarios incluidos en el destino de cuota se bloquean de escribir más datos en los archivos.

Ejemplo 3: Imposición de la cuota con asignación de usuarios activada

1. Debe crear una regla de política de cuota de tipo `user`, Especifique un usuario de UNIX o un usuario de Windows como destino de cuota con `user-mapping` establezca en ``on`` y cree la regla con un límite de disco duro y un límite de disco duro alcanzable.

La asignación entre los usuarios de UNIX y Windows debe configurarse anteriormente mediante el `vserver name-mapping create` comando.

```
cluster1::> quota policy rule create -vserver vs0 -policy-name default
-volume FG -type user -target rdavis -qtree "" -disk-limit 1TB -soft
-disk-limit 800GB -user-mapping on
```

2. Puede ver la regla de política de cuota:

```
cluster1::> quota policy rule show -vserver vs0 -policy-name default
-volume FG
```

| | | | | | | | |
|--------------|--------|-------|-----------------|------------|-----------------|-------------|------------------|
| Vserver: vs0 | | | Policy: default | | Volume: FG | | |
| Type | Target | Qtree | User Mapping | Disk Limit | Soft Disk Limit | Files Limit | Soft Files Limit |
| Threshold | | | | | | | |
| ----- | ----- | ----- | ----- | ----- | ----- | ----- | ----- |
| ----- | | | | | | | |
| user | rdavis | "" | on | 1TB | 800GB | - | - |
| - | | | | | | | |

3. Para activar la nueva regla de cuota, se inicializan las cuotas en el volumen:

```
cluster1::> volume quota on -vserver vs0 -volume FG -foreground true
[Job 49] Job succeeded: Successful
```

4. Puede comprobar que el estado de la cuota está activo:

```
cluster1::> volume quota show -vserver vs0 -volume FG
Vserver Name: vs0
Volume Name: FG
Quota State: on
Scan Status: -
Logging Messages: on
Logging Interval: 1h
Sub Quota Status: none
Last Quota Error Message: -
Collection of Quota Errors: -
```

5. Se puede ver la información de uso del disco y de uso de archivos del volumen FlexGroup mediante el informe de cuotas.

```
cluster1::> quota report -vserver vs0 -volume FG
Vserver: vs0
```

| Volume | Tree | Type | ID | ----Disk---- | | ----Files----- | | Quota |
|--------|------|------|----------------------------|--------------|-------|----------------|-------|-------|
| | | | | Used | Limit | Used | Limit | |
| FG | | user | rdavis,ABCCORP\RobertDavis | 0B | 1TB | 0 | - | |

El límite de cuota se comparte entre el usuario que aparece en el destino de cuota y su usuario de Windows o UNIX correspondiente.

Una vez alcanzado el límite del disco duro, tanto el usuario que figura en el destino de cuota como su usuario de Windows o UNIX correspondiente se bloquean de escribir más datos en los archivos.

Ejemplo 4: Verificación del tamaño de qtree cuando se habilita la cuota

1. Debe crear una regla de política de cuota de tipo tree y donde la regla tiene un límite que puede alcanzarse del disco duro y del disco duro.

```
cluster1::> quota policy rule create -vserver vs0 -policy-name default
-volume FG -type tree -target tree_4118314302 -qtree "" -disk-limit 48GB
-soft-disk-limit 30GB
```

2. Puede ver la regla de política de cuota:

```
cluster1::> quota policy rule show -vserver vs0
```

| Vserver: vs0 | | | Policy: default | | | Volume: FG | |
|--------------|-----------------|-------|-----------------|------------|-----------------|-------------|------------------|
| Type | Target | Qtree | User Mapping | Disk Limit | Soft Disk Limit | Files Limit | Soft Files Limit |
| tree | tree_4118314302 | "" | - | 48GB | - | 20 | - |

3. Para activar la nueva regla de cuota, se inicializan las cuotas en el volumen:

```
cluster1::> volume quota on -vserver vs0 -volume FG -foreground true
[Job 49] Job succeeded: Successful
```

- a. Se puede ver la información de uso del disco y de uso de archivos del volumen FlexGroup mediante el informe de cuotas.

```
cluster1:> quota report -vserver vs0
Vserver: vs0
----Disk---- ----Files----- Quota
Volume Tree Type ID Used Limit Used Limit Specifier
-----
FG tree_4118314302 tree 1 30.35GB 48GB 14 20 tree_4118314302
```

El límite de cuota se comparte entre el usuario que aparece en el destino de cuota y su usuario de Windows o UNIX correspondiente.

4. Desde un cliente NFS, utilice `df` comando para ver el uso total del espacio, el espacio disponible y el espacio utilizado.

```
scsps0472342001# df -m /t/10.53.2.189/FG-3/tree_4118314302
Filesystem 1M-blocks Used Available Use% Mounted on
10.53.2.189/FG-3 49152 31078 18074 63% /t/10.53.2.189/FG-3
```

Con el límite duro, el uso del espacio se calcula a partir de un cliente NFS de la siguiente forma:

- Uso total del espacio = límite duro para el árbol
 - Espacio libre = límite estricto menos el uso de espacio para qtrees
- Sin limitación estricta, el uso del espacio se calcula a partir de un cliente NFS de la siguiente forma:
- Uso del espacio = uso de cuota
 - Espacio total = suma de uso de cuota y espacio libre físico en el volumen

5. En el recurso compartido de SMB, utilice el Explorador de Windows para ver el uso de espacio total, el espacio disponible y el espacio utilizado.

En un recurso compartido de SMB, debe tener en cuenta las siguientes consideraciones para calcular el uso del espacio:

- Se tiene en cuenta el límite duro de cuota de usuario para el usuario y el grupo para calcular el espacio disponible total.
- El valor mínimo entre el espacio libre de la regla de cuota de árbol, la regla de cuota de usuario y la regla de cuota de grupo se considera el espacio libre para el recurso compartido SMB.
- El uso de espacio total es variable para SMB y depende del límite rígido que corresponde al espacio libre mínimo entre el árbol, el usuario y el grupo.

Aplique reglas y límites en el volumen de FlexGroups

Pasos

1. Crear reglas de cuota para destinos: `volume quota policy rule create -vserver vs0 -policy-name quota_policy_of_the_rule -volume flexgroup_vol -type {tree|user|group} -target target_for_rule -qtree qtree_name [-disk-limit`

```
hard_disk_limit_size] [-file-limit hard_limit_number_of_files] [-threshold threshold_disk_limit_size] [-soft-disk-limit soft_disk_limit_size] [-soft-file-limit soft_limit_number_of_files]
```

- En ONTAP 9.2 y ONTAP 9.1, el tipo de destino de cuota puede ser solo `user` o `group`. Para volúmenes de FlexGroup.

No se admite el tipo de cuota de árbol para volúmenes FlexGroup en ONTAP 9.2 y ONTAP 9.1.

- En ONTAP 9.3 y versiones posteriores, el tipo de destino de cuota puede ser `user`, `group`, o `tree`. Para volúmenes de FlexGroup.
- Como destino, no se admite una ruta de acceso cuando se crean reglas de cuota para los volúmenes FlexGroup.
- A partir de ONTAP 9.5, puede especificar el límite de disco duro, el límite de archivos duros, el límite de discos duros, el límite de archivos soft y las cuotas de límite de umbral para los volúmenes de FlexGroup.

En ONTAP 9.4 y versiones anteriores, no se puede especificar el límite de discos, el límite de archivos, el umbral del límite de discos, el límite de discos duros o el límite de archivos soft al crear reglas de cuota para los volúmenes de FlexGroup.

En el ejemplo siguiente se muestra una regla de cuota predeterminada que se crea para el tipo de destino de usuario:

```
cluster1::> volume quota policy rule create -vserver vs0 -policy-name quota_policy_vs0_1 -volume fg1 -type user -target "" -qtree ""
```

En el siguiente ejemplo, se muestra una regla de cuota de árbol que se crea para el qtree denominado qtre1:

```
cluster1::> volume quota policy rule create -policy-name default -vserver vs0 -volume fg1 -type tree -target "qtree1"
```

1. Active las cuotas para el volumen de FlexGroup especificado: `volume quota on -vserver svm_name -volume flexgroup_vol -foreground true`

```
cluster1::> volume quota on -vserver vs0 -volume fg1 -foreground true
```

1. Supervisar el estado de inicialización de la cuota: `volume quota show -vserver svm_name`

Los volúmenes FlexGroup pueden mostrar el `mixed` estado, que indica que todos los volúmenes constituyentes aún no están en el mismo estado.

```
cluster1::> volume quota show -vserver vs0
```

| Vserver | Volume | State | Scan Status |
|---------|--------|--------------|-------------|
| vs0 | fg1 | initializing | 95% |
| vs0 | vol1 | off | - |

2 entries were displayed.

1. Vea el informe de cuotas del volumen FlexGroup con cuotas activas: `volume quota report -vserver svm_name -volume flexgroup_vol`

No puede especificar una ruta con el `volume quota report` Comando para volúmenes de FlexGroup.

En el siguiente ejemplo, se muestra la cuota de usuario para el volumen fg1 de FlexGroup:

```
cluster1::> volume quota report -vserver vs0 -volume fg1
```

Vserver: vs0

| Quota | | | | ----Disk---- | | ----Files---- | |
|-----------|------|------|------|--------------|-------|---------------|-------|
| Volume | Tree | Type | ID | Used | Limit | Used | Limit |
| Specifier | | | | | | | |
| fg1 | | user | * | 0B | - | 0 | - * |
| fg1 | | user | root | 1GB | - | 1 | - * |

2 entries were displayed.

En el siguiente ejemplo se muestra la cuota de árbol para el volumen FlexGroup fg1:

```
cluster1::> volume quota report -vserver vs0 -volume fg1
```

Vserver: vs0

| Quota | | | | ----Disk---- | | ----Files---- | | Quota |
|-----------|--------|------|----|--------------|-------|---------------|-------|-------|
| Volume | Tree | Type | ID | Used | Limit | Used | Limit | |
| Specifier | | | | | | | | |
| fg1 | qtree1 | tree | 1 | 68KB | - | 18 | - | |
| fg1 | | tree | * | 0B | - | 0 | - * | |

2 entries were displayed.

Resultados

Las reglas y los límites de las cuotas se aplican en el volumen de FlexGroups.

El uso puede alcanzar hasta un 5 % mayor que un límite rígido configurado antes de que ONTAP aplique la cuota rechazando más tráfico.

Información relacionada

["Comandos de ONTAP 9"](#)

Posibilite la eficiencia del almacenamiento en un volumen de FlexGroup

Puede ejecutar la deduplicación y la compresión de datos de forma conjunta o independiente en un volumen FlexGroup para obtener un ahorro de espacio óptimo.

Lo que necesitará

El volumen FlexGroup debe estar en línea.

Pasos

1. Habilitar la eficiencia del almacenamiento en el volumen de FlexGroup: `volume efficiency on -vserver svm_name -volume volume_name`

Se habilitan las operaciones de eficiencia de almacenamiento en todos los componentes del volumen FlexGroup.

Si un volumen FlexGroup se amplía después de activar la eficiencia del almacenamiento en el volumen, la eficiencia del almacenamiento se habilita automáticamente en los nuevos componentes.

2. Habilite la operación de eficiencia del almacenamiento necesaria en el volumen de FlexGroup mediante el `volume efficiency modify` comando.

Puede habilitar la deduplicación inline, la deduplicación de postprocesamiento, la compresión inline y la compresión posterior al procesamiento en volúmenes de FlexGroup. También puede establecer el tipo de compresión (secundario o adaptable) y especificar una programación o una política de eficiencia para el volumen FlexGroup.

3. Si no utiliza programaciones ni políticas de eficiencia para ejecutar las operaciones de eficiencia del almacenamiento, inicie la operación de eficiencia: `volume efficiency start -vserver svm_name -volume volume_name`

Si se activan la deduplicación y la compresión de datos en un volumen, la compresión de datos se ejecuta inicialmente, seguida por la deduplicación. Este comando falla si ya hay alguna operación de eficiencia activa en el volumen de FlexGroup.

4. Compruebe las operaciones de eficiencia que están habilitadas en el volumen de FlexGroup: `volume efficiency show -vserver svm_name -volume volume_name`

```
cluster1::> volume efficiency show -vserver vs1 -volume fg1
Vserver Name: vs1
Volume Name: fg1
Volume Path: /vol/fg1
State: Enabled
Status: Idle
Progress: Idle for 17:07:25
Type: Regular
Schedule: sun-sat@0

...

Compression: true
Inline Compression: true
Incompressible Data Detection: false
Constituent Volume: false
Compression Quick Check File Size: 524288000
Inline Dedupe: true
Data Compaction: false
```

Protección de volúmenes de FlexGroup mediante copias de Snapshot

Es posible crear políticas de Snapshot que gestionen automáticamente la creación de copias de Snapshot, o bien puede crear manualmente copias de Snapshot para los volúmenes de FlexGroup. Se crea una copia snapshot válida para un volumen FlexGroup solo después de que ONTAP pueda crear con éxito una copia snapshot para cada componente del volumen FlexGroup.

Acerca de esta tarea

- Si tiene varios volúmenes de FlexGroup asociados con una política de Snapshot, debe asegurarse de que las programaciones de los volúmenes de FlexGroup no se superpongan.
- A partir de ONTAP 9.8, el número máximo de copias snapshot admitidas en un volumen FlexGroup es 1023.





A partir de ONTAP 9.8, el `volume snapshot show` El comando para volúmenes de FlexGroup informa del tamaño de la copia de Snapshot usando bloques lógicos, en lugar de calcular los bloques de propiedad más jóvenes. Este nuevo método de cálculo de tamaño puede hacer que el tamaño de la copia snapshot sea mayor que los cálculos de versiones anteriores de ONTAP.

Pasos

1. Cree una política de Snapshot o cree manualmente una copia Snapshot:

| | |
|----------------------|----------------------------|
| Si desea crear un... | Introduzca este comando... |
|----------------------|----------------------------|

| | |
|----------------------------|--|
| Política de Snapshot | <p>volume snapshot policy create</p> <div>  <p>Las programaciones asociadas con la política de Snapshot de un volumen FlexGroup deben tener un intervalo mayor de 30 minutos.</p> </div> <p>Cuando se crea un volumen de FlexGroup, el default La política de Snapshot se aplica al volumen de FlexGroup.</p> |
| Copia Snapshot manualmente | <p>volume snapshot create</p> <div>  <p>Después de crear una copia Snapshot para un volumen FlexGroup, no puede modificar los atributos de la copia Snapshot. Si desea modificar los atributos, debe eliminar y volver a crear la copia Snapshot.</p> </div> |

El acceso de cliente al volumen FlexGroup se detiene brevemente cuando se crea una copia Snapshot.

1. Compruebe que se haya creado una copia Snapshot válida para el volumen FlexGroup: `volume snapshot show -volume volume_name -fields state`

```
cluster1::> volume snapshot show -volume fg -fields state
vserver volume snapshot                state
-----
fg_vs    fg      hourly.2016-08-23_0505 valid
```

2. Vea las copias Snapshot para los componentes del volumen FlexGroup: `volume snapshot show -is -constituent true`

```
cluster1::> volume snapshot show -is-constituent true
```

| ---Blocks--- | | | | |
|--------------|----------|------------------------|-------|--------|
| Vserver | Volume | Snapshot | Size | Total% |
| Used% | | | | |
| ----- | ----- | ----- | ----- | ----- |
| fg_vs | fg__0001 | hourly.2016-08-23_0505 | 72MB | 0% |
| 27% | | | | |
| | fg__0002 | hourly.2016-08-23_0505 | 72MB | 0% |
| 27% | | | | |
| | fg__0003 | hourly.2016-08-23_0505 | 72MB | 0% |
| 27% | | | | |
| ... | | | | |
| | fg__0016 | hourly.2016-08-23_0505 | 72MB | 0% |
| 27% | | | | |

Mover los componentes de un volumen FlexGroup

Puede mover los componentes de un volumen FlexGroup de un agregado a otro para equilibrar la carga cuando ciertos componentes experimentan más tráfico. El movimiento de componentes también ayuda a liberar espacio en un agregado para cambiar el tamaño de los componentes existentes.

Lo que necesitará

Para mover un componente de volumen FlexGroup que está en una relación de SnapMirror, debe haber inicializado la relación de SnapMirror.

Acerca de esta tarea

No se puede realizar una operación de movimiento de volúmenes mientras los componentes del volumen FlexGroup se están expandiendo.

Pasos

1. Identifique el componente del volumen FlexGroup que desea mover:

```
volume show -vserver svm_name -is-constituent true
```

```
cluster1::> volume show -vserver vs2 -is-constituent true
```

| Vserver | Volume | Aggregate | State | Type | Size |
|-----------|-----------|-----------|--------|------|-------|
| Available | Used% | | | | |
| vs2 | fg1 | - | online | RW | 400TB |
| 15.12TB | 62% | | | | |
| vs2 | fg1__0001 | aggr1 | online | RW | 25TB |
| 8.12MB | 59% | | | | |
| vs2 | fg1__0002 | aggr2 | online | RW | 25TB |
| 2.50TB | 90% | | | | |
| ... | | | | | |

2. Identifique un agregado al que puede mover el componente de volumen FlexGroup:

```
volume move target-aggr show -vserver svm_name -volume vol_constituent_name
```

El espacio disponible en el agregado que seleccione debe ser mayor que el tamaño del componente del volumen FlexGroup que se está moviendo.

```
cluster1::> volume move target-aggr show -vserver vs2 -volume fg1_0002
```

| Aggregate Name | Available Size | Storage Type |
|---------------------------|----------------|--------------|
| aggr2 | 467.9TB | hdd |
| node12a_aggr3 | 100.34TB | hdd |
| node12a_aggr2 | 100.36TB | hdd |
| node12a_aggr1 | 100.36TB | hdd |
| node12a_aggr4 | 100.36TB | hdd |
| 5 entries were displayed. | | |

3. Compruebe que el componente del volumen de FlexGroup se puede mover al agregado previsto:

```
volume move start -vserver svm_name -volume vol_constituent_name -destination  
-aggregate aggr_name -perform-validation-only true
```

```
cluster1::> volume move start -vserver vs2 -volume fg1_0002 -destination  
-aggregate node12a_aggr3 -perform-validation-only true  
Validation succeeded.
```

4. Mueva el componente de volumen de FlexGroup:

```
volume move start -vserver svm_name -volume vol_constituent_name -destination  
-aggregate aggr_name [-allow-mixed-aggr-types {true|false}]
```

La operación de movimiento de volúmenes se ejecuta como un proceso en segundo plano.

A partir de ONTAP 9.5, puede mover los componentes de volúmenes de FlexGroup de un pool de estructura a un pool que no sea de estructura, o viceversa configurando el `-allow-mixed-aggr-types` parámetro a `true`. De forma predeterminada, la `-allow-mixed-aggr-types` opción establecida en `false`.



No puede utilizar el `volume move` Comando para habilitar el cifrado en volúmenes de FlexGroup.

```
cluster1::> volume move start -vserver vs2 -volume fg1_002 -destination
-aggregate node12a_aggr3
```



Si la operación de movimiento de volúmenes falla debido a una operación SnapMirror activa, debe anular la operación SnapMirror mediante la `snapmirror abort -h` comando. En algunos casos, la operación de anulación de SnapMirror también puede fallar. En tales situaciones, se debe anular la operación de movimiento de volúmenes y volver a intentarlo más tarde.

5. Compruebe el estado de la operación de movimiento de volúmenes:

```
volume move show -volume vol_constituent_name
```

El siguiente ejemplo muestra el estado de un componente de FlexGroup que completó la fase de replicación y se encuentra en la fase de transición de la operación de movimiento de volúmenes:

```
cluster1::> volume move show -volume fg1_002
Vserver   Volume      State      Move Phase  Percent-Complete Time-To-Complete
-----
vs2       fg1_002     healthy   cutover     -               -
```

Utilice agregados en FabricPool para volúmenes de FlexGroup existentes

A partir de ONTAP 9.5, FabricPool es compatible con FlexGroup Volumes. Si desea usar agregados en FabricPool para los volúmenes de FlexGroup existentes, puede convertir los agregados en los que reside el volumen de FlexGroup en agregados en FabricPool o migrar los componentes de volumen de FlexGroup a agregados en FabricPool.

Lo que necesitará

- El volumen FlexGroup debe tener la garantía de espacio establecida en `none`.
- Si desea convertir los agregados en los que reside el volumen de FlexGroup en agregados en FabricPool, los agregados deben usar todos los discos SSD.

Acerca de esta tarea

Si un volumen de FlexGroup existente reside en agregados que no forman parte de SSD, debe migrar los componentes del volumen FlexGroup a agregados en FabricPool.

Opciones

- Para convertir los agregados en los que el volumen de FlexGroup reside en agregados en FabricPool, realice los siguientes pasos:

- a. Establezca la política de organización en niveles en el volumen de FlexGroup existente: `volume modify -volume flexgroup_name -tiering-policy [auto|snapshot|none|backup]`

```
cluster-2::> volume modify -volume fg1 -tiering-policy auto
```

- b. Identifique los agregados en los que reside el volumen de FlexGroup: `volume show -volume flexgroup_name -fields aggr-list`

```
cluster-2::> volume show -volume fg1 -fields aggr-list
vserver volume aggr-list
-----
vs1      fg1      aggr1,aggr3
```

- c. Adjunte un almacén de objetos a cada agregado que aparece en la lista de agregados: `storage aggregate object-store attach -aggregate aggregate name -name object-store-name -allow-flexgroup true`

Debe asociar todos los agregados a un almacén de objetos.

```
cluster-2::> storage aggregate object-store attach -aggregate aggr1
-object-store-name Amazon01B1
```

- Para migrar los componentes de volumen de FlexGroup a agregados en FabricPool, realice los pasos siguientes:

- a. Establezca la política de organización en niveles en el volumen de FlexGroup existente: `volume modify -volume flexgroup_name -tiering-policy [auto|snapshot|none|backup]`

```
cluster-2::> volume modify -volume fg1 -tiering-policy auto
```

- b. Mueva cada componente del volumen FlexGroup a un agregado de FabricPool en el mismo clúster: `volume move start -volume constituent-volume -destination-aggregate FabricPool_aggregate -allow-mixed-aggr-types true`

Debe mover todos los componentes de volúmenes de FlexGroup a agregados en FabricPool (en caso de que los componentes de volumen FlexGroup estén en tipos de agregado mixtos) y garantizar que todos los componentes se equilibren entre los nodos del clúster.

```
cluster-2::> volume move start -volume fg1_001 -destination-aggregate
FP_aggr1 -allow-mixed-aggr-types true
```

Reequilibre los volúmenes FlexGroup

A partir de ONTAP 9.12.1, puede reequilibrar volúmenes de FlexGroup moviendo archivos de forma no disruptiva de un componente en FlexGroup a otro componente.

El reequilibrio de FlexGroup ayuda a redistribuir la capacidad cuando los desequilibrios se desarrollan a lo largo del tiempo gracias a la adición de nuevos ficheros y al crecimiento de ficheros. Después de iniciar manualmente la operación de reequilibrio, ONTAP selecciona los archivos y los mueve de forma automática y sin interrupciones.



Debe tener en cuenta que el reequilibrio de FlexGroup degrada el rendimiento del sistema cuando se mueve una gran cantidad de archivos como parte de un solo evento de reequilibrio o de varios eventos de reequilibrio debido a la creación de inodos de varias partes. Cada archivo movido como parte de un evento de reequilibrio tiene 2 inodos de varias partes asociados a ese archivo. Cuanto mayor sea el número de archivos con inodos de varias partes como porcentaje del número total de archivos en un FlexGroup, mayor será el impacto en el rendimiento. Ciertos casos de uso, como una conversión de FlexVol a FlexGroup, pueden dar lugar a una cantidad significativa de creación de inodo de varias partes.

El reequilibrio solo está disponible cuando todos los nodos del clúster ejecutan ONTAP 9.12.1 o versiones posteriores. Debe habilitar la funcionalidad de datos granular en cualquier volumen de FlexGroup que ejecute la operación de reequilibrio. Una vez habilitada esa funcionalidad, no podrá revertir a ONTAP 9.11.1 y versiones anteriores a menos que elimine este volumen o restaure desde una copia Snapshot que se creó antes de habilitar la configuración.

A partir de ONTAP 9.14.1, ONTAP introduce un algoritmo para mover archivos de forma proactiva y sin interrupciones en volúmenes que tienen habilitados datos granulares sin interacción del usuario. El algoritmo funciona en escenarios muy específicos y específicos para aliviar los cuellos de botella de rendimiento. Los escenarios en los que este algoritmo puede actuar incluyen una carga de escritura muy pesada en un conjunto concreto de archivos en un nodo del cluster o un archivo en crecimiento continuo en un directorio principal muy activo.

Consideraciones sobre el reequilibrio de FlexGroup

Debe saber cómo funciona el reequilibrio de FlexGroup y cómo interactúa con otras funciones de ONTAP.

- Conversión de FlexVol a FlexGroup

Se recomienda utilizar el reequilibrio automático de FlexGroup después de una conversión de FlexVol a FlexGroup. En su lugar, puede utilizar la función de movimiento de archivos retroactivo disruptiva disponible en ONTAP 9.10.1 y versiones posteriores, para introducir la `volume rebalance file-move` comando. Para obtener información sobre la sintaxis de comandos, consulte `volume rebalance file-move start` página de manual.

El reequilibrio con la función de reequilibrio automático de FlexGroup puede degradar el rendimiento al mover un gran número de archivos, como cuando se realiza una conversión de FlexVol a FlexGroup y, además, del 50 al 85 % de los datos del volumen FlexVol se mueven a un nuevo componente.

- Tamaño de archivo mínimo y máximo

La selección de archivos para el reequilibrado automático se basa en bloques guardados. El tamaño

mínimo de archivo considerado para el reequilibrio es de 100 MB por defecto (se puede configurar tan bajo como 20 MB utilizando el parámetro min-file-size que se muestra a continuación) y el tamaño máximo de archivo es de 100 GB.

- De las copias snapshot

Puede configurar el reequilibrado de FlexGroup para que solo tenga en cuenta los archivos que se van a mover, que no están presentes actualmente en ninguna copia snapshot. Cuando se inicia el reequilibrio, se muestra una notificación si se programa una operación de copia Snapshot en cualquier momento durante una operación de reequilibrio.

Las copias Snapshot están restringidas si un archivo se mueve y se está encuadrando en el destino. No se permite una operación de restauración de copias snapshot mientras se está reequilibrando archivos.

- Operaciones de SnapMirror

El reequilibrio de FlexGroup se debe realizar entre las operaciones programadas de SnapMirror. Se puede producir un error en una operación de SnapMirror si se va a reubicar un archivo antes de que comience una operación de SnapMirror si ese movimiento de archivos no se completa en el período de reintento de SnapMirror de 24 minutos. No se producirá un error en cualquier reubicación de archivos nueva que comience después de que se inició una transferencia de SnapMirror.

- Eficiencia del almacenamiento de compresión basada en archivos

Gracias a la eficiencia del almacenamiento de compresión basada en archivos, el archivo se descomprime antes de trasladarse al destino, por lo que se pierde el ahorro en la compresión. El ahorro de la compresión se recupera después de que se ejecuta un escáner en segundo plano iniciado manualmente en el volumen FlexGroup después del reequilibrio. Sin embargo, si algún archivo está asociado con una copia snapshot en cualquier volumen, el archivo se ignorará para la compresión.

- Deduplicación

La transferencia de archivos deduplicados puede provocar un aumento en el uso general del volumen FlexGroup. Durante el reequilibrio de archivos, solo se mueven bloques únicos al destino, liberando esa capacidad en el origen. Los bloques compartidos permanecen en el origen y se copian en el destino. Aunque logra el objetivo de reducir la capacidad utilizada en un componente de origen casi completo, también puede incrementar el uso general del volumen FlexGroup debido a las copias de bloques compartidos en los nuevos destinos. Esto también es posible cuando se mueven archivos que forman parte de una copia snapshot. No se reconoce completamente el ahorro de espacio hasta que se recicla la programación de la copia snapshot y ya no hay copias de los archivos en las copias snapshot.

- Volúmenes FlexClone

Si se está reequilibrando un archivo durante la creación de un volumen FlexClone, no se realizará el reequilibrado en el volumen FlexClone. El reequilibrio en el volumen FlexClone se debe realizar una vez que se haya creado.

- Movimiento de archivos

Cuando se mueve un archivo durante una operación de reequilibrio de FlexGroup, el tamaño de archivo se informa como parte de la contabilidad de cuotas tanto en los componentes de origen como de destino. Una vez completado el desplazamiento, la contabilidad de cuota vuelve a normal y el tamaño del archivo sólo se informa en el nuevo destino.

- Protección autónoma de ransomware

A partir de ONTAP 9.13.1, la protección autónoma frente a ransomware es compatible durante operaciones de reequilibrio disruptivas y no disruptivas.

- Volúmenes de almacenamiento de objetos

No se admite el reequilibrio de capacidad del volumen en los volúmenes de almacenes de objetos, como los bloques S3.

Habilite el reequilibrio de FlexGroup

A partir de ONTAP 9.12.1, se puede habilitar el reequilibrado automático de volúmenes FlexGroup no disruptivo para redistribuir archivos entre componentes de FlexGroup.

A partir de ONTAP 9.13.1, puede programar una sola operación de reequilibrio de FlexGroup para que comience en una fecha y hora del futuro.

Antes de empezar


Debe haber habilitado el `granular-data` Opción en el volumen FlexGroup antes de habilitar el reequilibrio de FlexGroup. Puede habilitarla mediante uno de los siguientes métodos:

- Cuando se crea un volumen FlexGroup con el `volume create` comando
- Mediante la modificación de un volumen de FlexGroup existente para habilitar el ajuste mediante la `volume modify` comando
- Configuración automática cuando se inicia el reequilibrio de FlexGroup mediante el `volume rebalance` comando

Pasos

Puede gestionar el reequilibrado de FlexGroup mediante System Manager de ONTAP o la CLI de ONTAP.

System Manager

1. Navegue hasta **almacenamiento > volúmenes** y localice el volumen FlexGroup para reequilibrar.
2. Seleccione  para ver los detalles del volumen.
3. Seleccione **Reequilibrio**.
4. En la ventana **volumen de reequilibrio**, cambie la configuración predeterminada según sea necesario.
5. Para programar la operación de reequilibrio, seleccione **Reequilibrio más tarde** e introduzca la fecha y la hora.

CLI

1. Iniciar reequilibrio automático: `volume rebalance start -vserver SVM_name -volume volume_name`

Opcionalmente, puede especificar las siguientes opciones:

`[-max-Runtime] <time interval>` Tiempo de ejecución máximo

`[-max-threshold <percent>]` Umbral de desequilibrio máximo por componente

`[-min-threshold <percent>]` Umbral de desequilibrio mínimo por componente

`[-max-file-moves <integer>]` Máximo de Movimientos Simultáneos de Archivos por Componente

`[-min-file-size {<integer>[KB|MB|GB|TB|PB]}]` Tamaño mínimo de archivo

`[-START-Time <mm/dd/yyyy-00:00:00>]` Fecha y hora de inicio de reequilibrio de horario

`[-exclude-snapshots {true|false}]` Excluir archivos atascados en copias snapshot


Ejemplo:

```
volume rebalance start -vserver vs0 -volume fg1
```

Modificar las configuraciones de reequilibrio de FlexGroup

Puede cambiar la configuración de reequilibrio de FlexGroup para actualizar el umbral de desequilibrio, el número de archivos simultáneos mueve el tamaño mínimo de archivo, el tiempo de ejecución máximo y para incluir o excluir copias de Snapshot. Las opciones para modificar el programa de reequilibrio de FlexGroup están disponibles a partir de ONTAP 9.13.1.

System Manager

1. Navegue hasta **almacenamiento > volúmenes** y localice el volumen FlexGroup para reequilibrar.
2. Seleccione  para ver los detalles del volumen.
3. Seleccione **Reequilibrar**.
4. En la ventana **volumen de reequilibrio**, cambie la configuración predeterminada según sea necesario.

CLI

1. Modificar reequilibrio automático: `volume rebalance modify -vserver SVM_name -volume volume_name`

Puede especificar una o varias de las siguientes opciones:

`[-max-Runtime] <time interval>` Tiempo de ejecución máximo

`[-max-threshold <percent>]` Umbral de desequilibrio máximo por componente

`[-min-threshold <percent>]` Umbral de desequilibrio mínimo por componente

`[-max-file-moves <integer>]` Máximo de Movimientos Simultáneos de Archivos por Componente

`[-min-file-size {<integer>[KB|MB|GB|TB|PB]}]` Tamaño mínimo de archivo


`[-START-Time <mm/dd/yyyy-00:00:00>]` Fecha y hora de inicio de reequilibrio de horario

`[-exclude-snapshots {true|false}]` Excluir archivos atascados en copias snapshot

Detenga el reequilibrio de FlexGroup

Una vez activado o programado el reequilibrio de FlexGroup, es posible detenerlo en cualquier momento.

System Manager

1. Vaya a **almacenamiento > volúmenes** y localice el volumen FlexGroup.
2. Seleccione  para ver los detalles del volumen.
3. Seleccione **Detener reequilibrio**.


CLI

1. Detenga el reequilibrio de FlexGroup: `volume rebalance stop -vserver SVM_name -volume volume_name`

Ver el estado de reequilibrio de FlexGroup

Puede mostrar el estado en una operación de reequilibrio de FlexGroup, la configuración de reequilibrio de FlexGroup, el tiempo de operación de reequilibrio y los detalles de la instancia de reequilibrio.

System Manager

1. Vaya a **almacenamiento > volúmenes** y localice el volumen FlexGroup.
2. Seleccione  Para ver los detalles de la FlexGroup.
3. **El estado de saldo de FlexGroup** se muestra cerca de la parte inferior del panel de detalles.
4. Para ver información sobre la última operación de reequilibrio, selecciona **Último estado de reequilibrio de volumen**.

CLI

1. Vea el estado de una operación de reequilibrio de FlexGroup: `volume rebalance show`

Ejemplo de estado de reequilibrio:

```
> volume rebalance show
Vserver: vs0

Imbalance
Volume      State      Total      Used      Target
Size        %
-----
fg1          idle      4GB      115.3MB      -
8KB         0%
```

Ejemplo de detalles de configuración de reequilibrio:

```
> volume rebalance show -config
Vserver: vs0

Min      Max      Threshold      Max
Volume  Exclude Runtime  Min    Max    File Moves
File Size Snapshot
-----
fg1      6h0m0s  5%      20%      25
4KB      true
```

Ejemplo de cómo reequilibrar los detalles del tiempo:

```
> volume rebalance show -time
Vserver: vs0
Volume                Start Time                Runtime
Max Runtime
-----
fg1                    Wed Jul 20 16:06:11 2022    0h1m16s
6h0m0s
```

Ejemplo de detalles de la instancia de reequilibrio:

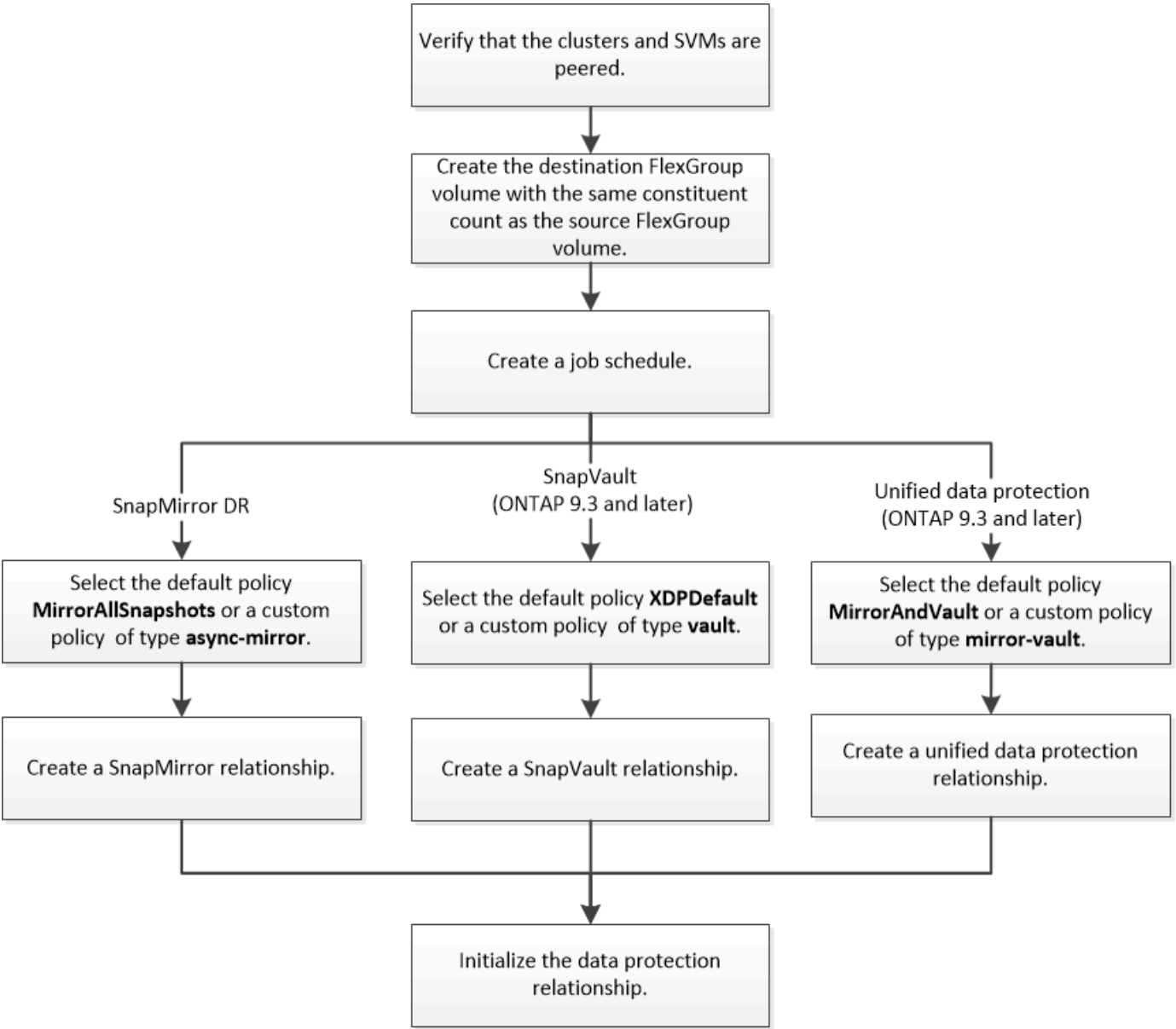
```
> volume rebalance show -instance
Vserver Name: vs0
Volume Name: fg1
Is Constituent: false
Rebalance State: idle
Rebalance Notice Messages: -
Total Size: 4GB
AFS Used Size: 115.3MB
Constituent Target Used Size: -
Imbalance Size: 8KB
Imbalance Percentage: 0%
Moved Data Size: -
Maximum Constituent Imbalance Percentage: 1%
Rebalance Start Time: Wed Jul 20 16:06:11 2022
Rebalance Stop Time: -
Rebalance Runtime: 0h1m32s
Rebalance Maximum Runtime: 6h0m0s
Maximum Imbalance Threshold per Constituent: 20%
Minimum Imbalance Threshold per Constituent: 5%
Maximum Concurrent File Moves per Constituent: 25
Minimum File Size: 4KB
Exclude Files Stuck in Snapshot Copies: true
```

Protección de datos para volúmenes de FlexGroup

Flujo de trabajo de protección de datos para volúmenes de FlexGroup

Puede crear relaciones de recuperación ante desastres (DR) de SnapMirror para los volúmenes de FlexGroup. A partir de ONTAP 9.3, también puede realizar backups y restauraciones de volúmenes de FlexGroup mediante la tecnología SnapVault, y puede crear una relación de protección de datos unificada que utilice el mismo destino para backup y recuperación ante desastres.

El flujo de trabajo de protección de datos consta de verificar las relaciones entre iguales de clústeres y SVM, crear un volumen de destino, crear una programación de trabajos, especificar una política, crear una relación de protección de datos e inicializar la relación.



Acerca de esta tarea

El tipo de relación SnapMirror es siempre XDP Para volúmenes de FlexGroup. El tipo de protección de datos que proporciona una relación de SnapMirror está determinado por la política de replicación que utiliza. Puede usar la directiva predeterminada o una directiva personalizada del tipo requerido para la relación de replicación que desea crear. En la siguiente tabla, se muestran los tipos de políticas predeterminadas y los tipos de políticas personalizadas compatibles con diferentes tipos de relaciones de protección de datos.

| Tipo de relación | Directiva predeterminada | Tipo de directiva personalizada |
|---|--------------------------|---------------------------------|
| Recuperación ante desastres de SnapMirror | MirrorAllSnapshots | reflejo asíncrono |
| Backup de SnapVault | XDPDefault | almacén |

| | | |
|-------------------------------|---------------------|--------------|
| Protección de datos unificada | Reflejo de AndVault | mirror-vault |
|-------------------------------|---------------------|--------------|

La política de MirrorLatest no es compatible con los volúmenes de FlexGroup.

Crear una relación de SnapMirror para volúmenes de FlexGroup

Es posible crear una relación de SnapMirror entre el volumen de FlexGroup de origen y el volumen de FlexGroup de destino en una SVM con relación entre iguales para replicar datos para la recuperación de desastres. Se pueden utilizar las copias reflejadas del volumen FlexGroup para recuperar los datos cuando se produce un desastre.

Lo que necesitará

Debe haber creado la relación de paridad de clústeres y la relación de paridad de SVM.

["Relaciones entre iguales de clústeres y SVM"](#)

Acerca de esta tarea

- Puede crear tanto relaciones SnapMirror de interconexión de clústeres como relaciones SnapMirror entre clústeres para volúmenes FlexGroup.
- A partir de ONTAP 9.3, puede ampliar los volúmenes de FlexGroup que se encuentren en una relación de SnapMirror.

Si utiliza una versión de ONTAP anterior a ONTAP 9.3, no debe expandir los volúmenes de FlexGroup después de establecer una relación de SnapMirror. Sin embargo, puede aumentar la capacidad de FlexGroup Volumes después de establecer una relación de SnapMirror. Si expande el volumen FlexGroup de origen después de dividir la relación de SnapMirror en versiones anteriores a ONTAP 9.3, debe realizar una transferencia completa al volumen de FlexGroup de destino.

Pasos

1. Cree un volumen de FlexGroup de destino del tipo `DP`. Esto tiene la misma cantidad de componentes que el volumen FlexGroup de origen:
 - a. En el clúster de origen, determine la cantidad de componentes en el volumen de FlexGroup de origen:


```
volume show -volume volume_name* -is-constituent true
```

```
cluster1::> volume show -volume srcFG* -is-constituent true
```

| Vserver | Volume | Aggregate | State | Type | Size |
|-----------|-------------|------------|--------|------|-------|
| Available | Used% | | | | |
| vss | srcFG | - | online | RW | 400TB |
| 172.86GB | 56% | | | | |
| vss | srcFG__0001 | Aggr_cmode | online | RW | 25GB |
| 10.86TB | 56% | | | | |
| vss | srcFG__0002 | aggr1 | online | RW | 25TB |
| 10.86TB | 56% | | | | |
| vss | srcFG__0003 | Aggr_cmode | online | RW | 25TB |
| 10.72TB | 57% | | | | |
| vss | srcFG__0004 | aggr1 | online | RW | 25TB |
| 10.73TB | 57% | | | | |
| vss | srcFG__0005 | Aggr_cmode | online | RW | 25TB |
| 10.67TB | 57% | | | | |
| vss | srcFG__0006 | aggr1 | online | RW | 25TB |
| 10.64TB | 57% | | | | |
| vss | srcFG__0007 | Aggr_cmode | online | RW | 25TB |
| 10.63TB | 57% | | | | |
| ... | | | | | |

- b. A partir del clúster de destino, cree un volumen de FlexGroup de destino de tipo DP Con el mismo número de componentes que el volumen FlexGroup de origen.

```
cluster2::> volume create -vserver vsd -aggr-list aggr1,aggr2 -aggr
-list-multiplier 8 -size 400TB -type DP dstFG
```

Warning: The FlexGroup volume "dstFG" will be created with the following number of constituents of size 25TB: 16.

Do you want to continue? {y|n}: y

[Job 766] Job succeeded: Successful

- c. En el clúster de destino, compruebe el número de componentes en el volumen de FlexGroup de destino: `volume show -volume volume_name* -is-constituent true`

```
cluster2::> volume show -volume dstFG* -is-constituent true
```

| Vserver | Volume | Aggregate | State | Type | Size |
|-----------|-------------|------------|--------|------|-------|
| Available | Used% | | | | |
| ----- | ----- | ----- | ----- | ---- | ----- |
| vsd | dstFG | - | online | DP | 400TB |
| 172.86GB | 56% | | | | |
| vsd | dstFG__0001 | Aggr_cmode | online | DP | 25GB |
| 10.86TB | 56% | | | | |
| vsd | dstFG__0002 | aggr1 | online | DP | 25TB |
| 10.86TB | 56% | | | | |
| vsd | dstFG__0003 | Aggr_cmode | online | DP | 25TB |
| 10.72TB | 57% | | | | |
| vsd | dstFG__0004 | aggr1 | online | DP | 25TB |
| 10.73TB | 57% | | | | |
| vsd | dstFG__0005 | Aggr_cmode | online | DP | 25TB |
| 10.67TB | 57% | | | | |
| vsd | dstFG__0006 | aggr1 | online | DP | 25TB |
| 10.64TB | 57% | | | | |
| vsd | dstFG__0007 | Aggr_cmode | online | DP | 25TB |
| 10.63TB | 57% | | | | |
| ... | | | | | |

2. Crear un programa de trabajo: `job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

Para la `-month`, `-dayofweek`, y `-hour` opciones, puede especificar `all` ejecutar el trabajo cada mes, cada día de la semana y cada hora, respectivamente.

En el ejemplo siguiente se crea una programación de trabajo denominada `my_weekly`. Es decir, los sábados a las 3:00 horas:

```
cluster1::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

3. Cree una directiva personalizada de tipo `async-mirror` Para la relación de SnapMirror: `snapmirror policy create -vserver SVM -policy snapmirror_policy -type async-mirror`
4. A partir del clúster de destino, cree una relación de SnapMirror entre el volumen de FlexGroup de origen y el volumen de FlexGroup de destino: `snapmirror create -source-path src_svm:src_flexgroup -destination-path dest_svm:dest_flexgroup -type XDP -policy snapmirror_policy -schedule sched_name`

Las relaciones de SnapMirror para volúmenes de FlexGroup deben ser de tipo XDP.

Si especifica un valor de aceleración para la relación de SnapMirror en el volumen FlexGroup, cada componente utiliza el mismo valor de aceleración. El valor del acelerador no está dividido entre los componentes.



No se pueden usar las etiquetas de SnapMirror para copias de Snapshot para volúmenes de FlexGroup.

En ONTAP 9.4 y anteriores, si la política no se especifica con el `snapmirror create` comando, el `MirrorAllSnapshots` la directiva se utiliza de forma predeterminada. En ONTAP 9.5, si la política no se especifica con el `snapmirror create` comando, el `MirrorAndVault` la directiva se utiliza de forma predeterminada.

```
cluster2::> snapmirror create -source-path vss:srcFG -destination-path  
vsd:dstFG -type XDP -policy MirrorAllSnapshots -schedule hourly  
Operation succeeded: snapmirror create for the relationship with  
destination "vsd:dstFG".
```

5. Desde el clúster de destino, inicialice la relación de SnapMirror realizando una transferencia básica:
`snapmirror initialize -destination-path dest_svm:dest_flexgroup`

Una vez finalizada la transferencia completa, el volumen FlexGroup de destino se actualiza periódicamente de acuerdo con la programación de la relación de SnapMirror.

```
cluster2::> snapmirror initialize -destination-path vsd:dstFG  
Operation is queued: snapmirror initialize of destination "vsd:dstFG".
```



Si creó cualquier relación de SnapMirror entre los volúmenes de FlexGroup con el clúster de origen que ejecuta ONTAP 9.3 y el clúster de destino que ejecuta ONTAP 9.2 o una versión anterior, y si creó cualquier qtrees en el volumen de FlexGroup de origen, la actualización de SnapMirror genera errores. Para recuperarse de esta situación, debe eliminar todos los qtrees no predeterminados en el volumen FlexGroup, deshabilitar la funcionalidad Qtree del volumen FlexGroup y, a continuación, eliminar todas las copias Snapshot que están habilitadas con la funcionalidad para qtrees. También debe realizar estos pasos antes de revertir de ONTAP 9.3 a una versión anterior de ONTAP si tiene la funcionalidad para qtrees habilitada en los volúmenes de FlexGroup. ["Deshabilite la funcionalidad Qtree en volúmenes FlexGroup antes de revertir"](#)

Después de terminar

Debe configurar la SVM de destino para el acceso a los datos mediante la configuración de configuraciones requeridas, como LIF y políticas de exportación.

Crear una relación de SnapVault para volúmenes de FlexGroup

Puede configurar una relación de SnapVault y asignar una política de SnapVault a la relación para crear un backup de SnapVault.

Lo que necesitará

Debe tener en cuenta las consideraciones que se deben tener en cuenta para crear una relación de SnapVault para los volúmenes de FlexGroup.

Pasos

1. Cree un volumen de FlexGroup de destino del tipo **DP**. Esto tiene la misma cantidad de componentes que el volumen FlexGroup de origen:

- a. En el clúster de origen, determine la cantidad de componentes en el volumen de FlexGroup de origen:

```
volume show -volume volume_name* -is-constituent true
```

```
cluster1::> volume show -volume src* -is-constituent true
Vserver    Volume          Aggregate      State      Type      Size
Available  Used%
-----
vss        src              -              online     RW        400TB
172.86GB   56%
vss        src__0001        Aggr_cmode     online     RW        25GB
10.86TB    56%
vss        src__0002        aggr1          online     RW        25TB
10.86TB    56%
vss        src__0003        Aggr_cmode     online     RW        25TB
10.72TB    57%
vss        src__0004        aggr1          online     RW        25TB
10.73TB    57%
vss        src__0005        Aggr_cmode     online     RW        25TB
10.67TB    57%
vss        src__0006        aggr1          online     RW        25TB
10.64TB    57%
vss        src__0007        Aggr_cmode     online     RW        25TB
10.63TB    57%
...
```

- b. A partir del clúster de destino, cree un volumen de FlexGroup de destino de tipo **DP**. Con el mismo número de componentes que el volumen FlexGroup de origen.

```
cluster2::> volume create -vserver vsd -aggr-list aggr1,aggr2 -aggr
-list-multiplier 8 -size 400TB -type DP dst
```

```
Warning: The FlexGroup volume "dst" will be created with the
following number of constituents of size 25TB: 16.
```

```
Do you want to continue? {y|n}: y
```

```
[Job 766] Job succeeded: Successful
```

- c. En el clúster de destino, compruebe el número de componentes en el volumen de FlexGroup de

```
destino: volume show -volume volume_name* -is-constituent true
```

```
cluster2::> volume show -volume dst* -is-constituent true
```

| Vserver | Volume | Aggregate | State | Type | Size |
|-----------|-----------|------------|--------|-------|-------|
| Available | Used% | | | | |
| ----- | ----- | ----- | ----- | ----- | ----- |
| ----- | ----- | | | | |
| vsd | dst | - | online | RW | 400TB |
| 172.86GB | 56% | | | | |
| vsd | dst__0001 | Aggr_cmode | online | RW | 25GB |
| 10.86TB | 56% | | | | |
| vsd | dst__0002 | aggr1 | online | RW | 25TB |
| 10.86TB | 56% | | | | |
| vsd | dst__0003 | Aggr_cmode | online | RW | 25TB |
| 10.72TB | 57% | | | | |
| vsd | dst__0004 | aggr1 | online | RW | 25TB |
| 10.73TB | 57% | | | | |
| vsd | dst__0005 | Aggr_cmode | online | RW | 25TB |
| 10.67TB | 57% | | | | |
| vsd | dst__0006 | aggr1 | online | RW | 25TB |
| 10.64TB | 57% | | | | |
| vsd | dst__0007 | Aggr_cmode | online | RW | 25TB |
| 10.63TB | 57% | | | | |
| ... | | | | | |

2. Crear un programa de trabajo: `job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

Para `-month`, `-dayofweek`, y `-hour`, puede especificar `all` para ejecutar el trabajo cada mes, día de la semana y hora, respectivamente.

En el ejemplo siguiente se crea una programación de trabajo denominada `my_weekly`. Es decir, los sábados a las 3:00 horas:

```
cluster1::> job schedule cron create -name my_weekly -dayofweek  
"Saturday" -hour 3 -minute 0
```

3. Cree una política de SnapVault y, a continuación, defina una regla para la política de SnapVault:
- Cree una directiva personalizada de tipo `vault`. Para la relación de SnapVault: `snapmirror policy create -vserver svm_name -policy policy_name -type vault`
 - Defina una regla para la política de SnapVault que determine qué copias Snapshot se transfieren durante las operaciones de inicialización y actualización: `snapmirror policy add-rule -vserver svm_name -policy policy_for_rule - snapmirror-label snapmirror-label -keep retention_count -schedule schedule`

Si no crea una política personalizada, debe especificar el `XDPDefault` Política de relaciones de SnapVault.

4. Crear una relación de SnapVault: `snapmirror create -source-path src_svm:src_flexgroup -destination-path dest_svm:dest_flexgroup -type XDP -schedule schedule_name -policy XDPDefault`

En ONTAP 9.4 y anteriores, si la política no se especifica con el `snapmirror create` comando, el `MirrorAllSnapshots` la directiva se utiliza de forma predeterminada. En ONTAP 9.5, si la política no se especifica con el `snapmirror create` comando, el `MirrorAndVault` la directiva se utiliza de forma predeterminada.

```
cluster2::> snapmirror create -source-path vss:srcFG -destination-path  
vsd:dstFG -type XDP -schedule Daily -policy XDPDefault
```

5. Desde el clúster de destino, inicialice la relación SnapVault realizando una transferencia básica:
`snapmirror initialize -destination-path dest_svm:dest_flexgroup`

```
cluster2::> snapmirror initialize -destination-path vsd:dst  
Operation is queued: snapmirror initialize of destination "vsd:dst".
```

Cree una relación de protección de datos unificada para FlexGroup Volumes

A partir de ONTAP 9.3, se pueden crear y configurar relaciones de protección de datos unificadas de SnapMirror para configurar la recuperación ante desastres y el archivado en el mismo volumen de destino.

Lo que necesitará

Debe tener en cuenta las consideraciones que se deben tener en cuenta para crear relaciones de protección de datos unificadas para volúmenes de FlexGroup.

["Consideraciones sobre la creación de una relación de backup de SnapVault y una relación de protección de datos unificada para volúmenes de FlexGroup"](#)

Pasos

1. Cree un volumen de FlexGroup de destino del tipo `DP` Esto tiene la misma cantidad de componentes que el volumen FlexGroup de origen:
 - a. En el clúster de origen, determine la cantidad de componentes en el volumen de FlexGroup de origen:
`volume show -volume volume_name* -is-constituent true`

```
cluster1::> volume show -volume srcFG* -is-constituent true
```

| Vserver | Volume | Aggregate | State | Type | Size |
|-----------|-------------|------------|--------|------|-------|
| Available | Used% | | | | |
| vss | srcFG | - | online | RW | 400TB |
| 172.86GB | 56% | | | | |
| vss | srcFG__0001 | Aggr_cmode | online | RW | 25GB |
| 10.86TB | 56% | | | | |
| vss | srcFG__0002 | aggr1 | online | RW | 25TB |
| 10.86TB | 56% | | | | |
| vss | srcFG__0003 | Aggr_cmode | online | RW | 25TB |
| 10.72TB | 57% | | | | |
| vss | srcFG__0004 | aggr1 | online | RW | 25TB |
| 10.73TB | 57% | | | | |
| vss | srcFG__0005 | Aggr_cmode | online | RW | 25TB |
| 10.67TB | 57% | | | | |
| vss | srcFG__0006 | aggr1 | online | RW | 25TB |
| 10.64TB | 57% | | | | |
| vss | srcFG__0007 | Aggr_cmode | online | RW | 25TB |
| 10.63TB | 57% | | | | |
| ... | | | | | |

- b. A partir del clúster de destino, cree un volumen de FlexGroup de destino de tipo DP Con el mismo número de componentes que el volumen FlexGroup de origen.

```
cluster2::> volume create -vserver vsd -aggr-list aggr1,aggr2 -aggr
-list-multiplier 8 -size 400TB -type DP dstFG
```

Warning: The FlexGroup volume "dstFG" will be created with the following number of constituents of size 25TB: 16.

Do you want to continue? {y|n}: y

[Job 766] Job succeeded: Successful

- c. En el clúster de destino, compruebe el número de componentes en el volumen de FlexGroup de destino: `volume show -volume volume_name* -is-constituent true`

```
cluster2::> volume show -volume dstFG* -is-constituent true
```

| Vserver | Volume | Aggregate | State | Type | Size |
|-----------|-------------|------------|--------|-------|-------|
| Available | Used% | | | | |
| ----- | ----- | ----- | ----- | ----- | ----- |
| vsd | dstFG | - | online | RW | 400TB |
| 172.86GB | 56% | | | | |
| vsd | dstFG__0001 | Aggr_cmode | online | RW | 25GB |
| 10.86TB | 56% | | | | |
| vsd | dstFG__0002 | aggr1 | online | RW | 25TB |
| 10.86TB | 56% | | | | |
| vsd | dstFG__0003 | Aggr_cmode | online | RW | 25TB |
| 10.72TB | 57% | | | | |
| vsd | dstFG__0004 | aggr1 | online | RW | 25TB |
| 10.73TB | 57% | | | | |
| vsd | dstFG__0005 | Aggr_cmode | online | RW | 25TB |
| 10.67TB | 57% | | | | |
| vsd | dstFG__0006 | aggr1 | online | RW | 25TB |
| 10.64TB | 57% | | | | |
| vsd | dstFG__0007 | Aggr_cmode | online | RW | 25TB |
| 10.63TB | 57% | | | | |
| ... | | | | | |

2. Crear un programa de trabajo: `job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

Para la `-month`, `-dayofweek`, y `-hour` opciones, puede especificar `all` ejecutar el trabajo cada mes, cada día de la semana y cada hora, respectivamente.

En el ejemplo siguiente se crea una programación de trabajo denominada `my_weekly`. Es decir, los sábados a las 3:00 horas:

```
cluster1::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

3. Cree una directiva personalizada de tipo `mirror-vault`, a continuación, defina una regla para la directiva de réplica y almacén:
 - a. Cree una directiva personalizada de tipo `mirror-vault` para la relación de protección de datos unificada: `snapmirror policy create -vserver svm_name -policy policy_name -type mirror-vault`
 - b. Definir una regla para la política de mirroring y almacén que determina qué copias Snapshot se transfieren durante las operaciones de inicialización y actualización: `snapmirror policy add-rule -vserver svm_name -policy policy_for_rule - snapmirror-label snapmirror-label -keep retention_count -schedule schedule`

Si no se especifica una política personalizada, el MirrorAndVault la política se utiliza para relaciones de protección de datos unificadas.

4. Cree una relación de protección de datos unificada: `snapmirror create -source-path src_svm:src_flexgroup -destination-path dest_svm:dest_flexgroup -type XDP -schedule schedule_name -policy MirrorAndVault`

En ONTAP 9.4 y anteriores, si la política no se especifica con el `snapmirror create` comando, el MirrorAllSnapshots la directiva se utiliza de forma predeterminada. En ONTAP 9.5, si la política no se especifica con el `snapmirror create` comando, el MirrorAndVault la directiva se utiliza de forma predeterminada.

```
cluster2::> snapmirror create -source-path vss:srcFG -destination-path  
vsd:dstFG -type XDP -schedule Daily -policy MirrorAndVault
```

5. Desde el clúster de destino, inicialice la relación de protección de datos unificada mediante una transferencia básica: `snapmirror initialize -destination-path dest_svm:dest_flexgroup`

```
cluster2::> snapmirror initialize -destination-path vsd:dstFG  
Operation is queued: snapmirror initialize of destination "vsd:dstFG".
```

Crear una relación de recuperación ante desastres de SVM para volúmenes de FlexGroup

A partir de ONTAP 9.9.1, se pueden crear relaciones de recuperación ante desastres de SVM con los volúmenes de FlexGroup. Una relación de recuperación ante desastres de SVM proporciona redundancia y la capacidad de recuperar FlexGroups en caso de desastre mediante la sincronización y la replicación de la configuración de SVM y sus datos. Se requiere una licencia de SnapMirror para la recuperación ante desastres de SVM.

Antes de empezar

No puede crear una relación de recuperación ante desastres de FlexGroup SVM con lo siguiente se aplica.

- Existe una configuración de FlexGroup FlexClone
- El volumen FlexGroup forma parte de una relación en cascada
- El volumen de FlexGroup forma parte de una relación de dispersión, y el clúster ejecuta una versión de ONTAP anterior a ONTAP 9.12.1. (A partir de ONTAP 9.13.1, las relaciones de fanout son compatibles).

Acerca de esta tarea

- Todos los nodos de ambos clústeres deben ejecutar la misma versión de ONTAP que el nodo en el que se añadió la compatibilidad con la recuperación ante desastres de SVM (ONTAP 9.9.1 o una versión posterior).
- La relación de DR de SVM entre los sitios primario y secundario debe estar en buen estado y debe tener suficiente espacio en las SVM primaria y secundaria para admitir los volúmenes FlexGroup.
- A partir de ONTAP 9.12.1, FabricPool, FlexGroup y SVM DR pueden trabajar conjuntamente. En las versiones anteriores a ONTAP 9.12.1, cualquiera de estas dos funciones funcionó conjuntamente, pero no

las tres.

- Cuando crea una relación de recuperación ante desastres de SVM de FlexGroup en la que el volumen de FlexGroup forma parte de una relación de fanout, debe tener en cuenta los siguientes requisitos:
 - El clúster de origen y de destino debe ejecutar ONTAP 9.13.1 o una versión posterior.
 - La recuperación de desastres de SVM con volúmenes de FlexGroup admite las relaciones de expansión de SnapMirror en ocho sitios.

Para obtener información sobre la creación de una relación de recuperación ante desastres de SVM, consulte ["Gestione la replicación de SVM de SnapMirror"](#).

Pasos

1. Cree una relación de recuperación ante desastres de SVM o utilice una relación existente.

["Replique toda una configuración de SVM"](#)

2. Cree un volumen FlexGroup en el sitio primario con el número necesario de componentes.

["Creación de un volumen de FlexGroup"](#).

Espere a que FlexGroup y todos sus componentes se creen antes de continuar.

3. Para replicar el volumen de FlexGroup, actualice la SVM en el sitio secundario: `snapmirror update -destination-path destination_svm_name: -source-path source_svm_name:`

También puede comprobar si ya existe una actualización de SnapMirror programada introduciendo `snapmirror show -fields schedule`

4. Desde el sitio secundario, compruebe que la relación de SnapMirror esté en buen estado: `snapmirror show`

```
cluster2::> snapmirror show
```

Progress

| Source | | Destination | Mirror | Relationship | Total | |
|---------|------|-------------|--------------|--------------|----------|---------|
| Last | | | | | | |
| Path | Type | Path | State | Status | Progress | Healthy |
| Updated | | | | | | |
| ----- | ---- | ----- | ----- | ----- | ----- | ----- |
| ----- | | | | | | |
| vs1: | XDP | vs1_dst: | Snapmirrored | | | |
| | | | Idle | | - | true - |

5. Desde el sitio secundario, compruebe que el nuevo volumen FlexGroup y sus componentes existen: `snapmirror show -expand`


```
cluster2::> snapmirror show -expand
```

| Progress | Source | Destination | Mirror | Relationship | Total | | |
|----------|------------------|-------------|----------------------|--------------|--------|----------|---------|
| Last | Path | Type | Path | State | Status | Progress | Healthy |
| Updated | | | | | | | |
| ----- | ---- | ----- | ----- | ----- | ----- | ----- | ----- |
| | vs1: | XDP | vs1_dst: | Snapmirrored | | | |
| | | | | Idle | | - | true - |
| | vs1:fg_src | XDP | vs1_dst:fg_src | Snapmirrored | | | |
| | | | | Idle | | - | true - |
| | vs1:fg_src__0001 | | | | | | |
| | | XDP | vs1_dst:fg_src__0001 | Snapmirrored | | | |
| | | | | Idle | | - | true - |
| | vs1:fg_src__0002 | | | | | | |
| | | XDP | vs1_dst:fg_src__0002 | Snapmirrored | | | |
| | | | | Idle | | - | true - |
| | vs1:fg_src__0003 | | | | | | |
| | | XDP | vs1_dst:fg_src__0003 | Snapmirrored | | | |
| | | | | Idle | | - | true - |
| | vs1:fg_src__0004 | | | | | | |
| | | XDP | vs1_dst:fg_src__0004 | Snapmirrored | | | |
| | | | | Idle | | - | true - |

6 entries were displayed.

Realice la transición de una relación de SnapMirror de FlexGroup existente a la recuperación ante desastres de SVM

Puede crear una relación de recuperación ante desastres de SVM de FlexGroup realizando la transición de una relación existente de SnapMirror para volúmenes de FlexGroup.

Lo que necesitará

- La relación de SnapMirror para volúmenes de FlexGroup está en buen estado.
- Los volúmenes de FlexGroup de origen y destino tienen el mismo nombre.

Pasos

1. En el destino de SnapMirror, resincronice la relación de SnapMirror de nivel de FlexGroup: `snapmirror`

resync

2. Cree la relación de SnapMirror de recuperación ante desastres de la SVM de FlexGroup. Utilice la misma política de SnapMirror que está configurada en las relaciones de SnapMirror para volúmenes de FlexGroup: `snapmirror create -destination-path dest_svm: -source-path src_svm: -identity-preserve true -policy MirrorAllSnapshots`



Debe utilizar el `-identity-preserve true` opción de `snapmirror create` comando al crear la relación de replicación.

3. Compruebe que la relación se rompe: `snapmirror show -destination-path dest_svm: -source-path src_svm:`

```
snapmirror show -destination-path fg_vs_renamed: -source-path fg_vs:
```

| Progress | Source | Destination | Mirror | Relationship | Total | |
|----------|--------|-------------|-----------------|--------------|--------|----------|
| Last | Path | Type | Path | State | Status | Progress |
| Updated | | | | | | Healthy |
| ----- | ----- | ----- | ----- | ----- | ----- | ----- |
| ----- | fg_vs: | XDP | fg_vs1_renamed: | Broken-off | | |
| | | | | Idle | - | true - |

4. Detenga la SVM de destino: `vserver stop -vserver vs_name`

```
vserver stop -vserver fg_vs_renamed
[Job 245] Job is queued: Vserver Stop fg_vs_renamed.
[Job 245] Done
```

5. Resincronice la relación de SnapMirror de SVM: `snapmirror resync -destination-path dest_svm: -source-path src_svm:`

```
snapmirror resync -destination-path fg_vs_renamed: -source-path fg_vs:
Warning: This Vserver has volumes which are the destination of FlexVol
or FlexGroup SnapMirror relationships. A resync on the Vserver
SnapMirror relationship will cause disruptions in data access
```

6. Compruebe que la relación de SnapMirror con el nivel de recuperación ante desastres de SVM alcanza un estado de inactividad en buen estado: `snapmirror show -expand`
7. Compruebe que la relación de SnapMirror de FlexGroup está en buen estado: `snapmirror show`

Convierta un volumen FlexVol en un volumen FlexGroup dentro de una relación SVM-DR

A partir de ONTAP 9.10.1, es posible convertir un volumen FlexVol en un volumen FlexGroup en un origen de SVM-DR.

Lo que necesitará

- El volumen FlexVol que se está convirtiendo debe estar en línea.
- Las operaciones y configuraciones del volumen FlexVol deben ser compatibles con el proceso de conversión.

Se genera un mensaje de error si el volumen FlexVol tiene alguna incompatibilidad y se cancela la conversión de volumen. Puede tomar acciones correctivas y volver a intentar la conversión.

Para obtener información detallada, consulte [Consideraciones sobre la conversión de volúmenes de FlexVol en volúmenes de FlexGroup](#)

Pasos

1. Inicio de sesión mediante el modo de privilegio avanzado: `set -privilege advanced`
2. En el destino, actualice la relación SVM-DR:

```
snapmirror update -destination-path destination_svm_name: -source-path source_svm_name:
```

3. Asegúrese de que la relación SVM-DR esté en estado de SnapMirred y no esté desdividida:

```
snapmirror show
```

4. En la SVM de destino, compruebe que el volumen de FlexVol esté listo para la conversión:

```
volume conversion start -vserver svm_name -volume vol_name -check-only true
```

Si este comando genera errores distintos a "éste es un volumen SVM-DR de destino", puede tomar la acción correctiva adecuada, ejecutar el comando de nuevo y continuar con la conversión.

5. En el destino, deshabilite las transferencias en la relación SVM-DR:

```
snapmirror quiesce -destination-path dest_svm:
```

6. Inicie la conversión:

```
volume conversion start -vserver svm_name -volume vol_name
```

7. Compruebe que la conversión se ha realizado correctamente:

```
volume show vol_name -fields -volume-style-extended,state
```

```
cluster-1::*> volume show my_volume -fields volume-style-extended,state
```

| vserver | volume | state | volume-style-extended |
|---------|-----------|--------|-----------------------|
| vs0 | my_volume | online | flexgroup |

8. Desde el clúster de destino, reanude las transferencias para la relación:

```
snapmirror resume -destination-path dest_svm:
```

9. Desde el clúster de destino, realice una actualización para propagar la conversión al destino:

```
snapmirror update -destination-path dest_svm:
```

10. Asegúrese de que la relación SVM-DR esté en estado de SnapMirred y no se rompa:

```
snapmirror show
```

11. Asegúrese de que la conversión se ha realizado en el destino:

```
volume show vol_name -fields -volume-style-extended,state
```

```
cluster-2::*> volume show my_volume -fields volume-style-extended,state
```

| vserver | volume | state | volume-style-extended |
|---------|-----------|--------|-----------------------|
| ----- | ----- | ----- | ----- |
| vs0_dst | my_volume | online | flexgroup |

Consideraciones que tener en cuenta para crear relaciones de SnapMirror en cascada y fanout para FlexGroups

Existen consideraciones y limitaciones de compatibilidad que debe tener en cuenta al crear relaciones en cascada y con ventilador de SnapMirror para volúmenes FlexGroup.

Consideraciones que tener en cuenta para crear relaciones en cascada

- Cada relación puede ser una relación entre clústeres o entre clústeres.
- Todos los tipos de normativas asíncronas, incluidos los duplicados asíncronos, los almacenes de reflejos y los almacenes, se admiten en ambas relaciones.
- Solo se admiten las políticas de reflejo asíncrono "MirrorAllSnapshots" y no "MirrorLatest".
- Se admiten actualizaciones simultáneas de relaciones XDP en cascada.
- Admite la extracción De A a B y B a C y la resincronización De A a C o la resincronización de C a
- Los volúmenes de FlexGroup a y B también admiten fanout cuando todos los nodos ejecutan ONTAP 9.9.1 o una versión posterior.
- Se admiten las operaciones de restauración de volúmenes FlexGroup B o C.
- Las transferencias en las relaciones de FlexGroup no son compatibles mientras el destino es el origen de una relación de restauración.
- El destino de una restauración de FlexGroup no puede ser el destino de ninguna otra relación de FlexGroup.
- Las operaciones de restauración de archivos de FlexGroup tienen las mismas restricciones que las operaciones normales de restauración de FlexGroup.
- Todos los nodos del clúster donde residen los volúmenes de FlexGroup B y C deben ejecutar ONTAP

9.9.1 o una versión posterior.

- Se admite toda la funcionalidad de expansión automática y expansión.
- En una configuración en cascada como A B a C, si A B y B a C tienen un número distinto de relaciones SnapMirror constituyentes, la operación de anulación del origen no es compatible con la relación de SnapMirror de B a C.
- System Manager no admite relaciones en cascada en ONTAP 9.9.1.
- Al convertir una relación De FlexVol A B a C en una relación de FlexGroup, primero debe convertir la B a C hop.
- Todas las configuraciones en cascada de FlexGroup para relaciones con tipos de política compatibles con REST también son compatibles con las API DE REST en configuraciones de FlexGroup en cascada.
- Al igual que sucede con las relaciones de FlexVol, la configuración en cascada de FlexGroup no es compatible con la `snapmirror protect` comando.

Consideraciones para crear relaciones de fanout

- Se admiten dos o más relaciones de fanout de FlexGroup; por ejemplo, A a B, A C, con un máximo de 8 patas de fanout.
- Cada relación puede ser entre clústeres o dentro del clúster.
- Se admiten actualizaciones simultáneas para las dos relaciones.
- Se admite toda la funcionalidad de expansión automática y expansión.
- Si las patas de fanout de la relación tienen un número diferente de relaciones SnapMirror constituyentes, la operación de anulación del origen no se admite en las relaciones De La A a la B y De La A a la C.
- Todos los nodos del clúster donde residen los FlexGroups de origen y destino deben ejecutar ONTAP 9.9.1 o una versión posterior.
- Todos los tipos de políticas asíncronas compatibles actualmente con SnapMirror de FlexGroup se admiten en las relaciones de ventilador.
- Es posible realizar operaciones de restauración de B a C FlexGroups.
- Todas las configuraciones de fanout con tipos de políticas compatibles con REST también son compatibles con las API DE REST en configuraciones de fanout de FlexGroup.

Consideraciones sobre la creación de una relación de backup de SnapVault y una relación de protección de datos unificada para volúmenes de FlexGroup

Debe tener en cuenta las consideraciones que se deben tener en cuenta para crear una relación de backup de SnapVault y una relación de protección de datos unificada para los volúmenes FlexGroup.

- Es posible resincronizar una relación de backup de SnapVault y una relación de protección de datos unificada mediante el `-preserve` Opción que permite conservar copias Snapshot en el volumen de destino que son más recientes que la copia de Snapshot común más reciente.
- La retención a largo plazo no es compatible con los volúmenes de FlexGroup.

La retención a largo plazo permite crear copias Snapshot directamente en el volumen de destino sin necesidad de almacenar las copias Snapshot en el volumen de origen.

- La `snapshot comando expiry-time FlexGroup Volumes` no admite la opción.

- No se puede configurar la eficiencia de almacenamiento en el volumen FlexGroup de destino de una relación de backup de SnapVault y una relación de protección de datos unificada.
- No se pueden cambiar los nombres de las copias Snapshot de una relación de backup de SnapVault y una relación de protección de datos unificada para volúmenes FlexGroup.
- Un volumen FlexGroup puede ser el volumen de origen de una sola relación de backup o restauración.

Un volumen de FlexGroup no puede ser el origen de dos relaciones de SnapVault, dos relaciones de restauración o una relación de backup de SnapVault y una relación de restauración.

- Si elimina una copia Snapshot en el volumen FlexGroup de origen y vuelve a crear una copia Snapshot con el mismo nombre, la siguiente transferencia de actualización al volumen FlexGroup de destino produce un error si el volumen de destino tiene una copia Snapshot del mismo nombre.

Esto se debe a que no se puede cambiar el nombre de las copias Snapshot para los volúmenes de FlexGroup.

Supervise las transferencias de datos de SnapMirror para volúmenes FlexGroup

Debe supervisar periódicamente el estado de las relaciones de SnapMirror para volúmenes de FlexGroup a fin de verificar que el volumen de FlexGroup de destino se actualiza periódicamente según la programación especificada.

Acerca de esta tarea

Debe realizar esta tarea desde el clúster de destino.

Pasos

1. Consulte el estado de la relación de SnapMirror de todas las relaciones de volúmenes FlexGroup:
`snapmirror show -relationship-group-type flexgroup`

```
cluster2::> snapmirror show -relationship-group-type flexgroup
```

| Progress | Source | Destination | Mirror | Relationship | Total | |
|----------|--------|-------------|--------|---------------|--------|----------|
| Last | Path | Type | Path | State | Status | Progress |
| Updated | | | | | | Healthy |
| ----- | ----- | ----- | ----- | ----- | ----- | ----- |
| ----- | vss:s | XDP | vsd:d | Snapmirrored | | |
| | | | | Idle | - | true - |
| | vss:s2 | XDP | vsd:d2 | Uninitialized | | |
| | | | | Idle | - | true - |

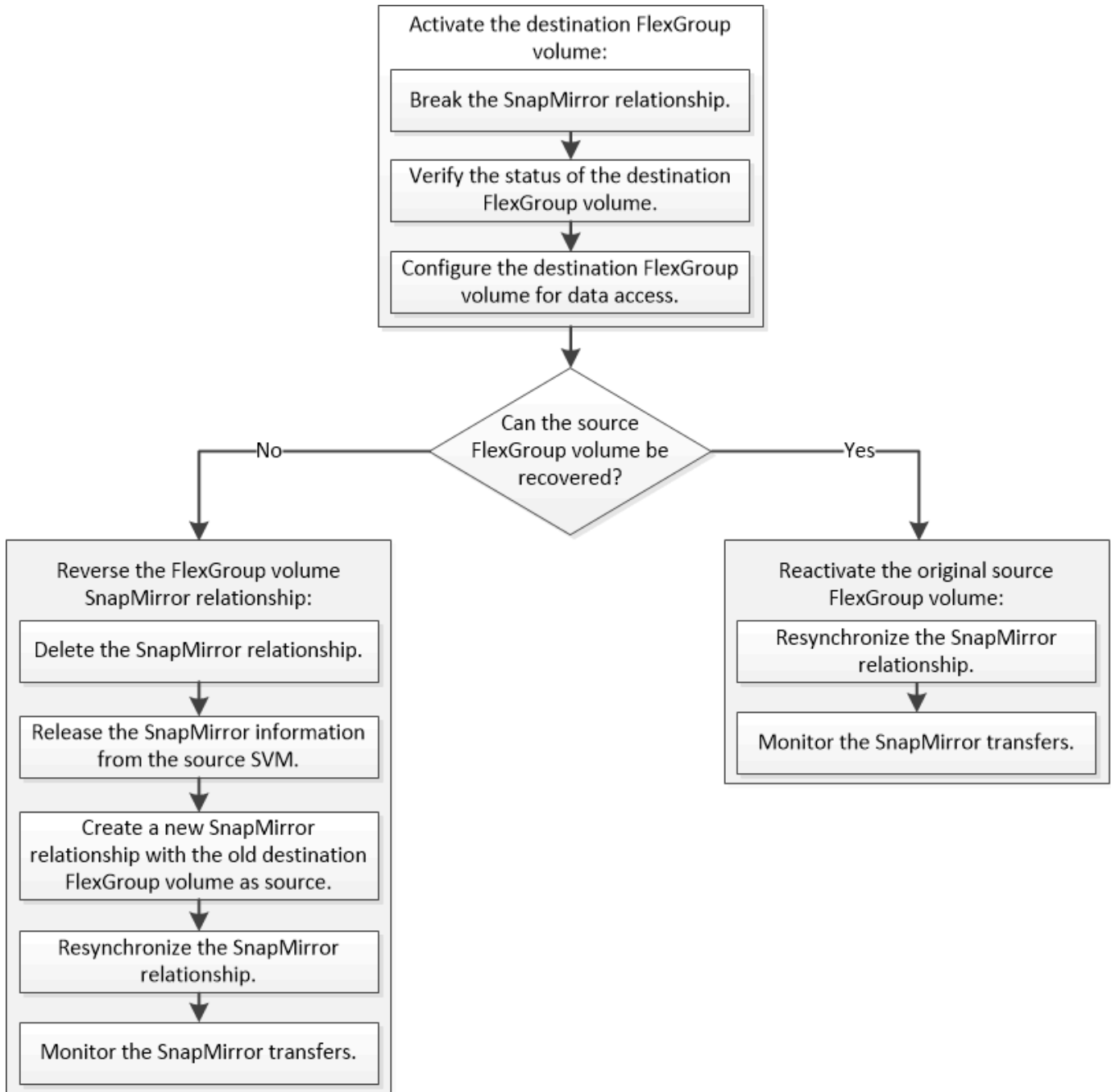
2 entries were displayed.

Gestione las operaciones de protección de datos para volúmenes de FlexGroup

Recuperación ante desastres para volúmenes FlexGroup

Flujo de trabajo de recuperación ante desastres para volúmenes de FlexGroup

Cuando ocurre un desastre en el volumen FlexGroup de origen, debe activar el volumen FlexGroup de destino y redirigir el acceso del cliente. En función de si se puede recuperar el volumen FlexGroup de origen, debe reactivar el volumen FlexGroup de origen o revertir la relación de SnapMirror.



Acerca de esta tarea

El acceso de los clientes al volumen de FlexGroup de destino se bloquea durante un breve periodo cuando se están ejecutando algunas operaciones de SnapMirror, como la pausa y la resincronización de SnapMirror. Si la operación de SnapMirror falla, es posible que algunos componentes permanezcan en este estado y se

deniegue el acceso al volumen de FlexGroup. En estos casos, debe volver a intentar la operación de SnapMirror.

Activar el volumen de FlexGroup de destino

Si el volumen de FlexGroup de origen no puede servir datos debido a eventos como daños en los datos, eliminación accidental o estado sin conexión, debe activar el volumen de FlexGroup de destino para proporcionar acceso a los datos hasta que recupere los datos en el volumen FlexGroup de origen. La activación implica la detención de futuras transferencias de datos de SnapMirror y la ruptura de la relación de SnapMirror.

Acerca de esta tarea

Debe realizar esta tarea desde el clúster de destino.

Pasos

1. Deshabilite las futuras transferencias para la relación de SnapMirror para volúmenes de FlexGroup:

```
snapmirror quiesce dest_svm:dest_flexgroup
```

```
cluster2::> snapmirror quiesce -destination-path vsd:dst
```

2. Rompa la relación de SnapMirror para volúmenes de FlexGroup: `snapmirror break dest_svm:dest_flexgroup`

```
cluster2::> snapmirror break -destination-path vsd:dst
```

3. Consulte el estado de la relación de SnapMirror: `snapmirror show -expand`


```
cluster2::> snapmirror show -expand
```

| Progress | Source | Destination | Mirror | Relationship | Total | | |
|-------------|--------|---------------|------------|--------------|--------|----------|---------|
| Last | Path | Type | Path | State | Status | Progress | Healthy |
| Updated | | | | | | | |
| ----- | ----- | ----- | ----- | ----- | ----- | ----- | ----- |
| ----- | | | | | | | |
| vss:s | XDP | vsd:dst | Broken-off | | | | |
| | | | Idle | | - | true | - |
| vss:s__0001 | XDP | vsd:dst__0001 | Broken-off | | | | |
| | | | Idle | | - | true | - |
| vss:s__0002 | XDP | vsd:dst__0002 | Broken-off | | | | |
| | | | Idle | | - | true | - |
| vss:s__0003 | XDP | vsd:dst__0003 | Broken-off | | | | |
| | | | Idle | | - | true | - |
| vss:s__0004 | XDP | vsd:dst__0004 | Broken-off | | | | |
| | | | Idle | | - | true | - |
| vss:s__0005 | XDP | vsd:dst__0005 | Broken-off | | | | |
| | | | Idle | | - | true | - |
| vss:s__0006 | XDP | vsd:dst__0006 | Broken-off | | | | |
| | | | Idle | | - | true | - |
| vss:s__0007 | XDP | vsd:dst__0007 | Broken-off | | | | |
| | | | Idle | | - | true | - |
| vss:s__0008 | XDP | vsd:dst__0008 | Broken-off | | | | |
| | | | Idle | | - | true | - |
| ... | | | | | | | |

El estado de la relación de SnapMirror de cada componente es Broken-off.

- Compruebe que el volumen FlexGroup de destino es de lectura/escritura: `volume show -vserver svm_name`

```
cluster2::> volume show -vserver vsd
```

| Vserver | Volume | Aggregate | State | Type | Size |
|-----------|----------|-----------|--------|--------|-------|
| Available | Used% | | | | |
| vsd | dst | - | online | **RW** | 2GB |
| 1.54GB | 22% | | | | |
| vsd | d2 | - | online | DP | 2GB |
| 1.55GB | 22% | | | | |
| vsd | root_vs0 | aggr1 | online | RW | 100MB |
| 94.02MB | 5% | | | | |

3 entries were displayed.

5. Redirija a los clientes al volumen FlexGroup de destino.

Reactivar el volumen FlexGroup de origen original después del desastre

Cuando el volumen FlexGroup de origen esté disponible, es posible volver a sincronizar los volúmenes FlexGroup de origen y de destino originales. Se pierden todos los datos nuevos en el volumen de FlexGroup de destino.

Acerca de esta tarea

Todas las reglas de cuota activas en el volumen de destino se desactivan y las reglas de cuota se eliminan antes de realizar la resincronización.

Puede utilizar el `volume quota policy rule create` y `volume quota modify` comandos para crear y reactivar reglas de cuota una vez completada la operación de resincronización.

Pasos

1. En el clúster de destino, resincronice la relación de SnapMirror para volúmenes de FlexGroup:
`snapmirror resync -destination-path dst_svm:dest_flexgroup`
2. Consulte el estado de la relación de SnapMirror: `snapmirror show -expand`

```
cluster2::> snapmirror show -expand
```

| Progress | Source | Destination | Mirror | Relationship | Total | | |
|----------|-------------|-------------|---------------|--------------|--------|----------|---------|
| Last | Path | Type | Path | State | Status | Progress | Healthy |
| Updated | | | | | | | |
| ----- | ----- | ----- | ----- | ----- | ----- | ----- | ----- |
| ----- | vss:s | XDP | vsd:dst | Snapmirrored | | | |
| | | | | Idle | - | true | - |
| | vss:s__0001 | XDP | vsd:dst__0001 | Snapmirrored | | | |
| | | | | Idle | - | true | - |
| | vss:s__0002 | XDP | vsd:dst__0002 | Snapmirrored | | | |
| | | | | Idle | - | true | - |
| | vss:s__0003 | XDP | vsd:dst__0003 | Snapmirrored | | | |
| | | | | Idle | - | true | - |
| | vss:s__0004 | XDP | vsd:dst__0004 | Snapmirrored | | | |
| | | | | Idle | - | true | - |
| | vss:s__0005 | XDP | vsd:dst__0005 | Snapmirrored | | | |
| | | | | Idle | - | true | - |
| | vss:s__0006 | XDP | vsd:dst__0006 | Snapmirrored | | | |
| | | | | Idle | - | true | - |
| | vss:s__0007 | XDP | vsd:dst__0007 | Snapmirrored | | | |
| | | | | Idle | - | true | - |
| | vss:s__0008 | XDP | vsd:dst__0008 | Snapmirrored | | | |
| | | | | Idle | - | true | - |
| ... | | | | | | | |

El estado de la relación de SnapMirror de cada componente es Snapmirrored.

Invertir una relación de SnapMirror entre volúmenes de FlexGroup durante la recuperación de desastres

Cuando un desastre deshabilita el volumen de FlexGroup de origen de una relación de SnapMirror, se puede utilizar el volumen de FlexGroup de destino para servir los datos mientras se repara o se reemplaza el volumen de FlexGroup de origen. Una vez que el volumen FlexGroup de origen está en línea, se puede hacer que el volumen FlexGroup de origen original sea un destino de solo lectura e invertir la relación de SnapMirror.

Acerca de esta tarea

Todas las reglas de cuota activas en el volumen de destino se desactivan y las reglas de cuota se eliminan antes de realizar la resincronización.

Puede utilizar el `volume quota policy rule create` y `volume quota modify` comandos para crear y reactivar reglas de cuota una vez completada la operación de resincronización.

Pasos

1. En el volumen FlexGroup de destino original, quite la relación de mirroring de protección de datos entre el volumen FlexGroup de origen y el volumen FlexGroup de destino: `snapmirror delete -destination-path svm_name:volume_name`

```
cluster2::> snapmirror delete -destination-path vsd:dst
```

2. En el volumen FlexGroup de origen original, quite la información de relación del volumen FlexGroup de origen: `snapmirror release -destination-path svm_name:volume_name -relationship -info-only`

Después de eliminar una relación de SnapMirror, debe eliminar la información de relaciones del volumen FlexGroup de origen antes de intentar una operación de resincronización.

```
cluster1::> snapmirror release -destination-path vsd:dst -relationship  
-info-only true
```

3. En el nuevo volumen de FlexGroup de destino, cree la relación de mirroring: `snapmirror create -source-path src_svm_name:volume_name -destination-path dst_svm_name:volume_name -type XDP -policy MirrorAllSnapshots`

```
cluster1::> snapmirror create -source-path vsd:dst -destination-path  
vss:src -type XDP -policy MirrorAllSnapshots
```

4. En el nuevo volumen FlexGroup de destino, resincronice la FlexGroup de origen: `snapmirror resync -source-path svm_name:volume_name`

```
cluster1::> snapmirror resync -source-path vsd:dst
```

5. Supervisar las transferencias de SnapMirror: `snapmirror show -expand`

```
cluster2::> snapmirror show -expand
```

```
Progress
Source          Destination Mirror Relationship Total
Last
Path           Type Path           State Status           Progress Healthy
Updated
-----
-----
vsd:dst         XDP  vss:src         Snapmirrored
Idle           -           true -
vss:dst__0001 XDP  vss:src__0001 Snapmirrored
Idle           -           true -
vss:dst__0002 XDP  vss:src__0002 Snapmirrored
Idle           -           true -
vss:dst__0003 XDP  vss:src__0003 Snapmirrored
Idle           -           true -
vss:dst__0004 XDP  vss:src__0004 Snapmirrored
Idle           -           true -
vss:dst__0005 XDP  vss:src__0005 Snapmirrored
Idle           -           true -
vss:dst__0006 XDP  vss:src__0006 Snapmirrored
Idle           -           true -
vss:dst__0007 XDP  vss:src__0007 Snapmirrored
Idle           -           true -
vss:dst__0008 XDP  vss:src__0008 Snapmirrored
Idle           -           true -
...
```

El estado de la relación de SnapMirror de cada componente muestra como Snapmirrored esto indica que la resincronización se realizó correctamente.

Expanda FlexGroup Volumes en una relación de SnapMirror

Expanda FlexGroup Volumes en una relación de SnapMirror

A partir de ONTAP 9.3, puede ampliar el volumen de FlexGroup de origen y el volumen de FlexGroup de destino que estén en una relación de SnapMirror añadiendo nuevos componentes a los volúmenes. Los volúmenes de destino se pueden expandir de forma manual o automática.

Acerca de esta tarea

- Tras la ampliación, el número de componentes en el volumen FlexGroup de origen y el volumen FlexGroup de destino de una relación de SnapMirror debe coincidir.

Si el número de componentes de los volúmenes no coincide, las transferencias de SnapMirror fallan.

- No debe realizar ninguna operación de SnapMirror cuando esté en curso el proceso de ampliación.
- Si se produce un desastre antes de que se complete el proceso de ampliación, es necesario interrumpir la relación de SnapMirror y esperar hasta que la operación se complete correctamente.



Debe interrumpir la relación de SnapMirror cuando solo esté en curso el proceso de ampliación en caso de desastre. En el caso de un desastre, la operación de pausa puede tardar un tiempo en completarse. Debe esperar a que la operación de pausa se complete correctamente antes de realizar una operación de resincronización. Si la operación de interrupción falla, debe volver a intentar la operación de interrupción. Si se produce un error en la operación de interrupción, algunos de los componentes nuevos pueden permanecer en el volumen de FlexGroup de destino después de la operación de interrupción. Es mejor eliminar estos componentes manualmente antes de continuar.

Amplíe el volumen de FlexGroup de origen de una relación de SnapMirror

A partir de ONTAP 9.3, puede ampliar el volumen de FlexGroup de origen de una relación de SnapMirror, añadiendo nuevos componentes al volumen de origen. Es posible expandir el volumen de origen del mismo modo que se expande un volumen de FlexGroup normal (volumen de lectura y escritura).

Pasos

1. Expanda el volumen de FlexGroup de origen: `volume expand -vserver vs_server_name -volume fg_src -aggr-list aggregate name,... [-aggr-list-multiplier constituents_per_aggr]`

```
cluster1::> volume expand -volume src_fg -aggr-list aggr1 -aggr-list
-multiplier 2 -vserver vs_src
```

```
Warning: The following number of constituents of size 50GB will be added
to FlexGroup "src_fg": 2.
```

```
Expanding the FlexGroup will cause the state of all Snapshot copies to
be set to "partial".
```

```
Partial Snapshot copies cannot be restored.
```

```
Do you want to continue? {y|n}: Y
```

```
[Job 146] Job succeeded: Successful
```

El estado de todas las copias Snapshot que se realizan antes de que el volumen se expanda a parcialmente.

Amplíe el volumen de FlexGroup de destino de una relación de SnapMirror

Puede ampliar el volumen de destino de FlexGroup y restablecer la relación de SnapMirror de forma automática o manual. De forma predeterminada, la relación de SnapMirror se establece para la expansión automática y el volumen de FlexGroup de destino se amplía automáticamente si el volumen de origen se amplía.

Lo que necesitará

- El volumen FlexGroup de origen se debe haber expandido.
- La relación de SnapMirror debe estar en SnapMirrored estado.

La relación de SnapMirror no debe romperse ni eliminarse.

Acerca de esta tarea

- Cuando se crea el volumen FlexGroup de destino, se configura el volumen para la expansión automática de forma predeterminada.

Puede modificar el volumen de destino de FlexGroup para la expansión manual, si es necesario.



La práctica recomendada es ampliar el volumen de FlexGroup de destino automáticamente.

- Todas las operaciones de SnapMirror producen errores hasta que el volumen de FlexGroup de origen y el volumen de FlexGroup de destino se hayan ampliado y tengan el mismo número de componentes.
- Si expande el volumen de FlexGroup de destino después de romper o eliminar la relación de SnapMirror, no puede volver a sincronizar la relación original.

Si piensa reutilizar el volumen de FlexGroup de destino, no deberá expandir el volumen después de eliminar la relación de SnapMirror.

Opciones

- Realice una transferencia de actualización para expandir automáticamente el volumen de FlexGroup de destino:
 - a. Realice una transferencia de actualización de SnapMirror: `snapmirror update -destination -path svm:vol_name`
 - b. Compruebe que el estado de la relación de SnapMirror sea en la SnapMirrored provincia: `snapmirror show`

```
cluster2::> snapmirror show
```

```
Progress
```

| Source | Destination | Mirror | Relationship | Total |
|---------|-------------|--------|--------------|----------|
| Last | | | | |
| Path | Type | Path | State | Status |
| Healthy | Updated | | | Progress |

```
-----
```

| | | | | |
|---------------|-----|---------------|--------------|------|
| vs_src:src_fg | | vs_dst:dst_fg | | |
| | XDP | | Snapmirrored | |
| | | | Idle | - |
| - | | | | true |

En función del tamaño y la disponibilidad de los agregados, los agregados se seleccionan automáticamente, y los nuevos componentes que coincidan con los constituyentes del volumen de

FlexGroup de origen se añadirán al volumen de FlexGroup de destino. Después de la ampliación, se activa automáticamente una operación de resincronización.

- Expanda el volumen de FlexGroup de destino manualmente:
 - a. Si la relación de SnapMirror se encuentra en el modo de expansión automática, establezca la relación de SnapMirror con el modo de expansión manual: `snapmirror modify -destination-path svm:vol_name -is-auto-expand-enabled false`

```
cluster2::> snapmirror modify -destination-path vs_dst:dst_fg -is
-auto-expand-enabled false
Operation succeeded: snapmirror modify for the relationship with
destination "vs_dst:dst_fg".
```

- b. Desactive la relación de SnapMirror: `snapmirror quiesce -destination-path svm:vol_name`

```
cluster2::> snapmirror quiesce -destination-path vs_dst:dst_fg
Operation succeeded: snapmirror quiesce for destination
"vs_dst:dst_fg".
```

- c. Expanda el volumen de FlexGroup de destino: `volume expand -vserver vs_server_name -volume fg_name -aggr-list aggregate name,... [-aggr-list-multiplier constituents_per_aggr]`

```
cluster2::> volume expand -volume dst_fg -aggr-list aggr1 -aggr-list
-multiplier 2 -vserver vs_dst

Warning: The following number of constituents of size 50GB will be
added to FlexGroup "dst_fg": 2.
Do you want to continue? {y|n}: y
[Job 68] Job succeeded: Successful
```

- d. Resincronice la relación de SnapMirror: `snapmirror resync -destination-path svm:vol_name`

```
cluster2::> snapmirror resync -destination-path vs_dst:dst_fg
Operation is queued: snapmirror resync to destination
"vs_dst:dst_fg".
```

- e. Compruebe que el estado de la relación de SnapMirror sea SnapMirrored: `snapmirror show`


```
cluster2::> snapmirror show
```

| Progress | Source | Destination | Mirror | Relationship | Total |
|---------------|---------|---------------|--------|--------------|----------|
| Last | Path | Type | Path | State | Status |
| Healthy | Updated | | | | Progress |
| ----- | ----- | ----- | ----- | ----- | ----- |
| ----- | ----- | | | | |
| vs_src:src_fg | XDP | vs_dst:dst_fg | | Snapmirrored | |
| | | | | Idle | - |
| - | | | | | true |

Restaurar un único archivo de SnapMirror desde un volumen de FlexGroup

A partir de ONTAP 9.8, puede restaurar un solo archivo desde un almacén de SnapMirror de FlexGroup o desde un destino UDP.

Acerca de esta tarea

- Puede restaurar desde un volumen FlexGroup de cualquier geometría a un volumen FlexGroup de cualquier geometría
- Solo se admite un archivo por operación de restauración
- Es posible restaurar el volumen de FlexGroup de origen original o uno nuevo de FlexGroup
- No se admite la búsqueda de archivos cercados remotos.

Se produce un error en la restauración de un archivo único si el archivo de origen está vallado.

- Puede reiniciar o limpiar una restauración de archivo único anulada
- Debe limpiar una transferencia fallida de restauración de archivos individuales mediante el `clean-up-failure` opción de `snapmirror restore` comando
- Se admite la ampliación de volúmenes de FlexGroup cuando hay una restauración de archivos individuales de FlexGroup en curso o en un estado anulado

Pasos

1. Restaure un archivo desde un volumen de FlexGroup: `snapmirror restore -destination-path destination_path -source-path source_path -file-list /f1 -throttle throttle -source-snapshot snapshot`

Lo siguiente es un ejemplo de una operación de restauración de archivos individuales de volúmenes de FlexGroup.

```
vserverA::> snapmirror restore -destination-path vs0:fg2 -source-path vs0:fgd -file-list /f1 -throttle 5 -source-snapshot snapmirror.81072cel-
```

d57b-11e9-94c0-005056a7e422_2159190496.2019-09-19_062631

[Job 135] Job is queued: snapmirror restore from source "vs0:fgd" for the snapshot snapmirror.81072ce1-d57b-11e9-94c0-005056a7e422_2159190496.2019-09-19_062631.

vserverA::> snapmirror show

| Source | | Destination | Mirror | Relationship | |
|---------|----------------|-------------|--------|--------------|--------------|
| Total | Last | | | | |
| Path | Type | Path | State | Status | Progress |
| Healthy | Updated | | | | |
| ----- | ---- | ----- | ----- | ----- | ----- |
| ----- | ----- | ----- | ----- | | |
| vs0:v1d | RST | vs0:v2 | - | Transferring | Idle 83.12KB |
| true | 09/19 11:38:42 | | | | |

vserverA::*> snapmirror show vs0:fg2

Source Path: vs0:fgd
Source Cluster: -
Source Vserver: vs0
Source Volume: fgd
Destination Path: vs0:fg2
Destination Cluster: -
Destination Vserver: vs0
Destination Volume: fg2
Relationship Type: RST
Relationship Group Type: none
Managing Vserver: vs0
SnapMirror Schedule: -
SnapMirror Policy Type: -
SnapMirror Policy: -
Tries Limit: -
Throttle (KB/sec): unlimited
Current Transfer Throttle (KB/sec): 2
Mirror State: -
Relationship Status: Transferring
File Restore File Count: 1
File Restore File List: f1
Transfer Snapshot: snapmirror.81072ce1-d57b-11e9-94c0-005056a7e422_2159190496.2019-09-19_062631
Snapshot Progress: 2.87MB
Total Progress: 2.87MB
Network Compression Ratio: 1:1
Snapshot Checkpoint: 2.97KB
Newest Snapshot: -
Newest Snapshot Timestamp: -

```
Exported Snapshot: -
Exported Snapshot Timestamp: -
Healthy: true
Physical Replica: -
Relationship ID: e6081667-dacb-11e9-94c0-005056a7e422
Source Vserver UUID: 81072ce1-d57b-11e9-94c0-005056a7e422
Destination Vserver UUID: 81072ce1-d57b-11e9-94c0-005056a7e422
Current Operation ID: 138f12e6-dacc-11e9-94c0-005056a7e422
Transfer Type: cg_file_restore
Transfer Error: -
Last Transfer Type: -
Last Transfer Error: -
Last Transfer Error Codes: -
Last Transfer Size: -
Last Transfer Network Compression Ratio: -
Last Transfer Duration: -
Last Transfer From: -
Last Transfer End Timestamp: -
Unhealthy Reason: -
Progress Last Updated: 09/19 07:07:36
Relationship Capability: 8.2 and above
Lag Time: -
Current Transfer Priority: normal
SMTape Operation: -
Constituent Relationship: false
Destination Volume Node Name: vserverA
Identity Preserve Vserver DR: -
Number of Successful Updates: 0
Number of Failed Updates: 0
Number of Successful Resyncs: 0
Number of Failed Resyncs: 0
Number of Successful Breaks: 0
Number of Failed Breaks: 0
Total Transfer Bytes: 0
Total Transfer Time in Seconds: 0
Source Volume MSIDs Preserved: -
OpMask: ffffffffffffffff
Is Auto Expand Enabled: -
Source Endpoint UUID: -
Destination Endpoint UUID: -
Is Catalog Enabled: false
```

Restaurar un volumen de FlexGroup a partir de un backup de SnapVault

Es posible realizar una operación de restauración de volumen completo de volúmenes de

FlexGroup desde una copia Snapshot en el volumen secundario de SnapVault. Es posible restaurar el volumen de FlexGroup en el volumen de origen original o en un volumen de FlexGroup nuevo.

Antes de empezar

Debe tener en cuenta determinadas consideraciones cuando se restaura desde backups de SnapVault para volúmenes de FlexGroup.

- Solo se admite una restauración básica con copias Snapshot parciales desde un backup de SnapVault. El número de componentes del volumen de destino debe coincidir con el número de componentes del volumen de origen cuando se tomó la copia Snapshot.
- Si se produce un error en una operación de restauración, no se permiten otras operaciones hasta que se completa la operación de restauración. Puede volver a intentar la operación de restauración o ejecutar la operación de restauración con el `cleanup` parámetro.
- Un volumen FlexGroup puede ser el volumen de origen de una sola relación de backup o restauración. Un volumen de FlexGroup no puede ser el origen de dos relaciones de SnapVault, dos relaciones de restauración o una relación de SnapVault y una relación de restauración.
- Las operaciones de backup y restauración de SnapVault no se pueden ejecutar en paralelo. Cuando hay una operación de restauración básica o una operación de restauración incremental en curso, debe desactivar las operaciones de backup.
- Debe cancelar una operación de restauración de una copia Snapshot parcial del volumen de FlexGroup de destino. No se puede cancelar la operación de restauración de una copia Snapshot parcial desde el volumen de origen.
- Si se cancela una operación de restauración, se debe reiniciar la operación de restauración con la misma copia Snapshot que se utilizó para la operación de restauración anterior.

Acerca de esta tarea

Todas las reglas de cuota activas en el volumen de FlexGroup de destino se desactivan antes de que se realice la restauración.

Puede utilizar el `volume quota modify` comando para reactivar las reglas de cuota una vez completada la operación de restauración.

Pasos

1. Restaure el volumen de FlexGroup: `snapmirror restore -source-path src_svm:src_flexgroup -destination-path dest_svm:dest_flexgroup -snapshot snapshot_name`
`snapshot_name` Es la copia Snapshot que se va a restaurar del volumen de origen al volumen de destino. Si no se especifica la copia de Snapshot, el volumen de destino se restaura de la copia de Snapshot más reciente.

```
vserverA::> snapmirror restore -source-path vserverB:dstFG -destination
-path vserverA:newFG -snapshot daily.2016-07-15_0010
Warning: This is a disruptive operation and the volume vserverA:newFG
will be read-only until the operation completes
Do you want to continue? {y|n}: y
```

Deshabilite la protección de SVM en un volumen de FlexGroup

Cuando la Marca SVM DR se establece en `protected` En un volumen FlexGroup, puede configurar el indicador como desprotegido para deshabilitar la recuperación ante desastres de SVM `protection` En un volumen de FlexGroup.

Lo que necesitará

- La relación de recuperación ante desastres de SVM entre el volumen primario y el secundario está en buen estado.
- El parámetro de protección DR de SVM se ha establecido en `protected`.

Pasos

1. Deshabilite la protección mediante `volume modify` comando para cambiar el `vserver-dr-protection` Parámetro del volumen de FlexGroup a. `unprotected`.

```
cluster2::> volume modify -vserver vs1 -volume fg_src -vserver-dr
-protection unprotected
[Job 5384] Job is queued: Modify fg_src.
[Job 5384] Steps completed: 4 of 4.
cluster2::>
```

2. Actualice la SVM en el sitio secundario: `snapmirror update -destination-path destination_svm_name: -source-path Source_svm_name:`
3. Compruebe que la relación de SnapMirror funciona correctamente: `snapmirror show`
4. Compruebe que la relación de SnapMirror de FlexGroup se ha eliminado: `snapmirror show -expand`

Habilite la protección de SVM en un volumen de FlexGroup

Cuando la Marca de protección de recuperación ante desastres de SVM se establece en `unprotected` En un volumen FlexGroup, puede establecer el indicador como `protected` Para habilitar la protección de recuperación ante desastres de SVM.

Lo que necesitará

- La relación de recuperación ante desastres de SVM entre el volumen primario y el secundario está en buen estado.
- El parámetro de protección DR de SVM se ha establecido en `unprotected`.

Pasos

1. Habilite la protección mediante `volume modify` para cambiar la `vserver-dr-protection` Parámetro del volumen de FlexGroup a. `protected`.

```
cluster2::> volume modify -vserver vs1 -volume fg_src -vserver-dr
-protection protected
[Job 5384] Job is queued: Modify fg_src.
[Job 5384] Steps completed: 4 of 4.
cluster2::>
```

2. Actualice la SVM en el sitio secundario: `snapmirror update -destination-path destination_svm_name -source-path source_svm_name`

```
snapmirror update -destination-path vs1_dst: -source-path vs1:
```

3. Compruebe que la relación de SnapMirror funciona correctamente: `snapmirror show`

```
cluster2::> snapmirror show
```

| Progress | | Destination Mirror | | Relationship | Total | | |
|----------|------|--------------------|--------------|--------------|-------|----------|---------|
| Source | | | | | | | |
| Last | | | | | | | |
| Path | Type | Path | State | Status | | Progress | Healthy |
| Updated | | | | | | | |
| ----- | ---- | ----- | ----- | ----- | | ----- | ----- |
| ----- | | | | | | | |
| vs1: | XDP | vs1_dst: | Snapmirrored | | | | |
| | | | Idle | | | - | true - |

4. Compruebe que la relación de SnapMirror de FlexGroup es correcta: `snapmirror show -expand`

```
cluster2::> snapmirror show -expand
```

| Progress | Source | Destination | Mirror | Relationship | Total | | |
|----------|------------------|-------------|----------------------|--------------|--------|----------|---------|
| Last | Path | Type | Path | State | Status | Progress | Healthy |
| Updated | | | | | | | |
| ----- | ---- | ----- | ----- | ----- | ----- | ----- | ----- |
| | vs1: | XDP | vs1_dst: | Snapmirrored | | | |
| | | | | Idle | | - | true - |
| | vs1:fg_src | XDP | vs1_dst:fg_src | Snapmirrored | | | |
| | | | | Idle | | - | true - |
| | vs1:fg_src__0001 | | | | | | |
| | | XDP | vs1_dst:fg_src__0001 | Snapmirrored | | | |
| | | | | Idle | | - | true - |
| | vs1:fg_src__0002 | | | | | | |
| | | XDP | vs1_dst:fg_src__0002 | Snapmirrored | | | |
| | | | | Idle | | - | true - |
| | vs1:fg_src__0003 | | | | | | |
| | | XDP | vs1_dst:fg_src__0003 | Snapmirrored | | | |
| | | | | Idle | | - | true - |
| | vs1:fg_src__0004 | | | | | | |
| | | XDP | vs1_dst:fg_src__0004 | Snapmirrored | | | |
| | | | | Idle | | - | true - |

6 entries were displayed.

Convertir volúmenes de FlexVol en volúmenes de FlexGroup

Información general sobre cómo convertir volúmenes de FlexVol en volúmenes de FlexGroup

Si desea expandir un volumen de FlexVol más allá del límite de espacio, puede convertir el volumen de FlexVol en un volumen de FlexGroup. A partir de ONTAP 9.7, se pueden convertir los volúmenes FlexVol o FlexVol independientes que estén en una relación de SnapMirror con los volúmenes FlexGroup.

Consideraciones sobre la conversión de volúmenes de FlexVol en volúmenes de FlexGroup

Es necesario conocer las funciones y las operaciones que se admiten antes de decidir convertir volúmenes FlexVol en volúmenes FlexGroup.

A partir de ONTAP 9.13.1, la protección autónoma contra ransomware puede permanecer habilitada durante las conversiones. Si la protección está activa, el FlexVol original se convertirá en el componente raíz FlexGroup tras la conversión. Si la protección está inactiva, se creará una nueva FlexGroup durante la conversión y la FlexVol original asumirá el rol de componente raíz.

Operaciones no admitidas durante la conversión

No se permiten las siguientes operaciones cuando la conversión del volumen está en curso:

- Movimiento de volúmenes
- Autobalancia agregada
- Reubicación de agregados
- Toma de control y retorno al nodo primario planificadas en una configuración de alta disponibilidad
- Restauración manual y automática en una configuración de alta disponibilidad
- Actualización y reversión del clúster
- Separación de volúmenes FlexClone
- Realojamiento de volúmenes
- Modificación del volumen y ajuste de tamaño automático
- Cambio de nombre del volumen
- Asociar un almacén de objetos a un agregado
- Conmutación de sitios negociada en la configuración de MetroCluster
- Operaciones de SnapMirror
- Restaurar de una copia Snapshot
- Operaciones de cuota
- Operaciones de eficiencia del almacenamiento

Se pueden realizar estas operaciones en el volumen FlexGroup después de realizar correctamente la conversión.

Configuraciones que no se admiten con volúmenes de FlexGroup

- Volumen sin conexión o restringido
- Volumen raíz de SVM
- SAN
- SMB 1,0
- Espacios de nombres de NVMe
- Servicio de copia de volúmenes redundantes (VSS) remoto

Convertir un volumen de FlexVol en un volumen de FlexGroup

A partir de ONTAP 9.7, se puede realizar una conversión sin movimiento de un volumen FlexVol a un volumen FlexGroup sin necesidad de una copia de datos ni de espacio en disco adicional.

Lo que necesitará

- Los volúmenes en transición se pueden convertir a volúmenes FlexGroup a partir de ONTAP 9.8. Si va a convertir un volumen que ha realizado la transición a FlexGroup, consulte el artículo de la base de conocimientos ["Cómo convertir un FlexVol en FlexGroup que se ha realizado la transición"](#) si quiere más información.
- El volumen FlexVol que se está convirtiendo debe estar en línea.
- Las operaciones y configuraciones del volumen FlexVol deben ser compatibles con el proceso de conversión.

Se genera un mensaje de error si el volumen FlexVol tiene alguna incompatibilidad y se anula la conversión de volumen. Puede tomar acciones correctivas y volver a intentar la conversión.

- Si un volumen FlexVol es muy grande (por ejemplo, de 80 a 100 TB) y muy completo (de 80 a 100 %), debe copiar los datos en lugar de convertirlos.



La conversión de un volumen FlexGroup de gran tamaño provoca un componente de volumen FlexGroup muy completo, que puede provocar problemas de rendimiento. Para obtener más información, consulte la sección titulada "Cuándo no crear un volumen de FlexGroup" en el informe técnico TR ["FlexGroup Volumes: Guía de prácticas recomendadas y de implementación"](#).

Pasos

1. Compruebe que el volumen FlexVol esté en línea: `volume show vol_name -volume-style -extended, state`

```
cluster-1::> volume show my_volume -fields volume-style-extended, state
vserver volume      state  volume-style-extended
-----
vs0      my_volume online flexvol
```

2. Compruebe si el volumen FlexVol se puede convertir sin problemas:

- a. Inicie sesión en el modo de privilegio avanzado: `set -privilege advanced`
- b. Compruebe el proceso de conversión: `volume conversion start -vserver vs1 -volume flexvol -check-only true`

Debe rectificar todos los errores antes de convertir el volumen.



No se puede volver a convertir un volumen de FlexGroup en un volumen de FlexVol.

3. Inicie la conversión: `volume conversion start -vserver svm_name -volume vol_name`

```
cluster-1::*> volume conversion start -vserver vs0 -volume my_volume

Warning: Converting flexible volume "my_volume" in Vserver "vs0" to a
FlexGroup
        will cause the state of all Snapshot copies from the volume to
be set
        to "pre-conversion". Pre-conversion Snapshot copies cannot be
        restored.
Do you want to continue? {y|n}: y
[Job 57] Job succeeded: success
```

4. Compruebe que la conversión se ha realizado correctamente: `volume show vol_name -fields -volume-style-extended,state`

```
cluster-1::*> volume show my_volume -fields volume-style-extended,state
vserver volume      state  volume-style-extended
-----
vs0      my_volume online flexgroup
```

Resultados

El volumen FlexVol se convierte en un volumen FlexGroup miembro único.

Después de terminar

Puede expandir el volumen de FlexGroup según sea necesario.

Convertir una relación de SnapMirror para volúmenes de FlexVol en una relación de SnapMirror para volúmenes de FlexGroup

Para convertir una relación de SnapMirror para volúmenes de FlexVol en una relación de SnapMirror para volúmenes de FlexGroup en ONTAP, primero se debe convertir el volumen de FlexVol de destino seguido del volumen de FlexVol de origen.

Acerca de esta tarea

- La conversión de FlexGroup solo se admite para relaciones de SnapMirror asíncronas.
- El tiempo de conversión depende de varias variables. Algunas de las variables incluyen:
 - CPU del controlador
 - Utilización de CPU por parte de otras aplicaciones
 - Cantidad de datos en la copia Snapshot inicial
 - Ancho de banda de red
 - Ancho de banda utilizado por otras aplicaciones

Antes de empezar

- El volumen FlexVol que se está convirtiendo debe estar en línea.

- El volumen de FlexVol de origen de la relación de SnapMirror no debe ser el volumen de origen de varias relaciones de SnapMirror.

A partir de ONTAP 9.9.1, se admiten las relaciones SnapMirror con fanout para los volúmenes FlexGroup. Para obtener más información, consulte ["Consideraciones que tener en cuenta para crear relaciones de SnapMirror en cascada y fanout para FlexGroups"](#).

- Las operaciones y configuraciones del volumen FlexVol deben ser compatibles con el proceso de conversión.

Se genera un mensaje de error si el volumen FlexVol tiene alguna incompatibilidad y se anula la conversión de volumen. Puede tomar acciones correctivas y volver a intentar la conversión.

Pasos

1. Compruebe que la relación de SnapMirror funciona correctamente:

```
snapmirror show
```

Sólo se pueden convertir relaciones de réplica de tipo XDP.

Ejemplo:

```
cluster2::> snapmirror show
```

| Progress | Source | Destination | Mirror | Relationship | Total | | |
|----------|-------------|-------------|-------------|--------------|--------|----------|---------|
| Last | Path | Type | Path | State | Status | Progress | Healthy |
| Updated | | | | | | | |
| ----- | ----- | ----- | ----- | ----- | ----- | ----- | ----- |
| ----- | vs0:src_dp | DP | vs2:dst_dp | Snapmirrored | | | |
| | | | | Idle | - | true | - |
| | vs0:src_xdp | XDP | vs2:dst_xdp | Snapmirrored | | | |
| | | | | Idle | - | true | - |

2. Compruebe si el volumen de origen es compatible para la conversión:

- a. Inicie sesión en el modo de privilegio avanzado:

```
set -privilege advanced
```

- b. Compruebe el proceso de conversión:

```
volume conversion start -vserver <src_svm_name> -volume <src_vol>
-check-only true
```

Ejemplo:

```
volume conversion start -vserver vs1 -volume src_vol -check-only true
```

+

Debe rectificar todos los errores antes de convertir el volumen.

3. Convierta el volumen de destino de FlexVol al volumen de FlexGroup.

a. Desactive la relación de SnapMirror de FlexVol:

```
snapmirror quiesce -destination-path <dest_svm:dest_volume>
```

Ejemplo:

```
cluster2::> snapmirror quiesce -destination-path vs2:dst_xdp
```

b. Inicie la conversión:

```
volume conversion start -vserver <dest_svm> -volume <dest_volume>
```

Ejemplo:

```
cluster-1::> volume conversion start -vserver vs2 -volume dst_xdp
```

Warning: After the volume is converted to a FlexGroup, it will not be possible

to change it back to a flexible volume.

Do you want to continue? {y|n}: y

[Job 510] Job succeeded: SnapMirror destination volume "dst_xdp" has been successfully converted to a FlexGroup volume.

You must now convert the relationship's source volume, "vs0:src_xdp", to a FlexGroup.

Then, re-establish the SnapMirror relationship using the "snapmirror resync" command.

4. Convierta el volumen FlexVol de origen a FlexGroup volume: `

```
volume conversion start -vserver <src_svm_name> -volume <src_vol_name>
```

Ejemplo:

```
cluster-1::> volume conversion start -vserver vs0 -volume src_xdp

Warning: Converting flexible volume "src_xdp" in Vserver "vs0" to a
FlexGroup
        will cause the state of all Snapshot copies from the volume to
be set
        to "pre-conversion". Pre-conversion Snapshot copies cannot be
        restored.
Do you want to continue? {y|n}: y
[Job 57] Job succeeded: success
```

5. Volver a sincronizar la relación:

```
snapmirror resync -destination-path dest_svm_name:dest_volume
```

Ejemplo:

```
cluster2::> snapmirror resync -destination-path vs2:dst_xdp
```

Después de terminar

Debe asegurarse de que, cuando el volumen FlexGroup de origen se expanda para incluir más componentes, el volumen de destino también se expanda.

Gestión de volúmenes de FlexCache

Información general de FlexCache

La tecnología NetApp FlexCache acelera el acceso a datos, reduce la latencia WAN y los costes de ancho de banda WAN para las cargas de trabajo de lectura intensiva, especialmente cuando los clientes necesitan acceder a los mismos datos repetidamente. Cuando se crea un volumen FlexCache, se crea una caché remota de un volumen ya existente (de origen) que solo contiene los datos a los que se accede activamente (datos activos) del volumen de origen.

Cuando un volumen FlexCache recibe una solicitud de lectura de los datos activos que contiene, puede responder más rápido que el volumen de origen, ya que no es necesario desplazarse tan lejos para llegar al cliente. Si un volumen de FlexCache recibe una solicitud de lectura de datos leídos de forma infrecuente (datos fríos), recupera los datos necesarios del volumen de origen y, a continuación, almacena los datos antes de servir la solicitud del cliente. Las solicitudes posteriores de lectura para esos datos se proporcionan

directamente desde el volumen FlexCache. Después de la primera solicitud, los datos ya no necesitan viajar a través de la red ni ser servidos desde un sistema con mucha carga. Por ejemplo, supongamos que está experimentando cuellos de botella en el clúster en un punto de acceso único para los datos solicitados con frecuencia. Puede utilizar volúmenes de FlexCache dentro del clúster para proporcionar varios puntos de montaje a los datos activos, por lo que se reducen los cuellos de botella y se aumenta el rendimiento. Como otro ejemplo, suponga que es necesario reducir el tráfico de red a un volumen al que se accede desde varios clústeres. Puede usar volúmenes de FlexCache para distribuir datos activos del volumen de origen a través de los clústeres dentro de la red. Esto reduce el tráfico WAN al proporcionar a los usuarios puntos de acceso más cercanos.

También puede usar la tecnología FlexCache para mejorar el rendimiento en entornos de cloud y cloud híbrido. Un volumen FlexCache puede ayudarle a trasladar cargas de trabajo al cloud híbrido mediante el almacenamiento en caché de los datos de un centro de datos local al cloud. También puede usar volúmenes de FlexCache para quitar silos de cloud mediante el almacenamiento en caché de los datos de un proveedor de cloud a otro o entre dos regiones del mismo proveedor de cloud.

A partir de ONTAP 9.10.1, usted puede ["activar bloqueo de archivos global"](#) En todos los volúmenes de FlexCache. El bloqueo global de archivos impide que un usuario acceda a un archivo que ya está abierto por otro usuario. A continuación, las actualizaciones del volumen de origen se distribuyen a todos los volúmenes de FlexCache de forma simultánea.

A partir de ONTAP 9.9.1, los volúmenes FlexCache mantienen una lista de archivos que no se encontraron. Esto ayuda a reducir el tráfico de red eliminando la necesidad de enviar varias llamadas al origen cuando los clientes buscan archivos que no existen.

Una lista de adicionales ["Funciones compatibles con volúmenes FlexCache y sus volúmenes de origen"](#), Incluyendo una lista de protocolos soportados por la versión ONTAP, también está disponible.

Puede obtener más información acerca de la arquitectura de la tecnología ONTAP FlexCache en ["TR-4743: FlexCache en ONTAP"](#).

Vídeos

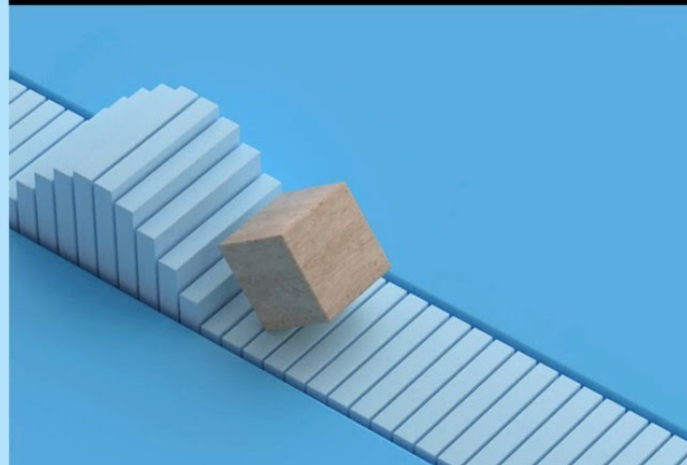
Cómo puede FlexCache reducir la latencia de WAN y los tiempos de lectura de los datos globales

ONTAP FlexCache

Data Access Where You Need It

Use Case

© 2020 NetApp, Inc. All rights reserved.



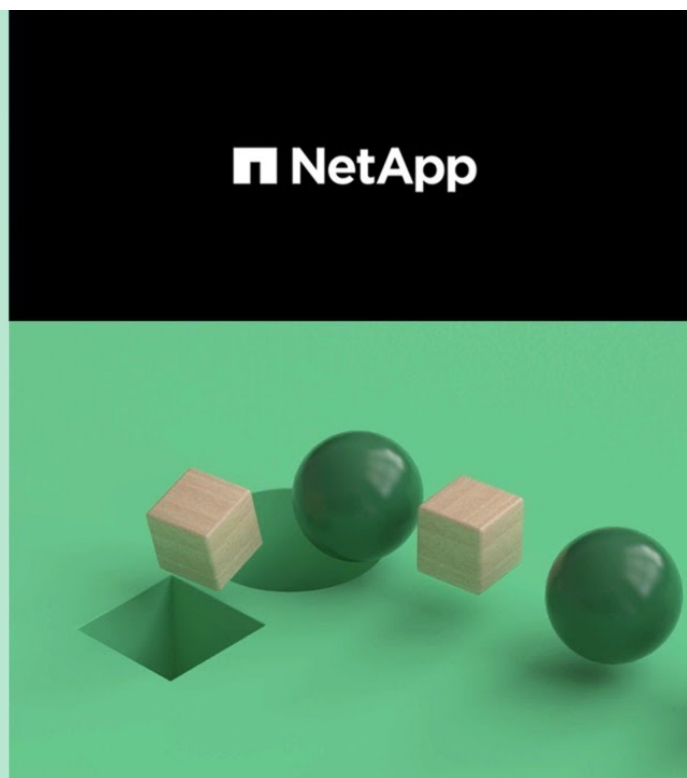
Conozca las ventajas en términos de rendimiento de ONTAP FlexCache.

ONTAP FlexCache

Data Access Where You Need It

Tech Clip

© 2020 NetApp, Inc. All rights reserved.



Funciones compatibles y no compatibles para volúmenes de FlexCache

A partir de ONTAP 9,5, se pueden configurar volúmenes de FlexCache. Los volúmenes FlexVol se admiten como volúmenes de origen, y los volúmenes FlexGroup se admiten como volúmenes FlexCache. A partir de ONTAP 9,7, tanto el volumen FlexVol como los

volúmenes FlexGroup se admiten como volúmenes de origen. Las funciones y los protocolos admitidos para el volumen de origen y el volumen FlexCache varían.

Protocolos compatibles

| Protocolo | ¿Admitido en el volumen de origen? | ¿Compatible con el volumen FlexCache? |
|-----------|---|---|
| NFSv3 | Sí | Sí |
| NFSv4 | Sí Para acceder a los volúmenes de caché que usan el protocolo NFSv4.x, tanto los clústeres de origen como los de caché deben usar ONTAP 9.10.1 o una versión posterior. El clúster de origen y el clúster FlexCache pueden tener versiones de ONTAP diferentes, pero ambas deben ser ONTAP 9.10.1 y versiones posteriores. Por ejemplo, el origen puede tener ONTAP 9.10.1 y la caché puede tener ONTAP 9.11.1. | Sí Compatible a partir de ONTAP 9.10.1. Para acceder a los volúmenes de caché que usan el protocolo NFSv4.x, tanto los clústeres de origen como los de caché deben usar ONTAP 9.10.1 o una versión posterior. El clúster de origen y el clúster FlexCache pueden tener versiones de ONTAP diferentes, pero ambas deben ser ONTAP 9.10.1 y versiones posteriores. Por ejemplo, el origen puede tener ONTAP 9.10.1 y la caché puede tener ONTAP 9.11.1. |
| NFSv4,2 | Sí | No |
| SMB | Sí | Sí Compatible a partir de ONTAP 9.8. |

Funciones admitidas

| Función | ¿Admitido en el volumen de origen? | ¿Compatible con el volumen FlexCache? |
|---------------------------------------|---|---------------------------------------|
| Protección autónoma contra ransomware | Sí Para los volúmenes de origen de FlexVol que comienzan con ONTAP 9.10.1, no se admiten los volúmenes de origen de FlexGroup. | No |

| | | |
|---------------------|--|--|
| Antivirus | <p>Sí</p> <p>Compatible a partir de ONTAP 9,7.</p> | <p>No aplicable</p> <p>Si configura el análisis antivirus en el origen, no es necesario en la caché. El análisis antivirus de origen detecta archivos infectados por virus antes de que se realicen las escrituras, independientemente del origen de escritura. Para obtener más información sobre el uso de análisis antivirus con FlexCache, consulte la "Informe técnico de FlexCache con ONTAP".</p> |
| Auditoría | <p>Sí</p> <p>Compatible a partir de ONTAP 9,7. Puede auditar los eventos de acceso a archivos NFS en las relaciones de FlexCache mediante la auditoría nativa de ONTAP. Para obtener más información, consulte Consideraciones para auditar volúmenes de FlexCache</p> | <p>Sí</p> <p>Compatible a partir de ONTAP 9,7. Puede auditar los eventos de acceso a archivos NFS en las relaciones de FlexCache mediante la auditoría nativa de ONTAP. Para obtener más información, consulte Consideraciones para auditar volúmenes de FlexCache</p> |
| Cloud Volumes ONTAP | <p>Sí</p> <p>Compatible a partir de ONTAP 9,6</p> | <p>Sí</p> <p>Compatible a partir de ONTAP 9,6</p> |
| Compactación | <p>Sí</p> <p>Compatible a partir de ONTAP 9,6</p> | <p>Sí</p> <p>Compatible a partir de ONTAP 9.7</p> |
| Compresión | <p>Sí</p> <p>Compatible a partir de ONTAP 9,6</p> | <p>Sí</p> <p>Compatible a partir de ONTAP 9,6</p> |
| Deduplicación | <p>Sí</p> | <p>Sí</p> <p>Los volúmenes FlexCache son compatibles con la deduplicación en línea desde ONTAP 9.6. La deduplicación entre volúmenes se admite en volúmenes FlexCache que comienzan con ONTAP 9.7.</p> |
| FabricPool | <p>Sí</p> | <p>Sí</p> <p>Compatible a partir de ONTAP 9.7</p> |

| | | |
|---|---|---|
| DR de FlexCache | Sí | Sí Compatible desde ONTAP 9.9.1, con protocolo NFSv3, solo. Los volúmenes de FlexCache deben estar en SVM independientes o en clústeres separados. |
| Volumen FlexGroup | Sí Compatible a partir de ONTAP 9.7 | Sí |
| Volumen FlexVol | Sí | No |
| FPolicy | Sí Compatible a partir de ONTAP 9.7 | Sí Compatible con NFS desde ONTAP 9.7. Compatible con el bloque de mensajes del servidor que empieza con ONTAP 9.14.1. |
| Configuración de MetroCluster | Sí Compatible a partir de ONTAP 9.7 | Sí Compatible a partir de ONTAP 9.7 |
| Transferencia de datos descargados (ODX) de Microsoft | Sí | No |
| Cifrado de agregados de NetApp (NAE) | Sí Compatible a partir de ONTAP 9,6 | Sí Compatible a partir de ONTAP 9,6 |
| Cifrado de volúmenes de NetApp (NVE) | Sí Compatible a partir de ONTAP 9,6 | Sí Compatible a partir de ONTAP 9,6 |
| Bloque NAS de ONTAP S3 | Sí Compatible a partir de ONTAP 9.12.1 | No |

| | | |
|--------------------------------------|---|---|
| Calidad de servicio | Sí | <p>Sí</p> <div>  <p>La calidad de servicio en el nivel de archivo no se admite para los volúmenes FlexCache.</p> </div> |
| Qtrees | <p>Sí</p> <p>A partir de ONTAP 9,6, se pueden crear y modificar qtrees. Los qtrees creados en el origen pueden accederse en la caché.</p> | No |
| Cuotas | <p>Sí</p> <p>A partir de ONTAP 9,6, la aplicación de cuotas de los volúmenes de origen FlexCache se admite para usuarios y grupos.</p> | <p>No</p> <p>En el modo de escritura FlexCache (el modo predeterminado), las escrituras en la caché se reenvían al volumen de origen. Las cuotas se aplican en el origen.</p> <div>  <p>A partir de ONTAP 9.6, se admite la cuota remota (rquota) en los volúmenes FlexCache.</p> </div> |
| Notificación de cambio de SMB | Sí | <p>Sí</p> <p>A partir de ONTAP 9.14.1, Notificar cambios de SMB es compatible en la caché.</p> |
| Volúmenes de SnapLock | No | No |
| Relaciones asíncronas de SnapMirror* | Sí | No |

| | | |
|--|--|--|
| | <p>*Orígenes de FlexCache:</p> <ul style="list-style-type: none"> • Es posible tener un volumen de FlexCache a partir de un FlexVol de origen • Es posible tener un volumen de FlexCache a partir de un FlexGroup de origen • Puede tener un volumen de FlexCache desde un volumen primario de origen en una relación de SnapMirror. • A partir de ONTAP 9.8, un volumen secundario de SnapMirror puede ser un volumen de origen de FlexCache. | Relaciones de SnapMirror Synchronous |
| No | No | SnapRestore |
| Sí | No | Copias Snapshot |
| Sí | No | Configuración de recuperación ante desastres de SVM |
| <p>Sí</p> <p>Con compatibilidad a partir con ONTAP 9.5. La SVM principal de una relación de recuperación ante desastres de SVM puede tener el volumen de origen; no obstante, si la relación de recuperación ante desastres de SVM está rota, debe volver a crearse la relación de FlexCache con un nuevo volumen de origen.</p> | <p>No</p> <p>Puede tener volúmenes FlexCache en SVM primarias, pero no en SVM secundarias. Cualquier volumen FlexCache de la SVM principal no se replica como parte de la relación de recuperación ante desastres de SVM.</p> | Protección de acceso a nivel de almacenamiento (ESCORIA) |
| No | No | Aprovisionamiento ligero |
| Sí | <p>Sí</p> <p>Compatible a partir de ONTAP 9.7</p> | Clonado de volúmenes |

| | | |
|---|--|--|
| Sí | No | Movimiento de volúmenes |
| Se admite la clonado de un volumen de origen y de los archivos en el volumen de origen a partir de ONTAP 9.6. | | |
| Sí | Sí (solo para componentes de volumen) ONTAP 9,6 y versiones posteriores admiten el movimiento de constituyentes de volúmenes de un volumen FlexCache. | Realojamiento de volúmenes |
| No | No | API de vStorage para integración de cabinas (VAAI) |



En las versiones de ONTAP 9 anteriores a la 9.5, los volúmenes FlexVol de origen solo pueden proporcionar datos a volúmenes FlexCache creados en sistemas que ejecutan Data ONTAP 8.2.x en 7-Mode. A partir de ONTAP 9.5, los volúmenes FlexVol de origen también pueden proporcionar datos a FlexCache Volumes en sistemas ONTAP 9. Para obtener más información sobre la migración de FlexCache de 7-Mode a ONTAP 9 FlexCache, consulte ["Informe técnico de NetApp 4743: FlexCache en ONTAP"](#).

Directrices para ajustar el tamaño de un volumen FlexCache

Antes de comenzar a aprovisionar los volúmenes, debe conocer los límites de FlexCache Volumes.

El límite de tamaño de un volumen FlexVol se aplica a un volumen de origen. El tamaño de un volumen de FlexCache puede ser menor o igual que el volumen de origen. La práctica recomendada para el tamaño de un volumen de FlexCache es tener al menos el 10 % del tamaño del volumen de origen.

También debe tener en cuenta los siguientes límites adicionales de FlexCache Volumes:

| Límite | ONTAP 9.5-9.6 | ONTAP 9,7 | ONTAP 9,8 y versiones posteriores |
|--|---------------|-----------|-----------------------------------|
| Número máximo de volúmenes de FlexCache que se pueden crear a partir de un volumen de origen | 10 | 10 | 100 |
| Número máximo recomendado de volúmenes de origen por nodo | 10 | 100 | 100 |
| Número máximo recomendado de volúmenes FlexCache por nodo | 10 | 100 | 100 |
| Número máximo recomendado de componentes FlexGroup en un volumen FlexCache por nodo | 40 | 800 | 800 |

| | | | |
|---|----|----|----|
| Número máximo de componentes por volumen FlexCache por nodo | 32 | 32 | 32 |
|---|----|----|----|

Información relacionada

["Interoperabilidad de NetApp"](#)

Cree un volumen de FlexCache

Puede crear un volumen de FlexCache en el mismo clúster para mejorar el rendimiento al acceder a un objeto activo. Si tiene centros de datos en diferentes ubicaciones, puede crear volúmenes de FlexCache en clústeres remotos para acelerar el acceso a los datos.

Acerca de esta tarea

- A partir de ONTAP 9,5, FlexCache admite los volúmenes FlexVol como volúmenes de origen y FlexGroup como volúmenes FlexCache.
- A partir de ONTAP 9,7, tanto el volumen FlexVol como los volúmenes FlexGroup se admiten como volúmenes de origen.
- A partir de ONTAP 9.14.0, se puede crear un volumen FlexCache sin cifrar a partir de un origen cifrado.

Antes de empezar

- Debe ejecutar ONTAP 9,5 o una versión posterior.
- Si utiliza ONTAP 9,6 o una versión anterior, debe ["Añadir una licencia de FlexCache"](#).

No se requiere una licencia de FlexCache para ONTAP 9,7 o una versión posterior. A partir de ONTAP 9,7, la funcionalidad FlexCache se incluye con ONTAP y ya no se requiere una licencia o activación.




Si un par de alta disponibilidad está usando ["Cifrar unidades SAS o NVMe \(SED, NSE, FIPS\)"](#), debe seguir las instrucciones del tema ["Devolver una unidad FIPS o SED al modo sin protección"](#) Para todas las unidades dentro de la pareja de ha antes de inicializar el sistema (opciones de arranque 4 o 9). Si las unidades se reasignan, es posible que no se produzcan pérdidas de datos futuras.


Ejemplo 4. Pasos

System Manager

1. Si el volumen de FlexCache está en un clúster diferente al volumen de origen, cree una relación de paridad de clústeres:
 - a. En el clúster local, haga clic en **Protección > Descripción general**.
 - b. Expanda **Configuración de interconexión de clústeres**, haga clic en **Agregar interfaces de red** y agregue interfaces de red de interconexión de clústeres para el clúster.

Repita este paso en el clúster remoto.

 - c. En el clúster remoto, haga clic en **Protección > Descripción general**. Haga clic en  En la sección Cluster peers y haga clic en **Generate Passphrase**.
 - d. Copie la clave de acceso generada y péguela en el clúster local.
 - e. En el clúster local, en Cluster peers, haga clic en **Peer Clusters** y pare los clústeres locales y remotos.
2. Si el volumen FlexCache está en el mismo clúster que el volumen de origen, pero está en una SVM diferente, cree una relación entre iguales para SVM de tipo «FlexCache»:

En Storage VM peers, haga clic en  Posteriormente **Peer Storage VMs** para poner en la misma conexión los equipos virtuales de almacenamiento.

3. Seleccione **almacenamiento > volúmenes**.
4. Seleccione **Agregar**.
5. Seleccione **Más opciones** y luego seleccione **Agregar como caché para un volumen remoto**.



Si está ejecutando ONTAP 9,8 o posterior y desea deshabilitar QoS o elegir una política de QoS personalizada, haga clic en **Más opciones** y, a continuación, en **Almacenamiento y optimización**, seleccione **Nivel de servicio de rendimiento**.

CLI

1. Si el volumen de FlexCache que se va a crear se encuentra en otro clúster, cree una relación de paridad de clústeres:
 - a. En el clúster de destino, cree una relación entre iguales con el clúster de origen de protección de datos:

```
cluster peer create -generate-passphrase -offer-expiration
MM/DD/YYYY HH:MM:SS|1...7days|1...168hours -peer-addr
s <peer_LIF_IPs> -initial-allowed-vserver-peers <svm_name>,...|*
-ipospace <ipospace_name>
```

A partir de ONTAP 9.6, el cifrado TLS se habilita de forma predeterminada al crear una relación de paridad de clústeres. El cifrado TLS es compatible con la comunicación entre clústeres entre los volúmenes de origen y FlexCache. También puede deshabilitar el cifrado TLS para la relación de paridad de clústeres, si es necesario.

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers *
```

Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
Expiration Time: 6/7/2017 08:16:10 EST
Initial Allowed Vserver Peers: *
Intercluster LIF IP: 192.140.112.101
Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed again.

- a. En el clúster de origen, autentique el clúster de origen con el clúster de destino:

```
cluster peer create -peer-addr <peer_LIF_IPs> -ipspace <ipspace>
```

```
cluster01::> cluster peer create -peer-addr
192.140.112.101,192.140.112.102
```

Notice: Use a generated passphrase or choose a passphrase of 8 or more characters.

To ensure the authenticity of the peering relationship, use a phrase or sequence of characters that would be hard to guess.

Enter the passphrase:
Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.

2. Si el volumen de FlexCache está en una SVM diferente a la del volumen de origen, cree una relación entre iguales de SVM con flexcache como aplicación:

- a. Si la SVM está en un clúster diferente, cree un permiso de SVM para las SVM entre iguales:

```
vserver peer permission create -peer-cluster <cluster_name>
-vserver <svm-name> -applications flexcache
```

En el siguiente ejemplo, se muestra cómo crear un permiso de paridad de SVM que se aplica a todas las SVM locales:


```
cluster1::> vserver peer permission create -peer-cluster cluster2
-vserver "*" -applications flexcache
```

Warning: This Vserver peer permission applies to all local Vservers. After that no explicit "vserver peer accept" command required for Vserver peer relationship creation request from peer cluster "cluster2" with any of the local Vservers. Do you want to continue? {y|n}: y

a. Cree la relación entre iguales de SVM:

```
vserver peer create -vserver <local_SVM> -peer-vserver
<remote_SVM> -peer-cluster <cluster_name> -applications flexcache
```

3. Cree un volumen de FlexCache:

```
volume flexcache create -vserver <cache_svm> -volume
<cache_vol_name> -auto-provision-as flexgroup -size <vol_size>
-origin-vserver <origin_svm> -origin-volume <origin_vol_name>
```

En el ejemplo siguiente se crea un volumen de FlexCache y se seleccionan automáticamente los agregados existentes para el aprovisionamiento:

```
cluster1::> volume flexcache create -vserver vs_1 -volume fc1 -auto
-provision-as flexgroup -origin-volume vol_1 -size 160MB -origin
-vserver vs_1
[Job 443] Job succeeded: Successful
```

En el siguiente ejemplo se crea un volumen FlexCache y se establece la ruta de unión:

```
cluster1::> flexcache create -vserver vs34 -volume fc4 -aggr-list
aggr34,aggr43 -origin-volume origin1 -size 400m -junction-path /fc4
[Job 903] Job succeeded: Successful
```

4. Verifique la relación de FlexCache desde el volumen de FlexCache y el volumen de origen.

a. Vea la relación de FlexCache en el clúster:

```
volume flexcache show
```

```
cluster1::> volume flexcache show
```

| Vserver | Volume | Size | Origin-Vserver | Origin-Volume |
|----------------|--------|-------|----------------|---------------|
| Origin-Cluster | | | | |
| vs_1 | fc1 | 160MB | vs_1 | vol_1 |

```
cluster1
```

b. Vea todas las relaciones de FlexCache en el clúster de origen:

```
volume flexcache origin show-caches
```

```
cluster::> volume flexcache origin show-caches
```

| Origin-Vserver | Origin-Volume | Cache-Vserver | Cache-Volume |
|----------------|---------------|---------------|--------------|
| Cache-Cluster | | | |
| vs0 | ovol1 | vs1 | cfg1 |
| clusA | | | |
| vs0 | ovol1 | vs2 | cfg2 |
| clusB | | | |
| vs_1 | vol_1 | vs_1 | fc1 |

```
cluster1
```

Resultado

El volumen FlexCache se ha creado correctamente. Los clientes pueden montar el volumen con la ruta de unión del volumen FlexCache.

Información relacionada

["Relaciones entre iguales de clústeres y SVM"](#)

Gestione volúmenes de FlexCache

Consideraciones para auditar volúmenes de FlexCache

A partir de ONTAP 9.7, puede auditar eventos de acceso a archivos NFS en relaciones de FlexCache mediante la auditoría de ONTAP nativa y la gestión de políticas de archivos con FPolicy.

A partir de ONTAP 9.14.1, se admite FPolicy para volúmenes FlexCache con NFS o SMB. Anteriormente, FPolicy no era compatible con FlexCache Volumes con SMB.

La auditoría nativa y FPolicy se configuran y gestionan con los mismos comandos de la CLI que se utilizan para volúmenes de FlexVol. Sin embargo, FlexCache Volumes tiene un comportamiento diferente.

- **Auditoría nativa**

- No se puede usar un volumen de FlexCache como destino de los registros de auditoría.
- Si desea auditar operaciones de lectura y escritura en volúmenes FlexCache, debe configurar la auditoría tanto en la SVM de caché como en la SVM de origen.

Esto se debe a que las operaciones del sistema de archivos se auditan donde se procesan. Es decir, las lecturas se auditan en la SVM caché y las escrituras se auditan en la SVM de origen.

- Para realizar el seguimiento del origen de las operaciones de escritura, el UUID de SVM y el MSID se agregan en el registro de auditoría para identificar el volumen FlexCache a partir del que se originó la escritura.
- Aunque es posible establecer listas de control de acceso del sistema (SACL) en un archivo con los protocolos NFSv4 o SMB, los volúmenes de FlexCache solo admiten NFSv3. Por lo tanto, SACL sólo se puede establecer en el volumen de origen.

- **FPolicy**

- Aunque las escrituras en un volumen FlexCache se realizan en el volumen de origen, las configuraciones de FPolicy supervisan las escrituras en el volumen de caché. Esto es distinto a la auditoría nativa, en la que las escrituras se auditan en el volumen de origen.
- Aunque ONTAP no requiere la misma configuración de FPolicy en SVM de caché y de origen, se recomienda poner en marcha dos configuraciones similares. Para ello, puede crear una nueva política de FPolicy para la caché, configurada como la de la SVM de origen, pero con el ámbito de la nueva política limitada a la SVM de caché.

Sincronizar las propiedades de un volumen FlexCache desde un volumen de origen

Algunas de las propiedades de volumen del volumen FlexCache siempre deben sincronizarse con las del volumen de origen. Si las propiedades de volumen de un volumen FlexCache no pueden sincronizarse automáticamente después de que se modifican las propiedades del volumen de origen, se pueden sincronizar manualmente las propiedades.

Acerca de esta tarea

Las siguientes propiedades de volumen de un volumen FlexCache siempre deben sincronizarse con las del volumen de origen:

- Estilo de seguridad (-security-style)
- Nombre del volumen (-volume-name)
- Tamaño máximo de directorio (-maxdir-size)
- Lectura mínima anticipada (-min-readahead)

Paso

1. En el volumen FlexCache, sincronice las propiedades del volumen:

```
volume flexcache sync-properties -vserver svm_name -volume flexcache_volume
```

```
cluster1::> volume flexcache sync-properties -vserver vs1 -volume fcl
```

Actualizar las configuraciones de una relación de FlexCache

Después de eventos como movimiento de volúmenes, reubicación de agregados o conmutación por error de almacenamiento, la información de configuración de volumen en el volumen de origen y el volumen de FlexCache se actualiza de forma automática. En caso de que se produzca un error en las actualizaciones automáticas, se genera un mensaje de EMS y, a continuación, se debe actualizar manualmente la configuración de la relación de FlexCache.

Si el volumen de origen y el volumen FlexCache están en el modo desconectado, es posible que deba realizar algunas operaciones adicionales para actualizar manualmente una relación de FlexCache.

Acerca de esta tarea

Si desea actualizar las configuraciones de un volumen FlexCache, debe ejecutar el comando desde el volumen de origen. Si desea actualizar las configuraciones de un volumen de origen, se debe ejecutar el comando desde el volumen FlexCache.

Paso

1. Actualice la configuración de la relación de FlexCache:

```
volume flexcache config-refresh -peer-vserver peer_svm -peer-volume  
peer_volume_to_update -peer-endpoint-type [origin | cache]
```

Activar actualizaciones de tiempo de acceso a archivos

A partir de ONTAP 9.11.1, puede habilitar el `-atime-update` Campo del volumen FlexCache para permitir actualizaciones del tiempo de acceso a los archivos. También puede establecer un período de actualización del tiempo de acceso con `-atime-update-period` atributo. La `-atime-update-period` atributo controla la frecuencia con la que se pueden realizar actualizaciones del tiempo de acceso y cuándo se pueden propagar al volumen de origen.

Descripción general

ONTAP proporciona un campo llamado de nivel de volumen `-atime-update`. Para administrar las actualizaciones del tiempo de acceso en archivos y directorios que se leen utilizando LECTURA, READLINK y READDIR. Atime se utiliza para tomar decisiones sobre el ciclo de vida de los datos en archivos y directorios a los que se accede con poca frecuencia. Los archivos a los que se accede con poca frecuencia se migran al almacenamiento de archivado y se mueven a cinta más adelante.

El campo `atime-update` está deshabilitado de forma predeterminada en los volúmenes FlexCache existentes y nuevos. Si utiliza FlexCache Volumes con versiones de ONTAP anteriores a 9.11.1, debería dejar deshabilitado el campo `atime-update` para que las cachés no se expulsan innecesariamente cuando se realiza una operación de lectura en el volumen de origen. Sin embargo, con las grandes cachés de FlexCache, los administradores usan herramientas especiales para gestionar los datos y ayudar a garantizar que los datos activos permanezcan en la caché y que los datos inactivos se purguen. Esto no es posible cuando `atime-update` está desactivado. Sin embargo, a partir de ONTAP 9.11.1, puede habilitar `-atime-update` y `-atime-update-period`, y utilice las herramientas necesarias para gestionar los datos almacenados en caché.

Antes de empezar

Todos los volúmenes de FlexCache deben ejecutar ONTAP 9.11.1 o una versión posterior.

Acerca de esta tarea

Ajuste `-atime-update-period` a 86400 segundos no permite más de una actualización de tiempo de acceso por periodo de 24 horas, independientemente del número de operaciones de lectura realizadas en un archivo.

Ajuste de `-atime-update-period` a 0 envía mensajes al origen de cada acceso de lectura. A continuación, el origen informa a cada volumen de FlexCache de que el `atime` está obsoleto, lo que afecta al rendimiento.

Pasos

1. Activar actualizaciones de tiempo de acceso a archivos y establecer la frecuencia de actualización:

```
volume modify -volume vol_name -vserver SVM_name -atime-update true -atime-update-period seconds
```

El ejemplo siguiente habilita `-atime-update` y conjuntos `-atime-update-period` a 86400 segundos o 24 horas:

```
c1: volume modify -volume origin1 vs1_c1 -atime-update true -atime-update-period 86400
```

2. Compruebe que `-atime-update` está activado:

```
volume show -volume vol_name -fields atime-update,atime-update-period
```

```
c1::*> volume show -volume cache1_origin1 -fields atime-update,atime-update-period
vserver volume          atime-update atime-update-period
-----
vs2_c1  cache1_origin1 true           86400
```

Activar el bloqueo global de archivos

A partir de ONTAP 9.10.1, el bloqueo global de archivos se puede aplicar para evitar lecturas en todos los archivos almacenados en caché relacionados.

Cuando el bloqueo global de archivos está habilitado, las modificaciones del volumen de origen se suspenden hasta que todos los volúmenes FlexCache estén en línea. Solo es necesario habilitar el bloqueo global de archivos cuando tiene control de la fiabilidad de las conexiones entre la caché y el origen debido a la suspensión y los posibles tiempos de espera de las modificaciones cuando los volúmenes FlexCache están sin conexión.

Antes de empezar

- El bloqueo global de archivos requiere que los clústeres que contienen el origen y todas las cachés asociadas ejecuten ONTAP 9.9.1 o posterior. El bloqueo de archivos global se puede habilitar en

volúmenes de FlexCache nuevos o existentes. El comando puede ejecutarse en un volumen y aplicarse a todos los volúmenes FlexCache asociados.

- Debe estar en el nivel de privilegio avanzado para habilitar el bloqueo global de archivos.
- Si vuelve a una versión de ONTAP anterior a la 9.9.1, el bloqueo global de archivos debe desactivarse primero en las cachés de origen y asociadas. Para desactivar, desde el volumen de origen, ejecute:
`volume flexcache prepare-to-downgrade -disable-feature-set 9.10.0`
- El proceso para activar el bloqueo global de archivos depende de si el origen tiene cachés existentes:
 - [\[enable-gfl-new\]](#)
 - [\[enable-gfl-existing\]](#)

Bloqueo de archivos global en los nuevos volúmenes de FlexCache

Pasos

1. Cree el volumen FlexCache con `-is-global-file-locking` establecer como verdadero:

```
volume flexcache create volume volume_name -is-global-file-locking-enabled true
```



El valor predeterminado de `-is-global-file-locking` es «falso». Cuando sea posterior `volume flexcache create` los comandos se ejecutan en un volumen, se deben pasar con `-is-global-file-locking enabled` establecer en «'true'».

Bloqueo de archivos global en volúmenes FlexCache existentes

Pasos

1. El bloqueo global de archivos se debe establecer desde el volumen de origen.
2. El origen no puede tener ninguna otra relación existente (por ejemplo, SnapMirror). Todas las relaciones existentes deben estar disociadas. Todas las cachés y los volúmenes deben conectarse en el momento de ejecutar el comando. Para comprobar el estado de la conexión, ejecute:

```
volume flexcache connection-status show
```

El estado de todos los volúmenes enumerados debe aparecer como `connected`. Para obtener más información, consulte ["Ver el estado de una relación de FlexCache"](#) o ["Sincronizar las propiedades de un volumen FlexCache desde un origen"](#).

3. Activar el bloqueo global de archivos en las cachés:

```
volume flexcache origin config show/modify -volume volume_name -is-global-file-locking-enabled true
```

Rellene previamente un volumen FlexCache

Puede rellenar previamente un volumen FlexCache para reducir el tiempo que lleva el acceso a los datos almacenados en caché.

Lo que necesitará

- Debe ser un administrador de clústeres en el nivel de privilegios avanzados

- Las rutas que se pasan para la prepopulación deben existir o la operación de prellenado falla.

Acerca de esta tarea

- Prellenar sólo lee archivos y rastrea directorios
- La `-isRecursion` el indicador se aplica a toda la lista de directorios pasados para rellenar previamente

Pasos

1. Rellene con antelación un volumen de FlexCache:

```
volume flexcache prepopulate -cache-vserver vs1 -cache-volume -path
-list path_list -isRecursion true|false
```

- La `-path-list` parámetro indica la ruta de acceso de directorio relativa que desea rellenar previamente a partir del directorio raíz de origen. Por ejemplo, si el directorio raíz de origen se denomina `/Origin` y contiene directorios `/Origin/dir1` y `/Origin/dir2`, puede especificar la lista de rutas de acceso de la siguiente forma: `-path-list dir1, dir2` o `-path-list /dir1, /dir2`.
- El valor predeterminado de `-isRecursion` El parámetro es `True`.

En este ejemplo se rellena una ruta de acceso de directorio única:

```
cluster1::*> flexcache prepopulate start -cache-vserver vs2 -cache
-volume fg_cachevol_1 -path-list /dir1
(volume flexcache prepopulate start)
[JobId 207]: FlexCache prepopulate job queued.
```

En este ejemplo se prellena archivos de varios directorios:

```
cluster1::*> flexcache prepopulate start -cache-vserver vs2 -cache
-volume fg_cachevol_1 -path-list /dir1,/dir2,/dir3,/dir4
(volume flexcache prepopulate start)
[JobId 208]: FlexCache prepopulate job queued.
```

En este ejemplo se prerellena un único archivo:

```
cluster1::*> flexcache prepopulate start -cache-vserver vs2 -cache
-volume fg_cachevol_1 -path-list /dir1/file1.txt
(volume flexcache prepopulate start)
[JobId 209]: FlexCache prepopulate job queued.
```

En este ejemplo se prerellena todos los archivos del origen:

```
cluster1::*> flexcache prepopulate start -cache-vserver vs2 -cache
-volume fg_cachevol_1 -path-list / -isRecursion true
(volume flexcache prepopulate start)
[JobId 210]: FlexCache prepopulate job queued.
```

Este ejemplo incluye una ruta no válida para la relleno previo:

```
cluster1::*> flexcache prepopulate start -cache-volume
vol_cache2_vs3_c2_vol_origin1_vs1_c1 -cache-vserver vs3_c2 -path-list
/dir1, dir5, dir6
(volume flexcache prepopulate start)

Error: command failed: Path(s) "dir5, dir6" does not exist in origin
volume
      "vol_origin1_vs1_c1" in Vserver "vs1_c1".
```

2. Mostrar el número de archivos leídos:

```
job show -id job_ID -ins
```

Eliminar una relación de FlexCache

Es posible eliminar una relación de FlexCache y el volumen de FlexCache si ya no se requiere el volumen de FlexCache.

Pasos

1. Desde el clúster que tiene el volumen de FlexCache, desconecte el volumen FlexCache:

```
volume offline -vserver svm_name -volume volume_name
```

2. Elimine el volumen FlexCache:

```
volume flexcache delete -vserver svm_name -volume volume_name
```

Los detalles de la relación de FlexCache se eliminarán del volumen de origen y del volumen de FlexCache.

Gestión de redes

Manos a la obra

Información general sobre la gestión de redes

Puede usar la siguiente información para realizar administración básica de redes de almacenamiento mediante System Manager o la CLI. Es posible configurar puertos de red físicos y virtuales (VLAN y grupos de interfaces), crear LIF mediante IPv4 e IPv6, gestionar servicios de enrutamiento y resolución de hosts en clústeres, utilizar el equilibrio de carga para optimizar el tráfico de red y supervisar un clúster mediante SNMP.

A menos que se indique lo contrario, los procedimientos de la CLI se aplican a todas las versiones de ONTAP 9.

Para comprender el impacto de las funciones de red disponibles con cada versión de ONTAP 9, consulte la ["Notas de la versión de ONTAP"](#).

A partir de ONTAP 9.8, puede usar System Manager para mostrar un gráfico que muestra los componentes y la configuración de la red. A partir de ONTAP 9.12, puede ver la asociación de LIF y subred en la cuadrícula Interfaces de red. Si utiliza el administrador de sistemas clásico (disponible solo en ONTAP 9.7 y versiones anteriores), consulte ["Gestión de la red"](#).

La nueva función de visualización de red permite a los usuarios ver la ruta de conexiones de red entre hosts, puertos, SVM, volúmenes, etc. en una interfaz gráfica.

El gráfico aparece cuando selecciona **Red > Descripción general** o cuando selecciona  En la sección **Red** del tablero de mandos.

En el gráfico se muestran las siguientes categorías de componentes:


- Hosts
- Puertos de almacenamiento
- Interfaces de red
- Máquinas virtuales de almacenamiento
- Componentes de acceso a datos

Cada sección muestra detalles adicionales que puede pasar el ratón sobre o seleccionar para realizar tareas de configuración y gestión de la red.

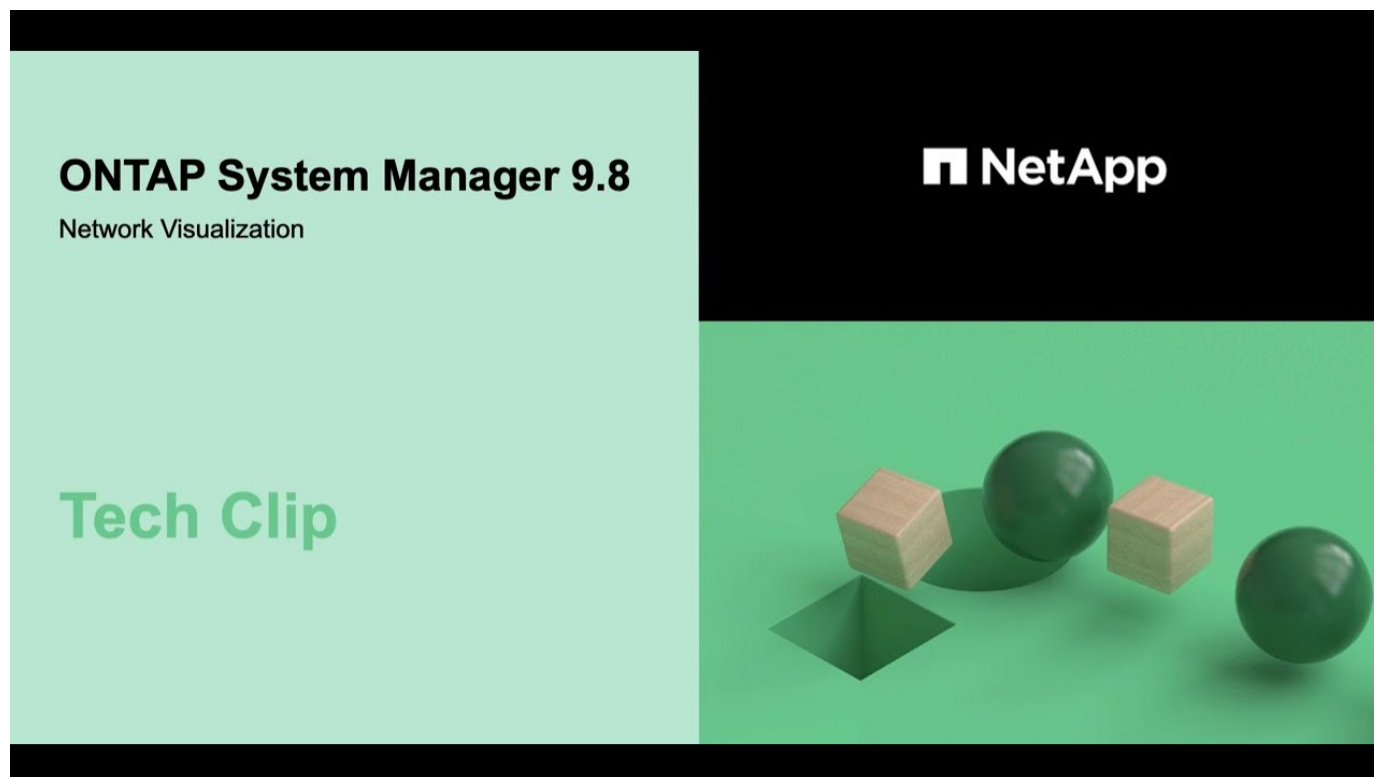
Ejemplos

A continuación se muestran algunos ejemplos de las muchas maneras en que puede interactuar con el gráfico para ver detalles sobre cada componente o iniciar acciones para administrar su red:

- Haga clic en un host para ver su configuración: Los puertos, las interfaces de red, las VM de almacenamiento y los componentes de acceso a datos asociados a él.
- Pase el ratón por la cantidad de volúmenes de una máquina virtual de almacenamiento para seleccionar un volumen para ver sus detalles.

- Seleccione una interfaz de iSCSI para ver el rendimiento durante la última semana.
- Haga clic en  junto a un componente para iniciar acciones para modificar ese componente.
- Determine rápidamente dónde pueden ocurrir los problemas en la red, indicado por una "X" junto a componentes que no son sanos.

Vídeo sobre visualización de red de System Manager



Verifique la configuración de red después de una actualización de ONTAP desde ONTAP 9,7x o una versión anterior

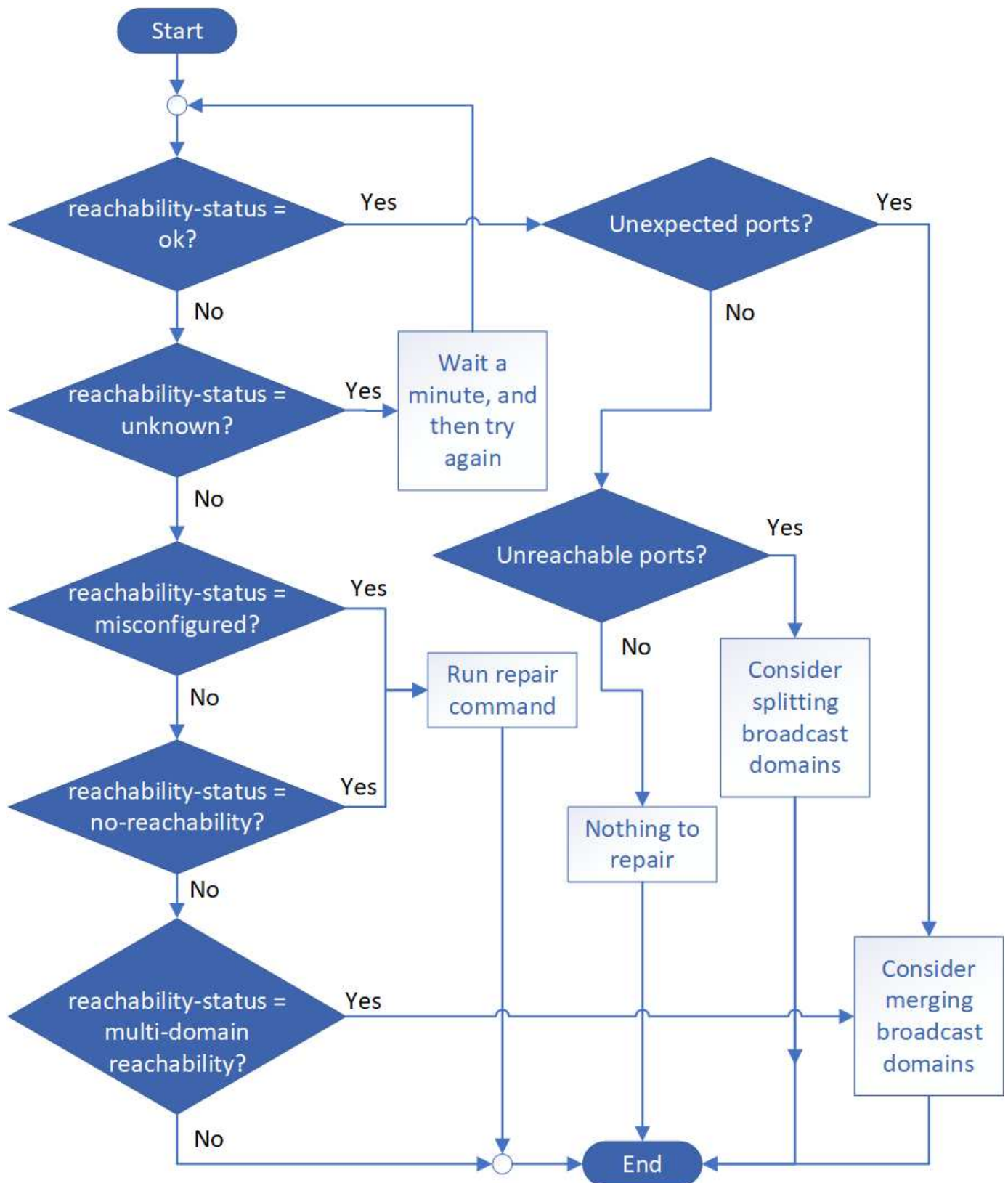
Después de realizar una actualización desde ONTAP 9,7x o anterior a ONTAP 9,8 o posterior, debe verificar la configuración de red. Después de la actualización, ONTAP supervisa automáticamente la accesibilidad de la capa 2.

Paso

1. Compruebe que cada puerto tiene accesibilidad al dominio de retransmisión esperado:

```
network port reachability show -detail
```

El resultado del comando contiene resultados de accesibilidad. Use el árbol de decisión y la tabla siguientes para comprender los resultados de la accesibilidad (estado de la accesibilidad) y determinar qué hacer, si es que hay algo, a continuación.



| accesibilidad-estado | Descripción |
|----------------------|-------------|
|----------------------|-------------|

| | |
|-----------------------------|--|
| de acuerdo | <p>El puerto tiene capacidad de acceso de capa 2 a su dominio de difusión asignado.</p> <p>Si el reachability-status es "ok", pero hay "puertos inesperados", considere combinar uno o más dominios de difusión. Para obtener más información, consulte "Fusionar dominios de retransmisión".</p> <p>Si el reachability-status es "ok", pero hay "puertos inaccesibles", considere dividir uno o más dominios de difusión. Para obtener más información, consulte "Divida los dominios de retransmisión".</p> <p>Si el estado de accesibilidad es "correcto" y no hay puertos inesperados o no accesibles, la configuración es correcta.</p> |
| función mal configurada | <p>El puerto no tiene posibilidad de recurrir a la capa 2 a su dominio de difusión asignado; sin embargo, el puerto tiene capacidad de acceso de capa 2 a un dominio de difusión diferente.</p> <p>Puede reparar la accesibilidad del puerto. Cuando ejecute el siguiente comando, el sistema asignará el puerto al dominio de retransmisión al que se le habrá accesibilidad:</p> <pre>network port reachability repair -node -port</pre> <p>Para obtener más información, consulte "Reparar la accesibilidad del puerto".</p> |
| ausencia de accesibilidad | <p>El puerto no tiene posibilidad de recurrir a ningún dominio de difusión existente de capa 2.</p> <p>Puede reparar la accesibilidad del puerto. Cuando ejecute el siguiente comando, el sistema asignará el puerto a un dominio de retransmisión creado automáticamente en el espacio IP predeterminado:</p> <pre>network port reachability repair -node -port</pre> <p>Para obtener más información, consulte "Reparar la accesibilidad del puerto".</p> |
| accesibilidad multi-dominio | <p>El puerto tiene la habilidad de la capa 2 para su dominio de broadcast asignado; sin embargo, también tiene la habilidad de la capa 2 para al menos otro dominio de broadcast.</p> <p>Examine la configuración física del conmutador y la conectividad para determinar si es incorrecta o si el dominio de difusión asignado al puerto necesita combinarse con uno o más dominios de difusión.</p> <p>Para obtener más información, consulte "Fusionar dominios de retransmisión" o "Reparar la accesibilidad del puerto".</p> |
| desconocido | <p>Si el estado de accesibilidad es "desconocido", espere unos minutos y vuelva a intentar el comando.</p> |

Después de reparar un puerto, necesita comprobar y resolver las LIF y VLAN desplazadas. Si el puerto era parte de un grupo de interfaces, también necesita comprender lo que ha sucedido con ese grupo de

interfaces. Para obtener más información, consulte ["Reparar la accesibilidad del puerto"](#).

Componentes de red

Componentes de red de una descripción general de un clúster

Antes de configurar el clúster, debe familiarizarse con los componentes de red de un clúster. La configuración de los componentes físicos de redes de un clúster en componentes lógicos proporciona la flexibilidad y la funcionalidad multi-tenancy en ONTAP.

Los diferentes componentes de red de un clúster son los siguientes:

- Puertos físicos

Las tarjetas de interfaz de red (NIC) y los adaptadores de bus host (HBA) proporcionan conexiones físicas (Ethernet y Fibre Channel) desde cada nodo a las redes físicas (redes de gestión y datos).

Para conocer los requisitos del sitio, la información de los switches, la información sobre el cableado de puertos y el cableado de los puertos integrados de la controladora, consulte la Hardware Universe en ["hwu.netapp.com"](http://hwu.netapp.com).

- Puertos lógicos

Las redes de área local virtual (VLAN) y los grupos de interfaces constituyen los puertos lógicos. Los grupos de interfaces tratan varios puertos físicos como un único puerto, mientras que las VLAN subdividen un puerto físico en varios puertos separados.

- Espacios IP

Puede usar un espacio IP para crear un espacio de direcciones IP distinto para cada SVM de un clúster. Esto permite a los clientes en dominios de red separados administrativamente acceder a los datos del clúster mientras utilizan direcciones IP superpuestas del mismo rango de subredes de direcciones IP.

- Dominios de retransmisión

Un dominio de retransmisión reside en un espacio IP y contiene un grupo de puertos de red, potencialmente de varios nodos del clúster, que pertenecen a la misma red de capa 2. Los puertos del grupo se usan en una SVM para el tráfico de datos.

- Subredes

Una subred se crea dentro de un dominio de difusión y contiene un grupo de direcciones IP que pertenecen a la misma subred de capa 3. Este pool de direcciones IP simplifica la asignación de direcciones IP durante la creación de la LIF.

- Interfaces lógicas

Una interfaz lógica (LIF) es una dirección IP o un nombre de puerto WWPN asociado a un puerto. Está asociado con atributos como grupos de conmutación por error, reglas de conmutación por error y reglas de firewall. Un LIF se comunica a través de la red a través del puerto (físico o lógico) al que está enlazado actualmente.

Los diferentes tipos de LIF de un clúster son las LIF de datos, las LIF de gestión de ámbito de clúster, las

LIF de gestión de ámbito de nodo, las LIF de interconexión de clústeres y las LIF de clúster. La propiedad de las LIF depende de la SVM en la que reside el LIF. Las LIF de datos son propiedad de las SVM de datos, las LIF de gestión de ámbito de nodo, la gestión de ámbito del clúster y las LIF de interconexión de clústeres son propiedad de las SVM de administrador y las LIF de clúster son propiedad de la SVM del clúster.

- Zonas DNS

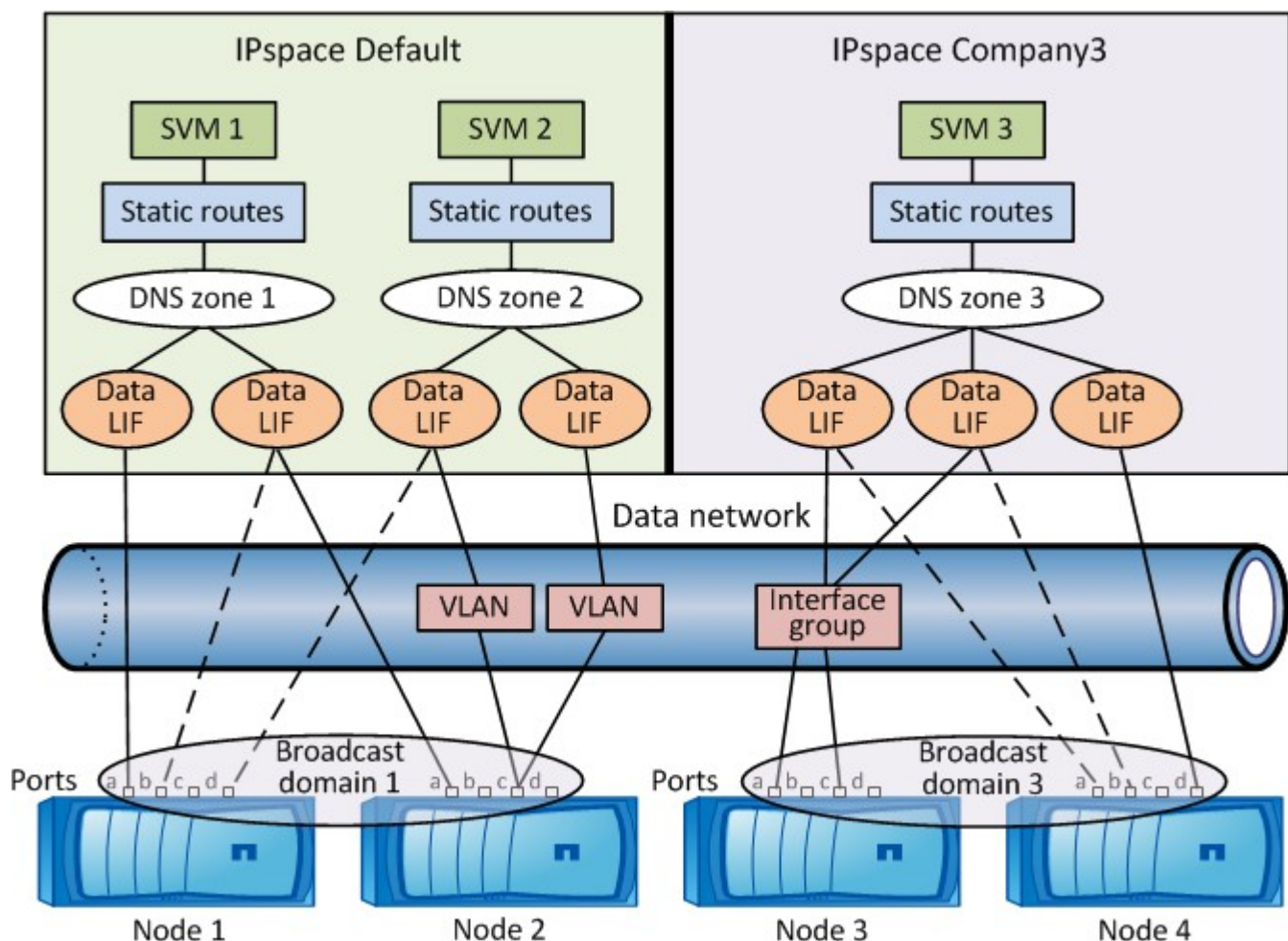
Puede especificarse la zona DNS durante la creación de LIF, con un nombre para la LIF que se va a exportar a través del servidor DNS del clúster. Varias LIF pueden compartir el mismo nombre, lo que permite que la característica de equilibrio de carga de DNS distribuya direcciones IP para el nombre según la carga.

Las instancias de SVM pueden tener varias zonas DNS.

- Enrutamiento

Cada SVM es autosuficiente con respecto a las redes. Una SVM es propietaria de LIF y rutas que pueden llegar a cada uno de los servidores externos configurados.

En la siguiente figura, se muestra cómo están asociados los diferentes componentes de red en un clúster de cuatro nodos:

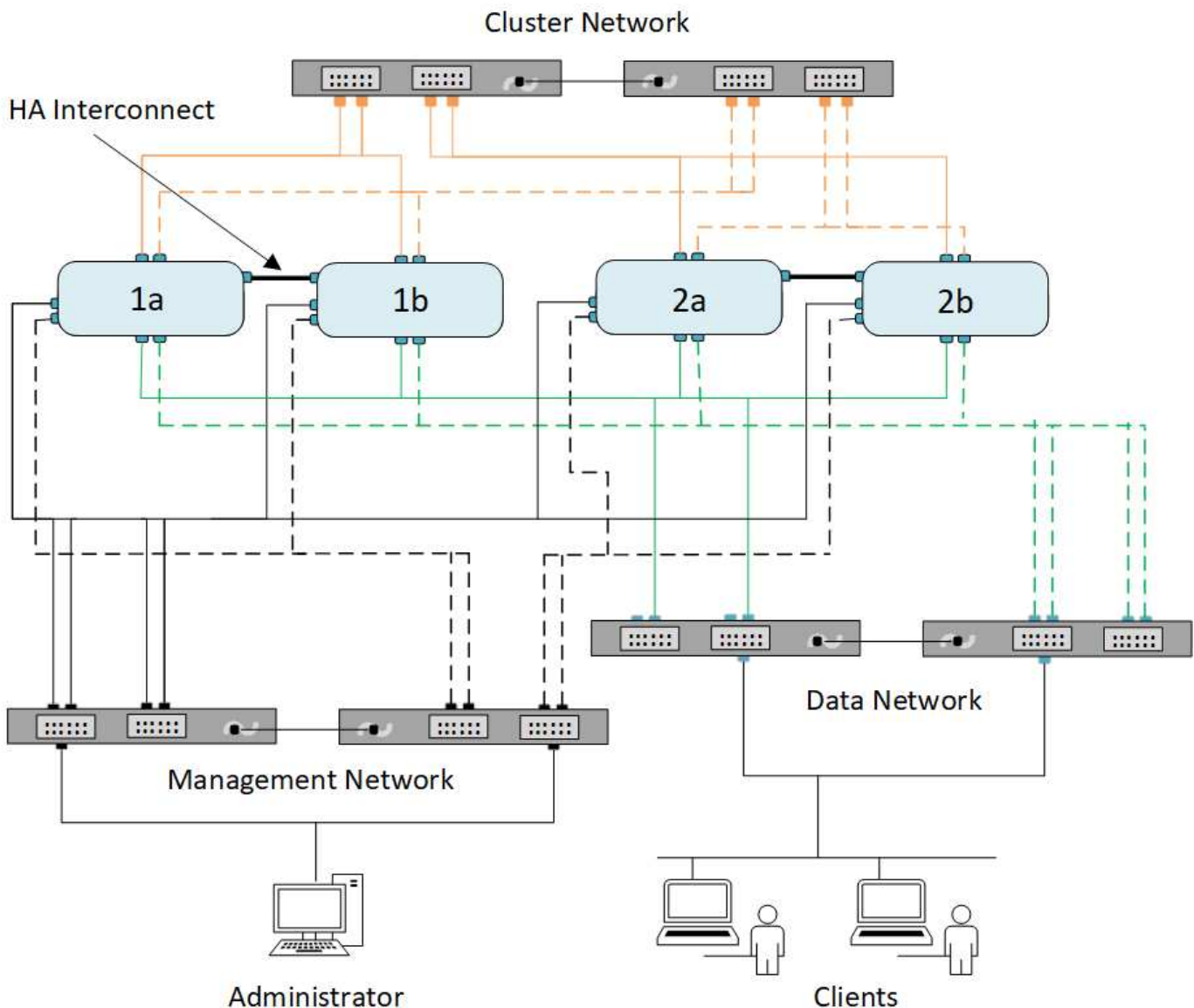


Directrices para el cableado de red

Las prácticas recomendadas para el cableado de red separan el tráfico en las siguientes redes: Clústeres, gestión y datos.

Debe cablear un clúster de modo que el tráfico del clúster esté en una red separada de todo el resto del tráfico. Se trata de una práctica opcional, pero recomendada. Mantener el tráfico de gestión de redes separado del tráfico dentro del clúster y de los datos. Al mantener redes independientes, puede mejorar el rendimiento, la facilidad de administración y mejorar el acceso a los nodos de seguridad y gestión.

En el siguiente diagrama se muestra el cableado de red de un clúster de alta disponibilidad de cuatro nodos que incluye tres redes independientes:



Debe seguir ciertas directrices al cablear las conexiones de red:

- Cada nodo debe estar conectado a tres redes distintas.

Una red es para la gestión, otra para el acceso a los datos y otra para la comunicación dentro del clúster.

Las redes de datos y gestión se pueden separar de forma lógica.

- Puede tener más de una conexión de red de datos a cada nodo para mejorar el flujo de tráfico de cliente (datos).
- Se puede crear un clúster sin conexiones de red de datos, pero debe incluir una conexión de interconexión de clúster.
- Siempre debe haber dos o más conexiones de clúster a cada nodo.

Para obtener más información sobre el cableado de red, consulte ["Centro de documentación de los sistemas AFF y FAS"](#) y la ["Hardware Universe"](#).

Relación entre dominios de retransmisión, grupos de conmutación por error y políticas de conmutación por error

Los dominios de retransmisión, los grupos de conmutación por error y las políticas de conmutación por error trabajan en conjunto para determinar qué puerto tomará el relevo cuando se produzca un error en el nodo o puerto en el que se ha configurado un LIF.

Un dominio de retransmisión enumera todos los puertos a los que se puede acceder en la misma red Ethernet de capa 2. Todos los demás puertos del dominio de retransmisión ven un paquete de retransmisión Ethernet enviado desde uno de los puertos. Esta característica de accesibilidad común de un dominio de retransmisión es importante para los LIF, ya que si una LIF se conmute a otro puerto del dominio de retransmisión, todavía podría llegar a todos los hosts locales y remotos a los que se pudiera acceder desde el puerto original.

Los grupos de conmutación por error definen los puertos dentro de un dominio de retransmisión que proporcionan cobertura de conmutación por error de LIF entre sí. Cada dominio de retransmisión tiene un grupo de conmutación al nodo de respaldo que incluye todos sus puertos. Este grupo de conmutación por error que contiene todos los puertos del dominio de retransmisión es el grupo de conmutación por error predeterminado y recomendado para la LIF. Puede crear grupos de conmutación por error con subconjuntos más pequeños que defina, como un grupo de conmutación por error de puertos que tengan la misma velocidad de enlace dentro de un dominio de difusión.

Una política de conmutación por error dicta cómo un LIF utiliza los puertos de un grupo de recuperación tras fallos cuando un nodo o puerto está inactivo. Considere la política de conmutación por error como un tipo de filtro que se aplica a un grupo de conmutación por error. Los destinos de conmutación por error de una LIF (el conjunto de puertos en los que se puede conmutar un LIF) están determinados por medio de la aplicación de la política de conmutación por error de la LIF al grupo de conmutación por error de la LIF en el dominio de retransmisión.

Puede ver los destinos de conmutación por error de una LIF con el siguiente comando CLI:

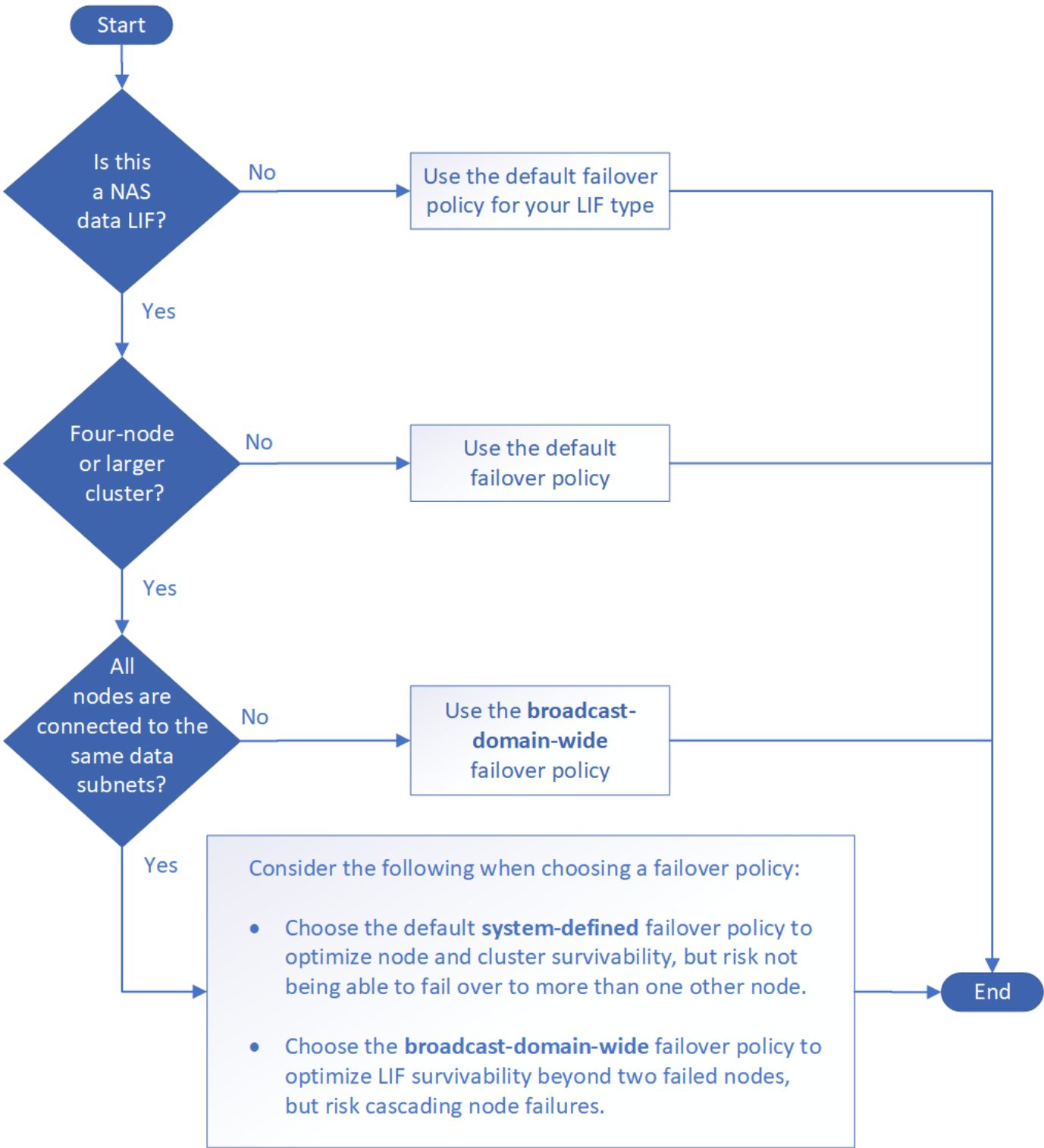
```
network interface show -failover
```

NetApp recomienda utilizar la política de conmutación por error predeterminada para el tipo de LIF.

Decidir qué política de conmutación por error de LIF se utilizará

Decidir si se utilizará la política de conmutación por error predeterminada recomendada o si se va a cambiar según el tipo y el entorno de LIF.

Árbol de decisión de directiva de conmutación por error



Políticas de conmutación por error predeterminadas por tipo de LIF

| Tipo de LIF | Política de conmutación por error predeterminada | Descripción |
|-------------|--|---|
| LIF de BGP | deshabilitado | LIF no conmuta al nodo de respaldo a otro puerto. |

| | | |
|-----------------------------------|-------------------------|---|
| LIF del clúster | solo local | LIF conmuta por error a los puertos del mismo nodo únicamente. |
| LIF de gestión del clúster | ámbito de difusión | LIF conmuta por error a los puertos del mismo dominio de retransmisión, en todos los nodos del clúster. |
| LIF de interconexión de clústeres | solo local | LIF conmuta por error a los puertos del mismo nodo únicamente. |
| LIF de datos NAS | definido por el sistema | LIF conmuta por error a otro nodo que no es el partner de alta disponibilidad. |
| LIF de gestión de nodos | solo local | LIF conmuta por error a los puertos del mismo nodo únicamente. |
| LIF de datos SAN | deshabilitado | LIF no conmuta al nodo de respaldo a otro puerto. |

La política de recuperación tras fallos "solo para sfo" no es un valor predeterminado, pero se puede usar cuando desee que la LIF realice la conmutación al nodo de respaldo en un puerto del nodo de inicio o del partner SFO únicamente.

Flujo de trabajo de conmutación al nodo de respaldo de ruta NAS (ONTAP 9,8 y versiones posteriores)

Acerca de la conmutación al nodo de respaldo en la ruta NAS (ONTAP 9,8 y posterior)

Este flujo de trabajo le guía por los pasos de configuración de redes para configurar la conmutación al nodo de respaldo de rutas NAS para ONTAP 9.8 y versiones posteriores. En este flujo de trabajo se dan por hechos los siguientes elementos:

- Desea utilizar las prácticas recomendadas de conmutación por error de la ruta NAS en un flujo de trabajo que simplifique la configuración de red.
- Desea utilizar la CLI, no con System Manager.
- Va a configurar una red en un sistema nuevo que ejecute ONTAP 9.8 o una versión posterior.

Si ejecuta una versión de ONTAP anterior a 9.8, debe utilizar el siguiente procedimiento de conmutación al nodo de respaldo de la ruta NAS para ONTAP 9.0 a 9.7:

- ["Flujo de trabajo de conmutación al nodo de respaldo de ruta NAS ONTAP 9.0-9.7"](#)

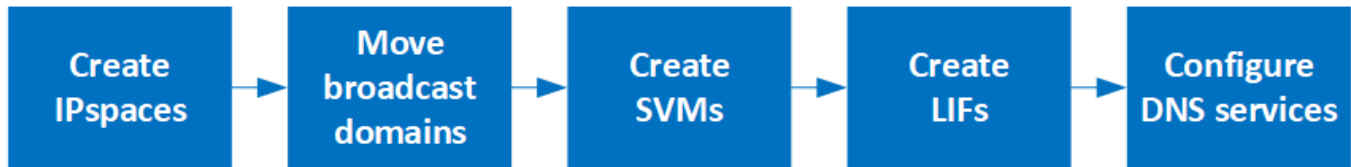
Si desea obtener detalles de administración de red, debe utilizar el material de referencia de administración de red:

- [Información general sobre la gestión de redes](#)

Flujo de trabajo (ONTAP 9,8 y posterior)

Si ya está familiarizado con los conceptos básicos de red, es posible que pueda ahorrar tiempo en la configuración de la red revisando este flujo de trabajo práctico para la configuración de conmutación por error de ruta NAS.

Un LIF NAS migra automáticamente a un puerto de red superviviente tras un error de enlace en su puerto actual. Puede confiar en los valores predeterminados de ONTAP para gestionar la recuperación tras fallos de rutas.



Un LIF SAN no migra (a menos que lo mueva manualmente después del fallo del enlace). En su lugar, la tecnología multivía en el host desvía el tráfico a otra LIF. Para obtener más información, consulte ["Administración de SAN"](#).

1

"Rellene la hoja de trabajo"

Utilice la hoja de trabajo para planificar la conmutación por error de ruta NAS.

2

"Cree espacios IP"

Cree un espacio de dirección IP distinto para cada SVM en un clúster.

3

"Mueva los dominios de retransmisión a los espacios IP"

Mover dominios de difusión a espacios IP.

4

"Cree SVM"

Cree SVM para servir datos a los clientes.

5

"Cree LIF"

Cree LIF en los puertos que desee utilizar para acceder a los datos.

6

"Configure los servicios DNS para la SVM"

Configure los servicios DNS para la SVM antes de crear un servidor NFS o SMB.

Hoja de datos para la configuración de conmutación al nodo de respaldo de ruta NAS (ONTAP 9,8 y posteriores)

Debe completar todas las secciones de la hoja de trabajo antes de configurar la conmutación por error de la ruta NAS.

Configuración del espacio IP

Puede usar un espacio IP para crear un espacio de direcciones IP distinto para cada SVM de un clúster. Esto permite a los clientes en dominios de red separados administrativamente acceder a los datos del clúster

mientras utilizan direcciones IP superpuestas del mismo rango de subredes de direcciones IP.

| Información | Necesario | Sus valores |
|---|-----------|-------------|
| Nombre del espacio IP El identificador único del espacio IP. | Sí | |

Configuración de dominio de retransmisión

Un dominio de retransmisión agrupa puertos que pertenecen a la misma red de capa 2 y establece la MTU para los puertos de dominio de retransmisión.

Los dominios de retransmisión se asignan a un espacio IP. Un espacio IP puede contener uno o varios dominios de retransmisión.



El puerto al que se conmuta por error un LIF debe ser miembro del grupo de conmutación por error de la LIF. Para cada dominio de retransmisión creado por ONTAP, también se crea un grupo a prueba de fallos con el mismo nombre que contiene todos los puertos del dominio de retransmisión.

| Información | Necesario | Sus valores |
|---|-----------|-------------|
| Nombre del espacio IP El espacio IP al que se asigna el dominio de retransmisión. Este espacio IP debe existir. | Sí | |
| Nombre de dominio de retransmisión El nombre del dominio de retransmisión. Este nombre debe ser único en el espacio IP. | Sí | |
| MTU El valor máximo de la unidad de transmisión para el dominio de transmisión, generalmente establecido en 1500 o 9000 . El valor MTU se aplica a todos los puertos del dominio de retransmisión y a los puertos que se añadan posteriormente al dominio de retransmisión. El valor MTU debe coincidir con todos los dispositivos conectados a esa red. Tenga en cuenta que el tráfico de gestión de puertos e0M y del procesador de servicios debe tener la MTU establecida en no más de 1500 bytes. | Sí | |

| | | |
|---|----|--|
| Puertos Los puertos se asignan a dominios de retransmisión según su accesibilidad. Una vez finalizada la asignación de puertos, compruebe la accesibilidad ejecutando el <code>network port reachability show</code> comando. Estos puertos pueden ser puertos físicos, VLAN o grupos de interfaces. | Sí | |
|---|----|--|

Configuración de subred

Una subred contiene pools de direcciones IP y una puerta de enlace predeterminada que se pueden asignar a las LIF utilizadas por las SVM que residen en el espacio IP.

- Al crear una LIF en una SVM, puede especificar el nombre de la subred en lugar de suministrar una dirección IP y una subred.
- Dado que puede configurarse una subred con una puerta de enlace predeterminada, no tiene que crear la puerta de enlace predeterminada en un paso independiente al crear una SVM.
- Un dominio de retransmisión puede contener una o varias subredes.
- Puede configurar las LIF de SVM que están en diferentes subredes mediante la asociación de más de una subred al dominio de retransmisión del espacio IP.
- Cada subred debe contener direcciones IP que no se superpongan con direcciones IP asignadas a otras subredes en el mismo espacio IP.
- Puede asignar direcciones IP específicas a LIF de datos de SVM y crear una puerta de enlace predeterminada para la SVM en lugar de usar una subred.

| Información | Necesario | Sus valores |
|---|-----------|-------------|
| Nombre del espacio IP El espacio IP al que se asignará la subred. Este espacio IP debe existir. | Sí | |
| Nombre de subred El nombre de la subred. Este nombre debe ser único en el espacio IP. | Sí | |
| Nombre de dominio de retransmisión El dominio de retransmisión al que se asignará la subred. Este dominio de retransmisión debe residir en el espacio IP especificado. | Sí | |

| | | |
|---|----|--|
| <p>Nombre de subred y máscara</p> <p>La subred y la máscara en la que residen las direcciones IP.</p> | Sí | |
| <p>Puerta de enlace</p> <p>No puede especificar una puerta de enlace predeterminada para la subred.</p> <p>Si no asigna una puerta de enlace al crear la subred, puede asignarla otra más adelante.</p> | No | |
| <p>Intervalos de direcciones IP</p> <p>Puede especificar un rango de direcciones IP o direcciones IP específicas.</p> <p>Por ejemplo, puede especificar un rango como:</p> <p>192.168.1.1–192.168.1.100, 192.168.1.112, 192.168.1.145</p> <p>Si no especifica un rango de direcciones IP, el rango completo de direcciones IP de la subred especificada está disponible para asignarse a las LIF.</p> | No | |
| <p>Forzar actualización de asociaciones de LIF</p> <p>Especifica si se fuerza la actualización de las asociaciones LIF existentes.</p> <p>De forma predeterminada, se produce un error en la creación de subredes si alguna interfaz de procesador de servicio o interfaces de red está utilizando las direcciones IP de los rangos proporcionados.</p> <p>El uso de este parámetro asocia cualquier interfaz tratada manualmente con la subred y permite que el comando se lleve a cabo correctamente.</p> | No | |

Configuración de SVM

Utiliza SVM para servir datos a los clientes y hosts.

Los valores registrados sirven para crear una SVM de datos predeterminada. Si crea una SVM de origen de MetroCluster, consulte "[Guía de instalación y configuración de MetroCluster estructural](#)" o la "[Guía de instalación y configuración de MetroCluster con ampliación](#)".

| Información | Necesario | Sus valores |
|-------------|-----------|-------------|
|-------------|-----------|-------------|

| | | |
|---|----|--|
| <p>Nombre de SVM</p> <p>El nombre de dominio completo (FQDN) de la SVM.</p> <p>Este nombre debe ser único en las ligas de clústeres.</p> | Sí | |
| <p>Nombre del volumen raíz</p> <p>El nombre del volumen raíz de la SVM.</p> | Sí | |
| <p>Nombre del agregado</p> <p>El nombre del agregado que contiene el volumen raíz de la SVM.</p> <p>Debe existir este agregado.</p> | Sí | |
| <p>Estilo de seguridad</p> <p>El estilo de seguridad para el volumen raíz de SVM.</p> <p>Los valores posibles son ntfs, unix y mezclado.</p> | Sí | |
| <p>Nombre del espacio IP</p> <p>El espacio IP al que se asigna la SVM.</p> <p>Este espacio IP debe existir.</p> | No | |
| <p>Configuración de idioma de SVM</p> <p>El idioma predeterminado que se usará para la SVM y sus volúmenes.</p> <p>Si no especifica un idioma predeterminado, el idioma de SVM predeterminado se establece en C.UTF-8.</p> <p>La configuración de idioma de SVM determina el conjunto de caracteres utilizado para mostrar los nombres de archivos y los datos de todos los volúmenes NAS de la SVM.</p> <p>Puede modificar el idioma después de crear la SVM.</p> | No | |

Configuración de LIF

Una SVM proporciona datos a clientes y hosts a través de una o varias interfaces lógicas de red (LIF).

| Información | Necesario | Sus valores |
|--|-----------|-------------|
| <p>Nombre de SVM</p> <p>El nombre de la SVM para la LIF.</p> | Sí | |

| | | |
|---|----|--|
| <p>Nombre de LIF Nombre de la LIF.</p> <p>Puede asignar varios LIF de datos por nodo y puede asignar LIF a cualquier nodo del clúster, siempre y cuando el nodo tenga puertos de datos disponibles.</p> <p>Para proporcionar redundancia, debe crear al menos dos LIF de datos para cada subred de datos, y las LIF asignadas a una subred en particular deben asignarse puertos principales en nodos diferentes.</p> <p>Importante: Si está configurando un servidor SMB para que aloje Hyper-V o SQL Server a través de SMB para soluciones de operaciones no disruptivas, la SVM debe tener al menos una LIF de datos en cada nodo del clúster.</p> | Sí | |
| <p>Política de servicios Política de servicio para la LIF.</p> <p>La política de servicio define qué servicios de red pueden utilizar la LIF. Hay disponibles políticas de servicio y servicios incorporados para gestionar el tráfico de datos y gestión de las SVM de los datos y del sistema.</p> | Sí | |
| <p>Protocolos permitidos Los LIF basados en IP no requieren protocolos permitidos; en su lugar, utilice la fila de políticas de servicio.</p> <p>Especifique los protocolos permitidos para LIF SAN en puertos FibreChannel. Estos son los protocolos que pueden utilizar esa LIF. Los protocolos que usan la LIF no se pueden modificar una vez creada la LIF. Debe especificar todos los protocolos al configurar la LIF.</p> | No | |
| <p>Nodo de inicio El nodo al que devuelve el LIF cuando el LIF se revierte a su puerto principal.</p> <p>Debería registrar un nodo de inicio para cada LIF de datos.</p> | Sí | |

| | | |
|---|-------------------------------|--|
| <p>Puerto inicial o dominio de retransmisión Elija una de las siguientes opciones:</p> <p>Puerto: Especifique el puerto al que regresa la interfaz lógica cuando la LIF se vuelve a su puerto de origen. Esto solo se realiza para la primera LIF de la subred de un espacio IP, si no es necesario.</p> <p>Dominio de difusión: Especifique el dominio de difusión, y el sistema seleccionará el puerto apropiado al que la interfaz lógica devuelve cuando el LIF vuelve a su puerto de origen.</p> | Sí | |
| <p>Nombre de subred La subred que se asignará a la SVM.</p> <p>Todos los LIF de datos utilizados para crear conexiones SMB disponibles de forma continua para servidores de aplicaciones deben estar en la misma subred.</p> | Sí (si se utiliza una subred) | |

Configuración de DNS

Debe configurar DNS en la SVM antes de crear un servidor NFS o SMB.

| Información | Necesario | Sus valores |
|---|-----------|-------------|
| <p>Nombre de SVM El nombre de la SVM en la que se creará el servidor NFS o SMB.</p> | Sí | |
| <p>Nombre de dominio DNS Lista de nombres de dominio que se anexan a un nombre de host al realizar la resolución de nombres de host a IP.</p> <p>Enumere primero el dominio local, seguido de los nombres de dominio para los que se realizan más a menudo las consultas DNS.</p> | Sí | |

| | | |
|--|----|--|
| <p>Direcciones IP de los servidores DNS</p> <p>Lista de direcciones IP para los servidores DNS que proporcionarán la resolución de nombres para el servidor NFS o SMB.</p> <p>Los servidores DNS enumerados deben contener los registros de ubicación de servicio (SRV) necesarios para localizar los servidores LDAP de Active Directory y los controladores de dominio para el dominio al que se unirá el servidor SMB.</p> <p>El registro SRV se utiliza para asignar el nombre de un servicio al nombre de equipo DNS de un servidor que ofrece ese servicio. Se produce un error en la creación del servidor SMB si ONTAP no puede obtener los registros de ubicación del servicio mediante consultas DNS locales.</p> <p>La forma más sencilla de garantizar que ONTAP pueda localizar los registros SRV de Active Directory es configurar los servidores DNS integrados de Active Directory como servidores DNS de SVM.</p> <p>Puede utilizar servidores DNS no integrados en Active Directory siempre que el administrador DNS haya agregado manualmente los registros SRV a la zona DNS que contenga información acerca de los controladores de dominio de Active Directory.</p> <p>Para obtener información acerca de los registros SRV integrados en Active Directory, consulte el tema "Cómo funciona la compatibilidad con DNS para Active Directory en Microsoft TechNet".</p> | Sí | |
|--|----|--|

Configuración de DNS dinámica

Antes de poder utilizar DNS dinámico para agregar automáticamente entradas DNS a los servidores DNS integrados en Active Directory, debe configurar DNS dinámico (DDNS) en la SVM.

Se crean registros de DNS para cada LIF de datos de la SVM. Si crea varias LIF de datos en la SVM, puede equilibrar las conexiones de clientes con las direcciones IP de datos asignadas. La carga DNS equilibra las conexiones que se realizan utilizando el nombre de host a las direcciones IP asignadas en un turno rotatorio.

| Información | Necesario | Sus valores |
|---|-----------|-------------|
| <p>Nombre de SVM</p> <p>La SVM en la que desea crear un servidor NFS o SMB.</p> | Sí | |

| | | |
|---|----|--|
| <p>Si se utiliza DDNS Especifica si se debe usar DDNS.</p> <p>Los servidores DNS configurados en la SVM deben ser compatibles con DDNS. De forma predeterminada, DDNS está desactivado.</p> | Sí | |
| <p>Si se utiliza DDNS seguro La DDNS segura solo es compatible con el DNS integrado en Active Directory.</p> <p>Si el DNS integrado en Active Directory sólo permite actualizaciones DDNS seguras, el valor de este parámetro debe ser TRUE.</p> <p>De forma predeterminada, la DDNS segura está desactivada.</p> <p>La DDNS segura solo se puede habilitar después de que se haya creado un servidor SMB o una cuenta de Active Directory para la SVM.</p> | No | |
| <p>FQDN del dominio DNS El FQDN del dominio DNS.</p> <p>Debe usar el mismo nombre de dominio configurado para los servicios de nombre DNS en la SVM.</p> | No | |

Flujo de trabajo de conmutación al nodo de respaldo de ruta NAS (ONTAP 9,7 y versiones anteriores)

Configuración de la conmutación por error de ruta NAS (ONTAP 9,7 y versiones anteriores)

Este flujo de trabajo le guía por los pasos de configuración de redes para configurar la conmutación por error de rutas NAS para ONTAP 9.0 - 9.7. En este flujo de trabajo se dan por hechos los siguientes elementos:

- Desea utilizar las prácticas recomendadas de conmutación por error de rutas NAS que simplifican la configuración de red.
- Desea utilizar la CLI, no con System Manager.
- Está configurando la conexión a redes en un sistema nuevo que ejecuta ONTAP 9.0 a 9.7.

Si ejecuta una versión de ONTAP posterior a 9.7, debe utilizar el procedimiento de conmutación al nodo de respaldo de la ruta NAS para ONTAP 9.8 o posterior:

- [ONTAP 9.8 y flujo de trabajo de conmutación al nodo de respaldo de ruta de NAS posterior](#)

Si desea obtener información detallada sobre los componentes y la administración de la red, debe utilizar el

material de referencia de administración de red:

- [Información general sobre la gestión de redes](#)

Flujo de trabajo (ONTAP 9,7 y anterior)

Si ya está familiarizado con los conceptos básicos de red, es posible que pueda ahorrar tiempo en la configuración de la red revisando este flujo de trabajo práctico para la configuración de conmutación por error de ruta NAS.

Un LIF NAS migra automáticamente a un puerto de red superviviente tras un error de enlace en su puerto actual. Si su red es plana, puede confiar en los valores predeterminados de ONTAP para gestionar la recuperación tras fallos de ruta. De lo contrario, debe configurar la conmutación por error de ruta siguiendo los pasos de este flujo de trabajo.



Un LIF SAN no migra (a menos que lo mueva manualmente después del fallo del enlace). En su lugar, la tecnología multivía en el host desvía el tráfico a otra LIF. Para obtener más información, consulte ["Administración de SAN"](#).

1

"Rellene la hoja de trabajo"

Utilice la hoja de trabajo para planificar la conmutación por error de ruta NAS.

2

"Cree espacios IP"

Cree un espacio de dirección IP distinto para cada SVM en un clúster.

3

"Cree dominios de retransmisión"

Crear dominios de retransmisión.

4

"Crear subredes"

Cree subredes.

5

"Cree SVM"

Cree SVM para servir datos a los clientes.

6

"Cree LIF"

Cree LIF en los puertos que desee utilizar para acceder a los datos.

7

"Configure los servicios DNS para la SVM"

Configure los servicios DNS para la SVM antes de crear un servidor NFS o SMB.

Hoja de datos para la configuración de conmutación al nodo de respaldo de ruta NAS (ONTAP 9,7 y versiones anteriores)

Debe completar todas las secciones de la hoja de trabajo antes de configurar la conmutación por error de la ruta NAS.

Configuración del espacio IP

Puede usar un espacio IP para crear un espacio de direcciones IP distinto para cada SVM de un clúster. Esto permite a los clientes en dominios de red separados administrativamente acceder a los datos del clúster mientras utilizan direcciones IP superpuestas del mismo rango de subredes de direcciones IP.

| Información | Necesario | Sus valores |
|-------------|-----------|-------------|
|-------------|-----------|-------------|

| | | |
|--|----|--|
| Nombre del espacio IP <ul style="list-style-type: none"> • El nombre del espacio IP. • El nombre debe ser único en el clúster. | Sí | |
|--|----|--|

Configuración de dominio de retransmisión


Un dominio de retransmisión agrupa puertos que pertenecen a la misma red de capa 2 y establece la MTU para los puertos de dominio de retransmisión.

Los dominios de retransmisión se asignan a un espacio IP. Un espacio IP puede contener uno o varios dominios de retransmisión.



El puerto al que se conmuta por error un LIF debe ser miembro del grupo de conmutación por error de la LIF. Cuando se crea un dominio de retransmisión, ONTAP crea automáticamente un grupo de conmutación por error con el mismo nombre. El grupo de conmutación por error contiene todos los puertos asignados al dominio de retransmisión.

| Información | Necesario | Sus valores |
|--|-----------|-------------|
| Nombre del espacio IP <ul style="list-style-type: none"> • El espacio IP al que se asigna el dominio de retransmisión. • Debe existir el espacio IP. | Sí | |
| Nombre de dominio de retransmisión <ul style="list-style-type: none"> • El nombre del dominio de retransmisión. • Este nombre debe ser único en el espacio IP. | Sí | |

| | | |
|--|-----------|--|
| <p>MTU</p> <ul style="list-style-type: none"> • La MTU del dominio de retransmisión. • Normalmente configurado en 1500 o 9000. • El valor MTU se aplica a todos los puertos del dominio de retransmisión y a los puertos que se añadan posteriormente al dominio de retransmisión. <div>  <p>El valor MTU debe coincidir con todos los dispositivos conectados a esa red. Tenga en cuenta que el tráfico de gestión de puertos e0M y del procesador de servicios debe tener la MTU establecida en no más de 1500 bytes.</p> </div> | <p>Sí</p> | |
| <p>Puertos</p> <ul style="list-style-type: none"> • Los puertos de red que se añadirán al dominio de retransmisión. • Los puertos asignados al dominio de retransmisión pueden ser puertos físicos, VLAN o grupos de interfaces (grupos de interfaces). • Si un puerto está en otro dominio de retransmisión, debe eliminarse para poder agregarlo al dominio de retransmisión. • Los puertos se asignan especificando el nombre del nodo y el puerto: Por ejemplo, 1:e0d. | <p>Sí</p> | |

Configuración de subred

Una subred contiene pools de direcciones IP y una puerta de enlace predeterminada que se pueden asignar a las LIF utilizadas por las SVM que residen en el espacio IP.

- Al crear una LIF en una SVM, puede especificar el nombre de la subred en lugar de suministrar una dirección IP y una subred.
- Dado que puede configurarse una subred con una puerta de enlace predeterminada, no tiene que crear la puerta de enlace predeterminada en un paso independiente al crear una SVM.
- Un dominio de retransmisión puede contener una o varias subredes.
Puede configurar las LIF de SVM que están en diferentes subredes mediante la asociación de más de una subred al dominio de retransmisión del espacio IP.
- Cada subred debe contener direcciones IP que no se superpongan con direcciones IP asignadas a otras subredes en el mismo espacio IP.
- Puede asignar direcciones IP específicas a LIF de datos de SVM y crear una puerta de enlace predeterminada para la SVM en lugar de usar una subred.

| Información | Necesario | Sus valores |
|--|-----------|-------------|
| Nombre del espacio IP <ul style="list-style-type: none"> • El espacio IP al que se asignará la subred. • Debe existir el espacio IP. | Sí | |
| Nombre de subred <ul style="list-style-type: none"> • El nombre de la subred. • El nombre debe ser único en el espacio IP. | Sí | |
| Nombre de dominio de retransmisión <ul style="list-style-type: none"> • El dominio de retransmisión al que se asignará la subred. • El dominio de retransmisión debe residir en el espacio IP especificado. | Sí | |
| Nombre de subred y máscara <ul style="list-style-type: none"> • La subred y la máscara en la que residen las direcciones IP. | Sí | |

| | | |
|--|----|--|
| <p>Puerta de enlace</p> <ul style="list-style-type: none"> • No puede especificar una puerta de enlace predeterminada para la subred. • Si no asigna una puerta de enlace al crear la subred, puede asignarla a la subred en cualquier momento. | No | |
| <p>Intervalos de direcciones IP</p> <ul style="list-style-type: none"> • Puede especificar un rango de direcciones IP o direcciones IP específicas. Por ejemplo, puede especificar un rango como: 192.168.1.1– 192.168.1.100, 192.168.1.112, 192.168.1.145 • Si no especifica un rango de direcciones IP, el rango completo de direcciones IP de la subred especificada está disponible para asignarse a las LIF. | No | |
| <p>Forzar actualización de asociaciones de LIF</p> <ul style="list-style-type: none"> • Especifica si se fuerza la actualización de las asociaciones LIF existentes. • De forma predeterminada, se produce un error en la creación de subredes si alguna interfaz de procesador de servicio o interfaces de red está utilizando las direcciones IP de los rangos proporcionados. • El uso de este parámetro asocia cualquier interfaz tratada manualmente con la subred y permite que el comando se lleve a cabo correctamente. | No | |

Configuración de SVM

Utiliza SVM para servir datos a los clientes y hosts.

Los valores registrados sirven para crear una SVM de datos predeterminada. Si crea una SVM de origen de MetroCluster, consulte ["Instale un MetroCluster FAS"](#) o la ["Instale un MetroCluster de ampliación"](#).

| Información | Necesario | Sus valores |
|--|-----------|-------------|
| Nombre de SVM <ul style="list-style-type: none">• El nombre de la SVM.• Debe utilizar un nombre de dominio completo (FQDN) para garantizar nombres SVM únicos en las ligas de clústeres. | Sí | |
| Nombre del volumen raíz <ul style="list-style-type: none">• El nombre del volumen raíz de la SVM. | Sí | |
| Nombre del agregado <ul style="list-style-type: none">• El nombre del agregado que contiene el volumen raíz de la SVM.• Debe existir este agregado. | Sí | |
| Estilo de seguridad <ul style="list-style-type: none">• El estilo de seguridad para el volumen raíz de SVM.• Los valores posibles son ntfs, unix y mezclado. | Sí | |
| Nombre del espacio IP <ul style="list-style-type: none">• El espacio IP al que se asigna la SVM.• Este espacio IP debe existir. | No | |


| | | |
|---|----|--|
| <p>Configuración de idioma de SVM</p> <ul style="list-style-type: none"> • El idioma predeterminado que se usará para la SVM y sus volúmenes. • Si no especifica un idioma predeterminado, el idioma de SVM predeterminado se establece en C.UTF-8. • La configuración de idioma de SVM determina el conjunto de caracteres utilizado para mostrar los nombres de archivos y los datos de todos los volúmenes NAS de la SVM. Puede modificar el idioma después de crear la SVM. | No | |
|---|----|--|

Configuración de LIF

Una SVM proporciona datos a clientes y hosts a través de una o varias interfaces lógicas de red (LIF).

| Información | Necesario | Sus valores |
|---|-----------|-------------|
| <p>Nombre de SVM</p> <ul style="list-style-type: none"> • El nombre de la SVM para la LIF. | Sí | |

| | | |
|---|--|------------|
| <p>Nombre de LIF</p> <ul style="list-style-type: none"> • Nombre de la LIF. • Puede asignar varios LIF de datos por nodo y puede asignar LIF a cualquier nodo del clúster, siempre y cuando el nodo tenga puertos de datos disponibles. • Para proporcionar redundancia, debe crear al menos dos LIF de datos para cada subred de datos, y las LIF asignadas a una subred en particular deben asignarse puertos principales en nodos diferentes. <p>Importante: Si está configurando un servidor SMB para que aloje Hyper-V o SQL Server a través de SMB para soluciones de operaciones no disruptivas, la SVM debe tener al menos una LIF de datos en cada nodo del clúster.</p> | Sí | |
| <p>Rol de LIF</p> <ul style="list-style-type: none"> • El rol de la LIF. • Los LIF de datos tienen asignado el rol de datos. | <p>Sí</p> <p>Obsoleto de ONTAP 9,6</p> | sql server |
| <p>Política de servicios</p> <p>Política de servicio para la LIF.</p> <p>La política de servicio define qué servicios de red pueden utilizar la LIF. Hay disponibles políticas de servicio y servicios incorporados para gestionar el tráfico de datos y gestión de las SVM de los datos y del sistema.</p> | <p>Sí</p> <p>A partir de ONTAP 9,6</p> | |

| | | |
|---|----|--|
| <p>Protocolos permitidos</p> <ul style="list-style-type: none"> • Los protocolos que pueden utilizar la LIF. • De forma predeterminada, se permiten SMB, NFS y FlexCache. <p>El protocolo FlexCache permite usar un volumen como volumen de origen para un volumen FlexCache en un sistema que ejecuta Data ONTAP en 7-Mode.</p> <div>  <p>Los protocolos que usan la LIF no se pueden modificar una vez creada la LIF. Debe especificar todos los protocolos al configurar la LIF.</p> </div> | No | |
| <p>Nodo de inicio</p> <ul style="list-style-type: none"> • El nodo al que devuelve el LIF cuando el LIF se revierte a su puerto principal. • Debería registrar un nodo de inicio para cada LIF de datos. | Sí | |
| <p>Puerto inicial o dominio de retransmisión</p> <ul style="list-style-type: none"> • El puerto al que devuelve la interfaz lógica cuando el LIF se revierte a su puerto raíz. • Debe registrar un puerto de inicio para cada LIF de datos. | Sí | |

| | | |
|---|-------------------------------|--|
| Nombre de subred <ul style="list-style-type: none"> • La subred que se asignará a la SVM. • Todos los LIF de datos utilizados para crear conexiones SMB disponibles de forma continua para servidores de aplicaciones deben estar en la misma subred. | Sí (si se utiliza una subred) | |
|---|-------------------------------|--|

Configuración de DNS

Debe configurar DNS en la SVM antes de crear un servidor NFS o SMB.

| Información | Necesario | Sus valores |
|--|-----------|-------------|
| Nombre de SVM <ul style="list-style-type: none"> • El nombre de la SVM en la que se creará el servidor NFS o SMB. | Sí | |
| Nombre de dominio DNS <ul style="list-style-type: none"> • Lista de nombres de dominio que se anexan a un nombre de host al realizar la resolución de nombres de host a IP. • Enumere primero el dominio local, seguido de los nombres de dominio para los que se realizan más a menudo las consultas DNS. | Sí | |

| | | |
|--|-----------|--|
| <p>Direcciones IP de los servidores DNS</p> <ul style="list-style-type: none"> • Lista de direcciones IP para los servidores DNS que proporcionarán la resolución de nombres para el servidor NFS o SMB. • Los servidores DNS enumerados deben contener los registros de ubicación de servicio (SRV) necesarios para localizar los servidores LDAP de Active Directory y los controladores de dominio para el dominio al que se unirá el servidor SMB. El registro SRV se utiliza para asignar el nombre de un servicio al nombre de equipo DNS de un servidor que ofrece ese servicio. Se produce un error en la creación del servidor SMB si ONTAP no puede obtener los registros de ubicación del servicio mediante consultas DNS locales. La forma más sencilla de garantizar que ONTAP pueda localizar los registros SRV de Active Directory es configurar los servidores DNS integrados de Active Directory como servidores DNS de SVM. Puede utilizar servidores DNS no integrados en Active Directory siempre que el administrador DNS haya agregado manualmente los registros SRV a la zona DNS que contenga información acerca de los controladores de dominio de Active Directory. • Para obtener información acerca de los registros SRV integrados en Active Directory, consulte el tema "Cómo funciona la compatibilidad con DNS para Active Directory en Microsoft TechNet". | <p>Sí</p> | |
|--|-----------|--|

Configuración de DNS dinámica

Antes de poder utilizar DNS dinámico para agregar automáticamente entradas DNS a los servidores DNS integrados en Active Directory, debe configurar DNS dinámico (DDNS) en la SVM.

Se crean registros de DNS para cada LIF de datos de la SVM. Si crea varias LIF de datos en la SVM, puede equilibrar las conexiones de clientes con las direcciones IP de datos asignadas. La carga DNS equilibra las conexiones que se realizan utilizando el nombre de host a las direcciones IP asignadas en un turno rotatorio.

| Información | Necesario | Sus valores |
|--|-----------|-------------|
| Nombre de SVM <ul style="list-style-type: none">• La SVM en la que desea crear un servidor NFS o SMB. | Sí | |
| Si se utiliza DDNS <ul style="list-style-type: none">• Especifica si se debe usar DDNS.• Los servidores DNS configurados en la SVM deben ser compatibles con DDNS. De forma predeterminada, DDNS está desactivado. | Sí | |
| Si se utiliza DDNS seguro <ul style="list-style-type: none">• La DDNS segura solo es compatible con el DNS integrado en Active Directory.• Si el DNS integrado en Active Directory sólo permite actualizaciones DDNS seguras, el valor de este parámetro debe ser TRUE.• De forma predeterminada, la DDNS segura está desactivada.• La DDNS segura solo se puede habilitar después de que se haya creado un servidor SMB o una cuenta de Active Directory para la SVM. | No | |

| | | |
|--|----|--|
| FQDN del dominio DNS | No | |
| <ul style="list-style-type: none"> • El FQDN del dominio DNS. • Debe usar el mismo nombre de dominio configurado para los servicios de nombre DNS en la SVM. | | |

Puertos de red

Configure la descripción general de los puertos de red

Los puertos son puertos físicos (NIC) o puertos virtualizados, como grupos de interfaces o VLAN.

Las redes de área local virtual (VLAN) y los grupos de interfaces constituyen los puertos virtuales. Los grupos de interfaces tratan varios puertos físicos como un único puerto, mientras que las VLAN subdividen un puerto físico en varios puertos lógicos distintos.

- Puertos físicos: Las LIF se pueden configurar directamente en puertos físicos.
- Grupo de interfaces: Agregado de puertos que contiene dos o más puertos físicos que actúan como un único puerto de enlace. Un grupo de interfaces puede ser de modo único, multimodo o multimodo dinámico.
- VLAN: Puerto lógico que recibe y envía tráfico etiquetado mediante VLAN (estándar IEEE 802.1Q). Las características del puerto VLAN incluyen el identificador de VLAN del puerto. Los puertos de puerto físico o de grupo de interfaces subyacentes se consideran puertos troncales VLAN y los puertos del switch conectados se deben configurar para que los identificadores de VLAN se queden troncales.

Los puertos de puerto físico o grupo de interfaces subyacentes de un puerto VLAN pueden seguir aumentando los LIF del host, que transmiten y reciben tráfico sin etiquetas.

- Puerto IP virtual (VIP): Puerto lógico que se utiliza como puerto raíz de un LIF VIP. El sistema crea los puertos VIP automáticamente y solo admite un número limitado de operaciones. Los puertos VIP son compatibles a partir de ONTAP 9.5.

La convención de nomenclatura de puertos es *enumeración*:

- El primer carácter describe el tipo de puerto.
"e" representa Ethernet.
- El segundo carácter indica la ranura numerada en la que se encuentra el adaptador de puerto.
- El tercer carácter indica la posición del puerto en un adaptador multipuerto.
"a" indica el primer puerto, "b" indica el segundo puerto, etc.

Por ejemplo: e0b Indica que un puerto Ethernet es el segundo puerto de la placa base del nodo.

Las VLAN deben nombrarse mediante la sintaxis `port_name-vlan-id`.

`port_name` especifica el puerto físico o el grupo de interfaces.

`vlan-id` Especifica la identificación de VLAN en la red. Por ejemplo: `e1c-80` Es un nombre de VLAN válido.

Configure los puertos de red

Combine puertos físicos para crear grupos de interfaces

Un grupo de interfaces, también conocido como Grupo de Agregación de Enlaces (LAG), se crea combinando dos o más puertos físicos en el mismo nodo en un único puerto lógico. El puerto lógico proporciona una mayor resiliencia, mayor disponibilidad y uso compartido de carga.

Tipos de grupos de interfaces

El sistema de almacenamiento admite tres tipos de grupos de interfaces: Modo único, modo estático y modo múltiple dinámico. Cada grupo de interfaces proporciona diferentes niveles de tolerancia a fallos. Los grupos de interfaces multimodo proporcionan métodos de equilibrio de carga del tráfico de red.

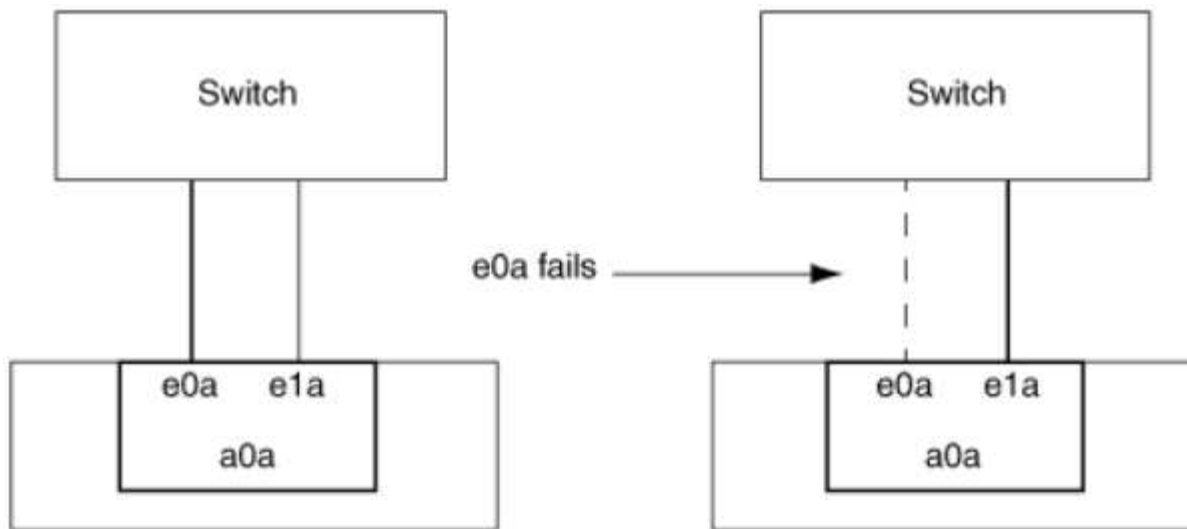
Características de los grupos de interfaces de un único modo

En un grupo de interfaces de un solo modo, solo una de las interfaces del grupo de interfaces está activa. Las otras interfaces están en espera y listas para hacerse cargo si falla la interfaz activa.

Características de los grupos de interfaces de un único modo:

- En caso de conmutación por error, el clúster supervisa el enlace activo y controla la conmutación por error. Dado que el clúster supervisa el enlace activo, no es necesario configurar el switch.
- Puede haber más de una interfaz en espera en un grupo de interfaces de un solo modo.
- Si un grupo de interfaces de un único modo abarca varios switches, debe conectar los switches con un enlace entre switches (ISL).
- Para un grupo de interfaces de un solo modo, los puertos del switch deben estar en el mismo dominio de retransmisión.
- Los paquetes ARP de supervisión de enlaces, que tienen la dirección de origen 0.0.0.0, se envían a través de los puertos para verificar que los puertos están en el mismo dominio de retransmisión.

La siguiente figura es un ejemplo de un grupo de interfaces de modo único. En la figura, `e0a` y `e1a` forman parte del grupo de interfaces de modo único `a0a`. Si la interfaz activa, `e0a`, falla, la interfaz `e1a` en espera toma el control y mantiene la conexión con el switch.



Para lograr la funcionalidad de modo único, el método recomendado es utilizar en su lugar grupos de conmutación por error. Al utilizar un grupo de conmutación por error, el segundo puerto puede seguir siendo utilizado para otros LIF y, por lo tanto, no tiene por qué quedar sin utilizar. Además, los grupos de conmutación por error pueden abarcar más de dos puertos y pueden abarcar puertos en varios nodos.

Características de los grupos de interfaces estáticas multimodo

La implementación del grupo de interfaces estáticas multimodo en ONTAP cumple con IEEE 802.3ad (estático). Cualquier switch compatible con agregados, pero no tiene intercambio de paquetes de control para configurar un agregado, se puede utilizar con grupos de interfaces estáticas multimodo.

Los grupos de interfaces estáticas multimodo no cumplen el estándar IEEE 802.3ad (dinámico), también conocido como Protocolo de control de agregación de enlaces (LACP). LACP equivale al Protocolo de agregación de puertos (PAgP), el protocolo de agregación de enlaces de propiedad de Cisco.

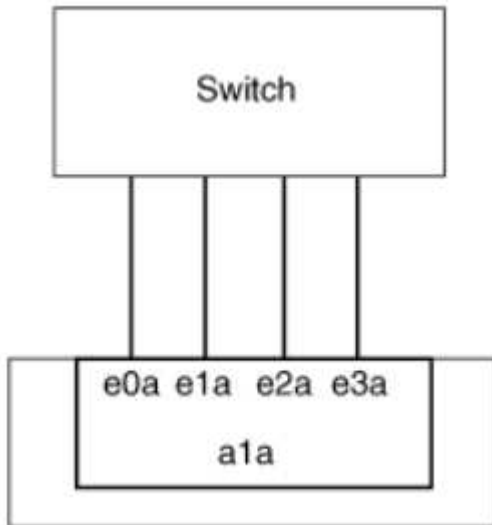
Las siguientes son características de un grupo de interfaces estáticas multimodo:

- Todas las interfaces del grupo de interfaces están activas y comparten una única dirección MAC.
 - Se distribuyen varias conexiones individuales entre las interfaces del grupo de interfaces.
 - Cada conexión o sesión utiliza una interfaz dentro del grupo de interfaces.
Cuando se utiliza el esquema de equilibrio de carga secuencial, todas las sesiones se distribuyen por los enlaces disponibles de forma individual y no están vinculadas a una interfaz determinada del grupo de interfaces.
- Los grupos de interfaces estáticas multimodo pueden recuperarse de un fallo de hasta interfaces n-1, donde n es el número total de interfaces que forman el grupo de interfaces.
- Si un puerto falla o está desenchufado, el tráfico que atravesaba el vínculo fallido se redistribuye automáticamente a una de las interfaces restantes.
- Los grupos de interfaces estáticas multimodo pueden detectar una pérdida de enlaces, pero además no pierden la conectividad con las configuraciones erróneas de switches o clientes que podrían afectar a la conectividad y al rendimiento.
- Un grupo de interfaces estáticas multimodo requiere un switch que admita la agregación de enlaces en varios puertos de switch.
El switch está configurado de modo que todos los puertos a los que están conectados los enlaces de un grupo de interfaces formen parte de un único puerto lógico. Es posible que algunos switches no admitan la

agregación de enlaces de puertos configurados para tramas gigantes. Para obtener más información, consulte la documentación de su proveedor de switches.

- Hay disponibles varias opciones de equilibrio de carga para distribuir el tráfico entre las interfaces de un grupo de interfaces estáticas multimodo.

La siguiente figura muestra un ejemplo de un grupo de interfaces estáticas multimodo. Las interfaces e0a, e1a, e2a y e3a forman parte del grupo de interfaces multimodo a1a. Las cuatro interfaces del grupo de interfaces multimodo a1a están activas.



Existen varias tecnologías que permiten distribuir el tráfico de un único enlace agregado por varios switches físicos. Las tecnologías utilizadas para lograr esta funcionalidad varían entre los productos de red. Los grupos de interfaces estáticas multimodo de ONTAP cumplen los estándares IEEE 802.3. Si se dice que una tecnología de agregación de enlaces de conmutación múltiple en particular interopera o se ajusta a los estándares IEEE 802.3, debe funcionar con ONTAP.

El estándar IEEE 802.3 indica que el dispositivo de transmisión de un enlace agregado determina la interfaz física para la transmisión. Por lo tanto, ONTAP sólo es responsable de distribuir el tráfico saliente y no puede controlar cómo llegan las tramas entrantes. Si desea gestionar o controlar la transmisión del tráfico entrante en un enlace agregado, dicha transmisión debe modificarse en el dispositivo de red conectado directamente.

Grupo de interfaces dinámicas multimodo

Los grupos de interfaces dinámicas multimodo implementan el protocolo de control de agregación de enlaces (LACP) para comunicar la pertenencia a grupos al switch conectado directamente. LACP permite detectar la pérdida del estado de enlace y la incapacidad del nodo para comunicarse con el puerto del switch de conexión directa.

La implementación de grupos de interfaces dinámicas multimodo en ONTAP cumple con IEEE 802.3 AD (802.1 AX). ONTAP no admite el Protocolo de agregación de puertos (PAgP), que es un protocolo de agregación de enlaces de propiedad de Cisco.

Un grupo de interfaces dinámicas multimodo requiere un switch compatible con LACP.

ONTAP implementa LACP en el modo activo no configurable que funciona bien con los switches configurados en modo activo o pasivo. ONTAP implementa los temporizadores LACP cortos y largos (para su uso con valores no configurables de 3 segundos y 90 segundos), tal y como se especifica en IEEE 802.3 AD (802.1AX).

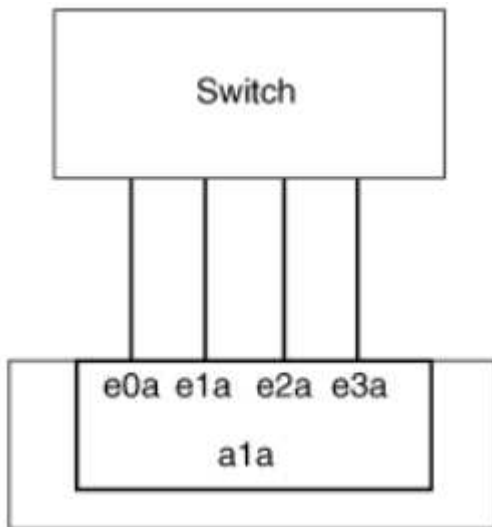
El algoritmo de equilibrio de carga de ONTAP determina el puerto de miembro que se va a utilizar para transmitir tráfico saliente y no controla cómo se reciben las tramas entrantes. El conmutador determina el miembro (puerto físico individual) de su grupo de canales de puertos que se utilizará para la transmisión, en función del algoritmo de equilibrio de carga configurado en el grupo de canales de puertos del conmutador. Por lo tanto, la configuración del switch determina el puerto miembro (puerto físico individual) del sistema de almacenamiento que recibirá tráfico. Para obtener más información sobre la configuración del switch, consulte la documentación de su proveedor de switches.

Si una interfaz individual no puede recibir paquetes de protocolo LACP sucesivos, dicha interfaz individual se marca como "lag_inactive" en el resultado del comando "ifgrp status". El tráfico existente se redirecciona automáticamente a las interfaces activas restantes.

Las siguientes reglas se aplican cuando se utilizan grupos de interfaces dinámicas multimodo:

- Deben configurarse los grupos de interfaces dinámicas multimodo para utilizar los métodos de equilibrio de carga por turnos, basados en puertos, IP, MAC o round-robin.
- En un grupo de interfaces dinámicas multimodo, todas las interfaces deben estar activas y compartir una única dirección MAC.

La siguiente figura muestra un ejemplo de un grupo de interfaces dinámicas multimodo. Las interfaces e0a, e1a, e2a y e3a forman parte del grupo de interfaces multimodo a1a. Las cuatro interfaces del grupo de interfaces dinámicas multimodo a1a están activas.



Equilibrio de carga en grupos de interfaces multimodo

Puede asegurarse de que todas las interfaces de un grupo de interfaces multimodo se utilicen de igual modo para el tráfico saliente, usando los métodos de dirección IP, dirección MAC, secuencial o equilibrio de carga basado en puertos para distribuir el tráfico de red de forma equitativa por los puertos de red de un grupo de interfaces multimodo.

Solo se puede especificar el método de equilibrio de carga de un grupo de interfaces multimodo cuando se crea el grupo de interfaces.

Mejor práctica: Se recomienda el equilibrio de carga basado en puerto siempre que sea posible. Utilice el equilibrio de carga basado en puerto a menos que haya un motivo o una limitación específicos en la red que lo impida.

Equilibrio de carga basado en puertos

El equilibrio de carga basado en puerto es el método recomendado.

Puede equilibrar el tráfico en un grupo de interfaces multimodo según los puertos de la capa de transporte (TCP/UDP) usando el método de equilibrio de carga basado en puerto.

El método de equilibrio de carga basado en puertos utiliza un algoritmo de funciones hash rápidas en las direcciones IP de origen y destino junto con el número de puerto de la capa de transporte.

Dirección IP y equilibrio de carga de direcciones MAC

Las direcciones IP y el equilibrio de carga de direcciones MAC son los métodos para equilibrar el tráfico de los grupos de interfaces multimodo.

Estos métodos de equilibrio de carga utilizan un algoritmo de funciones hash rápidas en las direcciones de origen y destino (dirección IP y dirección MAC). Si el resultado del algoritmo de funciones hash se asigna a una interfaz que no está en EL estado DE enlace ACTIVO, se utiliza la siguiente interfaz activa.



No seleccione el método de equilibrio de carga de direcciones MAC al crear grupos de interfaces en un sistema que se conecta directamente a un router. En este tipo de configuración, para cada trama IP saliente, la dirección MAC de destino es la dirección MAC del router. Como resultado, sólo se utiliza una interfaz del grupo de interfaces.

El equilibrio de carga de direcciones IP funciona del mismo modo para las direcciones IPv4 e IPv6.

Equilibrio de carga secuencial

Puede utilizar el equilibrio de carga secuencial para distribuir de forma equitativa paquetes entre varios vínculos mediante un algoritmo de operación por turnos. Puede utilizar la opción secuencial para equilibrar la carga del tráfico de una conexión única en varios enlaces con el fin de aumentar el rendimiento de la conexión.

No obstante, debido a que el equilibrio de carga secuencial puede provocar una entrega de paquetes fuera de servicio, puede resultar en un rendimiento extremadamente bajo. Por lo tanto, por lo general no se recomienda el equilibrio de carga secuencial.

Cree un grupo de interfaces o LAG

Puede crear un grupo de interfaces o LAG —de un solo modo, multimodo estático o modo múltiple dinámico (LACP)— para presentar una única interfaz a los clientes combinando las funcionalidades de los puertos de red agregados.

El procedimiento que siga depende de la interfaz que utilice: System Manager o CLI:

System Manager

Utilice System Manager para crear un LAG

Pasos

1. Seleccione **Red > Puerto Ethernet > + Grupo de agregación de enlaces** para crear un LAG.
2. Seleccione el nodo de la lista desplegable.
3. Elija una de las siguientes opciones:
 - a. ONTAP to **selecciona automáticamente el dominio de difusión (recomendado)**.
 - b. Para seleccionar manualmente un dominio de retransmisión.
4. Seleccione los puertos que van a formar LAG.
5. Seleccione el modo:
 - a. Único: Solo se utiliza un puerto a la vez.
 - b. Múltiples: Todos los puertos se pueden utilizar simultáneamente.
 - c. LACP: El protocolo LACP determina los puertos que se pueden utilizar.
6. Seleccione el equilibrio de carga:
 - a. Basado en IP
 - b. Basado en Mac
 - c. Puerto
 - d. Secuencial
7. Guarde los cambios.

The screenshot shows the 'Add Link Aggregation Group' dialog box in the ONTAP System Manager interface. The dialog has a dark blue header with the title 'Add Link Aggregation Group' and a close button (X). Below the header, there are several sections for configuration:

- NODE:** A dropdown menu showing 'sti47-vs1m-ucs521e'.
- BROADCAST DOMAIN:** A dropdown menu showing 'Automatically select broadcast domain (Recommended)'. A red arrow points to this dropdown with a note: 'Note: Instead of a global switch or checkbox, what if we expose BD dropdown with "Automatic" as a default selection?'.
- PORTS TO INCLUDE:** Two checkboxes labeled 'e0e' and 'e0f', both of which are unchecked.
- MODE:** Three radio button options: 'Single' (selected), 'Multiple', and 'LACP'. Below 'Single' is the text 'Only one port is used at a time.' Below 'Multiple' is 'All ports can be used simultaneously.' Below 'LACP' is 'The LACP protocol determines the ports that can be used.'
- LOAD DISTRIBUTION:** Two radio button options: 'IP based' (selected) and 'MAC based'. Below 'IP based' is the text 'Network traffic is distributed based on the destination IP address.' Below 'MAC based' is 'Network traffic is distributed based on the next-hop MAC addresses.'

At the bottom of the dialog, there are three small icons: a left arrow, a right arrow, and a refresh icon.

CLI

Utilice la CLI para crear un grupo de interfaces

Para obtener una lista completa de las restricciones de configuración que se aplican a los grupos de interfaces de puertos, consulte `network port ifgrp add-port` página de manual.

Al crear un grupo de interfaces multimodo, puede especificar cualquiera de los siguientes métodos de equilibrio de carga:

- `port`: El tráfico de red se distribuye sobre la base de los puertos de la capa de transporte (TCP/UDP). Este es el método de equilibrio de carga recomendado.
- `mac`: El tráfico de red se distribuye sobre la base de direcciones MAC.
- `ip`: El tráfico de red se distribuye sobre la base de direcciones IP.
- `sequential`: El tráfico de red se distribuye tal y como se recibe.



La dirección MAC de un grupo de interfaces se determina por el orden de los puertos subyacentes y cómo se inician estos puertos durante el arranque. Por lo tanto, no debe asumir que la dirección MAC de ifgrp permanece en reinicios o actualizaciones de ONTAP.

Paso

Utilice la `network port ifgrp create` comando para crear un grupo de interfaces.

Los grupos de interfaces deben nombrarse utilizando la sintaxis `a<number><letter>`. Por ejemplo, `a0a`, `a0b`, `a1c` y `a2a` son nombres de grupos de interfaces válidos.

Para obtener más información acerca de este comando, consulte ["Comandos de ONTAP 9"](#).

El siguiente ejemplo muestra cómo crear un grupo de interfaces llamado `a0a` con una función de distribución de puerto y un modo de modo múltiple:

```
network port ifgrp create -node cluster-1-01 -ifgrp a0a -distr-func port -mode multimode
```

Agregue un puerto a un grupo de interfaces o LAG

Puede agregar hasta 16 puertos físicos a un grupo de interfaces o LAG para todas las velocidades de puerto.

El procedimiento que siga depende de la interfaz que utilice: System Manager o CLI:

System Manager

Utilice System Manager para agregar un puerto a un LAG

Pasos

1. Seleccione **Red > Puerto Ethernet > LAG** para editar un LAG.
2. Seleccione puertos adicionales en el mismo nodo para agregarlos al LAG.
3. Guarde los cambios.

CLI

Utilice la CLI para agregar puertos a un grupo de interfaces

Paso

Añada puertos de red al grupo de interfaces:

```
network port ifgrp add-port
```

Para obtener más información acerca de este comando, consulte ["Comandos de ONTAP 9"](#).

En el siguiente ejemplo se muestra cómo agregar el puerto e0c a un grupo de interfaces llamado a0a:

```
network port ifgrp add-port -node cluster-1-01 -ifgrp a0a -port e0c
```

A partir de ONTAP 9.8, los grupos de interfaces se colocan automáticamente en un dominio de retransmisión adecuado un minuto después de agregar el primer puerto físico al grupo de interfaces. Si no desea que ONTAP haga esto y prefiere colocar manualmente el ifgrp en un dominio de difusión, especifique el `-skip-broadcast-domain-placement` parámetro como parte de la `ifgrp add-port` comando.

Quite un puerto de un grupo de interfaces o LAG

Puede quitar un puerto de un grupo de interfaces que aloje LIF, siempre y cuando no sea el último puerto del grupo de interfaces. No es necesario que el grupo de interfaces no deba ser LIF de host ni que el grupo de interfaces no sea el puerto de inicio de una LIF teniendo en cuenta que no está quitando el último puerto del grupo de interfaces. Sin embargo, si va a eliminar el último puerto, primero debe migrar o mover las LIF del grupo de interfaces.

Acerca de esta tarea

Puede eliminar hasta 16 puertos (interfaces físicas) de un grupo de interfaces o LAG.

El procedimiento que siga depende de la interfaz que utilice: System Manager o CLI:

System Manager

Utilice System Manager para quitar un puerto de un LAG

Pasos

1. Seleccione **Red > Puerto Ethernet > LAG** para editar un LAG.
2. Seleccione los puertos que desea eliminar del LAG.
3. Guarde los cambios.

CLI

Utilice la CLI para quitar puertos de un grupo de interfaces

Paso

Quite puertos de red de un grupo de interfaces:

```
network port ifgrp remove-port
```

En el ejemplo siguiente se muestra cómo quitar el puerto e0c de un grupo de interfaces llamado a0a:

```
network port ifgrp remove-port -node cluster-1-01 -ifgrp a0a -port e0c
```

Eliminar un grupo de interfaces o LAG

Puede eliminar grupos de interfaces o LAG si desea configurar LIF directamente en los puertos físicos subyacentes o si decide cambiar el grupo de interfaces, el modo LAG o la función de distribución.

Antes de empezar

- El grupo de interfaces o LAG no deben alojar una LIF.
- El grupo de interfaces o LAG no deben ser ni el puerto de inicio ni el destino de conmutación por error de una LIF.

El procedimiento que siga depende de la interfaz que utilice: System Manager o CLI:

System Manager

Utilice el Administrador del sistema para eliminar un LAG

Pasos

1. Seleccione **Red > Puerto Ethernet > LAG** para eliminar un LAG.
2. Seleccione el LAG que desea eliminar.
3. Elimine el LAG.

CLI

Utilice la CLI para eliminar un grupo de interfaces

Paso

Utilice la `network port ifgrp delete` comando para eliminar un grupo de interfaces.

Para obtener más información acerca de este comando, consulte ["Comandos de ONTAP 9"](#).

El siguiente ejemplo muestra cómo eliminar un grupo de interfaces llamado a0b:

```
network port ifgrp delete -node cluster-1-01 -ifgrp a0b
```

Configure las VLAN en puertos físicos

Puede utilizar VLAN en ONTAP para proporcionar segmentación lógica de redes mediante la creación de dominios de retransmisión independientes que se definen en función del puerto del switch en lugar de los dominios de retransmisión tradicionales, definidos en límites físicos.

Una VLAN puede abarcar varios segmentos de red física. Las estaciones finales que pertenecen a una VLAN están relacionadas por función o aplicación.

Por ejemplo, las estaciones finales de una VLAN podrían agruparse por departamentos, como ingeniería y contabilidad, o por proyectos, como release1 y reubicación2. Debido a que la proximidad física de las estaciones finales no es esencial en una VLAN, puede dispersar geográficamente las estaciones finales y todavía contener el dominio de difusión en una red conmutada.

En ONTAP 9.13.1 y 9.14.1, los puertos sin etiquetar que ninguna interfaz lógica (LIF) no utiliza y su ausencia de conectividad VLAN nativa en el switch conectado se marcan como degradados. Esto sirve para ayudar a identificar los puertos no utilizados y no indica una interrupción del servicio. Las VLAN nativas permiten el tráfico sin etiquetas en el puerto base ifgrp, como las emisiones CFM de ONTAP. Configure las VLAN nativas en el switch para evitar el bloqueo del tráfico sin etiquetar.

Puede gestionar las VLAN si crea, elimina o muestra información acerca de ellas.



No debe crear una VLAN en una interfaz de red con el mismo identificador que la VLAN nativa del switch. Por ejemplo, si la interfaz de red e0b se encuentra en una VLAN 10 nativa, no se debe crear una VLAN e0b-10 en esa interfaz.

Cree una VLAN

Puede utilizar System Manager o el para crear VLAN con el fin de mantener dominios de retransmisión independientes en el mismo dominio de redes `network port vlan create` comando.

Antes de empezar

Confirme que se han cumplido los siguientes requisitos:

- Los switches implementados en la red deben cumplir los estándares IEEE 802.1Q o tener una implementación de VLAN específica por proveedor.
- Para admitir varias VLAN, una estación final debe estar configurada de forma estática para que pertenezca a una o varias VLAN.
- La VLAN no está conectada a un puerto que aloja una LIF de clúster.
- La VLAN no está conectada a los puertos asignados al espacio IP del clúster.
- La VLAN no se crea en un puerto del grupo de interfaces que no contiene puertos miembro.

Acerca de esta tarea

La creación de una VLAN asocia la VLAN con el puerto de red en un nodo especificado de un clúster.

Cuando se configura una VLAN por primera vez en un puerto, el puerto podría estar inactivo, lo que podría dar lugar a una desconexión temporal de la red. Las adiciones posteriores de VLAN al mismo puerto no afectan al estado del puerto.



No debe crear una VLAN en una interfaz de red con el mismo identificador que la VLAN nativa del switch. Por ejemplo, si la interfaz de red e0b se encuentra en una VLAN 10 nativa, no se debe crear una VLAN e0b-10 en esa interfaz.

El procedimiento que siga depende de la interfaz que utilice: System Manager o CLI:

System Manager

Utilice System Manager para crear una VLAN

A partir de ONTAP 9.12.0, puede seleccionar automáticamente el dominio de difusión o seleccionar manualmente en de la lista. Antes, los dominios de retransmisión siempre se seleccionaban automáticamente en función de la conectividad de la capa 2. Si selecciona manualmente un dominio de retransmisión, aparecerá una advertencia que indica que la selección manual de un dominio de retransmisión podría provocar la pérdida de conectividad.

Pasos

1. Seleccione **Red > Puerto Ethernet > + VLAN**.
2. Seleccione el nodo de la lista desplegable.
3. Elija una de las siguientes opciones:
 - a. ONTAP to **selecciona automáticamente el dominio de difusión (recomendado)**.
 - b. Para seleccionar manualmente un dominio de difusión de la lista.
4. Seleccione los puertos para formar la VLAN.
5. Especifique el ID de VLAN.
6. Guarde los cambios.

CLI

Utilice la CLI para crear una VLAN

En determinadas circunstancias, si desea crear el puerto VLAN en un puerto degradado sin que corrija el problema del hardware o los errores de configuración de software, puede establecer el `-ignore-health-status` parámetro de `network port modify` comando como `true`.

Pasos

1. Utilice la `network port vlan create` Comando para crear una VLAN.
2. Debe especificar cualquiera de los dos `vlan-name` o la `port y.. vlan-id` Al crear una VLAN. El nombre de la VLAN es una combinación del nombre del puerto (o grupo de interfaces) y del identificador de VLAN del switch de red, con un guión entre. Por ejemplo: `e0c-24` y.. `e1c-80` Son nombres de VLAN válidos.

El ejemplo siguiente muestra cómo crear una VLAN `e1c-80` conectado al puerto de red `e1c` en el nodo `cluster-1-01`:

```
network port vlan create -node cluster-1-01 -vlan-name e1c-80
```

A partir de ONTAP 9.8, las VLAN se colocan automáticamente en dominios de retransmisión adecuados un minuto después de su creación. Si no desea que ONTAP realice esto y prefiere colocar la VLAN manualmente en un dominio de retransmisión, especifique el `-skip-broadcast-domain-placement` parámetro como parte de la `vlan create` comando.

Para obtener más información acerca de este comando, consulte ["Comandos de ONTAP 9"](#).

Editar una VLAN

Puede cambiar el dominio de retransmisión o deshabilitar una VLAN.

Utilice System Manager para editar una VLAN

A partir de ONTAP 9.12.0, puede seleccionar automáticamente el dominio de difusión o seleccionar manualmente en de la lista. Los dominios de retransmisión anteriores siempre se seleccionaron automáticamente en función de la conectividad de la capa 2. Si selecciona manualmente un dominio de retransmisión, aparecerá una advertencia que indica que la selección manual de un dominio de retransmisión podría provocar la pérdida de conectividad.

Pasos

1. Seleccione **Red > Puerto Ethernet > VLAN**.
2. Seleccione el icono de edición.
3. Debe realizar una de las siguientes acciones:
 - Cambie el dominio de difusión seleccionando otro de la lista.
 - Desactive la casilla de verificación **Activado**.
4. Guarde los cambios.

Elimine una VLAN

Es posible que tenga que eliminar una VLAN antes de extraer una NIC de su ranura. Cuando se elimina una VLAN, se elimina automáticamente de todas las reglas y grupos de conmutación por error que la usan.

Antes de empezar

Asegúrese de que no hay ninguna LIF asociada con la VLAN.

Acerca de esta tarea

Si se elimina la última VLAN de un puerto, se puede producir una desconexión temporal de la red del puerto.

El procedimiento que siga depende de la interfaz que utilice: System Manager o CLI:

System Manager

Utilice System Manager para eliminar una VLAN

Pasos

1. Seleccione **Red > Puerto Ethernet > VLAN**.
2. Seleccione la VLAN que desea eliminar.
3. Haga clic en **Eliminar**.

CLI

Utilice la CLI para eliminar una VLAN

Paso

Utilice la `network port vlan delete` Comando para eliminar una VLAN.

El siguiente ejemplo muestra cómo eliminar una VLAN `e1c-80` desde el puerto de red `e1c` en el nodo `cluster-1-01`:

```
network port vlan delete -node cluster-1-01 -vlan-name e1c-80
```

Modifique los atributos de puerto de red

Puede modificar la configuración de la autonegociación, el dúplex, el control de flujo, la velocidad y el estado de un puerto de red física.

Antes de empezar

El puerto que desea modificar no debe estar alojando ningún LIF.

Acerca de esta tarea

- No se recomienda modificar la configuración administrativa de las interfaces de red 100 GbE, 40 GbE, 10 GbE o 1 GbE.

Los valores configurados para el modo doble y la velocidad del puerto se denominan configuración administrativa. Según las limitaciones de la red, la configuración administrativa puede diferir de la configuración operativa (es decir, el modo doble y la velocidad que utiliza realmente el puerto).

- No se recomienda modificar la configuración administrativa de los puertos físicos subyacentes en un grupo de interfaces.

La `-up-admin` el parámetro (disponible en el nivel de privilegio avanzado) modifica la configuración administrativa del puerto.

- No se recomienda establecer el `-up-admin` Configuración de administración en `FALSE` para todos los puertos de un nodo, o para el puerto que aloja la última LIF de clúster operativo en un nodo.
- No se recomienda modificar el tamaño de MTU del puerto de gestión, `e0M`.
- El tamaño de MTU de un puerto en un dominio de retransmisión no se puede cambiar del valor MTU que se establece para el dominio de retransmisión.

- El tamaño de MTU de una VLAN no puede superar el valor del tamaño de MTU de su puerto base.

Pasos

1. Modifique los atributos de un puerto de red:

```
network port modify
```

2. Puede ajustar la `-ignore-health-status` el campo a `true` para especificar que el sistema puede ignorar el estado del puerto de red de un puerto especificado.

El estado del puerto de red cambia automáticamente del estado degradado al correcto, y este puerto ahora se puede utilizar para alojar LIF. Debe establecer el control de flujo de los puertos del clúster a `none`. De forma predeterminada, el control de flujo se establece en `full`.

El comando siguiente deshabilita el control de flujo en el puerto `e0b` estableciendo el control de flujo en `none`:

```
network port modify -node cluster-1-01 -port e0b -flowcontrol-admin none
```

Convertir puertos NIC de 40 GbE en varios puertos 10 GbE para la conectividad 10 GbE

Es posible convertir las tarjetas de interfaz de red (NIC) X1144A-R6 40 GbE y X91440A-R6 para admitir cuatro puertos 10 GbE.

Si va a conectar una plataforma de hardware que admita una de estas NIC a un clúster que admita la interconexión de clúster 10 GbE y las conexiones de datos del cliente, la NIC debe convertirse para proporcionar las conexiones 10 GbE necesarias.

Antes de empezar

Debe utilizar un cable de cable de conexión compatible.

Acerca de esta tarea

Para obtener una lista completa de las plataformas compatibles con las NIC, consulte ["Hardware Universe"](#).



En la NIC X1144A-R6, solo el puerto A puede convertirse para admitir las cuatro conexiones 10 GbE. Una vez convertido el puerto A, el puerto e no está disponible para su uso.

Pasos

1. Entre en el modo de mantenimiento.
2. Convierta el NIC del soporte de 40 GbE al soporte de 10 GbE.

```
nicadmin convert -m [40G | 10G] [port-name]
```

3. Tras utilizar el comando `convert`, detenga el nodo.
4. Instale o cambie el cable.
5. Según el modelo de hardware, use el SP (Service Processor) o BMC (Baseboard Management Controller) para apagar y encender el nodo para que la conversión surta efecto.

Quitar una NIC del nodo (ONTAP 9,8 y versiones posteriores)

Este tema se aplica a ONTAP 9,8 y versiones posteriores. Es posible que tenga que extraer una NIC defectuosa de su ranura o mover la NIC a otra ranura para realizar tareas de mantenimiento.

Pasos

1. Apague el nodo.
2. Extraiga físicamente la NIC de su ranura.
3. Encienda el nodo.
4. Compruebe que el puerto se ha eliminado:

```
network port show
```



ONTAP quita automáticamente el puerto de cualquier grupo de interfaces. Si el puerto era el único miembro de un grupo de interfaces, se elimina el grupo de interfaces.

5. Si el puerto tenía alguna VLAN configurada en él, se desplazarán. Las VLAN desplazadas se pueden ver mediante el siguiente comando:

```
cluster controller-replacement network displaced-vlans show
```



La `displaced-interface show`, `displaced-vlans show`, y `displaced-vlans restore` los comandos son únicos y no requieren el nombre del comando completo, que comienza con `cluster controller-replacement network`.

6. Estas VLAN se eliminan, pero se pueden restaurar mediante el siguiente comando:

```
displaced-vlans restore
```

7. Si el puerto tenía alguna LIF configurada en él, ONTAP elige automáticamente nuevos puertos raíz para esas LIF en otro puerto del mismo dominio de retransmisión. Si no se encuentra ningún puerto de inicio adecuado en el mismo servidor de almacenamiento, se considera que esos LIF están desplazados. Puede ver las LIF desplazadas mediante el siguiente comando:

```
displaced-interface show
```

8. Cuando se agrega un nuevo puerto al dominio de retransmisión en el mismo nodo, los puertos iniciales para las LIF se restauran automáticamente. Como alternativa, puede establecer el puerto de inicio mediante `network interface modify -home-port -home-node` or use the `displaced-interface restore` comando.

Eliminar una NIC del nodo (ONTAP 9,7 o anterior)

Este tema se aplica a ONTAP 9.7 o anterior. Es posible que tenga que extraer una NIC

defectuosa de su ranura o mover la NIC a otra ranura para realizar tareas de mantenimiento.

Antes de empezar

- Todas las LIF alojadas en los puertos NIC deben haberse migrado o eliminado.
- Ninguno de los puertos NIC puede ser el puerto principal de ningún LIF.
- Debe tener privilegios avanzados para eliminar los puertos de una NIC.

Pasos

1. Elimine los puertos de la NIC:

```
network port delete
```

2. Compruebe que los puertos se han eliminado:

```
network port show
```

3. Repita el paso 1, si el resultado del comando network Port show sigue mostrando el puerto eliminado.

Supervise los puertos de red

Supervise el estado de los puertos de red

La gestión de ONTAP de los puertos de red incluye supervisión automática del estado y un conjunto de monitores de estado para ayudarle a identificar puertos de red que podrían no ser adecuados para alojar LIF.

Acerca de esta tarea

Si un monitor de estado determina que un puerto de red no es bueno, advierte a los administradores a través de un mensaje de EMS o Marca el puerto como degradado. ONTAP evita el alojamiento de LIF en puertos de red degradados si existen destinos de conmutación al nodo de respaldo alternativos en buen estado para esa LIF. Un puerto puede degradarse debido a un evento de fallo de software, como el enlace flapping (enlaces que rebotan rápidamente entre arriba y abajo) o la partición de red:

- Los puertos de red del espacio IP del clúster se marcan como degradados cuando experimentan el enlace flopping o la pérdida de la capacidad de acceso de la capa 2 (L2) a otros puertos de red en el dominio de retransmisión.
- Los puertos de red de los espacios IP que no pertenecen al clúster se marcan como degradados cuando experimentan un enlace flapping.

Debe tener en cuenta los siguientes comportamientos de un puerto degradado:

- No se puede incluir un puerto degradado en una VLAN o en un grupo de interfaces.

Si un puerto del miembro de un grupo de interfaces se Marca como degradado, pero el grupo de interfaces sigue marcado como correcto, las LIF se pueden alojar en ese grupo de interfaces.

- Los LIF se migran automáticamente de puertos degradados a puertos en buen estado.
- Durante un evento de conmutación por error, no se considera un puerto degradado como destino de conmutación por error. Si no hay puertos en buen estado disponibles, puertos LIF degradados del host según la política de conmutación al respaldo normal.

- No puede crear, migrar o revertir un LIF a un puerto degradado.

Puede modificar el `ignore-health-status` configuración del puerto de red a `true`. Luego puede alojar una LIF en los puertos en buen estado.

Pasos

1. Inicie sesión en el modo de privilegio avanzado:

```
set -privilege advanced
```

2. Compruebe qué monitores de estado están habilitados para supervisar el estado del puerto de red:

```
network options port-health-monitor show
```

El estado de un puerto está determinado por el valor de los monitores de estado.

Los siguientes monitores de estado están disponibles y están habilitados de manera predeterminada en ONTAP:

- Monitor de estado de enlace: Monitores de enlace flapping

Si un puerto tiene un enlace que flaquear más de una vez en cinco minutos, este puerto se Marca como degradado.

- Monitor de estado de accesibilidad L2: Controla si todos los puertos configurados en el mismo dominio de difusión tienen accesibilidad L2 entre sí

Este monitor de estado genera problemas de accesibilidad L2 en todos los espacios IP; sin embargo, solo Marca los puertos del espacio IP del clúster como degradados.

- Monitor CRC: Supervisa las estadísticas de CRC en los puertos

Este monitor de estado no Marca un puerto como degradado, pero genera un mensaje de EMS cuando se observa una tasa de fallo de CRC muy alta.

3. Habilite o deshabilite cualquiera de los monitores de estado de un espacio IP según lo desee mediante el `network options port-health-monitor modify` comando.
4. Consulte el estado detallado de un puerto:

```
network port show -health
```

El resultado del comando muestra el estado del puerto, `ignore health status` configuración y lista de motivos por los que el puerto está marcado como degradado.

Un estado de estado de puerto puede ser `healthy` o `degraded`.

Si la `ignore health status` el ajuste es `true`, indica que el estado del puerto se ha modificado de `degraded` para `healthy` el administrador.

Si la `ignore health status` el ajuste es `false`, el estado del puerto lo determina automáticamente el sistema.

Supervisar la accesibilidad de los puertos de red (ONTAP 9,8 y posteriores)

La supervisión de la accesibilidad está integrada en ONTAP 9.8 y versiones posteriores. Utilice esta supervisión para identificar cuándo la topología de red física no coincide con la configuración de ONTAP. En algunos casos, ONTAP puede reparar la accesibilidad de los puertos. En otros casos, se requieren pasos adicionales.

Acerca de esta tarea

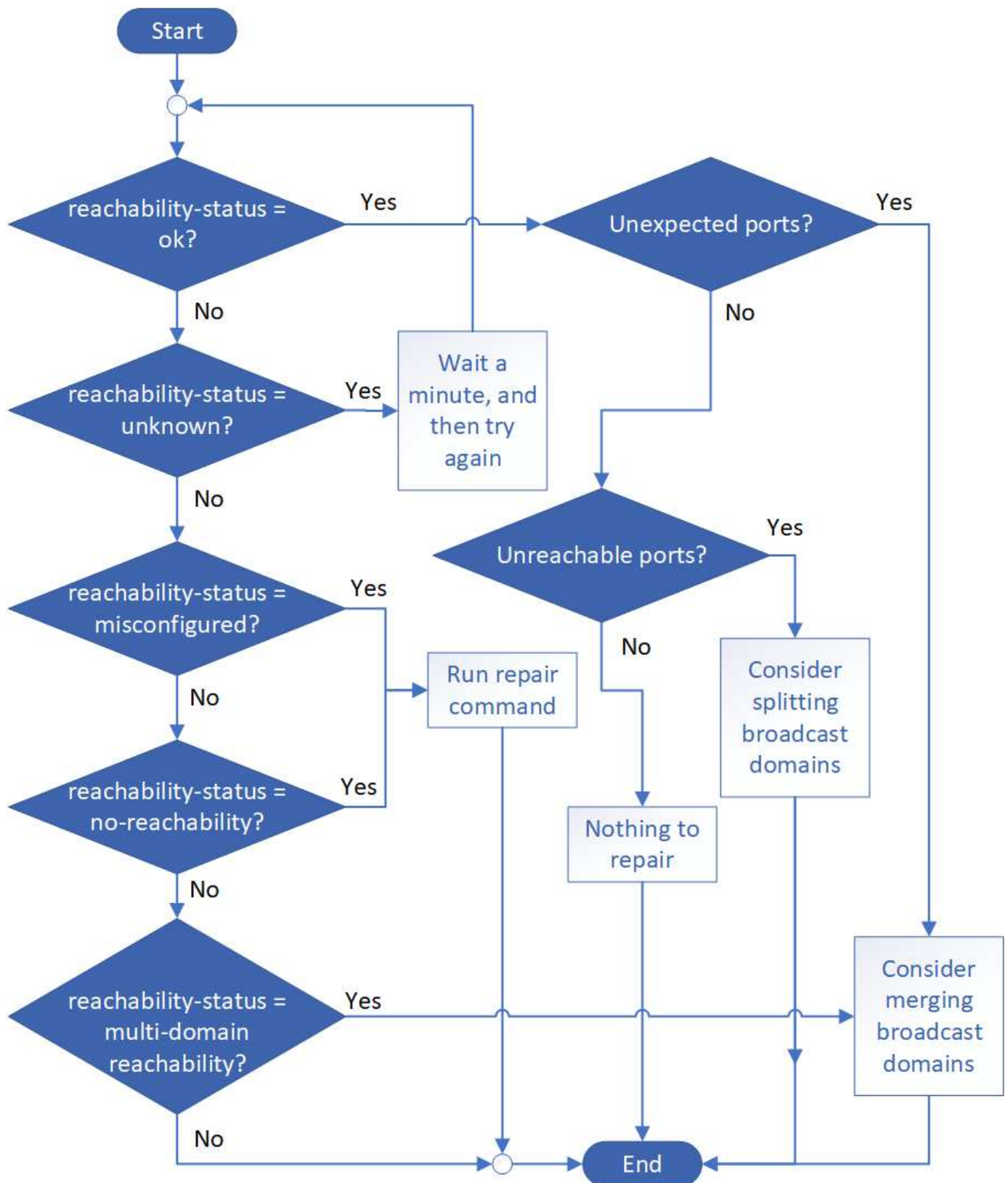
Utilice estos comandos para verificar, diagnosticar y reparar configuraciones incorrectas de red procedentes de la configuración de ONTAP que no coinciden con el cableado físico o la configuración del switch de red.

Paso

1. Ver accesibilidad de puertos:

```
network port reachability show
```

2. Utilice el árbol de decisiones y la tabla siguientes para determinar el siguiente paso, si existe alguno.



| Accesibilidad-estado | Descripción |
|----------------------|-------------|
|----------------------|-------------|

| | |
|---------------------------|---|
| de acuerdo | <p>El puerto tiene capacidad de acceso de capa 2 a su dominio de difusión asignado. Si el reachability-status es "ok", pero hay "puertos inesperados", considere combinar uno o más dominios de difusión. Para obtener más información, consulte la siguiente fila <i>inesperado ports</i>.</p> <p>Si el reachability-status es "ok", pero hay "puertos inaccesibles", considere dividir uno o más dominios de difusión. Para obtener más información, consulte la siguiente fila <i>ports</i> sin acceso.</p> <p>Si el estado de accesibilidad es "correcto" y no hay puertos inesperados o no accesibles, la configuración es correcta.</p> |
| Puertos inesperados | <p>El puerto tiene la habilidad de la capa 2 para su dominio de broadcast asignado; sin embargo, también tiene la habilidad de la capa 2 para al menos otro dominio de broadcast.</p> <p>Examine la configuración física del conmutador y la conectividad para determinar si es incorrecta o si el dominio de difusión asignado al puerto necesita combinarse con uno o más dominios de difusión.</p> <p>Para obtener más información, consulte "Fusionar dominios de retransmisión".</p> |
| Puertos inaccesibles | <p>Si un solo dominio de difusión se ha particionado en dos conjuntos de accesibilidad diferentes, puede dividir un dominio de difusión para sincronizar la configuración de ONTAP con la topología de red física.</p> <p>Normalmente, la lista de puertos inaccesibles define el conjunto de puertos que se deben dividir en otro dominio de retransmisión después de verificar que la configuración física y de switch es correcta.</p> <p>Para obtener más información, consulte "Divida los dominios de retransmisión".</p> |
| función mal configurada | <p>El puerto no tiene posibilidad de recurrir a la capa 2 a su dominio de difusión asignado; sin embargo, el puerto tiene capacidad de acceso de capa 2 a un dominio de difusión diferente.</p> <p>Puede reparar la accesibilidad del puerto. Cuando ejecute el siguiente comando, el sistema asignará el puerto al dominio de retransmisión al que se le habrá accesibilidad:</p> <pre>network port reachability repair -node -port</pre> <p>Para obtener más información, consulte "Reparar la accesibilidad del puerto".</p> |
| ausencia de accesibilidad | <p>El puerto no tiene posibilidad de recurrir a ningún dominio de difusión existente de capa 2.</p> <p>Puede reparar la accesibilidad del puerto. Cuando ejecute el siguiente comando, el sistema asignará el puerto a un dominio de retransmisión creado automáticamente en el espacio IP predeterminado:</p> <pre>network port reachability repair -node -port</pre> <p>Para obtener más información, consulte "Reparar la accesibilidad del puerto".</p> |

| | |
|-----------------------------|---|
| accesibilidad multi-dominio | <p>El puerto tiene la habilidad de la capa 2 para su dominio de broadcast asignado; sin embargo, también tiene la habilidad de la capa 2 para al menos otro dominio de broadcast.</p> <p>Examine la configuración física del conmutador y la conectividad para determinar si es incorrecta o si el dominio de difusión asignado al puerto necesita combinarse con uno o más dominios de difusión.</p> <p>Para obtener más información, consulte "Fusionar dominios de retransmisión" o "Reparar la accesibilidad del puerto".</p> |
| desconocido | Si el estado de accesibilidad es "desconocido", espere unos minutos y vuelva a intentar el comando. |

Después de reparar un puerto, necesita comprobar y resolver las LIF y VLAN desplazadas. Si el puerto era parte de un grupo de interfaces, también necesita comprender lo que ha sucedido con ese grupo de interfaces. Para obtener más información, consulte ["Reparar la accesibilidad del puerto"](#).

Descripción general de los puertos ONTAP

Algunos puertos conocidos se reservan para comunicaciones ONTAP con servicios específicos. Se producirán conflictos de puertos si un valor de puerto en el entorno de red de almacenamiento es el mismo que en el puerto ONTAP.

En la siguiente tabla se enumeran los puertos TCP y UDP que utiliza ONTAP.

| Servicio | Puerto/protocolo | Descripción |
|--------------|------------------|--|
| ssh | 22/TCP | Inicio de sesión seguro en shell |
| telnet | 23/TCP | Inicio de sesión remoto |
| DNS | 53/TCP | Cargue el DNS equilibrado |
| http | 80/TCP | Protocolo de transferencia de Hyper Text |
| rpcind | 111/TCP | Llamada a procedimiento remoto |
| rpcind | 111/UDP | Llamada a procedimiento remoto |
| ntp | 123/UDP | Protocolo de hora de red |
| msrpc | 135/UDP | MSRPC |
| netbios-ssn | 139/TCP | Sesión de servicio NetBIOS |
| snmp | 161/UDP | Protocolo simple de gestión de red |
| https | 443/TCP | HTTP sobre TLS |
| microsoft-ds | 445/TCP | Microsoft-ds |
| montaje | 635/TCP | Montaje NFS |
| montaje | 635/UDP | Montaje NFS |
| nombre | 953/UDP | Daemon de nombres |

| | | |
|-------------------------------------|-------------------|--|
| nfs | 2049/UDP | Daemon de servidor NFS |
| nfs | 2049/TCP | Daemon de servidor NFS |
| vrn | 2050/TCP | Protocolo de volumen remoto de NetApp |
| iscsi | 3260/TCP | Puerto de destino iSCSI |
| lockd | 4045/TCP | Daemon de bloqueo NFS |
| lockd | 4045/UDP | Daemon de bloqueo NFS |
| NSM | 4046/TCP | Monitor de estado de red |
| NSM | 4046/UDP | Monitor de estado de red |
| rquotad | 4049/UDP | Protocolo rquotad NFS |
| krb524 | 4444/UDP | Kerberos 524 |
| mdns | 5353/UDP | DNS de multidifusión |
| HTTPS | 5986/UDP | Puerto HTTPS: Protocolo binario de escucha |
| https | 8443/TCP | Herramienta GUI de 7MTT a través de https |
| ndmp | 10000/TCP | Protocolo de gestión de datos de red |
| Conexión de clústeres entre iguales | 11104/TCP | Cluster peering, bidireccional |
| Cluster peering, bidireccional | 11105/TCP | Conexión de clústeres entre iguales |
| NDMP | 18600 - 18699/TCP | NDMP |
| NDMP | 30000/TCP | acepte conexiones de control a través de tomas seguras |
| puerto de testigos cifs | 40001/TCP | puerto de testigos cifs |
| tls | 50000/TCP | Seguridad de la capa de transporte |
| iscsi | 65200/TCP | Puerto iSCSI |

Puertos internos ONTAP

En la siguiente tabla se enumeran los puertos TCP y UDP que ONTAP utiliza internamente. Estos puertos se utilizan para establecer comunicación entre LIF dentro del clúster:

| Puerto/protocolo | Descripción |
|------------------|--------------------------|
| 514 | Syslog |
| 900 | RPC de clúster de NetApp |
| 902 | RPC de clúster de NetApp |
| 904 | RPC de clúster de NetApp |
| 905 | RPC de clúster de NetApp |

| | |
|-----|--------------------------|
| 910 | RPC de clúster de NetApp |
| 911 | RPC de clúster de NetApp |
| 913 | RPC de clúster de NetApp |
| 914 | RPC de clúster de NetApp |
| 915 | RPC de clúster de NetApp |
| 918 | RPC de clúster de NetApp |
| 920 | RPC de clúster de NetApp |
| 921 | RPC de clúster de NetApp |
| 924 | RPC de clúster de NetApp |
| 925 | RPC de clúster de NetApp |
| 927 | RPC de clúster de NetApp |
| 928 | RPC de clúster de NetApp |
| 929 | RPC de clúster de NetApp |
| 931 | RPC de clúster de NetApp |
| 932 | RPC de clúster de NetApp |
| 933 | RPC de clúster de NetApp |
| 934 | RPC de clúster de NetApp |
| 935 | RPC de clúster de NetApp |
| 936 | RPC de clúster de NetApp |
| 937 | RPC de clúster de NetApp |
| 939 | RPC de clúster de NetApp |
| 940 | RPC de clúster de NetApp |
| 951 | RPC de clúster de NetApp |
| 954 | RPC de clúster de NetApp |
| 955 | RPC de clúster de NetApp |
| 956 | RPC de clúster de NetApp |
| 958 | RPC de clúster de NetApp |
| 961 | RPC de clúster de NetApp |
| 963 | RPC de clúster de NetApp |
| 964 | RPC de clúster de NetApp |
| 966 | RPC de clúster de NetApp |
| 967 | RPC de clúster de NetApp |
| 982 | RPC de clúster de NetApp |
| 983 | RPC de clúster de NetApp |

| | |
|-------|--|
| 5125 | Puerto de control alternativo para el disco |
| 5133 | Puerto de control alternativo para el disco |
| 5144 | Puerto de control alternativo para el disco |
| 65502 | SSH de alcance del nodo |
| 65503 | Uso compartido de LIF |
| 7810 | RPC de clúster de NetApp |
| 7811 | RPC de clúster de NetApp |
| 7812 | RPC de clúster de NetApp |
| 7813 | RPC de clúster de NetApp |
| 7814 | RPC de clúster de NetApp |
| 7815 | RPC de clúster de NetApp |
| 7816 | RPC de clúster de NetApp |
| 7817 | RPC de clúster de NetApp |
| 7818 | RPC de clúster de NetApp |
| 7819 | RPC de clúster de NetApp |
| 7820 | RPC de clúster de NetApp |
| 7821 | RPC de clúster de NetApp |
| 7822 | RPC de clúster de NetApp |
| 7823 | RPC de clúster de NetApp |
| 7824 | RPC de clúster de NetApp |
| 8023 | Telnet de alcance de nodo |
| 8514 | Alcance del nodo RSH |
| 9877 | Puerto de cliente KMIP (solo host local interno) |

Espacios IP

Configure la descripción general de IPspaces

Los espacios IP permiten configurar un único clúster ONTAP para que los clientes puedan acceder a él desde más de un dominio de red separado por administración, incluso si esos clientes utilizan el mismo rango de subred de direcciones IP. Esto permite la separación del tráfico de clientes para privacidad y seguridad.

Un espacio IP define un espacio de dirección IP diferente en el que residen las máquinas virtuales de almacenamiento (SVM). Los puertos y las direcciones IP definidos para un espacio IP solo se aplican dentro de ese espacio IP. Se mantiene una tabla de enrutamiento distinta para cada SVM dentro de un espacio IP; por lo tanto, no se produce ninguna ruta de tráfico entre SVM o entre espacio IP.



Los espacios IP admiten direcciones IPv4 e IPv6 en sus dominios de enrutamiento.

Si gestiona almacenamiento para una única organización, no necesitará configurar espacios IP. Si va a gestionar almacenamiento para varias empresas en un único clúster de ONTAP y tiene la seguridad de que ninguno de sus clientes tiene configuraciones de red en conflicto, tampoco necesitará utilizar espacios IP. En muchos casos, el uso de máquinas virtuales de almacenamiento (SVM), con sus propias tablas de enrutamiento IP distintas, puede utilizarse para segregar configuraciones de red únicas en lugar de usar espacios IP.

Ejemplo de uso de espacios IP

Una aplicación común para el uso de espacios IP es cuando un proveedor de servicios de almacenamiento (SSP) necesita conectar a los clientes de las empresas A y B a un clúster ONTAP en las instalaciones del SSP y ambas empresas utilizan los mismos rangos de direcciones IP privadas.

El SSP crea SVM en el clúster para cada cliente y proporciona una ruta de red dedicada de dos SVM a la red de la empresa A y de las otras dos SVM a la red de la empresa B.

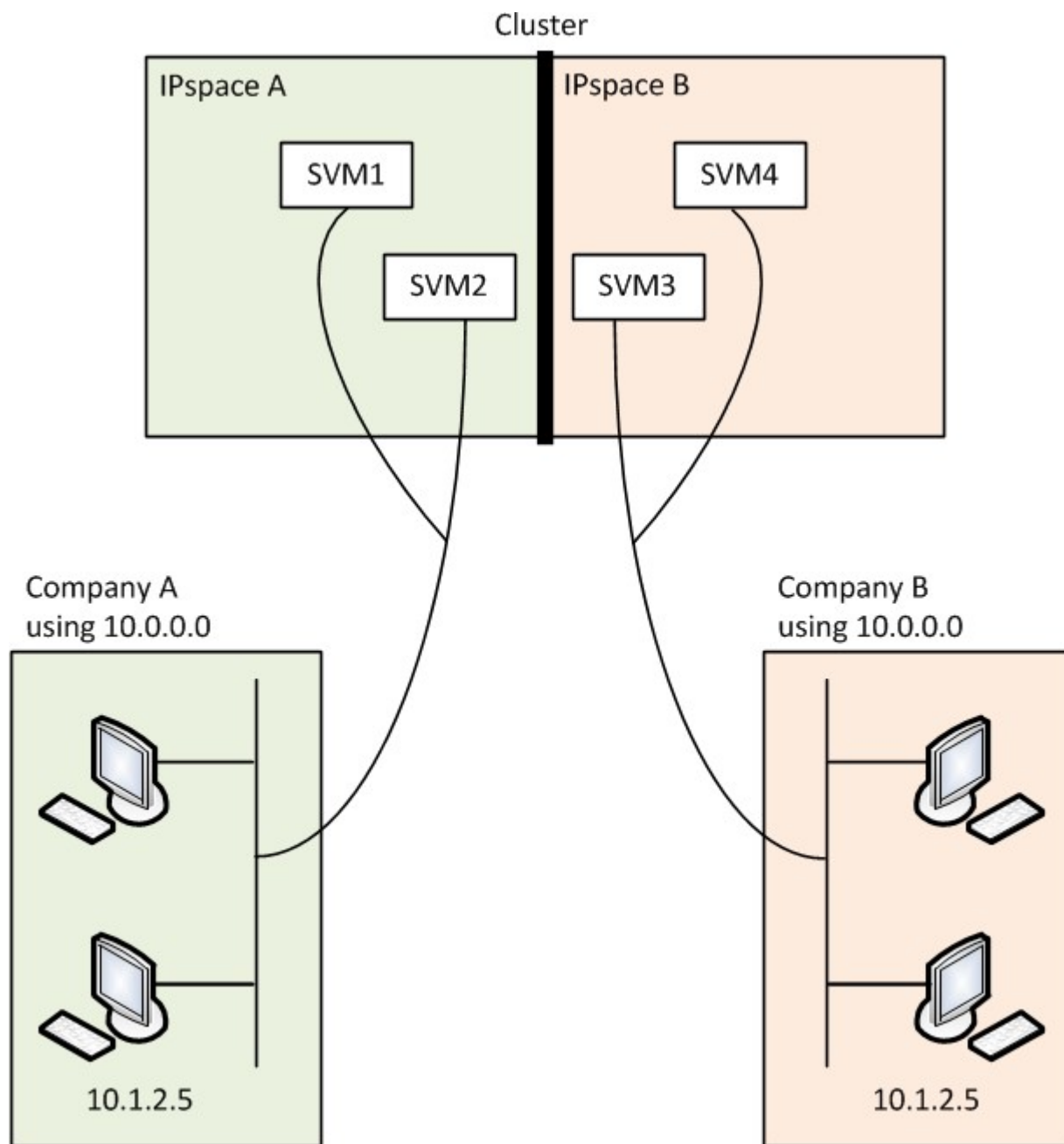
Este tipo de implementación se muestra en la siguiente ilustración y funciona si ambas empresas utilizan rangos de direcciones IP no privados. Sin embargo, la ilustración muestra a ambas empresas que utilizan los mismos rangos de direcciones IP privadas, lo que causa problemas.



Ambas empresas utilizan la subred de direcciones IP privadas 10.0.0.0, causando los siguientes problemas:

- Las SVM del clúster en la ubicación del SSP tienen direcciones IP contradictorias si ambas compañías deciden utilizar la misma dirección IP para sus SVM correspondientes.
- Incluso si las dos empresas acuerdan usar diferentes direcciones IP para sus SVM, pueden surgir problemas.
- Por ejemplo, si un cliente en la red de A tiene la misma dirección IP que un cliente en la red de B, los paquetes destinados a un cliente en el espacio de direcciones De A pueden enrutarse a un cliente en el espacio de direcciones de B, y viceversa.
- Si las dos empresas deciden utilizar espacios de direcciones mutuamente excluyentes (Por ejemplo, A utiliza 10.0.0.0 con una máscara de red de 255.128.0.0 y B utiliza 10.128.0.0 con una máscara de red de 255.128.0.0), El SSP debe configurar las rutas estáticas en el clúster para enrutar el tráfico correctamente a las redes De A y B.

- Esta solución no es escalable (debido a rutas estáticas) ni segura (el tráfico de difusión se envía a todas las interfaces del clúster). para superar estos problemas, el SSP define dos espacios IP en el clúster, uno para cada empresa. Como no se enrutará ningún tráfico de entre espacios IP, los datos de cada empresa se dirigen de forma segura a su red respectiva aunque todas las SVM se hayan configurado en el espacio de direcciones 10.0.0.0, como se muestra en la siguiente ilustración:



Además, las direcciones IP a las que hacen referencia los distintos archivos de configuración, como el `/etc/hosts` archivo, la `/etc/hosts.equiv` archivos, y the `/etc/rc` Archivo, está relativo a ese espacio IP. Por lo tanto, los espacios IP permiten que el SSP configure la misma dirección IP para los datos de configuración y autenticación de varias SVM, sin conflictos.

Propiedades estándar de los espacios IP

Los espacios IP especiales se crean de forma predeterminada cuando se crea por primera vez el clúster. Además, se crean máquinas virtuales de almacenamiento (SVM) especiales para cada espacio IP.

Cuando se inicializa el clúster, se crean dos espacios IP automáticamente:

- Espacio IP «predeterminado»

Este espacio IP es un contenedor de puertos, subredes y SVM que proporcionan datos. Si su configuración no necesita espacios IP separados para los clientes, todas las SVM se pueden crear en este espacio IP. Este espacio IP también contiene los puertos de gestión del clúster y de gestión de nodos.

- Espacio IP de «cluster»

Este espacio IP contiene todos los puertos del clúster de todos los nodos del clúster. Se crea automáticamente cuando se crea el clúster. Proporciona conectividad a la red de clústeres privada interna. A medida que más nodos se unen al clúster, los puertos del clúster de esos nodos se añaden al espacio IP «Cluster».

Hay una SVM del sistema para cada espacio IP. Cuando crea un espacio IP, se crea una SVM del sistema predeterminada del mismo nombre:

- La SVM del sistema para el espacio IP de «clúster» transporta tráfico de clústeres entre nodos de un clúster en la red de clúster privada interna.

Lo gestiona el administrador del clúster y tiene el nombre «Cluster».

- La SVM del sistema para el espacio IP «predeterminado» transporta el tráfico de gestión del clúster y los nodos, incluido el tráfico de interconexión de clústeres entre clústeres.

Lo gestiona el administrador del clúster y utiliza el mismo nombre que el clúster.

- La SVM del sistema para un espacio IP personalizado que crea transporta el tráfico de gestión de esa SVM.

El administrador del clúster lo gestiona y utiliza el mismo nombre que el espacio IP.

Puede haber una o varias SVM para los clientes en un espacio IP. Cada SVM del cliente tiene sus propios volúmenes de datos y configuraciones, y se administra independientemente de las otras SVM.

Cree espacios IP

Los espacios IP son espacios de direcciones IP distintos en los que residen las máquinas virtuales de almacenamiento (SVM). Puede crear espacios IP cuando necesite que sus SVM tengan su propia capacidad de almacenamiento, administración y enrutamiento seguros. Puede usar un espacio IP para crear un espacio de direcciones IP distinto para cada SVM de un clúster. Esto permite a los clientes en dominios de red separados administrativamente acceder a los datos del clúster mientras utilizan direcciones IP superpuestas del mismo rango de subredes de direcciones IP.

Acerca de esta tarea

Existe un límite para todo el clúster de 512 espacios IP. El límite para todo el clúster se reduce a 256 espacios IP para clústeres que contienen nodos con 6 GB de RAM. Consulte la Hardware Universe para determinar si se aplican límites adicionales a su plataforma.

["Hardware Universe de NetApp"](#)



El nombre del espacio IP no puede ser "todos" porque "todos" es un nombre reservado del sistema.

Antes de empezar

Para realizar esta tarea, debe ser un administrador de clústeres.

Paso

1. Cree un espacio IP:

```
network ipspace create -ipspace ipspace_name
```

`ipspace_name` Es el nombre del espacio IP que desea crear. El siguiente comando crea el espacio IP `ipspace1` en un clúster:

```
network ipspace create -ipspace ipspace1
```

2. Visualice los espacios IP:

```
network ipspace show
```

| IPspace | Vserver List | Broadcast Domains |
|----------|--------------|-------------------|
| Cluster | Cluster | Cluster |
| Default | Cluster1 | Default |
| ipspace1 | ipspace1 | - |

Se crea el espacio IP, junto con la SVM del sistema para el espacio IP. La SVM del sistema transporta el tráfico de gestión.

Después de terminar

Si crea un espacio IP en un clúster de en una configuración de MetroCluster, los objetos IPspace se deben replicar manualmente en los clústeres de partners. Las SVM que se crean y se asignan a un espacio IP antes de que se replique el espacio IP no se replicarán en los clústeres asociados.

Los dominios de retransmisión se crean automáticamente en el espacio IP «predeterminado» y se pueden mover entre espacios IP mediante el siguiente comando:

```
network port broadcast-domain move
```

Por ejemplo, si desea mover un dominio de difusión de "default" a "ips1", utilizando el siguiente comando:

```
network port broadcast-domain move -ipspace Default -broadcast-domain  
Default -to-ipspace ips1
```


Mostrar espacios IP

Puede mostrar la lista de espacios IP que hay en un clúster y puede ver las máquinas virtuales de almacenamiento (SVM), los dominios de retransmisión y los puertos asignados a cada espacio IP.

Paso

Muestre los espacios IP y las SVM en un clúster:

```
network ipspace show [-ip space ipspace_name]
```

El siguiente comando muestra todos los espacios IP, las SVM y los dominios de retransmisión del clúster:

```
network ipspace show
IPspace          Vserver List          Broadcast Domains
-----
Cluster
Default          Cluster              Cluster
                  vs1, cluster-1        Default
ipspace1         vs3, vs4, ipspace1    bcast1
```

El siguiente comando muestra los nodos y puertos que forman parte del espacio IP ipspace1:

```
network ipspace show -ip space ipspace1
IPspace name: ipspace1
Ports: cluster-1-01:e0c, cluster-1-01:e0d, cluster-1-01:e0e, cluster-1-
02:e0c, cluster-1-02:e0d, cluster-1-02:e0e
Broadcast Domains: Default-1
Vservers: vs3, vs4, ipspace1
```

Elimine un espacio IP

Si ya no necesita un espacio IP, puede eliminarlo.

Antes de empezar

No debe haber dominios de retransmisión, interfaces de red ni SVM asociados al espacio IP que desea eliminar.

Los espacios IP definidos por el sistema «predeterminados» y «clúster» no se pueden eliminar.

Paso

Eliminar un espacio IP:

```
network ipspace delete -ipspace ipspace_name
```

El siguiente comando elimina el espacio IP ipspace1 del clúster:

```
network ipspace delete -ipspace ipspace1
```

Dominios de retransmisión

Dominio de retransmisión (ONTAP 9,8 y posteriores)

Información general sobre dominios de retransmisión (ONTAP 9,8 y posteriores)

Los dominios de difusión están destinados a agrupar puertos de red que pertenecen a la misma red de capa 2. Los puertos del grupo pueden usarse en una máquina virtual de almacenamiento (SVM) para el tráfico de datos o gestión.

Un dominio de retransmisión reside en un espacio IP. Durante la inicialización del clúster, el sistema crea dos dominios de retransmisión predeterminados:

- El dominio de retransmisión "predeterminado" contiene puertos que se encuentran en el espacio IP "predeterminado".

Estos puertos se utilizan principalmente para servir datos. Los puertos de gestión de clústeres y gestión de nodos también están en este dominio de retransmisión.

- El dominio de retransmisión "Cluster" contiene puertos que están en el espacio IP de "Cluster".

Estos puertos se utilizan para la comunicación del clúster e incluyen todos los puertos de clúster de todos los nodos del clúster.

El sistema crea dominios de retransmisión adicionales en el espacio IP predeterminado cuando sea necesario. El dominio de retransmisión "predeterminado" contiene el puerto raíz de la LIF de gestión, además de cualquier otro puerto que tenga acceso a ese puerto desde una nueva capa 2. Los dominios de retransmisión adicionales se denominan "default-1", "default-2", etc.

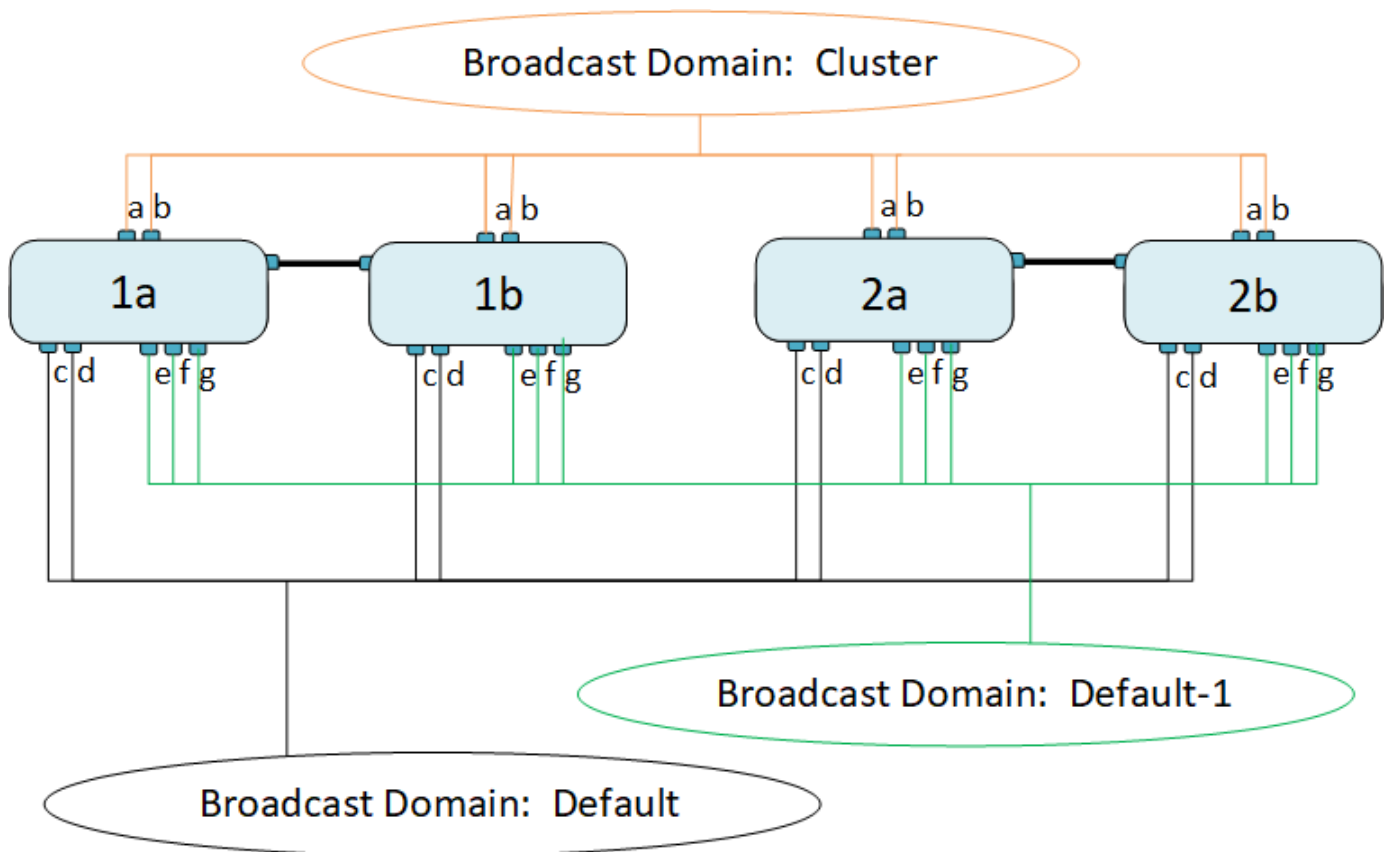
Ejemplo de uso de dominios de retransmisión

Un dominio de retransmisión es un conjunto de puertos de red en el mismo espacio IP que también tiene capacidad para el uno al otro de la capa 2, lo que suele incluir puertos de muchos nodos del clúster.

En la ilustración, se muestran los puertos asignados a tres dominios de retransmisión en un clúster de cuatro nodos:

- El dominio de retransmisión "Cluster" se crea automáticamente durante la inicialización del clúster. Contiene los puertos a y b de cada nodo del clúster.
- El dominio de retransmisión "predeterminado" también se crea automáticamente durante la inicialización del clúster y contiene los puertos c y d de cada nodo del clúster.
- El sistema crea automáticamente todos los dominios de retransmisión adicionales durante la inicialización

del clúster en función de la accesibilidad de red de la capa 2. Estos dominios de retransmisión adicionales se denominan default-1, default-2, etc.



Un grupo de conmutación por error con el mismo nombre y los mismos puertos de red que cada dominio de retransmisión se crea automáticamente. El sistema administra automáticamente este grupo de conmutación por error, lo que significa que, a medida que se agregan o quitan puertos del dominio de retransmisión, se agregan o se quitan automáticamente de este grupo de conmutación por error.

Añada un dominio de retransmisión

Los dominios de retransmisión agrupan los puertos de red del clúster que pertenecen a la misma red de capa 2. Los puertos pueden entonces ser utilizados por las SVM.

A partir de ONTAP 9.8, los dominios de retransmisión se crean automáticamente durante la operación de creación de clústeres o unión. A partir de ONTAP 9.12.0, además de los dominios de retransmisión creados automáticamente, puede añadir manualmente un dominio de retransmisión en System Manager.

Antes de empezar

Los puertos que desea añadir al dominio de retransmisión no deben pertenecer a otro dominio de retransmisión. Si los puertos que desea utilizar pertenecen a otro dominio de retransmisión, pero no se utilizan, quite esos puertos del dominio de retransmisión original.

Acerca de esta tarea

- Todos los nombres de dominio de retransmisión deben ser únicos en un espacio IP.
- Los puertos agregados a un dominio de difusión pueden ser puertos de red físicos, VLAN o grupos de agregación de enlaces/grupos de interfaces (LAG/ifgrps).
- Si los puertos que desea usar pertenecen a otro dominio de retransmisión, pero no se utilizan, elimínelos

del dominio de retransmisión existente antes de agregarlos al nuevo.

- La unidad de transmisión máxima (MTU) de los puertos agregados a un dominio de retransmisión se actualiza al valor MTU establecido en el dominio de retransmisión.
- El valor de MTU debe coincidir con todos los dispositivos conectados a esa red de capa 2, excepto en el caso del puerto e0M que gestiona el tráfico de gestión.
- Si no especifica un nombre de espacio IP, el dominio de retransmisión se crea en el espacio IP «predeterminado».

Para facilitar la configuración del sistema, se crea automáticamente un grupo de conmutación por error con el mismo nombre que contiene los mismos puertos.

System Manager

Pasos

1. Seleccione **Red > Descripción general > dominio de difusión**.
2. Haga clic en **+ Add**
3. Asigne un nombre al dominio de retransmisión.
4. Establezca la MTU.
5. Seleccione el espacio IP.
6. Guarde el dominio de retransmisión.

Puede editar o eliminar un dominio de retransmisión después de que se haya agregado.

CLI

En ONTAP 9.7 o una versión anterior, se puede crear manualmente un dominio de retransmisión.

Si utiliza ONTAP 9,8 y versiones posteriores, los dominios de difusión se crean automáticamente en función de la accesibilidad de capa 2. Para obtener más información, consulte ["Reparar la accesibilidad del puerto"](#).

Pasos

1. Vea los puertos que no están asignados actualmente a un dominio de retransmisión:

```
network port show
```

Si la pantalla es grande, utilice `network port show -broadcast-domain` comando para ver solo puertos sin asignar.

2. Cree un dominio de retransmisión:

```
network port broadcast-domain create -broadcast-domain  
broadcast_domain_name -mtu mtu_value [-ipSPACE ipSPACE_name] [-ports  
ports_list]
```

a. `broadcast_domain_name` es el nombre del dominio de retransmisión que desea crear.

b. `mtu_value` Es el tamaño de MTU para paquetes IP; 1500 y 9000 son valores típicos.

Este valor se aplica a todos los puertos que se agregan a este dominio de difusión.

c. `ipSPACE_name` Es el nombre del espacio IP al que se agregará este dominio de retransmisión.

El espacio IP «predeterminado» se utiliza a menos que especifique un valor para este parámetro.

d. `ports_list` es la lista de puertos que se agregarán al dominio de retransmisión.

Los puertos se añaden con el formato `node_name:port_number`, por ejemplo, `node1:e0c`.

3. Compruebe que el dominio de retransmisión se ha creado como desea:

```
network port show -instance -broadcast-domain new_domain
```

Ejemplo

El siguiente comando crea el dominio de broadcast bcast1 en el espacio IP predeterminado, establece la MTU en 1500 y agrega cuatro puertos:

```
network port broadcast-domain create -broadcast-domain bcast1 -mtu 1500 -ports cluster1-01:e0e,cluster1-01:e0f,cluster1-02:e0e,cluster1-02:e0f
```

Después de terminar

Puede definir el pool de direcciones IP disponibles en el dominio de retransmisión mediante la creación de una subred, o puede asignar SVM e interfaces al espacio IP en este momento. Para obtener más información, consulte ["Relaciones entre iguales de clústeres y SVM"](#).

Si necesita cambiar el nombre de un dominio de difusión existente, utilice `network port broadcast-domain rename` comando.

Agregar o quitar puertos de un dominio de retransmisión (ONTAP 9,8 y versiones posteriores)

Los dominios de retransmisión se crean automáticamente durante la operación de creación o unión del clúster. No es necesario quitar los puertos de los dominios de retransmisión manualmente.

Si la posibilidad de recurrir a un puerto de red ha cambiado, ya sea mediante la conectividad física de red o la configuración de un switch, y un puerto de red pertenece a un dominio de difusión diferente, consulte el siguiente tema:


["Reparar la accesibilidad del puerto"](#)

System Manager

A partir de ONTAP 9.14.1, puede usar System Manager para reasignar los puertos Ethernet en los dominios de retransmisión. Es recomendable asignar cada puerto Ethernet a un dominio de retransmisión. Por lo tanto, si anula la asignación de un puerto Ethernet de un dominio de retransmisión, debe reasignarlo a un dominio de retransmisión diferente.

Pasos

Para reasignar puertos Ethernet, realice los siguientes pasos:

1. Seleccione **Red > Descripción general**.
2. En la sección **Dominios de difusión**, seleccione  junto al nombre de dominio.
3. En el menú desplegable, seleccione **Editar**.
4. En la página **Editar dominio de difusión**, deseccione los puertos Ethernet que desea reasignar a otro dominio.
5. Para cada puerto no seleccionado, se muestra la ventana **Reasignar puerto Ethernet**. Seleccione el dominio de difusión al que desea reasignar el puerto y, a continuación, seleccione **Reasignar**.
6. Seleccione todos los puertos que desea asignar al dominio de difusión actual y guarde los cambios.

CLI

Si la posibilidad de recurrir a un puerto de red ha cambiado, ya sea mediante la conectividad física de red o la configuración de un switch, y un puerto de red pertenece a un dominio de difusión diferente, consulte el siguiente tema:

"Reparar la accesibilidad del puerto"

Como alternativa, puede agregar o eliminar puertos manualmente de los dominios de retransmisión mediante `network port broadcast-domain add-ports` o la `network port broadcast-domain remove-ports` comando.

Antes de empezar

- Para realizar esta tarea, debe ser un administrador de clústeres.
- Los puertos que desea agregar a un dominio de difusión no deben pertenecer a otro dominio de difusión.
- Los puertos que ya pertenecen a un grupo de interfaces no se pueden agregar individualmente a un dominio de retransmisión.

Acerca de esta tarea

Las siguientes reglas se aplican al agregar y quitar puertos de red:

| Al agregar puertos... | Al quitar puertos... |
|---|--|
| Los puertos pueden ser puertos de red, VLAN o grupos de interfaces (ifgrps). | N.A. |
| Los puertos se añaden al grupo de conmutación al nodo de respaldo definido por el sistema del dominio de retransmisión. | Los puertos se quitan de todos los grupos de conmutación al nodo de respaldo en el dominio de retransmisión. |
| El MTU de los puertos se actualiza con el valor de MTU establecido en el dominio de retransmisión. | El MTU de los puertos no cambia. |

El espacio IP de los puertos se actualiza al valor IPspace del dominio de retransmisión.

Los puertos se mueven al espacio IP "predeterminado" sin ningún atributo de dominio de difusión.



Si elimina el último puerto miembro de un grupo de interfaces mediante `network port ifgrp remove-port` comando, esto hace que se elimine el puerto del grupo de interfaces del dominio de retransmisión porque no se permite un puerto de grupo de interfaces vacío en un dominio de retransmisión.

Pasos

1. Muestra los puertos asignados o no asignados actualmente a un dominio de retransmisión mediante el `network port show` comando.
2. Añada o quite puertos de red del dominio de retransmisión:

| Si desea... | Usar... |
|--|---|
| Añada puertos a un dominio de retransmisión | <code>network port broadcast-domain add-ports</code> |
| Quite puertos de un dominio de retransmisión | <code>network port broadcast-domain remove-ports</code> |

3. Compruebe que los puertos se han agregado o eliminado del dominio de retransmisión:

```
network port show
```

Para obtener más información sobre estos comandos, consulte ["Comandos de ONTAP 9"](#).

Ejemplos de cómo agregar y quitar puertos

El siguiente comando agrega el puerto e0g en el nodo cluster-1-01 y el puerto e0g en el nodo cluster-1-02 al dominio de retransmisión bcast1 en el espacio IP predeterminado:

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain bcast1  
-ports cluster-1-01:e0g,cluster1-02:e0g
```

El siguiente comando añade dos puertos de clúster al clúster de retransmisión en el espacio IP del clúster:

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain Cluster  
-ports cluster-2-03:e0f,cluster2-04:e0f -ip-space Cluster
```

El siguiente comando elimina el puerto e0e en el cluster no1-01 del dominio de broadcast bcast1 en el espacio IP predeterminado:

```
cluster-1::> network port broadcast-domain remove-ports -broadcast-domain  
bcast1 -ports cluster-1-01:e0e
```


Mover dominios de difusión a espacios IP (ONTAP 9,8 y posteriores)

Mueva los dominios de retransmisión que el sistema creó basándose en la capacidad de la capa 2 a los espacios IP que creó.

Antes de mover el dominio de retransmisión, debe comprobar la accesibilidad de los puertos en los dominios de retransmisión.

El análisis automático de puertos puede determinar qué puertos pueden llegar entre sí y colocarlos en el mismo dominio de difusión, pero este análisis no puede determinar el espacio IP adecuado. Si el dominio de retransmisión pertenece a un espacio IP no predeterminado, deberá moverlo manualmente siguiendo los pasos de esta sección.

Antes de empezar

Los dominios de retransmisión se configuran automáticamente como parte de las operaciones de creación y unión de clústeres. ONTAP define el dominio de retransmisión "predeterminado" como el conjunto de puertos que tienen conectividad de capa 2 con el puerto de inicio de la interfaz de gestión en el primer nodo creado en el clúster. Si es necesario, se crean otros dominios de difusión y se denominan **default-1**, **default-2**, etc.

Cuando un nodo se une a un clúster existente, sus puertos de red unen automáticamente los dominios de retransmisión existentes en función de su accesibilidad de la capa 2. Si no tienen la posibilidad de recurrir a un dominio de retransmisión existente, los puertos se colocan en uno o varios dominios de retransmisión nuevos.

Acerca de esta tarea

- Los puertos de las LIF del clúster se colocan automáticamente en el espacio IP «clúster».
- Los puertos con accesibilidad al puerto inicial de la LIF de gestión de nodos se colocan en el dominio de retransmisión "predeterminado".
- ONTAP crea automáticamente otros dominios de retransmisión como parte de la operación de creación o unión del clúster.
- A medida que se añaden las VLAN y los grupos de interfaces, se colocan automáticamente en el dominio de retransmisión adecuado un minuto después de crearlo.

Pasos

1. Compruebe la accesibilidad de los puertos en los dominios de retransmisión. ONTAP supervisa automáticamente la accesibilidad de la capa 2. Utilice el siguiente comando para comprobar que cada puerto se ha agregado a un dominio de difusión y que tiene la posibilidad de recurrir a "ok".

```
network port reachability show -detail
```

2. Si es necesario, mueva los dominios de retransmisión a otros espacios IP:

```
network port broadcast-domain move
```

Por ejemplo, si desea mover un dominio de difusión de "default" a "ips1":

```
network port broadcast-domain move -ipspace Default -broadcast-domain Default  
-to-ipspace ips1
```

Mover dominios de difusión a espacios IP (ONTAP 9,8 y posteriores)

Mueva los dominios de retransmisión que el sistema creó basándose en la capacidad de

la capa 2 a los espacios IP que creó.

Antes de mover el dominio de retransmisión, debe comprobar la accesibilidad de los puertos en los dominios de retransmisión.

El análisis automático de puertos puede determinar qué puertos pueden llegar entre sí y colocarlos en el mismo dominio de difusión, pero este análisis no puede determinar el espacio IP adecuado. Si el dominio de retransmisión pertenece a un espacio IP no predeterminado, deberá moverlo manualmente siguiendo los pasos de esta sección.

Antes de empezar

Los dominios de retransmisión se configuran automáticamente como parte de las operaciones de creación y unión de clústeres. ONTAP define el dominio de retransmisión "predeterminado" como el conjunto de puertos que tienen conectividad de capa 2 con el puerto de inicio de la interfaz de gestión en el primer nodo creado en el clúster. Si es necesario, se crean otros dominios de difusión y se denominan **default-1**, **default-2**, etc.

Cuando un nodo se une a un clúster existente, sus puertos de red unen automáticamente los dominios de retransmisión existentes en función de su accesibilidad de la capa 2. Si no tienen la posibilidad de recurrir a un dominio de retransmisión existente, los puertos se colocan en uno o varios dominios de retransmisión nuevos.

Acerca de esta tarea

- Los puertos de las LIF del clúster se colocan automáticamente en el espacio IP «clúster».
- Los puertos con accesibilidad al puerto inicial de la LIF de gestión de nodos se colocan en el dominio de retransmisión "predeterminado".
- ONTAP crea automáticamente otros dominios de retransmisión como parte de la operación de creación o unión del clúster.
- A medida que se añaden las VLAN y los grupos de interfaces, se colocan automáticamente en el dominio de retransmisión adecuado un minuto después de crearlo.

Pasos

1. Compruebe la accesibilidad de los puertos en los dominios de retransmisión. ONTAP supervisa automáticamente la accesibilidad de la capa 2. Utilice el siguiente comando para comprobar que cada puerto se ha agregado a un dominio de difusión y que tiene la posibilidad de recurrir a "ok".

```
network port reachability show -detail
```

2. Si es necesario, mueva los dominios de retransmisión a otros espacios IP:

```
network port broadcast-domain move
```

Por ejemplo, si desea mover un dominio de difusión de "default" a "ips1":

```
network port broadcast-domain move -ipspace Default -broadcast-domain Default  
-to-ipspace ips1
```

Dividir dominios de retransmisión (ONTAP 9,8 y posteriores)

Si la posibilidad de recurrir a un puerto de red ha cambiado, ya sea mediante la conectividad de red física o la configuración del switch. Además, un grupo de puertos de red previamente configurados en un único dominio de difusión se ha particionado en dos conjuntos diferentes de accesibilidad, puede dividir un dominio de difusión para

sincronizar la configuración de ONTAP con la topología de red física.

Para determinar si un dominio de difusión de puerto de red se divide en más de un conjunto de accesibilidad, utilice `network port reachability show -details` Y preste atención a qué puertos no tienen conectividad entre sí ("puertos no accesibles"). Normalmente, la lista de puertos inaccesibles define el conjunto de puertos que se deben dividir en otro dominio de retransmisión, después de verificar que la configuración física y del switch es precisa.

Paso

Divida un dominio de retransmisión en dos dominios de retransmisión:

```
network port broadcast-domain split -ipSpace <ipSpace_name> -broadcast
-domain <broadcast_domain_name> -new-broadcast-domain
<broadcast_domain_name> -ports <node:port,node:port>
```

- `ipSpace_name` es el nombre del espacio ip donde reside el dominio de difusión.
- `-broadcast-domain` es el nombre del dominio de difusión que se dividirá.
- `-new-broadcast-domain` es el nombre del nuevo dominio de difusión que se creará.
- `-ports` es el nombre del nodo y el puerto que se añadirán al nuevo dominio de retransmisión.

Fusionar dominios de retransmisión (ONTAP 9,8 y posteriores)

Si se ha cambiado la posibilidad de recurrir a puertos de red, ya sea mediante una conectividad de red física o mediante una configuración de switch, y dos grupos de puertos de red previamente configurados en varios dominios de retransmisión ahora pueden volver a compartir, la fusión de dos dominios de difusión se puede utilizar para sincronizar la configuración de ONTAP con la topología de red física.

Para determinar si varios dominios de difusión pertenecen a un conjunto de accesibilidad, utilice el comando "Network Port Reachability show -details" y preste atención a qué puertos están configurados en otro dominio de difusión tienen realmente conectividad entre sí ("puertos inesperados"). Generalmente, la lista de puertos inesperados define el conjunto de puertos que se deben combinar en el dominio de retransmisión después de verificar que la configuración física y de switch es precisa.

Paso

Fusionar los puertos de un dominio de difusión en un dominio de difusión existente:

```
network port broadcast-domain merge -ipSpace <ipSpace_name> -broadcast
-domain <broadcast_domain_name> -into-broadcast-domain
<broadcast_domain_name>
```

- `ipSpace_name` es el nombre del espacio ip donde residen los dominios de difusión.
- `-broadcast-domain` es el nombre del dominio de difusión que se combinará.
- `-into-broadcast-domain` es el nombre del dominio de difusión que recibirá puertos adicionales.

Cambiar el valor de MTU para los puertos en un dominio de retransmisión (ONTAP 9,8 y posteriores)

Puede modificar el valor MTU para un dominio de retransmisión para cambiar el valor de MTU para todos los puertos en ese dominio de retransmisión. Esto se puede hacer para admitir cambios de topología que se han realizado en la red.

Antes de empezar

El valor de MTU debe coincidir con todos los dispositivos conectados a esa red de capa 2, excepto en el caso del puerto e0M que gestiona el tráfico de gestión.

Acerca de esta tarea

Al cambiar el valor de MTU, se produce una breve interrupción en el tráfico de los puertos afectados. El sistema muestra un símbolo del sistema de que debe responder con y para hacer el cambio de la MTU.

Paso

Cambie el valor de MTU para todos los puertos de un dominio de retransmisión:

```
network port broadcast-domain modify -broadcast-domain  
<broadcast_domain_name> -mtu <mtu_value> [-ipSPACE <ipSPACE_name>]
```

- `broadcast_domain` es el nombre del dominio de retransmisión.
- `mtu` Es el tamaño de MTU para paquetes IP; 1500 y 9000 son valores típicos.
- `ipSPACE` Es el nombre del espacio IP en el que reside el dominio de retransmisión. El espacio IP «predeterminado» se utiliza a menos que especifique un valor para esta opción. El siguiente comando cambia la MTU a 9000 para todos los puertos del dominio de broadcast `bcast1`:

```
network port broadcast-domain modify -broadcast-domain <Default-1> -mtu <  
9000 >  
Warning: Changing broadcast domain settings will cause a momentary data-  
serving interruption.  
Do you want to continue? {y|n}: <y>
```

Mostrar dominios de retransmisión (ONTAP 9,8 y posteriores)

Puede mostrar la lista de dominios de retransmisión dentro de cada espacio IP de un clúster. El resultado también muestra la lista de puertos y el valor MTU para cada dominio de retransmisión.

Paso

Muestre los dominios de retransmisión y los puertos asociados en el clúster:

```
network port broadcast-domain show
```

El siguiente comando muestra todos los dominios de retransmisión y los puertos asociados en el clúster:

```
network port broadcast-domain show
```

| IPspace | Broadcast | | | Update |
|---------|-------------|-------|------------------|----------------|
| Name | Domain Name | MTU | Port List | Status Details |
| ----- | ----- | ----- | ----- | ----- |
| Cluster | Cluster | 9000 | | |
| | | | cluster-1-01:e0a | complete |
| | | | cluster-1-01:e0b | complete |
| | | | cluster-1-02:e0a | complete |
| | | | cluster-1-02:e0b | complete |
| Default | Default | 1500 | | |
| | | | cluster-1-01:e0c | complete |
| | | | cluster-1-01:e0d | complete |
| | | | cluster-1-02:e0c | complete |
| | | | cluster-1-02:e0d | complete |
| | Default-1 | 1500 | | |
| | | | cluster-1-01:e0e | complete |
| | | | cluster-1-01:e0f | complete |
| | | | cluster-1-01:e0g | complete |
| | | | cluster-1-02:e0e | complete |
| | | | cluster-1-02:e0f | complete |
| | | | cluster-1-02:e0g | complete |

El siguiente comando muestra los puertos del dominio de retransmisión predeterminado-1 que tienen un estado de actualización de error, lo que indica que el puerto no se ha podido actualizar correctamente:

```
network port broadcast-domain show -broadcast-domain Default-1 -port
-update-status error
```

| IPspace | Broadcast | | | Update |
|---------|-------------|-------|------------------|----------------|
| Name | Domain Name | MTU | Port List | Status Details |
| ----- | ----- | ----- | ----- | ----- |
| Default | Default-1 | 1500 | | |
| | | | cluster-1-02:e0g | error |

Para obtener más información, consulte ["Comandos de ONTAP 9"](#).

Eliminar un dominio de retransmisión

Si ya no necesita un dominio de retransmisión, puede eliminarlo. Esto mueve los puertos asociados a ese dominio de retransmisión al espacio IP "predeterminado".

Antes de empezar

No debe haber subredes, interfaces de red ni SVM asociadas al dominio de retransmisión que desee eliminar.

Acerca de esta tarea

- El dominio de retransmisión "Cluster" creado por el sistema no se puede eliminar.
- Cuando se elimina el dominio de retransmisión, se quitan todos los grupos de conmutación por error relacionados con el dominio de retransmisión.


El procedimiento que siga depende de la interfaz que utilice: System Manager o CLI:

System Manager

A partir de ONTAP 9.12.0, puede utilizar System Manager para eliminar un dominio de difusión

La opción delete no se muestra cuando el dominio de retransmisión contiene puertos o está asociado a una subred.

Pasos

1. Seleccione **Red > Descripción general > dominio de difusión**.
2. Seleccione  > **Eliminar** junto al dominio de difusión que desea eliminar.

CLI

Utilice la CLI para eliminar un dominio de difusión

Paso

Eliminar un dominio de retransmisión:

```
network port broadcast-domain delete -broadcast-domain broadcast_domain_name
[-ipspace ipspace_name]
```

El siguiente comando elimina el dominio de difusión predeterminado-1 en IPspace1:

```
network port broadcast-domain delete -broadcast-domain Default-1 -ipspace
ipspace1
```

Dominio de retransmisión (ONTAP 9,7 y anterior)

Información general sobre el dominio de retransmisión (ONTAP 9,7 y anteriores)

Los dominios de difusión están destinados a agrupar puertos de red que pertenecen a la misma red de capa 2. Los puertos del grupo pueden usarse en una máquina virtual de almacenamiento (SVM) para el tráfico de datos o gestión.

Un dominio de retransmisión reside en un espacio IP. Durante la inicialización del clúster, el sistema crea dos dominios de retransmisión predeterminados:

- El dominio de retransmisión predeterminado contiene puertos que se encuentran en el espacio IP predeterminado.
Estos puertos se utilizan principalmente para servir datos. Los puertos de gestión de clústeres y gestión de nodos también están en este dominio de retransmisión.
- El dominio de retransmisión del clúster contiene puertos que se encuentran en el espacio IP del clúster.
Estos puertos se utilizan para la comunicación del clúster e incluyen todos los puertos de clúster de todos los nodos del clúster.

Si ha creado espacios IP únicos para separar el tráfico de cliente, debe crear un dominio de retransmisión en cada uno de esos espacios IP.



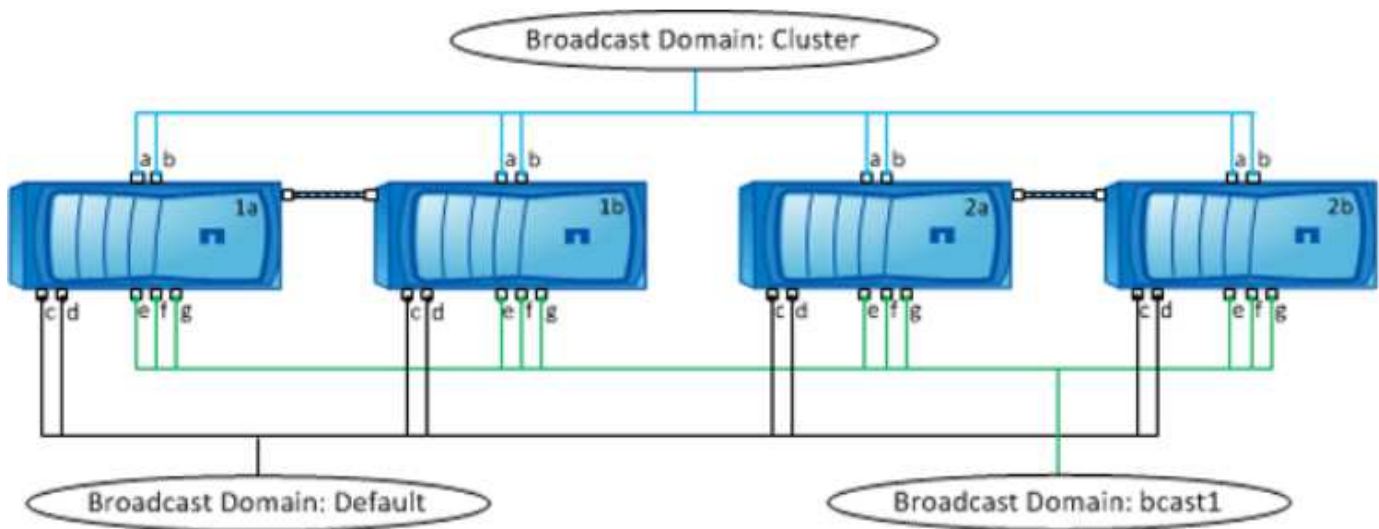
Cree un dominio de retransmisión para agrupar los puertos de red del clúster que pertenecen a la misma red de capa 2. Los puertos pueden entonces ser utilizados por las SVM.

Ejemplo de uso de dominios de retransmisión

Un dominio de retransmisión es un conjunto de puertos de red en el mismo espacio IP que también tiene capacidad para el uno al otro de la capa 2, lo que suele incluir puertos de muchos nodos del clúster.

En la ilustración, se muestran los puertos asignados a tres dominios de retransmisión en un clúster de cuatro nodos:

- El dominio de retransmisión de clúster se crea automáticamente durante la inicialización del clúster. Contiene los puertos a y b de cada nodo del clúster.
 - El dominio de retransmisión predeterminado también se crea automáticamente durante la inicialización del clúster; contiene los puertos c y d de cada nodo del clúster.
 - El dominio de difusión bcast1 se ha creado manualmente y contiene los puertos e, f y g de cada nodo del clúster.
- Este dominio de retransmisión lo creó el administrador del sistema específicamente para que un nuevo cliente acceda a los datos a través de una nueva SVM.



Un grupo de conmutación por error con el mismo nombre y los mismos puertos de red que cada dominio de retransmisión se crea automáticamente. El sistema administra automáticamente este grupo de conmutación por error, lo que significa que, a medida que se agregan o quitan puertos del dominio de retransmisión, se agregan o se quitan automáticamente de este grupo de conmutación por error.

Determinar qué puertos se pueden usar para un dominio de retransmisión (ONTAP 9,7 y versiones anteriores)

Antes de poder configurar un dominio de retransmisión para añadir al espacio IP nuevo, debe determinar qué puertos están disponibles para el dominio de retransmisión.



Esta tarea es relevante para ONTAP 9.0 - 9.7, no para ONTAP 9.8.

Antes de empezar

Para realizar esta tarea, debe ser un administrador de clústeres.

Acerca de esta tarea

- Los puertos pueden ser puertos físicos, VLAN o grupos de interfaces (grupos de interfaces).
- Los puertos que desea añadir al nuevo dominio de retransmisión no se pueden asignar a un dominio de retransmisión existente.
- Si los puertos que desea agregar al dominio de retransmisión ya se encuentran en otro dominio de retransmisión (por ejemplo, el dominio de retransmisión predeterminado en el espacio IP predeterminado), debe eliminar los puertos de ese dominio de retransmisión antes de asignarles el nuevo dominio de retransmisión.
- Los puertos que tienen asignadas LIF no se pueden quitar de un dominio de retransmisión.
- Dado que las LIF de gestión del clúster y de gestión de nodos se asignan al dominio de retransmisión predeterminado en el espacio IP predeterminado, los puertos asignados a estas LIF no se pueden quitar del dominio de retransmisión predeterminado.

Pasos

1. Determine las asignaciones de puertos actuales.

```
network port show
```

| Node | Port | IPspace | Broadcast | Domain | Link | MTU | Admin/Oper |
|-------|------|---------|-----------|--------|-------|------|------------|
| ----- | ---- | ----- | ----- | ----- | ----- | ---- | ----- |
| node1 | | | | | | | |
| | e0a | Cluster | Cluster | | up | 9000 | auto/1000 |
| | e0b | Cluster | Cluster | | up | 9000 | auto/1000 |
| | e0c | Default | Default | | up | 1500 | auto/1000 |
| | e0d | Default | Default | | up | 1500 | auto/1000 |
| | e0e | Default | Default | | up | 1500 | auto/1000 |
| | e0f | Default | Default | | up | 1500 | auto/1000 |
| | e0g | Default | Default | | up | 1500 | auto/1000 |
| node2 | | | | | | | |
| | e0a | Cluster | Cluster | | up | 9000 | auto/1000 |
| | e0b | Cluster | Cluster | | up | 9000 | auto/1000 |
| | e0c | Default | Default | | up | 1500 | auto/1000 |
| | e0d | Default | Default | | up | 1500 | auto/1000 |
| | e0e | Default | Default | | up | 1500 | auto/1000 |
| | e0f | Default | Default | | up | 1500 | auto/1000 |
| | e0g | Default | Default | | up | 1500 | auto/1000 |

En este ejemplo, el resultado del comando proporciona la siguiente información:

- Puertos e0c, e0d, e0e, e0f, y. e0g En cada nodo se asigna al dominio de retransmisión predeterminado.
- Estos puertos están potencialmente disponibles para su uso en el dominio de retransmisión del espacio IP que desea crear.

- Determine qué puertos del dominio de retransmisión predeterminado se asignan a las interfaces LIF y, por lo tanto, no se pueden mover a un nuevo dominio de retransmisión.

```
network interface show
```

| Vserver | Logical Interface | Status Admin/Oper | Network Address/Mask | Current Node | Current Port | Is Home |
|----------|-------------------|-------------------|----------------------|--------------|--------------|---------|
| ----- | ----- | ----- | ----- | ----- | ----- | ---- |
| Cluster | | | | | | |
| | node1_clus1 | up/up | 10.0.2.40/24 | node1 | e0a | true |
| | node1_clus2 | up/up | 10.0.2.41/24 | node1 | e0b | true |
| | node2_clus1 | up/up | 10.0.2.42/24 | node2 | e0a | true |
| | node2_clus2 | up/up | 10.0.2.43/24 | node2 | e0b | true |
| cluster1 | | | | | | |
| | cluster_mgmt | up/up | 10.0.1.41/24 | node1 | e0c | true |
| | node1_mgmt | up/up | 10.0.1.42/24 | node1 | e0c | true |
| | node2_mgmt | up/up | 10.0.1.43/24 | node2 | e0c | true |

En el ejemplo siguiente, el resultado del comando proporciona la siguiente información:

- Los puertos del nodo están asignados al puerto e0c En cada nodo y el nodo de inicio del LIF administrativo del clúster están en e0c encendido node1.
- Puertos e0d, e0e, e0f, y. e0g En cada nodo no se alojan las LIF y se puede quitar del dominio de retransmisión predeterminado y, a continuación, se puede agregar a un nuevo dominio de retransmisión para el nuevo espacio IP.

Crear un dominio de retransmisión (ONTAP 9.7 y versiones anteriores)

En ONTAP 9.7 y versiones anteriores, se crea un dominio de retransmisión para agrupar los puertos de red del clúster que pertenecen a la misma red de capa 2. Los puertos pueden entonces ser utilizados por las SVM. Debe crear un dominio de retransmisión para un espacio IP personalizado. Las SVM creadas en el espacio IP utilizan los puertos del dominio de retransmisión.



Esta tarea es relevante para ONTAP 9.0 - 9.7, no para ONTAP 9.8.

Antes de empezar

Para realizar esta tarea, debe ser un administrador de clústeres.

A partir de ONTAP 9.8, los dominios de retransmisión se crean automáticamente durante la operación de creación de clústeres o unión. Si ejecuta ONTAP 9.8 o una versión posterior, no necesita estos pasos.

En ONTAP 9.7 y versiones anteriores, los puertos que desea agregar al dominio de retransmisión no deben pertenecer a otro dominio de retransmisión.

Acerca de esta tarea

El puerto al que se conmuta por error un LIF debe ser miembro del grupo de conmutación por error de la LIF.

Cuando se crea un dominio de retransmisión, ONTAP crea automáticamente un grupo de conmutación por error con el mismo nombre. El grupo de conmutación por error contiene todos los puertos asignados al dominio de retransmisión.

- Todos los nombres de dominio de retransmisión deben ser únicos en un espacio IP.
- Los puertos que se añaden a un dominio de retransmisión pueden ser puertos de red físicos, VLAN o grupos de interfaces (ifgrps).
- Si los puertos que desea utilizar pertenecen a otro dominio de retransmisión, pero no se utilizan, utilice `network port broadcast-domain remove-ports` comando para quitar los puertos del dominio de retransmisión existente.
- El MTU de los puertos añadidos a un dominio de retransmisión se actualiza al valor MTU establecido en el dominio de retransmisión.
- El valor de MTU debe coincidir con todos los dispositivos conectados a esa red de capa 2, excepto en el caso del puerto e0M que gestiona el tráfico de gestión.
- Si no especifica un nombre de espacio IP, el dominio de retransmisión se crea en el espacio IP «predeterminado».

Para facilitar la configuración del sistema, se crea automáticamente un grupo de conmutación por error con el mismo nombre que contiene los mismos puertos.

Pasos

1. Vea los puertos que no están asignados actualmente a un dominio de retransmisión:

```
network port show
```

Si la pantalla es grande, utilice `network port show -broadcast-domain` comando para ver solo puertos sin asignar.

2. Cree un dominio de retransmisión:

```
network port broadcast-domain create -broadcast-domain broadcast_domain_name  
-mtu mtu_value [-ipSPACE ipSPACE_name] [-ports ports_list]
```

◦ *broadcast_domain_name* es el nombre del dominio de retransmisión que desea crear.

◦ *mtu_value* Es el tamaño de MTU para paquetes IP; 1500 y 9000 son valores típicos.

Este valor se aplica a todos los puertos que se agregan a este dominio de difusión.

◦ *ipSPACE_name* Es el nombre del espacio IP al que se agregará este dominio de retransmisión.

El espacio IP «predeterminado» se utiliza a menos que especifique un valor para este parámetro.

◦ *ports_list* es la lista de puertos que se agregarán al dominio de retransmisión.

Los puertos se añaden con el formato *node_name:port_number*, por ejemplo, *node1:e0c*.

3. Compruebe que el dominio de retransmisión se ha creado como desea:

```
network port show -instance -broadcast-domain new_domain
```

Ejemplo

El siguiente comando crea el dominio de broadcast bcast1 en el espacio IP predeterminado, establece la MTU

en 1500 y agrega cuatro puertos:

```
network port broadcast-domain create -broadcast-domain bcast1 -mtu 1500 -ports
cluster1-01:e0e,cluster1-01:e0f,cluster1-02:e0e,cluster1-02:e0f
```

Después de terminar

Puede definir el pool de direcciones IP disponibles en el dominio de retransmisión mediante la creación de una subred, o puede asignar SVM e interfaces al espacio IP en este momento. Para obtener más información, consulte ["Relaciones entre iguales de clústeres y SVM"](#).

Si necesita cambiar el nombre de un dominio de difusión existente, utilice `network port broadcast-domain rename` comando.

Agregar o quitar puertos de un dominio de retransmisión (ONTAP 9,7 y versiones anteriores)

Es posible añadir puertos de red cuando se crea inicialmente un dominio de retransmisión, o bien añadir puertos a un dominio de retransmisión o quitar puertos de este ya existente. Esto le permite utilizar de forma eficiente todos los puertos del clúster.

Si los puertos que desea añadir al nuevo dominio de retransmisión ya se encuentran en otro dominio de retransmisión, debe quitar los puertos de ese dominio de retransmisión antes de asignarles el nuevo dominio de retransmisión.



Esta tarea es relevante para ONTAP 9.0 - 9.7, no para ONTAP 9.8.

Antes de empezar

- Para realizar esta tarea, debe ser un administrador de clústeres.
- Los puertos que desea agregar a un dominio de difusión no deben pertenecer a otro dominio de difusión.
- Los puertos que ya pertenecen a un grupo de interfaces no se pueden agregar individualmente a un dominio de retransmisión.

Acerca de esta tarea

Las siguientes reglas se aplican al agregar y quitar puertos de red:

| Al agregar puertos... | Al quitar puertos... |
|---|--|
| Los puertos pueden ser puertos de red, VLAN o grupos de interfaces (ifgrps). | N.A. |
| Los puertos se añaden al grupo de conmutación al nodo de respaldo definido por el sistema del dominio de retransmisión. | Los puertos se quitan de todos los grupos de conmutación al nodo de respaldo en el dominio de retransmisión. |
| El MTU de los puertos se actualiza con el valor de MTU establecido en el dominio de retransmisión. | El MTU de los puertos no cambia. |
| El espacio IP de los puertos se actualiza al valor IPspace del dominio de retransmisión. | Los puertos se mueven al espacio IP "predeterminado" sin ningún atributo de dominio de difusión. |



Si elimina el último puerto miembro de un grupo de interfaces mediante `network port ifgrp remove-port` comando, esto hace que se elimine el puerto del grupo de interfaces del dominio de retransmisión porque no se permite un puerto de grupo de interfaces vacío en un dominio de retransmisión.

Pasos

1. Muestra los puertos asignados o no asignados actualmente a un dominio de retransmisión mediante el `network port show` comando.
2. Añada o quite puertos de red del dominio de retransmisión:

| Si desea... | Usar... |
|--|---|
| Añada puertos a un dominio de retransmisión | <code>network port broadcast-domain add-ports</code> |
| Quite puertos de un dominio de retransmisión | <code>network port broadcast-domain remove-ports</code> |

3. Compruebe que los puertos se han agregado o eliminado del dominio de retransmisión:

```
network port show
```

Para obtener más información sobre estos comandos, consulte ["Comandos de ONTAP 9"](#).

Ejemplos de cómo agregar y quitar puertos

El siguiente comando agrega el puerto e0g en el nodo cluster-1-01 y el puerto e0g en el nodo cluster-1-02 al dominio de retransmisión bcast1 en el espacio IP predeterminado:

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain bcast1  
-ports cluster-1-01:e0g,cluster1-02:e0g
```

El siguiente comando añade dos puertos de clúster al clúster de retransmisión en el espacio IP del clúster:

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain Cluster  
-ports cluster-2-03:e0f,cluster2-04:e0f -ipspace Cluster
```

El siguiente comando elimina el puerto e0e en el cluster no1-01 del dominio de broadcast bcast1 en el espacio IP predeterminado:

```
cluster-1::> network port broadcast-domain remove-ports -broadcast-domain bcast1  
-ports cluster-1-01:e0e
```

Dividir dominios de retransmisión (ONTAP 9.7 o anterior)

Puede modificar un dominio de retransmisión existente dividiéndolo en dos dominios de retransmisión diferentes, y cada dominio de retransmisión contendrá algunos de los puertos originales asignados al dominio de retransmisión original.

Acerca de esta tarea

- Si los puertos están en un grupo de conmutación por error, todos los puertos de un grupo de conmutación por error deben estar divididos.
- Si los puertos tienen LIF asociadas, las LIF no pueden formar parte de los rangos de una subred.

Paso

Divida un dominio de retransmisión en dos dominios de retransmisión:

```
network port broadcast-domain split -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -new-broadcast-domain
<broadcast_domain_name> -ports <node:port,node:port>
```

- `ipspace_name` Es el nombre del espacio IP donde reside el dominio de retransmisión.
- `-broadcast-domain` es el nombre del dominio de difusión que se dividirá.
- `-new-broadcast-domain` es el nombre del nuevo dominio de difusión que se creará.
- `-ports` es el nombre del nodo y el puerto que se añadirán al nuevo dominio de retransmisión.

Fusionar dominios de retransmisión (ONTAP 9,7 y anteriores)

Puede mover todos los puertos de un dominio de difusión a un dominio de difusión existente mediante el comando **MERGE**.

Esta operación reduce los pasos necesarios si quita todos los puertos de un dominio de retransmisión y luego añade los puertos a un dominio de retransmisión existente.

Paso

Fusionar los puertos de un dominio de difusión en un dominio de difusión existente:

```
network port broadcast-domain merge -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -into-broadcast-domain
<broadcast_domain_name>
```

- `ipspace_name` Es el nombre del espacio IP donde residen los dominios de retransmisión.
- `-broadcast-domain` es el nombre del dominio de difusión que se combinará.
- `-into-broadcast-domain` es el nombre del dominio de difusión que recibirá puertos adicionales.

Ejemplo

El siguiente ejemplo fusiona el dominio de broadcast `bd-data1` en el dominio de broadcast `bd-data2`:

```
network port -ipspace Default broadcast-domain bd-data1 into-broadcast-domain bd-
data2
```

Cambiar el valor de MTU para los puertos en un dominio de retransmisión (ONTAP 9,7 y anteriores)

Puede modificar el valor MTU para un dominio de retransmisión para cambiar el valor de MTU para todos los puertos en ese dominio de retransmisión. Esto se puede hacer para

admitir cambios de topología que se han realizado en la red.

Antes de empezar

El valor de MTU debe coincidir con todos los dispositivos conectados a esa red de capa 2, excepto en el caso del puerto e0M que gestiona el tráfico de gestión.

Acerca de esta tarea

Al cambiar el valor de MTU, se produce una breve interrupción en el tráfico de los puertos afectados. El sistema muestra un símbolo del sistema de que debe responder con y para hacer el cambio de la MTU.

Paso

Cambie el valor de MTU para todos los puertos de un dominio de retransmisión:

```
network port broadcast-domain modify -broadcast-domain  
<broadcast_domain_name> -mtu <mtu_value> [-ipSPACE <ipSPACE_name>]
```

- `broadcast_domain` es el nombre del dominio de retransmisión.
- `mtu` Es el tamaño de MTU para paquetes IP; 1500 y 9000 son valores típicos.
- `ipSPACE` Es el nombre del espacio IP en el que reside el dominio de retransmisión. El espacio IP «predeterminado» se utiliza a menos que especifique un valor para esta opción. El siguiente comando cambia la MTU a 9000 para todos los puertos del dominio de broadcast `bcast1`:

```
network port broadcast-domain modify -broadcast-domain <Default-1> -mtu <  
9000 >  
Warning: Changing broadcast domain settings will cause a momentary data-  
serving interruption.  
Do you want to continue? {y|n}: <y>
```

Mostrar dominios de retransmisión (ONTAP 9,7 y anteriores)

Puede mostrar la lista de dominios de retransmisión dentro de cada espacio IP de un clúster. El resultado también muestra la lista de puertos y el valor MTU para cada dominio de retransmisión.

Paso

Muestre los dominios de retransmisión y los puertos asociados en el clúster:

```
network port broadcast-domain show
```

El siguiente comando muestra todos los dominios de retransmisión y los puertos asociados en el clúster:

```
network port broadcast-domain show
```

| IPspace | Broadcast | | | Update |
|---------|-------------|-------|------------------|----------------|
| Name | Domain Name | MTU | Port List | Status Details |
| ----- | ----- | ----- | ----- | ----- |
| Cluster | Cluster | 9000 | | |
| | | | cluster-1-01:e0a | complete |
| | | | cluster-1-01:e0b | complete |
| | | | cluster-1-02:e0a | complete |
| | | | cluster-1-02:e0b | complete |
| Default | Default | 1500 | | |
| | | | cluster-1-01:e0c | complete |
| | | | cluster-1-01:e0d | complete |
| | | | cluster-1-02:e0c | complete |
| | | | cluster-1-02:e0d | complete |
| | bcast1 | 1500 | | |
| | | | cluster-1-01:e0e | complete |
| | | | cluster-1-01:e0f | complete |
| | | | cluster-1-01:e0g | complete |
| | | | cluster-1-02:e0e | complete |
| | | | cluster-1-02:e0f | complete |
| | | | cluster-1-02:e0g | complete |

El siguiente comando muestra los puertos del dominio de difusión bcast1 que tienen el estado de actualización del error, lo que indica que el puerto no se ha podido actualizar correctamente:

```
network port broadcast-domain show -broadcast-domain bcast1 -port-update
-status error
```

| IPspace | Broadcast | | | Update |
|---------|-------------|-------|------------------|----------------|
| Name | Domain Name | MTU | Port List | Status Details |
| ----- | ----- | ----- | ----- | ----- |
| Default | bcast1 | 1500 | | |
| | | | cluster-1-02:e0g | error |

Para obtener más información, consulte ["Comandos de ONTAP 9"](#).

Eliminar un dominio de retransmisión

Si ya no necesita un dominio de retransmisión, puede eliminarlo. Esto mueve los puertos asociados a ese dominio de retransmisión al espacio IP "predeterminado".

Antes de empezar

No debe haber subredes, interfaces de red ni SVM asociadas al dominio de retransmisión que desee eliminar.

Acerca de esta tarea

- El dominio de retransmisión "Cluster" creado por el sistema no se puede eliminar.
- Cuando se elimina el dominio de retransmisión, se quitan todos los grupos de conmutación por error relacionados con el dominio de retransmisión.


El procedimiento que siga depende de la interfaz que utilice: System Manager o CLI:

System Manager

A partir de ONTAP 9.12.0, puede utilizar System Manager para eliminar un dominio de difusión

La opción delete no se muestra cuando el dominio de retransmisión contiene puertos o está asociado a una subred.

Pasos

1. Seleccione **Red > Descripción general > dominio de difusión**.
2. Seleccione  > **Eliminar** junto al dominio de difusión que desea eliminar.

CLI

Utilice la CLI para eliminar un dominio de difusión

Paso

Eliminar un dominio de retransmisión:

```
network port broadcast-domain delete -broadcast-domain broadcast_domain_name
[-ipspace ipspace_name]
```

El siguiente comando elimina el dominio de difusión predeterminado-1 en IPspace1:

```
network port broadcast-domain delete -broadcast-domain Default-1 -ipspace
ipspace1
```

Grupos y políticas de conmutación por error

Información general sobre recuperación tras fallos de LIF

La conmutación por error de LIF hace referencia a la migración automática de una LIF a un puerto de red diferente en respuesta a un error de enlace en el puerto actual de la LIF. Este es un componente clave para proporcionar alta disponibilidad para las conexiones a SVM. Configurar la conmutación por error de LIF implica crear un grupo de conmutación por error, modificar la LIF para utilizar el grupo de conmutación por error y especificar una política de conmutación por error.

Un grupo de conmutación al nodo de respaldo contiene un conjunto de puertos de red (puertos físicos, VLAN y grupos de interfaces) desde uno o más nodos de un clúster. Los puertos de red presentes en el grupo de conmutación por error definen los destinos de conmutación por error disponibles para la LIF. Un grupo de recuperación tras fallos puede tener asignadas LIF de datos NAS, gestión de clústeres y nodos, interconexión de clústeres.



Cuando se configura una LIF sin un destino de conmutación por error válido, se produce una interrupción cuando la LIF intenta conmutar por error. Puede utilizar el comando "network interface show -failover" para verificar la configuración de recuperación tras fallos.

Cuando se crea un dominio de retransmisión, se crea automáticamente un grupo de conmutación por error con el mismo nombre que contiene los mismos puertos de red. El sistema administra automáticamente este grupo de conmutación por error, lo que significa que, a medida que se agregan o quitan puertos del dominio de retransmisión, se agregan o se quitan automáticamente de este grupo de conmutación por error. Este enfoque se proporciona como una eficiencia para los administradores que no quieren gestionar sus propios grupos de conmutación al nodo de respaldo.

Cree un grupo de recuperación tras fallos

Puede crear un grupo de recuperación tras fallos de puertos de red para que un LIF pueda migrar automáticamente a otro puerto si se produce un fallo de enlace en el puerto actual de la LIF. Esto permite al sistema redirigir el tráfico de red a otros puertos disponibles en el clúster.

Acerca de esta tarea

Utilice la `network interface failover-groups create` comando para crear el grupo y para agregar puertos al grupo.

- Los puertos que se añaden a un grupo de conmutación por error pueden ser puertos de red, VLAN o grupos de interfaces (ifgrps).
- Todos los puertos agregados al grupo de conmutación por error deben pertenecer al mismo dominio de retransmisión.
- Un único puerto puede residir en varios grupos de conmutación por error.
- Si tiene LIF en diferentes VLAN o dominios de retransmisión, debe configurar grupos de conmutación al nodo de respaldo para cada VLAN o dominio de retransmisión.
- Los grupos de recuperación tras fallos no se aplican en entornos SAN iSCSI o FC.

Paso

Crear un grupo de recuperación tras fallos:

```
network interface failover-groups create -vserver vs1 -failover-group failover_group_name -targets ports_list
```

- `vserver_name` Es el nombre de la SVM que puede usar el grupo de conmutación al nodo de respaldo.
- `failover_group_name` es el nombre del grupo de conmutación por error que desea crear.
- `ports_list` es la lista de puertos que se agregarán al grupo de conmutación por error. Los puertos se añaden con el formato `node_name>:<port_number>`, por ejemplo, 1:e0c.

El siguiente comando crea un grupo de conmutación por error fg3 para SVM vs3 y añade dos puertos:

```
network interface failover-groups create -vserver vs3 -failover-group fg3 -targets cluster1-01:e0e,cluster1-02:e0e
```

Después de terminar

- Debería aplicar el grupo de recuperación tras fallos a una LIF ahora que se ha creado el grupo de recuperación tras fallos.
- La aplicación de un grupo de conmutación por error que no proporcione un destino de conmutación por error válido para una LIF da lugar a un mensaje de advertencia.

Si una LIF que no tiene un destino de conmutación por error válido intenta conmutar al respaldo, se podría producir una interrupción del servicio.

Configure los ajustes de recuperación tras fallos en un LIF

Puede configurar una LIF para que conmute por error a un grupo específico de puertos de red aplicando una política de conmutación por error y un grupo de conmutación por error a la LIF. También puede deshabilitar un LIF para no conmutar por error a otro puerto.

Acerca de esta tarea

- Cuando se crea una LIF, la conmutación por error de LIF se habilita de forma predeterminada y la lista de puertos de destino disponibles está determinada por el grupo de conmutación por error y la política de recuperación tras fallos predeterminados según el tipo de LIF y la política de servicio.

A partir de 9.5, puede especificar una política de servicio para la LIF que define qué servicios de red pueden utilizar la LIF. Algunos servicios de red imponen restricciones de conmutación por error en una LIF.



Si se cambia la política de servicio de un LIF de una forma que restringe aún más la conmutación por error, el sistema actualiza automáticamente la política de conmutación por error de LIF.

- Puede modificar el comportamiento de la conmutación por error de las LIF especificando valores para los parámetros `-failover-group` y `-failover-policy` en el comando `network interface modify`.
- La modificación de una LIF que hace que la LIF no tenga ningún destino de conmutación por error válido da como resultado un mensaje de advertencia.

Si una LIF que no tiene un destino de conmutación por error válido intenta conmutar al respaldo, se podría producir una interrupción del servicio.

- A partir de ONTAP 9.11.1, en plataformas de cabina SAN all-flash (ASA), la conmutación por error de LIF iSCSI se activa automáticamente en LIF iSCSI recién creados en los equipos virtuales de almacenamiento recién creados.

Además, puede ["Habilite manualmente la recuperación tras fallos de LIF iSCSI en LIF iSCSI preexistentes"](#), Es decir, LIF que se crearon antes de actualizar a ONTAP 9.11.1 o una versión posterior.

- En la lista siguiente se describe cómo la configuración `-failover-policy` afecta a los puertos de destino seleccionados del grupo de conmutación por error:



Para la conmutación por error de LIF iSCSI, solo las políticas de conmutación por error `local-only`, `sfo-partner-only` y `disabled` sean compatibles.

- `broadcast-domain-wide` se aplica a todos los puertos de todos los nodos del grupo de conmutación por error.

- `system-defined` Se aplica solo a esos puertos del nodo principal de la LIF y a otro nodo del clúster, normalmente un partner distinto de SFO, si existe.
- `local-only` Se aplica solo a los puertos en el nodo principal de la LIF.
- `sfo-partner-only` Se aplica solo a esos puertos del nodo principal de la LIF y a su partner SFO.
- `disabled` Indica que el LIF no está configurado para la conmutación al nodo de respaldo.

Paso

Configurar la conmutación por error para una interfaz existente:

```
network interface modify -vserver <vserver_name> -lif <lif_name> -failover
-policy <failover_policy> -failover-group <failover_group>
```

Ejemplos de configuración de la conmutación por error y desactivación de la conmutación por error

El siguiente comando establece la política de conmutación por error en todo el dominio de difusión y utiliza los puertos del grupo de conmutación por error fg3 como destinos de conmutación por error para los datos de LIF 1 en SVM vs3:

```
network interface modify -vserver vs3 -lif data1 failover-policy
broadcast-domain-wide - failover-group fg3

network interface show -vserver vs3 -lif * -fields failover-
group,failover-policy

vserver lif          failover-policy          failover-group
-----
vs3      data1        broadcast-domain-wide  fg3
```

El siguiente comando deshabilita la recuperación tras fallos para los datos LIF 1 en SVM vs3:

```
network interface modify -vserver vs3 -lif data1 failover-policy disabled
```

Comandos para gestionar las políticas y los grupos de conmutación por error

Puede utilizar el `network interface failover-groups` comandos para gestionar grupos de conmutación por error. Utilice la `network interface modify` Comando para gestionar los grupos de conmutación por error y las políticas de conmutación por error que se aplican a una LIF.

| | |
|---|--|
| Si desea... | Se usa este comando... |
| Agregar puertos de red a un grupo de recuperación tras fallos | <code>network interface failover-groups add-targets</code> |

| | |
|---|---|
| Quitar puertos de red de un grupo de recuperación tras fallos | <code>network interface failover-groups remove-targets</code> |
| Modifique los puertos de red de un grupo de conmutación por error | <code>network interface failover-groups modify</code> |
| Mostrar los grupos de conmutación por error actuales | <code>network interface failover-groups show</code> |
| Configurar la conmutación por error en una LIF | <code>network interface modify -failover -group -failover-policy</code> |
| Mostrar el grupo de conmutación por error y la política de conmutación por error que usa cada LIF | <code>network interface show -fields failover-group, failover-policy</code> |
| Cambiar el nombre de un grupo de conmutación por error | <code>network interface failover-groups rename</code> |
| Eliminar un grupo de recuperación tras fallos | <code>network interface failover-groups delete</code> |



Modificar un grupo de conmutación por error de forma que no proporcione un destino de conmutación por error válido para cualquier LIF del clúster puede provocar una interrupción del servicio cuando un LIF intenta conmutar por error.

Para obtener más información, consulte las páginas de manual de `network interface failover-groups` y `network interface modify` comandos.

Subredes (solo administradores de clúster)

Información general de la subred

Las subredes permiten asignar bloques o pools específicos de direcciones IP para la configuración de red ONTAP. Esto permite crear LIF con mayor facilidad ya que especifica un nombre de subred en lugar de tener que especificar la dirección IP y los valores de máscara de red.

Una subred se crea dentro de un dominio de difusión y contiene un grupo de direcciones IP que pertenecen a la misma subred de capa 3. Las direcciones IP de una subred se asignan a los puertos en el dominio de retransmisión cuando se crean las LIF. Una vez eliminadas las LIF, se devolverán las direcciones IP al pool de subredes y estarán disponibles para futuras LIF.

Se recomienda utilizar subredes porque hacen que la gestión de direcciones IP sea mucho más sencilla y hacen que la creación de las LIF sea un proceso más sencillo. Además, si especifica una puerta de enlace al definir una subred, se añadirá automáticamente a la SVM una ruta predeterminada a esa puerta de enlace cuando se cree una LIF con dicha subred.

Cree una subred

Puede crear una subred para asignar bloques específicos de direcciones IPv4 o IPv6 que se usarán más adelante al crear LIF para la SVM.

Esto permite crear LIF con mayor facilidad ya que especifica un nombre de subred en lugar de tener que especificar la dirección IP y los valores de máscara de red para cada LIF.

Antes de empezar

Para realizar esta tarea, debe ser un administrador de clústeres.

El dominio de retransmisión y el espacio IP en el que va a agregar la subred ya deben existir.

Acerca de esta tarea

- Todos los nombres de subred deben ser únicos en un espacio IP.
- Al añadir rangos de direcciones IP a una subred, debe asegurarse de que no haya direcciones IP superpuestas en la red para que distintas subredes, o hosts, no intenten utilizar la misma dirección IP.
- Si especifica una puerta de enlace al definir una subred, se añadirá automáticamente a la SVM una ruta predeterminada a esa puerta de enlace cuando se cree una LIF con dicha subred. Si no utiliza subredes, o si no especifica una puerta de enlace al definir una subred, deberá utilizar `route create` Comando para añadir una ruta a la SVM de forma manual.

Procedimiento

El procedimiento que siga depende de la interfaz que utilice: System Manager o CLI:

System Manager

A partir de ONTAP 9.12.0, puede usar System Manager para crear una subred.

Pasos

1. Seleccione **Red > Descripción general > subredes**.
2. Haga clic en **+ Add** para crear una subred.
3. Asigne un nombre a la subred.
4. Especifique la dirección IP de la subred.
5. Defina la máscara de subred.
6. Defina el rango de direcciones IP que componen la subred.
7. Si es útil, especifique una puerta de enlace.
8. Seleccione el dominio de retransmisión al que pertenece la subred.
9. Guarde los cambios.
 - a. Si la dirección IP o el rango introducido ya están en uso por una interfaz, se muestra el siguiente mensaje:
An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?
 - b. Al hacer clic en **Aceptar**, la LIF existente se asociará a la subred.

CLI

Use la CLI para crear una subred.

```
network subnet create -subnet-name subnet_name -broadcast-domain  
<broadcast_domain_name> [- ipspace <ipspace_name>] -subnet  
<subnet_address> [-gateway <gateway_address>] [-ip-ranges  
<ip_address_list>] [-force-update-lif-associations <true>]
```

- `subnet_name` es el nombre de la subred de la capa 3 que desea crear.

El nombre puede ser una cadena de texto como "Mgmt" o puede ser un valor IP de subred específico como 192.0.2.0/24.

- `broadcast_domain_name` es el nombre del dominio de difusión en el que residirá la subred.
- `ipspace_name` Es el nombre del espacio IP del que forma parte el dominio de retransmisión.

El espacio IP «predeterminado» se utiliza a menos que especifique un valor para esta opción.

- `subnet_address` Es la dirección IP y la máscara de la subred; por ejemplo, 192.0.2.0/24.
- `gateway_address` es la puerta de enlace de la ruta predeterminada de la subred; por ejemplo, 192.0.2.1.
- `ip_address_list` Es la lista o el intervalo de direcciones IP que se asignarán a la subred.

Las direcciones IP pueden ser direcciones individuales, un rango de direcciones IP o una combinación de ellas en una lista separada por comas.

- El valor `true` se puede establecer para `-force-update-lif-associations` opción.

Este comando falla si cualquier procesador de servicios o interfaz de red están utilizando actualmente las direcciones IP del rango especificado. Si se establece este valor en `true`, se asocia cualquier interfaz dirigida manualmente a la subred actual y se permite que el comando se realice correctamente.

El siguiente comando crea una subred `sub1` en el dominio de difusión `predeterminado-1` en el espacio IP `predeterminado`. Añade una máscara y una dirección IP de subred IPv4, la puerta de enlace y un rango de direcciones IP:

```
network subnet create -subnet-name sub1 -broadcast-domain Default-1
-subnet 192.0.2.0/24 - gateway 192.0.2.1 -ip-ranges 192.0.2.1-
192.0.2.100, 192.0.2.122
```

El siguiente comando crea una subred `sub2` en los valores predeterminados de dominio de difusión en el espacio IP `"predeterminado"`. Añade un rango de direcciones IPv6:

```
network subnet create -subnet-name sub2 -broadcast-domain Default
-subnet 3FFE::/64 - gateway 3FFE::1 -ip-ranges "3FFE::10-3FFE::20"
```

Después de terminar

Puede asignar SVM e interfaces a un espacio IP en las direcciones de la subred.

Si necesita cambiar el nombre de una subred existente, utilice `network subnet rename` comando.

Añada o quite direcciones IP de una subred


Puede añadir direcciones IP al crear inicialmente una subred, o bien añadir direcciones IP a una subred que ya exista. También es posible quitar direcciones IP de una subred existente. Esto le permite asignar solo las direcciones IP necesarias para las SVM.

El procedimiento que siga depende de la interfaz que utilice: System Manager o CLI:

System Manager

A partir de ONTAP 9.12.0, puede utilizar System Manager para agregar o quitar direcciones IP a o desde una subred

Pasos

1. Seleccione **Red > Descripción general > subredes**.
2. Seleccione  > **Editar** junto a la subred que desea cambiar.
3. Añadir o quitar direcciones IP.
4. Guarde los cambios.
 - a. Si la dirección IP o el rango introducido ya están en uso por una interfaz, se muestra el siguiente mensaje:
An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?
 - b. Al hacer clic en **Aceptar**, la LIF existente se asociará a la subred.

CLI

Utilice la CLI para agregar o quitar direcciones IP a o desde una subred

Acerca de esta tarea

Al añadir direcciones IP, recibirá un error si alguna interfaz de red o procesador de servicios utiliza las direcciones IP del rango que se va a añadir. Si desea asociar cualquier interfaz de dirección manual con la subred actual, puede establecer la `-force-update-lif-associations` opción a `true`.

Al quitar direcciones IP, recibirá un error si alguna interfaz de red o procesador de servicios utiliza las direcciones IP que se están quitando. Si desea que las interfaces sigan usando las direcciones IP una vez que se hayan eliminado de la subred, puede configurar el `-force-update-lif-associations` opción a `true`.

Paso

Añada o quite direcciones IP de una subred:

| Si desea... | Se usa este comando... |
|--|--|
| Añada direcciones IP a una subred | intervalos adicionales de subred de red |
| Quite las direcciones IP de una subred | intervalos de eliminación de subred de red |

Para obtener más información sobre estos comandos, consulte las páginas man.

El siguiente comando agrega las direcciones IP 192.0.2.82 a 192.0.2.85 a la subred sub1:

```
network subnet add-ranges -subnet-name <sub1> -ip-ranges <192.0.2.82-192.0.2.85>
```

El siguiente comando elimina la dirección IP 198.51.100.9 de la subred sub3:


```
network subnet remove-ranges -subnet-name <sub3> -ip-ranges  
<198.51.100.9>
```

Si el rango actual incluye de 1 a 10 y de 20 a 40, y desea agregar de 11 a 19 y de 41 a 50 (básicamente permitiendo de 1 a 50), puede superponer el rango existente de direcciones utilizando el comando siguiente. Este comando añade solo las direcciones nuevas y no afecta a las direcciones existentes:

```
network subnet add-ranges -subnet-name <sub3> -ip-ranges <198.51.10.1-  
198.51.10.50>
```

Cambie las propiedades de la subred

Es posible cambiar la dirección de subred y el valor de la máscara, la dirección de la puerta de enlace o el rango de direcciones IP en una subred existente.

Acerca de esta tarea


- Al modificar direcciones IP, debe asegurarse de que no haya direcciones IP superpuestas en la red, de modo que distintas subredes, o hosts, no intente utilizar la misma dirección IP.
- Si añade o cambia la dirección IP de puerta de enlace, la puerta de enlace modificada se aplica a las nuevas SVM cuando se crea una LIF en ellas mediante la subred. Se crea una ruta predeterminada a la puerta de enlace para la SVM si aún no existe la ruta. Puede que deba añadir manualmente una nueva ruta a la SVM cuando cambie la dirección IP de puerta de enlace.

El procedimiento que siga depende de la interfaz que utilice: System Manager o CLI:

System Manager

A partir de ONTAP 9.12.0, puede utilizar System Manager para cambiar las propiedades de subred

Pasos

1. Seleccione **Red > Descripción general > subredes**.
2. Seleccione  **Editar** junto a la subred que desea cambiar.
3. Realice cambios.
4. Guarde los cambios.
 - a. Si la dirección IP o el rango introducido ya están en uso por una interfaz, se muestra el siguiente mensaje:
An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?
 - b. Al hacer clic en **Aceptar**, la LIF existente se asociará a la subred.

CLI

Utilice la CLI para cambiar las propiedades de subred

Paso

Modificar propiedades de subred:

```
network subnet modify -subnet-name <subnet_name> [-ipSPACE
<ipSPACE_name>] [-subnet <subnet_address>] [-gateway <gateway_address>]
[-ip-ranges <ip_address_list>] [-force-update-lif-associations <true>]
```

- `subnet_name` es el nombre de la subred que desea modificar.
- `ipSPACE` Es el nombre del espacio IP en el que reside la subred.
- `subnet` es la nueva dirección y máscara de la subred, si procede; por ejemplo, 192.0.2.0/24.
- `gateway` es la nueva puerta de enlace de la subred, si corresponde; por ejemplo, 192.0.2.1. Al introducir " se elimina la entrada de la puerta de enlace.
- `ip_ranges` Es la nueva lista o rango de direcciones IP que se asignarán a la subred, si corresponde. Las direcciones IP pueden ser direcciones individuales, un rango o direcciones IP, o una combinación de ambas. El intervalo especificado aquí sustituye a las direcciones IP existentes.
- `force-update-lif-associations` Cuando cambie el rango de direcciones IP, será necesario. Puede establecer el valor en **verdadero** para esta opción al modificar el rango de direcciones IP. Este comando falla si cualquier procesador de servicios o interfaz de red están usando las direcciones IP del rango especificado. Al establecer este valor en **true**, se asocia cualquier interfaz de dirección manual con la subred actual y se permite que el comando tenga éxito.

El siguiente comando modifica la dirección IP de la puerta de enlace de la subred sub3:

```
network subnet modify -subnet-name <sub3> -gateway <192.0.3.1>
```

Mostrar subredes

Puede mostrar la lista de direcciones IP asignadas a cada subred dentro de un espacio IP. El resultado también muestra el número total de direcciones IP disponibles en cada subred y el número de direcciones que se están utilizando actualmente.

El procedimiento que siga depende de la interfaz que utilice: System Manager o CLI:

System Manager

A partir de ONTAP 9.12.0, puede utilizar el Administrador del sistema para mostrar subredes

Pasos

1. Seleccione **Red > Descripción general > subredes**.
2. Consulte la lista de subredes.

CLI

Utilice la CLI para mostrar subredes

Paso

Mostrar la lista de subredes y los intervalos de direcciones IP asociados que se utilizan en esas subredes:

```
network subnet show
```

El siguiente comando muestra las subredes y las propiedades de subred:

```
network subnet show

IPspace: Default
Subnet
Name      Subnet          Broadcast
-----  -
sub1      192.0.2.0/24     bcast1
192.0.2.100
sub3      198.51.100.0/24  bcast3
198.51.100.7,198.51.100.9
Gateway
-----
192.0.2.1
198.51.100.1
Avail/
Total
5/9
3/3
Ranges
192.0.2.92-
```

Eliminar una subred


Si ya no necesita una subred y desea desasignar las direcciones IP que han sido asignadas a la subred, puede eliminarla.

El procedimiento que siga depende de la interfaz que utilice: System Manager o CLI:

System Manager

A partir de ONTAP 9.12.0, puede utilizar System Manager para eliminar una subred

Pasos

1. Seleccione **Red > Descripción general > subredes**.
2. Seleccione  > **Eliminar** junto a la subred que desea eliminar.
3. Guarde los cambios.

CLI

Utilice la CLI para eliminar una subred

Acerca de esta tarea

Recibirá un error si alguna interfaz de red o procesador de servicios está utilizando actualmente direcciones IP en los rangos especificados. Si desea que las interfaces sigan usando las direcciones IP incluso después de eliminar la subred, puede establecer la opción `-force-update-lif-associates TRUE` para eliminar la asociación de la subred con las LIF.

Paso

Eliminar una subred:

```
network subnet delete -subnet-name subnet_name [-ipspace ipspace_name] [-force-update-lif-associations true]
```

El siguiente comando elimina la subred sub1 en IPspace 1:

```
network subnet delete -subnet-name sub1 -ipspace ipspace1
```

Cree SVM

Debe crear una SVM para servir datos a los clientes.

Antes de empezar

- Para realizar esta tarea, debe ser un administrador de clústeres.
- Se debe saber qué estilo de seguridad tendrá el volumen raíz de la SVM.

Si piensa implementar una solución Hyper-V o SQL Server sobre SMB en esta SVM, debe utilizar el estilo de seguridad NTFS para el volumen raíz. Los volúmenes que contienen archivos de Hyper-V o archivos de base de datos de SQL se deben establecer en seguridad NTFS en el momento en el que se crean. Al establecer el estilo de seguridad del volumen raíz en NTFS, se asegura de que no se creen volúmenes de datos de estilo de seguridad mixtos o UNIX de forma accidental.

- A partir de ONTAP 9.13.1, puede establecer una capacidad máxima para una máquina virtual de almacenamiento. También puede configurar alertas cuando la SVM se acerca a un nivel de umbral de capacidad. Para obtener más información, consulte [Gestionar la capacidad de SVM](#).

System Manager

Puede usar System Manager para crear una máquina virtual de almacenamiento.

Pasos

1. Seleccione **Storage VMs**.
2. Haga clic en **+ Add** Para crear una máquina virtual de almacenamiento.
3. Asigne un nombre a la máquina virtual de almacenamiento.
4. Seleccione el protocolo de acceso:
 - SMB/CIFS Y NFS
 - iSCSI
 - FC
 - NVMe
 - i. Si selecciona **Activar SMB/CIFS**, complete la siguiente configuración:

| Campo o casilla de verificación | Descripción |
|---|---|
| Nombre del administrador | Especifique el nombre de usuario del administrador para la máquina virtual de almacenamiento SMB/CIFS. |
| Contraseña | Especifique la contraseña de administrador para la máquina virtual de almacenamiento SMB/CIFS. |
| Nombre del servidor | Especifique el nombre del servidor para la máquina virtual de almacenamiento SMB/CIFS. |
| Dominio de Active Directory | Especifique el dominio de Active Directory para proporcionar autenticación de usuarios para la máquina virtual de almacenamiento SMB/CIFS. |
| Unidad organizacional | Especifique la unidad organizativa en el dominio de Active Directory asociado con el servidor SMB/CIFS. "CN=Computers" es el valor predeterminado, que se puede modificar. |
| Cifra datos al acceder a los recursos compartidos de la máquina virtual de almacenamiento | Seleccione esta casilla de comprobación para cifrar datos mediante SMB 3.0 para evitar el acceso no autorizado a archivos en los recursos compartidos de la máquina virtual de almacenamiento SMB/CIFS. |
| Dominios | Añada, elimine o reordene los dominios enumerados para la máquina virtual de almacenamiento de SMB/CIFS. |

| | |
|-------------------------------------|--|
| Servidores de nombres | Añada, elimine o reordene los servidores de nombres para la máquina virtual de almacenamiento SMB/CIFS. |
| Idioma predeterminado | Especifica la configuración de codificación de idioma predeterminada para la máquina virtual de almacenamiento y sus volúmenes. Use la interfaz de línea de comandos para cambiar la configuración de cada volumen dentro de una máquina virtual de almacenamiento. |
| Interfaz de red | <p>Para cada interfaz de red que configure para el equipo virtual de almacenamiento, seleccione una subred existente (si existe al menos una) o especifique sin subred y complete los campos Dirección IP y Máscara de subred.</p> <p>Si resulta útil, active la casilla de verificación usar la misma máscara de subred y puerta de enlace para todas las siguientes interfaces.</p> <p>Puede permitir que el sistema seleccione automáticamente el puerto de inicio o seleccionar manualmente el que desea utilizar en la lista.</p> |
| Administrar cuenta de administrador | Seleccione esta casilla de comprobación si desea gestionar la cuenta de administrador de máquina virtual de almacenamiento. Cuando se selecciona, especifique el nombre de usuario, la contraseña, confirme la contraseña e indique si desea añadir una interfaz de red para la gestión de máquinas virtuales de almacenamiento. |

1. Si selecciona **Activar NFS**, complete la siguiente configuración:

| Campo o casilla de verificación | Descripción |
|---|--|
| Casilla de verificación permitir el acceso de cliente NFS | Seleccione esta casilla de comprobación cuando todos los volúmenes creados en el equipo virtual de almacenamiento NFS deban usar la ruta de volumen raíz "/" para montar y recorrer. Añada reglas a la directiva de exportación "default" para permitir una transversal de montaje ininterrumpida. |

| | |
|-----------------------|---|
| Bases de datos | <p>Haga clic en + Add para crear reglas.</p> <ul style="list-style-type: none"> • Especificación del cliente: Especifique los nombres de host, direcciones IP, grupos de red o dominios. • Protocolos de acceso: Seleccione una combinación de las siguientes opciones: <ul style="list-style-type: none"> ◦ SMB/CIFS ◦ FlexCache ◦ NFS <ul style="list-style-type: none"> ▪ NFSv3 ▪ NFSv4 • Detalles de acceso: Para cada tipo de usuario, especifique el nivel de acceso, ya sea de sólo lectura, de lectura/escritura o de superusuario. Los tipos de usuario incluyen: <ul style="list-style-type: none"> ◦ Todo ◦ All (como usuario anónimo) ◦ UNIX ◦ Kerberos 5 ◦ Kerberos 5i ◦ Kerberos 5p ◦ NTLM <p>Guarde la regla.</p> |
| Idioma predeterminado | <p>Especifica la configuración de codificación de idioma predeterminada para la máquina virtual de almacenamiento y sus volúmenes. Use la interfaz de línea de comandos para cambiar la configuración de cada volumen dentro de una máquina virtual de almacenamiento.</p> |
| Interfaz de red | <p>Para cada interfaz de red que configure para el equipo virtual de almacenamiento, seleccione una subred existente (si existe al menos una) o especifique sin subred y complete los campos Dirección IP y Máscara de subred. Si resulta útil, active la casilla de verificación usar la misma máscara de subred y puerta de enlace para todas las siguientes interfaces . Puede permitir que el sistema seleccione automáticamente el puerto de inicio o seleccionar manualmente el que desea utilizar en la lista.</p> |

| | |
|-------------------------------------|--|
| Administrar cuenta de administrador | Seleccione esta casilla de comprobación si desea gestionar la cuenta de administrador de máquina virtual de almacenamiento. Cuando se selecciona, especifique el nombre de usuario, la contraseña, confirme la contraseña e indique si desea añadir una interfaz de red para la gestión de máquinas virtuales de almacenamiento. |
|-------------------------------------|--|

1. Si selecciona **Activar iSCSI**, complete la siguiente configuración:

| Campo o casilla de verificación | Descripción |
|-------------------------------------|---|
| Interfaz de red | Para cada interfaz de red que configure para el equipo virtual de almacenamiento, seleccione una subred existente (si existe al menos una) o especifique sin subred y complete los campos Dirección IP y Máscara de subred . Si resulta útil, active la casilla de verificación usar la misma máscara de subred y puerta de enlace para todas las siguientes interfaces . Puede permitir que el sistema seleccione automáticamente el puerto de inicio o seleccionar manualmente el que desea utilizar en la lista. |
| Administrar cuenta de administrador | Seleccione esta casilla de comprobación si desea gestionar la cuenta de administrador de máquina virtual de almacenamiento. Cuando se selecciona, especifique el nombre de usuario, la contraseña, confirme la contraseña e indique si desea añadir una interfaz de red para la gestión de máquinas virtuales de almacenamiento. |

1. Si selecciona **Habilitar FC**, complete la siguiente configuración:

| Campo o casilla de verificación | Descripción |
|-------------------------------------|--|
| Configure los puertos FC | Seleccione las interfaces de red en los nodos que desea incluir en la máquina virtual de almacenamiento. Se recomiendan dos interfaces de red por nodo. |
| Administrar cuenta de administrador | Seleccione esta casilla de comprobación si desea gestionar la cuenta de administrador de máquina virtual de almacenamiento. Cuando se selecciona, especifique el nombre de usuario, la contraseña, confirme la contraseña e indique si desea añadir una interfaz de red para la gestión de máquinas virtuales de almacenamiento. |

1. Si selecciona **Habilitar NVMe/FC**, complete la siguiente configuración:

| Campo o casilla de verificación | Descripción |
|-------------------------------------|--|
| Configure los puertos FC | Seleccione las interfaces de red en los nodos que desea incluir en la máquina virtual de almacenamiento. Se recomiendan dos interfaces de red por nodo. |
| Administrar cuenta de administrador | Seleccione esta casilla de comprobación si desea gestionar la cuenta de administrador de máquina virtual de almacenamiento. Cuando se selecciona, especifique el nombre de usuario, la contraseña, confirme la contraseña e indique si desea añadir una interfaz de red para la gestión de máquinas virtuales de almacenamiento. |

1. Si selecciona **Habilitar NVMe/TCP**, complete la siguiente configuración:

| Campo o casilla de verificación | Descripción |
|-------------------------------------|---|
| Interfaz de red | Para cada interfaz de red que configure para el equipo virtual de almacenamiento, seleccione una subred existente (si existe al menos una) o especifique sin subred y complete los campos Dirección IP y Máscara de subred . Si resulta útil, active la casilla de verificación usar la misma máscara de subred y puerta de enlace para todas las siguientes interfaces . Puede permitir que el sistema seleccione automáticamente el puerto de inicio o seleccionar manualmente el que desea utilizar en la lista. |
| Administrar cuenta de administrador | Seleccione esta casilla de comprobación si desea gestionar la cuenta de administrador de máquina virtual de almacenamiento. Cuando se selecciona, especifique el nombre de usuario, la contraseña, confirme la contraseña e indique si desea añadir una interfaz de red para la gestión de máquinas virtuales de almacenamiento. |

1. Guarde los cambios.

CLI

Use la interfaz de línea de comandos de ONTAP para crear una subred.

Pasos

1. Determine qué agregados son candidatos para contener el volumen raíz de la SVM.

```
storage aggregate show -has-mroot false
```

Debe elegir un agregado que tenga al menos 1 GB de espacio libre para contener el volumen raíz. Si piensa configurar la auditoría NAS en el SVM, debe tener como mínimo 3 GB de espacio libre

adicional en el agregado raíz, y el espacio adicional se utilizará para crear el volumen de almacenamiento provisional de auditoría cuando la auditoría esté habilitada.



Si la auditoría de NAS ya está habilitada en una SVM existente, el volumen provisional del agregado se crea inmediatamente después de que la creación de un agregado se haya completado correctamente.

2. Registre el nombre del agregado en el que desea crear el volumen raíz de la SVM.
3. Si piensa especificar un idioma cuando crea la SVM y no conoce el valor que desea usar, identifique y registre el valor del idioma que desea especificar:

```
vserver create -language ?
```

4. Si piensa especificar una política de Snapshot al crear la SVM y no conoce el nombre de la política, enumere las políticas disponibles, identifique y registre el nombre de la política de Snapshot que desea usar:

```
volume snapshot policy show -vserver vserver_name
```

5. Si piensa especificar una política de cuota cuando crea la SVM y no conoce el nombre de la política, enumere las políticas disponibles, identifique y registre el nombre de la política de cuota que desea utilizar:

```
volume quota policy show -vserver vserver_name
```

6. Cree una SVM:

```
vserver create -vserver vserver_name -aggregate aggregate_name -rootvolume  
root_volume_name -rootvolume-security-style {unix|ntfs|mixed} [-ipspace  
IPspace_name] [-language <language>] [-snapshot-policy  
snapshot_policy_name] [-quota-policy quota_policy_name] [-comment comment]
```

```
vserver create -vserver vs1 -aggregate aggr3 -rootvolume vs1_root  
-rootvolume-security-style ntfs -ipspace ipspace1 -language  
en_US.UTF-8
```

```
[Job 72] Job succeeded: Vserver creation completed
```

7. Compruebe que la configuración de SVM sea correcta.

```
vserver show -vserver vs1
```

```
Vserver: vs1
Vserver Type: data
Vserver Subtype: default
Vserver UUID: 11111111-1111-1111-1111-111111111111
Root Volume: vs1_root
Aggregate: aggr3
NIS Domain: -
Root Volume Security Style: ntfs
LDAP Client: -
Default Volume Language Code: en_US.UTF-8
Snapshot Policy: default
Comment:
Quota Policy: default
List of Aggregates Assigned: -
Limit on Maximum Number of Volumes allowed: unlimited
Vserver Admin State: running
Vserver Operational State: running
Vserver Operational State Stopped Reason: -
Allowed Protocols: nfs, cifs, ndmp
Disallowed Protocols: fcp, iscsi
QoS Policy Group: -
Config Lock: false
IPspace Name: ipspace1
Is Vserver Protected: false
```

En este ejemplo, el comando crea la SVM llamada "vs1" en el espacio IP "ipspace1". El volumen raíz se denomina "vs1_root" y se crea en aggr3 con estilo de seguridad NTFS.



A partir de ONTAP 9.13.1, puede establecer una plantilla de grupo de políticas de calidad de servicio adaptativa, aplicando un límite máximo y mínimo de rendimiento a los volúmenes en la SVM. Solo puede aplicar esta política después de crear la SVM. Para obtener más información sobre este proceso, consulte [Defina una plantilla de grupo de políticas adaptativas](#).

Interfaces lógicas (LIF)

Descripción general de LIF

Descripción general de la configuración de LIF

Una LIF (interfaz lógica) representa un punto de acceso de red a un nodo del clúster. Puede configurar las LIF en los puertos a través de los que el clúster envía y recibe comunicaciones a través de la red.

Un administrador de clúster puede crear, ver, modificar, migrar, revertir, O elimine las LIF. Un administrador de SVM solo puede ver las LIF asociadas con la SVM.

Una LIF es una dirección IP o un WWPN con características asociadas, como una política de servicio, un puerto raíz, un nodo raíz, una lista de puertos a los que se debe conmutar y una política de firewall. Puede configurar las LIF en los puertos a través de los que el clúster envía y recibe comunicaciones a través de la red.



A partir de ONTAP 9.10.1, las políticas de firewall están obsoletas y sustituidas por completo por políticas de servicios LIF. Para obtener más información, consulte ["Configurar políticas de firewall para LIF"](#).

Los LIF pueden alojarse en los siguientes puertos:

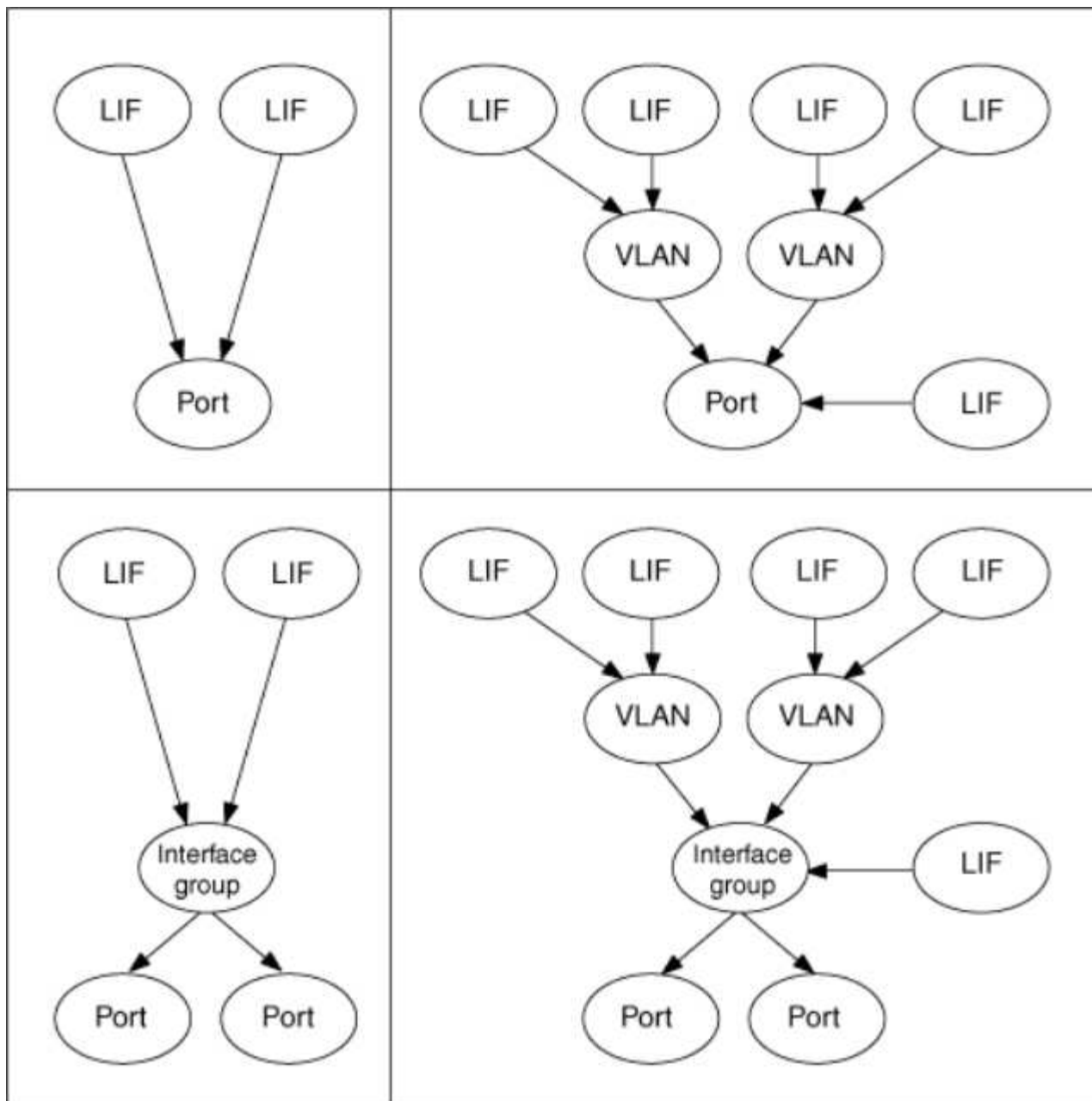
- Puertos físicos que no forman parte de los grupos de interfaces
- Grupos de interfaces
- VLAN
- Puertos físicos o grupos de interfaces que alojan VLAN
- Puertos IP virtual (VIP)

A partir de ONTAP 9.5, los LIF VIP son compatibles y están alojados en los puertos VIP.

Mientras configura los protocolos SAN como FC en una LIF, estará asociado con un WWPN.

["Administración de SAN"](#)

En la siguiente figura se muestra la jerarquía de puertos en un sistema ONTAP:



Recuperación tras fallos y restauración de LIF

Una recuperación tras fallos de LIF se produce cuando un LIF se mueve de su nodo o puerto principal a su nodo o puerto asociados de alta disponibilidad. ONTAP puede activar de forma automática una recuperación tras fallos de LIF o manualmente un administrador de clústeres para determinados eventos, como un enlace de Ethernet físico inactivo o un nodo que borra el quórum de la base de datos replicada (RDB). Cuando se produce una recuperación tras fallos en LIF, ONTAP sigue funcionando con normalidad en el nodo asociado hasta que se resuelva el motivo de la conmutación al nodo de respaldo. Cuando el nodo principal o el puerto recuperan el estado, el LIF se revierte del partner de alta disponibilidad de nuevo a su puerto o nodo principal. Esta reversión se denomina retorno al nodo primario.

Para la conmutación por error y la devolución de LIF, los puertos de cada nodo deben pertenecer al mismo dominio de retransmisión. Para comprobar que los puertos relevantes de cada nodo pertenecen al mismo dominio de retransmisión, consulte lo siguiente:

- ONTAP 9,8 y versiones posteriores: ["Reparar la accesibilidad del puerto"](#)

- ONTAP 9.7 y anteriores: ["Añada o quite puertos de un dominio de retransmisión"](#)

En el caso de los LIF con recuperación tras fallos de LIF habilitada (automática o manual), se aplica lo siguiente:

- En el caso de los LIF con una política de servicio de datos, puede comprobar las restricciones de la política de conmutación al respaldo:
 - ONTAP 9,6 y versiones posteriores: ["LIF y políticas de servicio en ONTAP 9.6 y posteriores"](#)
 - ONTAP 9,5 y anteriores: ["Roles de LIF en ONTAP 9.5 y versiones anteriores"](#)
- La reversión automática de LIF se produce cuando la reversión automática se establece en `true` Y cuando el puerto de inicio de la LIF está en buen estado y puede alojar la LIF.
- En una toma de control de nodo, planificada o sin planificar, la LIF del nodo que se toma el control y conmuta al partner de alta disponibilidad. El puerto en el que se produce un fallo en el LIF viene determinado por VIF Manager.
- Una vez finalizada la conmutación al respaldo, el LIF funciona normalmente.
- Cuando se inicia una devolución, el LIF se revierte a su nodo principal y a su puerto, si la reversión automática está establecida en `true`.
- Cuando un enlace ethernet deja de funcionar en un puerto que aloja uno o varios LIF, el VIF Manager migra las LIF del puerto inactivo a un puerto distinto del mismo dominio de retransmisión. El nuevo puerto podría estar en el mismo nodo o en su compañero de alta disponibilidad. Después de restaurar el enlace y si la reversión automática se establece en `true`, El Gestor de VIF devuelve las LIF a su nodo de inicio y puerto de inicio.
- Cuando un nodo interrumpe el quórum de base de datos replicada (RDB), el gestor VIF migra las LIF del nodo de quórum a su compañero de alta disponibilidad. Cuando el nodo vuelve al quórum y, si la reversión automática está establecida en `true`, El Gestor de VIF devuelve las LIF a su nodo de inicio y puerto de inicio.

Compatibilidad de LIF con tipos de puertos

Los LIF pueden tener características diferentes para admitir diferentes tipos de puertos.



Cuando se configuran las LIF de interconexión de clústeres y gestión en la misma subred, es posible que el tráfico de gestión esté bloqueado por un firewall externo y que se produzca un error en las conexiones de AutoSupport y NTP. Puede recuperar el sistema ejecutando el `network interface modify -vserver vservice name -lif intercluster LIF -status-admin up|down` Comando para cambiar la LIF de interconexión de clústeres. Sin embargo, debe configurar la LIF entre clústeres y la LIF de gestión en subredes diferentes para evitar este problema.

| LUN | Descripción |
|-----|-------------|
|-----|-------------|

| | |
|-----------------------------|---|
| LIF de datos | <p>Una LIF asociada con una máquina virtual de almacenamiento (SVM) y se utiliza para comunicarse con los clientes.</p> <p>Puede tener varios LIF de datos en un puerto. Estas interfaces pueden migrar o realizar una conmutación al nodo de respaldo en todo el clúster. Puede modificar una LIF de datos para que sirva como LIF de gestión de SVM modificando su política de firewall en la gestión.</p> <p>Las sesiones establecidas en servidores NIS, LDAP, Active Directory, WINS y DNS utilizan LIF de datos.</p> |
| LIF de clúster | <p>Una LIF que se utiliza para transportar tráfico dentro del clúster entre nodos de un clúster. Las LIF del clúster siempre se deben crear en los puertos del clúster.</p> <p>Los LIF de clúster pueden conmutar por error entre los puertos de clúster del mismo nodo, pero no se pueden migrar ni realizar una conmutación por error a un nodo remoto. Cuando un nuevo nodo se une a un clúster, las direcciones IP se generan automáticamente. Sin embargo, si desea asignar direcciones IP manualmente a las LIF del clúster, debe asegurarse de que las nuevas direcciones IP se encuentren en el mismo rango de subred que las LIF del clúster existentes.</p> |
| LIF de gestión de clústeres | <p>LIF que proporciona una interfaz de gestión única para todo el clúster.</p> <p>Un LIF de gestión de clústeres puede conmutar al respaldo a cualquier nodo del clúster. No puede conmutar al respaldo en los puertos de clústeres o de interconexión de clústeres</p> |
| LIF entre clústeres | <p>Un LIF que se utiliza para comunicación entre clústeres, backup y replicación. Antes de que se pueda establecer una relación de paridad de clústeres, debe crear una LIF de interconexión de clústeres en cada nodo del clúster.</p> <p>Estos LIF solo pueden conmutar por error a los puertos del mismo nodo. No se pueden migrar ni realizar una conmutación por error a otro nodo del clúster.</p> |
| LIF de gestión de nodos | <p>Una LIF que proporciona una dirección IP dedicada para gestionar un nodo en particular en un clúster. Las LIF de gestión de nodos se crean en el momento de crear o unirse al clúster. Estas LIF se utilizan para el mantenimiento del sistema, por ejemplo, cuando un nodo se vuelve inaccesible desde el clúster.</p> |
| LIF VIP | <p>Una LIF VIP es cualquier LIF de datos creada en un puerto VIP. Para obtener más información, consulte "Configurar las LIF de IP virtual (VIP)".</p> |

LIF y políticas de servicio (ONTAP 9,6 y posteriores)

Puede asignar políticas de servicio (en lugar de roles de LIF o políticas de firewall) a las LIF que determinan el tipo de tráfico que se admiten para las LIF. Las políticas de servicio definen una colección de servicios de red compatibles con una LIF. ONTAP proporciona un conjunto de políticas de servicio integradas que se pueden asociar con una LIF.

Puede mostrar las políticas de servicio y sus detalles mediante el siguiente comando:

```
network interface service-policy show
```

Las funciones que no están vinculadas a un servicio específico utilizarán un comportamiento definido por el sistema para seleccionar LIF para conexiones salientes.

Políticas de servicio para SVM del sistema

La SVM de administrador y cualquier SVM del sistema contienen políticas de servicio que se pueden usar para las LIF de esa SVM, incluidas las LIF de gestión y interconexión de clústeres. Estas políticas se crean automáticamente en el sistema cuando se crea un espacio IP.

En la tabla siguiente se enumeran las políticas incorporadas para las LIF en las SVM del sistema a partir de ONTAP 9.12.1. Para otras versiones, muestre las políticas de servicio y sus detalles usando el siguiente comando:

```
network interface service-policy show
```

| Política | Servicios incluidos | Función equivalente | Descripción |
|---|---|---|--|
| interconexión de clústeres predeterminada | interconexión de clústeres núcleo, gestión https | interconexión de clústeres | Lo usan las LIF que transportan el tráfico de interconexión de clústeres. Nota: ONTAP 9.5 dispone de interconexión de clústeres-core con el nombre net-interconexión de clústeres. |
| ruta predeterminada-anuncio | gestión: bgp | - | Utilizado por LIF que llevan conexiones de pares BGP Nota: Disponible en ONTAP 9,5 con el nombre net-route-announce service policy. |
| gestión predeterminada | núcleo de gestión, https de gestión, http de gestión, management-ssh, management-autosupport, management-ems, management-dns-client, management-ad-client, management-ldap-client, management-nis-client, management-ntp-client, management-log-reenvio | gestión de nodos o gestión de clústeres | Utilice esta política de gestión de ámbito del sistema para crear LIF de gestión de ámbito de nodos y clústeres propiedad de una SVM del sistema. Estas LIF se pueden utilizar para conexiones salientes a servidores DNS, AD, LDAP o NIS, así como algunas conexiones adicionales para admitir aplicaciones que se ejecuten en nombre de todo el sistema. A partir de ONTAP 9.12.1, puede utilizar el management-log-forwarding Servicio para controlar qué LIF se utilizan para reenviar registros de auditoría a un servidor de syslog remoto. |

La tabla siguiente enumera los servicios que las LIF pueden utilizar en una SVM del sistema a partir de ONTAP 9.11.1:

| Servicio | Limitaciones de conmutación por error | Descripción |
|--------------------------------------|---------------------------------------|---|
| interconexión de clústeres principal | solo nodo principal | Servicios principales de interconexión de clústeres |
| núcleo de gestión | - | Servicios centrales de gestión |
| gestión-ssh | - | Servicios para acceso de gestión SSH |
| gestión-http | - | Servicios para el acceso de gestión HTTP |
| gestión de https | - | Servicios para el acceso de gestión HTTPS |
| management-autosupport | - | Servicios relacionados con el envío de cargas útiles AutoSupport |
| gestión: bgp | solo puerto de inicio | Servicios relacionados con las interacciones entre colegas de BGP |
| backup-ndmp-control | - | Servicios para controles de backup NDMP |
| management-ems | - | Servicios de acceso a mensajería de gestión |
| management-ntp-client | - | Se introdujo en ONTAP 9.10.1. De servicios para el acceso de clientes NTP. |
| management-ntp-server | - | Introducido en ONTAP 9.11.1. Servicios para el acceso de gestión de servidores NTP |
| gestión-portmap | - | Servicios para la gestión de portmap |
| management-rsh-server | - | Servicios para la administración de servidores rsh |
| servidor-snmp-de-gestión | - | Servicios para la gestión de servidores SNMP |
| management-telnet-server | - | Servicios para la gestión de servidores telnet |
| gestión-registro-reenvío | - | Introducido en ONTAP 9.12.1. Servicios para el reenvío de registros de auditoría |

Políticas de servicio para SVM de datos

Todos los SVM de datos contienen políticas de servicio que pueden usar los LIF en esa SVM.

La tabla siguiente enumera las políticas incorporadas para las LIF en SVM de datos a partir de ONTAP 9.11.1. Para otras versiones, muestre las políticas de servicio y sus detalles usando el siguiente comando:

```
network interface service-policy show
```

| Política | Servicios incluidos | Protocolo de datos equivalente | Descripción |
|-----------------------------------|--|--------------------------------|--|
| gestión predeterminada | gestión-https, management-http, management-ssh, management-dns-client, management-ad-client, management-ldap-client, management-nis-client | ninguno | Utilice esta política de gestión de ámbito de la SVM para crear LIF de gestión de SVM propiedad de una SVM de datos. Estos LIF se pueden usar para proporcionar acceso SSH o HTTPS a los administradores de SVM. Cuando sea necesario, estas LIF se pueden utilizar para conexiones salientes con servidores DNS, AD, LDAP o NIS externos. |
| bloques de datos predeterminados | núcleo de datos, iscsi de datos | iscsi | Lo utilizan las LIF para transportar tráfico de datos SAN orientado a bloques. A partir de ONTAP 9.10.1, queda obsoleta la política de "bloques de datos predeterminados". En su lugar, utilice la política de servicio "Default-data-iscsi". |
| archivos de datos predeterminados | cliente-fpolicy de datos, servidor dns de datos, flexcache de datos, cifs de datos, nfs de datos, management-dns-client, management-ad-client, management-ldap-client, management-nis-client | nfs, cifs, fcache | Utilice la política predeterminada para archivos de datos para crear LIF NAS que admitan protocolos de datos basados en archivos. A veces solo hay una LIF en la SVM, por lo tanto esta política permite utilizar la LIF para conexiones salientes con un servidor DNS, AD, LDAP o NIS externo. Puede quitar estos servicios a de esta política si prefiere que estas conexiones solo utilicen LIF de gestión. |
| datos-iscsi predeterminados | núcleo de datos, iscsi de datos | iscsi | Lo utilizan los LIF que transportan tráfico de datos iSCSI. |
| default-data-nvme-tcp | núcleo de datos, nvme-tcp de datos | nvme-tcp | Lo usan las LIF que transportan el tráfico de datos NVMe/TCP. |

En la siguiente tabla, se enumeran los servicios que se pueden usar en una SVM de datos junto con las restricciones que cada servicio impone a la política de conmutación por error de un LIF a fecha de ONTAP 9.11.1:

| Servicio | Restricciones de conmutación por error | Descripción |
|-------------|--|--------------------------------------|
| gestión-ssh | - | Servicios para acceso de gestión SSH |

| | | |
|--------------------------|-----------------------|---|
| gestión-http | - | Introducido en ONTAP 9.10.1 Servicios para el acceso de gestión HTTP |
| gestión de https | - | Servicios para el acceso de gestión HTTPS |
| gestión-portmap | - | Servicios para el acceso de gestión de portmap |
| servidor-snmp-de-gestión | - | Introducido en ONTAP 9.10.1 Servicios para el acceso de gestión de servidores SNMP |
| núcleo de datos | - | Servicios de datos centrales |
| nfs de datos | - | Servicio de datos NFS |
| cifs de datos | - | Servicio de datos CIFS |
| flexcache para datos | - | Servicio de datos FlexCache |
| data iscsi | solo puerto de inicio | Servicio de datos iSCSI |
| backup-ndmp-control | - | Introducido en ONTAP 9.10.1 Backup NDMP controla el servicio de datos |
| servidor dns de datos | - | Introducido en ONTAP 9.10.1 Servicio de datos del servidor DNS |
| cliente-fpolicy-data | - | Servicio de datos de políticas de selección de archivos |
| data-nvme-tcp | solo puerto de inicio | Introducido en ONTAP 9.10.1 Servicio de datos TCP de NVMe |
| servidor de datos s3 | - | Servicio de datos del servidor simple Storage Service (S3) |

Debe tener en cuenta cómo se asignan las políticas de servicio a las LIF en las SVM de datos:

- Si se crea una SVM de datos con una lista de servicios de datos, las políticas de servicio "default-data-files" y "default-data-Blocks" incorporadas en esa SVM se crean con los servicios especificados.
- Si se crea una SVM de datos sin especificar una lista de servicios de datos, las políticas de servicio "default-data-files" y "default-data-Blocks" incorporadas en esa SVM se crean utilizando una lista predeterminada de servicios de datos.

La lista de servicios de datos predeterminada incluye los servicios iSCSI, NFS, NVMe, SMB y FlexCache.

- Cuando se crea una LIF con una lista de protocolos de datos, se asigna a la LIF una política de servicio

equivalente a los protocolos de datos especificados.

- Si no existe una política de servicio equivalente, se crea una política de servicio personalizada.
- Cuando se crea una LIF sin una política de servicio o lista de protocolos de datos, la política de servicio de archivos de datos predeterminados se asigna a la LIF de forma predeterminada.

Servicio básico de datos

El servicio de núcleo de datos permite a los componentes que previamente usaban los LIF con el rol de datos para trabajar como se esperaba en los clústeres que se habían actualizado para gestionar LIF mediante políticas de servicio en lugar de roles de LIF (que quedaron obsoletos en ONTAP 9.6).

La especificación del núcleo de datos como servicio no abre ningún puerto en el firewall, pero el servicio debe incluirse en cualquier política de servicio de una SVM de datos. Por ejemplo, la política de servicio archivos de datos predeterminados contiene los siguientes servicios de forma predeterminada:

- núcleo de datos
- nfs de datos
- cifs de datos
- flexcache para datos

El servicio de núcleo de datos se debería incluir en la política para garantizar que todas las aplicaciones que utilizan el LIF funcionan como se espera, pero los otros tres servicios se pueden eliminar, si se desea.

Servicio LIF en el cliente

A partir de ONTAP 9.10.1, ONTAP proporciona servicios LIF en el cliente para varias aplicaciones. Estos servicios proporcionan control sobre qué LIF se utilizan para conexiones salientes en nombre de cada aplicación.

Los siguientes servicios nuevos dan a los administradores control sobre los LIF que se usan como direcciones de origen para ciertas aplicaciones.

| Servicio | Restricciones de SVM | Descripción |
|---------------------------|----------------------|---|
| cliente ad-administración | - | A partir de ONTAP 9.11.1, ONTAP proporciona servicio de cliente de Active Directory para conexiones salientes con un servidor AD externo. |
| management-dns-client | - | A partir de ONTAP 9.11.1, ONTAP proporciona servicio de cliente DNS para conexiones salientes a un servidor DNS externo. |
| management-ldap-client | - | A partir de ONTAP 9.11.1, ONTAP proporciona servicio de cliente LDAP para conexiones salientes a un servidor LDAP externo. |
| management-nis-client | - | A partir de ONTAP 9.11.1, ONTAP proporciona servicio de cliente NIS para conexiones salientes a un servidor NIS externo. |

| | | |
|-----------------------|---------------|--|
| management-ntp-client | solo sistemas | A partir de ONTAP 9.10.1, ONTAP proporciona servicio de cliente NTP para conexiones salientes con un servidor NTP externo. |
| cliente-fpolicy-data | solo datos | A partir de ONTAP 9.8, ONTAP proporciona un servicio de cliente para conexiones de FPolicy de salida. |

Cada uno de los nuevos servicios se incluye automáticamente en algunas de las políticas de servicio integradas, pero los administradores pueden eliminarlos de las directivas integradas o agregarlos a políticas personalizadas para controlar qué LIF se utilizan para las conexiones salientes en nombre de cada aplicación.

Roles de LIF (ONTAP 9,5 y anteriores)

Los LIF con diferentes roles tienen características diferentes. Una función de LIF determina el tipo de tráfico que se admite a través de la interfaz, junto con las reglas de conmutación por error aplicables, las restricciones de firewall aplicadas, la seguridad, el equilibrio de carga y el comportamiento de enrutamiento de cada LIF. Una LIF puede tener cualquiera de los siguientes roles: Clúster, gestión de clústeres, datos, interconexión de clústeres, gestión de nodos, y undef (sin definir). El rol Undef se utiliza para los LIF BGP.

A partir de ONTAP 9.6, los roles de LIF quedan obsoletos. Debería especificar políticas de servicio para las LIF en lugar de un rol. No es necesario especificar un rol de LIF al crear una LIF con una política de servicio.

Seguridad de LIF

| | LIF de datos | LIF de clúster | LIF de gestión de nodos | LIF de gestión de clústeres | LIF entre clústeres |
|-------------------------------------|-----------------|-----------------------|-------------------------|-----------------------------|---------------------|
| ¿Necesita una subred IP privada? | No | Sí | No | No | No |
| ¿Necesita una red segura? | No | Sí | No | No | Sí |
| Política de firewall predeterminada | Muy restrictivo | Completamente abierto | Mediano | Mediano | Muy restrictivo |
| ¿Se puede personalizar el firewall? | Sí | No | Sí | Sí | Sí |

Recuperación tras fallos de LIF

| | LIF de datos | LIF de clúster | LIF de gestión de nodos | LIF de gestión de clústeres | LIF entre clústeres |
|--|--------------|----------------|-------------------------|-----------------------------|---------------------|
|--|--------------|----------------|-------------------------|-----------------------------|---------------------|

| | | | | | |
|-------------------------------|---|--|--|--|--|
| Comportamiento predeterminado | Solo esos puertos del mismo grupo de recuperación tras fallos que se encuentran en el nodo principal de la LIF y en un nodo partner distinto de SFO | Solo aquellos puertos del mismo grupo de conmutación al nodo de respaldo que se encuentran en el nodo raíz de la LIF | Solo aquellos puertos del mismo grupo de conmutación al nodo de respaldo que se encuentran en el nodo raíz de la LIF | Cualquier puerto del mismo grupo de recuperación tras fallos | Solo aquellos puertos del mismo grupo de conmutación al nodo de respaldo que se encuentran en el nodo raíz de la LIF |
| ¿Se puede personalizar? | Sí | No | Sí | Sí | Sí |

Enrutamiento de LIF

| | LIF de datos | LIF de clúster | LIF de gestión de nodos | LIF de gestión de clústeres | LIF entre clústeres |
|---|--|----------------|---|---|---|
| ¿Cuándo es necesaria una ruta predeterminada? | Cuando los clientes o el controlador de dominio están en una subred IP diferente | Nunca | Cuando cualquiera de los tipos de tráfico principales requiere acceso a una subred IP diferente | Cuando el administrador se conecta desde otra subred IP | Cuando otras LIF de interconexión de clústeres se encuentran en una subred IP diferente |
| ¿Cuándo se necesita una ruta estática a una subred IP específica? | Raras | Nunca | Raras | Raras | Cuando los nodos de otro clúster tienen sus LIF de interconexión de clústeres en subredes IP diferentes |
| ¿Cuándo se necesita una ruta de host estática a un servidor específico? | Para tener uno de los tipos de tráfico enumerados en LIF de gestión de nodos, vaya a través de una LIF de datos y no a una LIF de gestión de nodos. Esto requiere un cambio de firewall correspondiente. | Nunca | Raras | Raras | Raras |

Reequilibrado de LIF

| | LIF de datos | LIF de clúster | LIF de gestión de nodos | LIF de gestión de clústeres | LIF entre clústeres |
|-------------------------------|--------------|----------------|-------------------------|-----------------------------|---------------------|
| DNS: ¿Usar como servidor DNS? | Sí | No | No | No | No |
| DNS: ¿Exportar como zona? | Sí | No | No | No | No |

Tipos de tráfico principales de LIF

| | LIF de datos | LIF de clúster | LIF de gestión de nodos | LIF de gestión de clústeres | LIF entre clústeres |
|------------------------------|---|--------------------|---|------------------------------|-----------------------------|
| Tipos de tráfico principales | Servidor NFS, servidor CIFS, cliente NIS, Active Directory, LDAP, WINS, cliente DNS y servidor, iSCSI y servidor FC | Dentro del clúster | Servidor SSH, servidor HTTPS, cliente NTP, SNMP, cliente AutoSupport, Cliente DNS, cargando actualizaciones de software | Servidor SSH, servidor HTTPS | Replicación entre clústeres |

Administre las LIF

Configure las políticas de servicio de LIF

Puede configurar políticas de servicio de LIF para identificar un único servicio o una lista de servicios que utilizarán una LIF.

Crear una política de servicio para LIF

Puede crear una política de servicio para las LIF. Puede asignar una política de servicio a uno o más LIF y, por lo tanto, permitir que la LIF lleve tráfico para un único servicio o una lista de servicios.

Se necesitan privilegios avanzados para ejecutar el `network interface service-policy create` comando.

Acerca de esta tarea

Hay disponibles políticas de servicio y servicios incorporados para gestionar el tráfico de datos y gestión de las SVM de los datos y del sistema. La mayoría de los casos de uso se resuelven con una política de servicio integrada, en lugar de crear una política de servicio personalizada.

Puede modificar estas políticas de servicio integradas, si es necesario.

Pasos

1. Vea los servicios que están disponibles en el clúster:

```
network interface service show
```

Los servicios representan las aplicaciones a las que accede una LIF, así como las aplicaciones que presta servicio el clúster. Cada servicio incluye cero o más puertos TCP y UDP en los que la aplicación está escuchando.

Están disponibles los siguientes servicios adicionales de datos y gestión:

```
cluster1::> network interface service show
```

| Service | Protocol:Ports |
|----------------------------|-----------------|
| ----- | ----- |
| cluster-core | - |
| data-cifs | - |
| data-core | - |
| data-flexcache | - |
| data-iscsi | - |
| data-nfs | - |
| intercluster-core | tcp:11104-11105 |
| management-autosupport | - |
| management-bgp | tcp:179 |
| management-core | - |
| management-https | tcp:443 |
| management-ssh | tcp:22 |
| 12 entries were displayed. | |

2. Vea las políticas de servicio que hay en el clúster:


```
cluster1::> network interface service-policy show
```

| Vserver | Policy | Service: Allowed Addresses |
|----------|------------------------|---|
| ----- | | |
| ----- | | |
| cluster1 | | |
| | default-intercluster | intercluster-core: 0.0.0.0/0 management-https: 0.0.0.0/0 |
| | default-management | management-core: 0.0.0.0/0 management-autosupport: 0.0.0.0/0 management-ssh: 0.0.0.0/0 management-https: 0.0.0.0/0 |
| | default-route-announce | management-bgp: 0.0.0.0/0 |
| Cluster | | |
| | default-cluster | cluster-core: 0.0.0.0/0 |
| vs0 | | |
| | default-data-blocks | data-core: 0.0.0.0/0 data-iscsi: 0.0.0.0/0 |
| | default-data-files | data-core: 0.0.0.0/0 data-nfs: 0.0.0.0/0 data-cifs: 0.0.0.0/0 data-flexcache: 0.0.0.0/0 |
| | default-management | data-core: 0.0.0.0/0 management-ssh: 0.0.0.0/0 management-https: 0.0.0.0/0 |

```
7 entries were displayed.
```

3. Cree una política de servicio:

```
cluster1::> set -privilege advanced
```

```
Warning: These advanced commands are potentially dangerous; use them  
only when directed to do so by technical support.
```

```
Do you wish to continue? (y or n): y
```

```
cluster1::> network interface service-policy create -vserver <svm_name>  
-policy <service_policy_name> -services <service_name> -allowed  
-addresses <IP_address/mask,...>
```

- "service_name" especifica una lista de servicios que deben incluirse en la política.
- "IP_address/mask" especifica la lista de máscaras de subred para las direcciones que pueden tener acceso a los servicios en la directiva de servicio. De forma predeterminada, todos los servicios especificados se agregan con una lista de direcciones permitida predeterminada de 0.0.0.0/0, que permite el tráfico de todas las subredes. Cuando se proporciona una lista de direcciones permitidas de forma no predeterminada, las LIF que usan la directiva se configuran para bloquear todas las solicitudes con una dirección de origen que no coincide con ninguna de las máscaras especificadas.

El siguiente ejemplo muestra cómo crear una política de servicio de datos, *svm1_data_policy*, para una SVM que incluye los servicios *NFS* y *SMB*:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver svm1
-policy svm1_data_policy -services data-nfs,data-cifs,data-core
```

El ejemplo siguiente muestra cómo crear una política de servicio de interconexión de clústeres:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver cluster1
-policy intercluster1 -services intercluster-core
```

4. Comprobar que se ha creado la política de servicio.

```
cluster1::> network interface service-policy show
```

El siguiente resultado muestra las políticas de servicio disponibles:

```
cluster1::> network interface service-policy show
```

| Vserver | Policy | Service: Allowed Addresses |
|----------|------------------------|---|
| ----- | | |
| ----- | | |
| cluster1 | | |
| | default-intercluster | intercluster-core: 0.0.0.0/0 management-https: 0.0.0.0/0 |
| | intercluster1 | intercluster-core: 0.0.0.0/0 |
| | default-management | management-core: 0.0.0.0/0 management-autosupport: 0.0.0.0/0 management-ssh: 0.0.0.0/0 management-https: 0.0.0.0/0 |
| | default-route-announce | management-bgp: 0.0.0.0/0 |
| Cluster | | |
| | default-cluster | cluster-core: 0.0.0.0/0 |
| vs0 | | |
| | default-data-blocks | data-core: 0.0.0.0/0 data-iscsi: 0.0.0.0/0 |
| | default-data-files | data-core: 0.0.0.0/0 data-nfs: 0.0.0.0/0 data-cifs: 0.0.0.0/0 data-flexcache: 0.0.0.0/0 |
| | default-management | data-core: 0.0.0.0/0 management-ssh: 0.0.0.0/0 management-https: 0.0.0.0/0 |
| | svm1_data_policy | data-core: 0.0.0.0/0 data-nfs: 0.0.0.0/0 data-cifs: 0.0.0.0/0 |

```
9 entries were displayed.
```

Después de terminar

Asigne la política de servicio a una LIF en el momento de la creación o al modificar una LIF existente.

Asigne una política de servicio a una LIF

Puede asignar una política de servicio a una LIF en el momento de crear la LIF o al modificarla. Una política de servicio define la lista de servicios que se pueden utilizar con la LIF.

Acerca de esta tarea

Puede asignar políticas de servicio para las LIF en las SVM de administrador y de datos.

Paso

Según cuándo desee asignar la política de servicio a una LIF, realice una de las siguientes acciones:

| Si está... | Asignar la política de servicio... |
|-------------------|--|
| Crear una LIF | Interfaz de red <code>create -vserver svm_name -lif <lif_name> -home-node <node_name> -home-Port <port_name> {{(-address <IP_address> -netmask <IP_address>) -subnet-name <subnet_name>}} -service-policy <service_policy_name></code> |
| Modificar una LIF | modificación de la interfaz de red <code>-vserver <svm_name> -lif <lif_name> -service-policy <service_policy_name></code> |

Al especificar una política de servicio para una LIF, no es necesario especificar el protocolo de datos y el rol para la LIF. También se admite la creación de LIF especificando el rol y protocolos de datos.



Una política de servicio solo puede ser utilizada por las LIF en la misma SVM que especificó al crear la política de servicio.

Ejemplos

En el ejemplo siguiente se muestra cómo modificar la política de servicio de una LIF para utilizar la política de servicio de gestión predeterminada:

```
cluster1::> network interface modify -vserver cluster1 -lif lif1 -service-policy default-management
```

Comandos para gestionar las políticas de servicio de LIF

Utilice la `network interface service-policy` Comandos para gestionar las políticas de servicio de LIF.

Antes de empezar

Modificar la política de servicio de una LIF en una relación de SnapMirror activa interrumpe la programación de replicación. Si convierte una LIF de interconexión de clústeres a que no se interconexión entre clústeres (o viceversa), esos cambios no se replican en el clúster con conexión entre iguales. Para actualizar el clúster del mismo nivel después de modificar la política de servicio LIF, ejecute primero el `snapmirror abort` operación entonces [resincronice la relación de replicación](#).

| Si desea... | Se usa este comando... |
|---|--|
| Crear una política de servicio (se requieren privilegios avanzados) | <code>network interface service-policy create</code> |

| Si desea... | Se usa este comando... |
|---|--|
| Agregar una entrada de servicio adicional a una política de servicio existente (se requieren privilegios avanzados) | <code>network interface service-policy add-service</code> |
| Clonar una política de servicio existente (se requieren privilegios avanzados) | <code>network interface service-policy clone</code> |
| Modificar una entrada de servicio en una política de servicio existente (se requieren privilegios avanzados) | <code>network interface service-policy modify-service</code> |
| Quitar una entrada de servicio de una política de servicio existente (se requieren privilegios avanzados) | <code>network interface service-policy remove-service</code> |
| Cambiar el nombre de una política de servicio existente (se requieren privilegios avanzados) | <code>network interface service-policy rename</code> |
| Eliminar una política de servicio existente (se requieren privilegios avanzados) | <code>network interface service-policy delete</code> |
| Restaurar una política de servicio integrada a su estado original (se requieren privilegios avanzados) | <code>network interface service-policy restore-defaults</code> |
| Mostrar las políticas de servicio existentes | <code>network interface service-policy show</code> |

Crear una LIF (interfaz de red)

Una SVM sirve datos a los clientes a través de una o varias interfaces lógicas de red (LIF). Debe crear LIF en los puertos que desee utilizar para acceder a datos. Una LIF (interfaz de red) es una dirección IP asociada a un puerto físico o lógico. Si hay un fallo de un componente, un LIF puede conmutar al respaldo o migrarse a un puerto físico diferente, lo que continúa comunicándose con la red.

Mejor práctica

Los puertos de switch conectados a ONTAP se deben configurar como puertos periféricos de árbol de expansión para reducir los retrasos durante la migración de LIF.

Antes de empezar

- Para realizar esta tarea, debe ser un administrador de clústeres.
- El puerto de red físico o lógico subyacente debe haber sido configurado con el estado administrativo activo.
- Si tiene pensado utilizar un nombre de subred para asignar la dirección IP y el valor de máscara de red para una LIF, la subred ya debe existir.

Las subredes contienen un grupo de direcciones IP que pertenecen a la misma subred de capa 3. Se

crean con System Manager o el `network subnet create` comando.

- El mecanismo para especificar el tipo de tráfico que maneja una LIF ha cambiado. Para ONTAP 9.5 y versiones anteriores, LIF usaba funciones para especificar el tipo de tráfico que gestionaría. A partir de ONTAP 9.6, los LIF utilizan políticas de servicio para especificar el tipo de tráfico que manejaría.

Acerca de esta tarea

- No puede asignar protocolos NAS y SAN a la misma LIF.

Los protocolos admitidos son SMB, NFS, FlexCache, iSCSI y FC. iSCSI y FC no se pueden combinar con otros protocolos. Sin embargo, puede haber protocolos SAN basados en NAS y Ethernet en el mismo puerto físico.

- No debe configurar los LIF que lleven tráfico SMB para revertir automáticamente a sus nodos de inicio. Esta recomendación es obligatoria si el servidor SMB va a alojar una solución para las operaciones no disruptivas con Hyper-V o SQL Server sobre SMB.
- Puede crear tanto LIF IPv4 como IPv6 en el mismo puerto de red.
- Todos los servicios de asignación de nombres y resolución de nombres de host que utiliza una SVM, como DNS, NIS, LDAP y Active Directory, Debe ser accesible desde al menos un LIF que gestiona el tráfico de datos de la SVM.
- Una LIF que gestiona tráfico dentro del clúster entre nodos no debe estar en la misma subred que una LIF que gestiona el tráfico de gestión o una LIF que gestiona el tráfico de datos.
- Crear una LIF que no tiene un destino de conmutación por error válido da lugar a un mensaje de advertencia.
- Si tiene un gran número de LIF en su clúster, puede verificar la capacidad de LIF admitida en el clúster:
 - System Manager: A partir de ONTAP 9.12.0, vea el rendimiento en la cuadrícula de interfaz de red.
 - CLI: Utilice el `network interface capacity show` Comando y la capacidad de LIF admitida en cada nodo mediante el `network interface capacity details show` (en el nivel de privilegio avanzado).
- A partir de ONTAP 9.7, si ya existen otras LIF para la SVM en la misma subred, no es necesario especificar el puerto de inicio de la LIF. ONTAP elige automáticamente un puerto aleatorio en el nodo raíz especificado en el mismo dominio de retransmisión que las otras LIF ya configuradas en la misma subred.

A partir de la versión 9.4 de ONTAP, se admite FC-NVMe. Si crea una LIF FC-NVMe, debe tener en cuenta lo siguiente:

- El protocolo NVMe debe ser compatible con el adaptador de FC en el que se crea la LIF.
- FC-NVMe puede ser el único protocolo de datos en las LIF de datos.
- Debe configurarse un LIF que gestiona el tráfico de gestión para cada máquina virtual de almacenamiento (SVM) compatible con SAN.
- Las LIF y los espacios de nombres de NVMe deben alojarse en el mismo nodo.
- Solo se puede configurar una LIF NVMe que gestiona el tráfico de datos por SVM.
- Cuando se crea una interfaz de red con una subred, ONTAP selecciona automáticamente una dirección IP disponible desde la subred seleccionada y la asigna a la interfaz de red. Puede cambiar la subred si hay más de una subred, pero no puede cambiar la dirección IP.
- Cuando crea (añade) una SVM, para una interfaz de red, no puede especificar una dirección IP que esté en el rango de una subred existente. Recibirá un error de conflicto de subred. Este problema se produce en otros flujos de trabajo de una interfaz de red, como crear o modificar interfaces de red entre clústeres

en configuraciones de SVM o configuración de clústeres.

- A partir de ONTAP 9.10.1, el `network interface` Los comandos de la CLI incluyen un `-rdma -protocols` Parámetro para configuraciones NFS over RDMA. Es compatible con la creación de interfaces de red para NFS sobre configuraciones RDMA en System Manager, que comienza en ONTAP 9.12.1. Para obtener más información, consulte [Configure LIF para NFS sobre RDMA](#).
- A partir de ONTAP 9.11.1, la conmutación automática por error en LIF iSCSI está disponible en las plataformas de cabinas SAN all-flash (ASA).

La conmutación por error de LIF iSCSI se habilita automáticamente (la normativa de conmutación por error se establece en `sfo-partner-only` y el valor de reversión automática se establece en `true`) En los LIF iSCSI recientemente creados si no existen LIF iSCSI en la SVM especificada o si todos los LIF iSCSI existentes en la SVM especificada ya se habilitan con conmutación por error de LIF iSCSI.

Si, tras actualizar a ONTAP 9.11.1 o una versión posterior, tiene LIF iSCSI existentes en una SVM que no se habilitaron con la función de conmutación por error de LIF iSCSI y crea nuevos LIF iSCSI en la misma SVM, los nuevos LIF iSCSI asumen la misma política de conmutación por error (`disabled`) De los LIF iSCSI existentes en la SVM.

"Conmutación por error de LIF de iSCSI para plataformas ASA"

A partir de ONTAP 9.7, ONTAP elige automáticamente el puerto inicial de una LIF, siempre que al menos una LIF ya exista en la misma subred en ese espacio IP. ONTAP elige un puerto principal en el mismo dominio de retransmisión que otras LIF de esa subred. Puede seguir especificando un puerto de inicio, pero ya no será necesario (a menos que aún no haya ninguna LIF en esa subred en el espacio IP especificado).

A partir de ONTAP 9.12.0, el procedimiento que siga depende de la interfaz que utilice—System Manager o la CLI:

System Manager

Utilice System Manager para agregar una interfaz de red

Pasos

1. Seleccione **Red > Descripción general > interfaces de red**.
2. Seleccione **+ Add**.
3. Seleccione uno de los siguientes roles de interfaz:
 - a. SQL Server
 - b. Interconexión de clústeres
 - c. Gestión de SVM
4. Seleccione el protocolo:
 - a. SMB/CIFS Y NFS
 - b. iSCSI
 - c. FC
 - d. NVMe/FC
 - e. NVMe/TCP
5. Asigne un nombre a la LIF o acepte el nombre generado a partir de sus selecciones anteriores.
6. Acepte el nodo de inicio o use el menú desplegable para seleccionar uno.
7. Si al menos una subred está configurada en el espacio IP de la SVM seleccionada, se muestra la lista desplegable de subred.
 - a. Si selecciona una subred, selecciónela en el menú desplegable.
 - b. Si continúa sin una subred, se mostrará el menú desplegable dominio de retransmisión:
 - i. Especifique la dirección IP. Si la dirección IP está en uso, aparecerá un mensaje de advertencia.
 - ii. Especifique una máscara de subred.
8. Seleccione el puerto de inicio en el dominio de difusión, automáticamente (recomendado) o seleccionando uno en el menú desplegable. El control de puerto de inicio se muestra en función del dominio de difusión o de la selección de subred.
9. Guarde la interfaz de red.

CLI

Utilice la CLI para crear un LIF

Pasos

1. Determine los puertos de dominio de retransmisión que desea usar para la LIF.

```
network port broadcast-domain show -ipspace ipspace1
```


| IPspace Name | Broadcast Domain name | MTU | Port List | Update Status | Details |
|--------------|-----------------------|------|--|--|---------|
| ipspace1 | default | 1500 | node1:e0d node1:e0e node2:e0d node2:e0e | complete complete complete complete | |

2. Compruebe que la subred que desea utilizar para las LIF contiene suficientes direcciones IP sin usar.

```
network subnet show -ipspace ipspace1
```

3. Cree uno o varios LIF en los puertos que desee utilizar para acceder a los datos.

```
network interface create -vserver _SVM_name_ -lif _lif_name_
-service-policy _service_policy_name_ -home-node _node_name_ -home
-port port_name {-address _IP_address_ - netmask _Netmask_value_ |
-subnet-name _subnet_name_} -firewall- policy _policy_ -auto-revert
{true|false}
```

- **-home-node** Es el nodo al que devuelve el LIF cuando el `network interface revert` El comando se ejecuta en la LIF.

También puede especificar si el LIF debe volver automáticamente al nodo raíz y al puerto raíz con la opción `-auto-revert`.

- **-home-port** Es el puerto físico o lógico al que devuelve la LIF cuando el `network interface revert` El comando se ejecuta en la LIF.
- Puede especificar una dirección IP con el `-address` y.. `-netmask` o puede activar la asignación desde una subred con el `-subnet_name` opción.
- Al usar una subred para suministrar la dirección IP y la máscara de red, si la subred se definió con una puerta de enlace, se añadirá automáticamente a la SVM una ruta predeterminada a esa puerta de enlace cuando se cree una LIF con dicha subred.
- Si asigna direcciones IP manualmente (sin una subred), es posible que deba configurar una ruta predeterminada para una puerta de enlace si hay clientes o controladores de dominio en una subred IP diferente. La `network route create` La página man contiene información sobre la creación de una ruta estática dentro de una SVM.
- **-auto-revert** Permite especificar si un LIF de datos se revierte automáticamente a su nodo principal en circunstancias como el inicio, los cambios en el estado de la base de datos de gestión o el momento en que se realiza la conexión de red. El valor predeterminado es `false`, pero puede establecerlo en `true` según las políticas de administración de red del entorno.
- **-service-policy** A partir de ONTAP 9.5, puede asignar una política de servicio para la LIF con el `-service-policy` opción.
Cuando se especifica una política de servicio para una LIF, la política se usa para construir un rol predeterminado, una política de conmutación por error y una lista de protocolos de datos para la

LIF. En ONTAP 9.5, las políticas de servicio solo se admiten para los servicios entre iguales de BGP y interconexión de clústeres. En ONTAP 9.6, puede crear políticas de servicio para varios servicios de datos y gestión.

- ° `-data-protocol` Permite crear una LIF compatible con los protocolos FCP o NVMe/FC. Esta opción no es necesaria al crear una LIF de IP.

4. **Opcional:** Asigne una dirección IPv6 en la opción `-address`:

- Utilice el comando `network ndp prefix show` para ver la lista de prefijos RA aprendidos en varias interfaces.

La `network ndp prefix show` el comando está disponible en el nivel de privilegio avanzado.

- Utilice el formato `prefix::id` Para construir la dirección IPv6 manualmente.

`prefix` es el prefijo aprendido en varias interfaces.

Para obtener la `id`, elija un número hexadecimal aleatorio de 64 bits.

5. Compruebe que la configuración de la interfaz LIF es correcta.

```
network interface show -vserver vs1
```

| | Logical | Status | Network | Current | Current Is |
|---------|-----------|------------|---------------|---------|------------|
| Vserver | Interface | Admin/Oper | Address/Mask | Node | Port |
| Home | | | | | |
| ----- | ----- | ----- | ----- | ----- | ----- |
| ---- | | | | | |
| vs1 | | | | | |
| | lif1 | up/up | 10.0.0.128/24 | node1 | e0d |
| true | | | | | |

6. Confirmar que la configuración del grupo de recuperación tras fallos es la deseada.

```
network interface show -failover -vserver vs1
```

| | Logical | Home | Failover | Failover |
|--|-----------|-----------|----------------|----------|
| Vserver | interface | Node:Port | Policy | Group |
| ----- | ----- | ----- | ----- | ----- |
| vs1 | | | | |
| | lif1 | node1:e0d | system-defined | ipspace1 |
| Failover Targets: node1:e0d, node1:e0e, node2:e0d, node2:e0e | | | | |

7. Compruebe que se pueda acceder a la dirección IP configurada:

| | |
|-----------------------|-------------|
| Para verificar una... | Usar... |
| Dirección IPv4 | ping de red |

Ejemplos

El siguiente comando crea una LIF y especifica la dirección IP y los valores de máscara de red mediante el `-address` y.. `-netmask` parámetros:

```
network interface create -vserver vs1.example.com -lif datalif1
-service-policy default-data-files -home-node node-4 -home-port e1c
-address 192.0.2.145 -netmask 255.255.255.0 -auto-revert true
```

El siguiente comando crea una LIF y asigna valores de dirección IP y máscara de red a partir de la subred especificada (denominada `cliente1_sub`):

```
network interface create -vserver vs3.example.com -lif datalif3
-service-policy default-data-files -home-node node-3 -home-port e1c
-subnet-name cliente1_sub - auto-revert true
```

El siguiente comando crea una LIF de NVMe/FC y especifica el `nvme-fc` protocolo de datos:

```
network interface create -vserver vs1.example.com -lif datalif1 -data
-protocol nvme-fc -home-node node-4 -home-port 1c -address 192.0.2.145
-netmask 255.255.255.0 -auto-revert true
```

Modificar una LIF

Puede modificar una LIF cambiando los atributos, como el nodo inicial o el nodo actual, el estado administrativo, la dirección IP, la máscara de red, la política de conmutación por error política de firewall y política de servicio. También puede cambiar la familia de direcciones de un LIF de IPv4 a IPv6.

Acerca de esta tarea

- Cuando se modifica el estado administrativo de una LIF a inactivo, se retienen todos los bloqueos de NFSv4 extraordinarios hasta que se devuelva el estado administrativo de la LIF a.

Para evitar conflictos de bloqueos que se pueden producir cuando otros LIF intentan acceder a los archivos bloqueados, debe mover los clientes de NFSv4 a una LIF diferente antes de establecer el estado administrativo como inactivo.

- No puede modificar los protocolos de datos que utiliza una LIF FC. Sin embargo, puede modificar los servicios asignados a una política de servicio o cambiar la política de servicio asignada a una LIF de IP.

Para modificar los protocolos de datos que utiliza una LIF FC, debe eliminar y volver a crear la LIF. Para realizar cambios en la política de servicio en una LIF de IP, hay una breve interrupción mientras se realizan las actualizaciones.

- No puede modificar el nodo de inicio ni el nodo actual de una LIF de gestión de ámbito de nodo.
- Cuando se usa una subred para cambiar la dirección IP y el valor de máscara de red de una LIF, se asigna una dirección IP desde la subred especificada; si la dirección IP anterior de la LIF procede de una subred diferente, la dirección IP se devuelve a esa subred.
- Para modificar la familia de direcciones de un LIF de IPv4 a IPv6, debe usar la notación de dos puntos para la dirección IPv6 y añadir un nuevo valor para `-netmask-length` parámetro.
- No puede modificar las direcciones IPv6 locales de enlace configuradas automáticamente.
- La modificación de una LIF que hace que la LIF no tenga ningún destino de conmutación por error válido da como resultado un mensaje de advertencia.

Si una LIF que no tiene un destino de conmutación por error válido intenta conmutar al respaldo, se podría producir una interrupción del servicio.

- A partir de ONTAP 9.5, puede modificar la política de servicio asociada con una LIF.

En ONTAP 9.5, las políticas de servicio solo se admiten para los servicios entre iguales de BGP y interconexión de clústeres. En ONTAP 9.6, puede crear políticas de servicio para varios servicios de datos y gestión.

- A partir de ONTAP 9.11.1, la conmutación por error automática de LIF iSCSI está disponible en las plataformas de cabinas SAN all-flash (ASA).


Para los LIF iSCSI preexistentes, lo que significa las LIF creadas antes de actualizar a la versión 9.11.1 o posterior, puede modificar la política de conmutación por error a. "[Activar recuperación tras fallos automática de LIF iSCSI](#)".

El procedimiento que siga depende de la interfaz que utilice: System Manager o CLI:

System Manager

A partir de ONTAP 9.12.0, puede utilizar System Manager para editar una interfaz de red

Pasos

1. Seleccione **Red > Descripción general > interfaces de red**.
2. Seleccione  > **Editar** junto a la interfaz de red que desea cambiar.
3. Cambie una o varias de las opciones de configuración de la interfaz de red. Para obtener más información, consulte ["Cree una LIF"](#).
4. Guarde los cambios.

CLI

Utilice la CLI para modificar un LIF

Pasos

1. Modifique los atributos de una LIF mediante el `network interface modify` comando.

En el ejemplo siguiente se muestra cómo modificar la dirección IP y la máscara de red de los datos de LIF 2 mediante una dirección IP y el valor de máscara de red de la subred cliente1_sub:

```
network interface modify -vserver vs1 -lif datalif2 -subnet-name
client1_sub
```

En el ejemplo siguiente se muestra cómo modificar la política de servicio de una LIF.

```
network interface modify -vserver siteA -lif node1_inter1 -service
-policy example
```

2. Compruebe que sea posible acceder a las direcciones IP.

| Si está usando... | Utilice... |
|-------------------|----------------------------|
| Direcciones IPv4 | <code>network ping</code> |
| Direcciones IPv6 | <code>network ping6</code> |

Migre una LIF

Puede que tenga que migrar un LIF a un puerto diferente en el mismo nodo o a un nodo distinto dentro del clúster, si el puerto está defectuoso o requiere mantenimiento. Migrar una LIF es similar a la conmutación por error de LIF, pero la migración de LIF es una operación manual, mientras que la conmutación por error de LIF es la migración automática de una LIF en respuesta a un fallo de enlace en el puerto de red actual de la LIF.

Antes de empezar

- Debe haber configurado un grupo de conmutación por error para las LIF.
- Los puertos y el nodo de destino deben estar operativos y deben poder acceder a la misma red que el puerto de origen.

Acerca de esta tarea

- Los LIF BGP residen en el puerto principal y no se pueden migrar a ningún otro nodo o puerto.
- Antes de quitar el NIC del nodo, debe migrar las LIF alojadas en los puertos que pertenecen a un NIC a otros puertos del clúster.
- Debe ejecutar el comando para migrar una LIF de clúster desde el nodo donde se aloja la LIF del clúster.
- Un LIF de ámbito de nodo, como un LIF de gestión de ámbito de nodo, LIF de clúster, LIF de interconexión de clústeres, no se puede migrar a un nodo remoto.
- Cuando se migra un LIF de NFSv4 entre nodos, se produce un retraso de hasta 45 segundos antes de que el LIF esté disponible en un puerto nuevo.

Para solucionar este problema, utilice NFSv4.1 donde no se encuentra ninguna demora.

- Puede migrar LIF iSCSI en plataformas de cabinas all-flash SAN (ASA) que ejecuten ONTAP 9.11.1 o versiones posteriores.

La migración de LIF iSCSI se limita a los puertos del nodo principal o del compañero de alta disponibilidad.

- Si la plataforma no es una plataforma de cabina SAN All-Flash (ASA) que ejecute ONTAP versión 9.11.1 o posterior, no se pueden migrar LIF iSCSI de un nodo a otro nodo.

Para solucionar esta restricción, debe crear una LIF iSCSI en el nodo de destino. Descubra ["Creación de LIF iSCSI"](#).


- Si desea migrar una LIF (interfaz de red) para NFS over RDMA, debe asegurarse de que el puerto de destino sea compatible con roce. Debe ejecutar ONTAP 9.10.1 o posterior para migrar un LIF con la CLI, o ONTAP 9.12.1 para realizar la migración mediante System Manager. En System Manager, una vez seleccionado el puerto de destino para roce, debe seleccionar la casilla junto a **utilizar puertos para roce** para completar la migración correctamente. Más información acerca de ["Configurar LIF para NFS a través de RDMA"](#).
- Se produce un error en las operaciones de descarga de la copia VAAI de VMware cuando se migra la LIF de origen o destino. Obtenga información acerca de la descarga de copias:
 - ["Entornos NFS"](#)
 - ["Entornos SAN"](#)


El procedimiento que siga depende de la interfaz que utilice: System Manager o CLI:

System Manager

Utilice System Manager para migrar una interfaz de red

Pasos

- 1. Seleccione **Red > Descripción general > interfaces de red**.
- 2. Seleccione  > **Migrate** junto a la interfaz de red que desea cambiar.



Para una LIF iSCSI, en el cuadro de diálogo **Migrate Interface**, seleccione el nodo de destino y el puerto del socio HA.

Si desea migrar la LIF iSCSI de forma permanente, marque la casilla. La LIF de iSCSI debe estar desconectada para poder migrarla de forma permanente. Además, una vez que se migra permanentemente un LIF iSCSI, no se puede revertir. No hay ninguna opción de reversión.

- 3. Haga clic en **migrar**.
- 4. Guarde los cambios.

CLI

Utilice la CLI para migrar un LIF

Paso

En función de si desea migrar una LIF específica o todas las LIF, realice la acción correspondiente:

| Si desea migrar... | Introduzca el siguiente comando... |
|--|--|
| Una LIF específica | <code>network interface migrate</code> |
| Todas las LIF de gestión de datos y clústeres en un nodo | <code>network interface migrate-all</code> |
| Todas las LIF están fuera de un puerto | <code>network interface migrate-all -node <node> -port <port></code> |

El ejemplo siguiente muestra cómo migrar una LIF llamada `datalif1` En la SVM `vs0` al puerto `e0d` encendido `node0b`:

```
network interface migrate -vserver vs0 -lif datalif1 -dest-node node0b -dest-port e0d
```

En el ejemplo siguiente se muestra cómo migrar todas las LIF de datos y de gestión del clúster desde el nodo (local) actual:

```
network interface migrate-all -node local
```

Revierte una LIF a su puerto raíz

Puede revertir un LIF a su puerto raíz después de producirse un fallo o una migración a otro puerto, ya sea de forma manual o automática. Si el puerto de inicio de un LIF determinado no está disponible, el LIF se mantiene en su puerto actual y no se revierte.

Acerca de esta tarea

- Si lleva administrativamente el puerto de inicio de un LIF al estado activo antes de configurar la opción de reversión automática, la LIF no vuelve al puerto de inicio.
- LIF no revierte automáticamente a menos que el valor de la opción de "reversión automática" se configure en TRUE.
- Debe asegurarse de que esté habilitada la opción de "reversión automática" para que las LIF puedan revertir a sus puertos de inicio.

El procedimiento que siga depende de la interfaz que utilice: System Manager o CLI:

System Manager
Utilice System Manager para revertir una interfaz de red a su puerto doméstico

- Pasos
1. Seleccione **Red > Descripción general > interfaces de red**.
 2. Seleccione **⋮ > Revert** junto a la interfaz de red que desea cambiar.
 3. Seleccione **Revert** para revertir una interfaz de red a su puerto de inicio.

CLI
Utilice la CLI para revertir una LIF a su puerto doméstico

Paso

Revierte una LIF a su puerto de inicio de forma manual o automática:

| | |
|---|--|
| Si desea revertir una LIF a su puerto raíz... | Después, introduzca el siguiente comando... |
| Manualmente | <code>network interface revert -vserver vservice_name -lif lif_name</code> |
| Automáticamente | <code>network interface modify -vserver vservice_name -lif lif_name -auto-revert true</code> |

ONTAP 9.8 y versiones posteriores: Recupere desde una LIF de clúster configurada incorrectamente

No se puede crear un clúster cuando la red del clúster se cableado a un switch, pero no todos los puertos configurados en el espacio IP del clúster pueden llegar a los otros puertos configurados en el espacio IP del clúster.

Acerca de esta tarea

En un clúster de switches, si una interfaz de red de clúster (LIF) está configurada en el puerto incorrecto o si se conecta un puerto de clúster a la red incorrecta, el `cluster create` el comando puede fallar y generar el siguiente error:

Not all local cluster ports have reachability to one another.
Use the "network port reachability show -detail" command for more details.

Los resultados de la `network port show` Puede que el comando muestre que se agregan varios puertos al espacio IP del clúster porque están conectados a un puerto que está configurado en una LIF del clúster. Sin embargo, los resultados de la `network port reachability show -detail` comando muestra qué puertos no tienen conectividad entre sí.

Para recuperar desde un LIF de clúster configurado en un puerto que no sea accesible a los otros puertos configurados con LIF del clúster, realice los pasos siguientes:

Pasos

1. Restablezca el puerto de inicio de la LIF del clúster en el puerto correcto:

```
network port modify -home-port
```

2. Quite los puertos que no tienen LIF del clúster configuradas en ellos desde el dominio de retransmisión del clúster:

```
network port broadcast-domain remove-ports
```

3. Cree el clúster:

```
cluster create
```

Resultado

Una vez finalizada la creación del clúster, el sistema detecta la configuración correcta y coloca los puertos en los dominios de retransmisión correctos.

Eliminar una LIF

Puede eliminar una interfaz de red (LIF) que ya no sea necesaria.

Antes de empezar

Las LIF que deben eliminarse no deben estar en uso.

Pasos

1. Marque las LIF que desea eliminar como administrativas usando el siguiente comando:

```
network interface modify -vserver vservice_name -lif lif_name -status  
-admin down
```

2. Utilice la `network interface delete` Comando para eliminar una o todas las LIF:

| | |
|----------------------|---|
| Si desea eliminar... | Introduzca el comando ... |
| Una LIF específica | <code>network interface delete -vserver vserver_name -lif lif_name</code> |
| Todas las LIF | <code>network interface delete -vserver vserver_name -lif *</code> |

El siguiente comando elimina la LIF mgmtlif2:

```
network interface delete -vserver vs1 -lif mgmtlif2
```

3. Utilice la `network interface show` Comando para confirmar que la LIF se ha eliminado.

Equilibre las cargas de red

Visión general de la red de balance

Puede configurar su clúster para que sirva las solicitudes de cliente desde LIF cargadas correctamente. Esto da como resultado un uso más equilibrado de LIF y puertos, lo que a su vez permite un mejor rendimiento del clúster.

El equilibrio de carga de DNS ayuda a seleccionar una LIF de datos cargada correctamente y a equilibrar el tráfico de red de usuario en todos los puertos disponibles (físicos, grupos de interfaces y VLAN).

Con el equilibrio de carga de DNS, las LIF se asocian a la zona de equilibrio de carga de una SVM. Un servidor DNS de todo el sitio está configurado para reenviar todas las solicitudes de DNS y devolver el LIF menos cargado en función del tráfico de red y la disponibilidad de los recursos de puertos (uso de CPU, rendimiento, conexiones abiertas, etc.). El equilibrio de carga de DNS ofrece las siguientes ventajas:

- Las nuevas conexiones de clientes se equilibran entre los recursos disponibles.
- No es necesaria ninguna intervención manual para decidir qué LIF se usarán en el montaje de una SVM en particular.
- El equilibrio de carga de DNS admite NFSv3, NFSv4, NFSv4.1, SMB 2.0, SMB 2.1, SMB 3.0 y S3.

Cómo funciona el equilibrio de carga de DNS

Los clientes montan una SVM especificando una dirección IP (asociada a una LIF) o un nombre de host (asociado a varias direcciones IP). De forma predeterminada, el servidor DNS de todo el sitio selecciona los LIF por turnos, lo que equilibra la carga de trabajo entre todos los LIF.

El equilibrio de carga por turnos puede sobrecargar algunos LIF, por lo que tiene la opción de utilizar una zona de equilibrio de carga DNS que gestiona la resolución de nombres de host en una SVM. Con una zona de equilibrio de carga DNS, se garantiza un mejor equilibrio de las conexiones de los nuevos clientes en los recursos disponibles, lo que mejora el rendimiento del clúster.

Una zona de equilibrio de carga DNS es un servidor DNS dentro del clúster que evalúa de forma dinámica la

carga de todas las LIF y devuelve un LIF cargado correctamente. En una zona de equilibrio de carga, DNS asigna un peso (métrica), basado en la carga, a cada LIF.

A cada LIF se le asigna un peso en función de la carga de puertos y el uso de CPU de su nodo raíz. Las LIF que están en puertos menos cargados tienen una probabilidad mayor de ser devueltas en una consulta DNS. Los pesos también se pueden asignar manualmente.

Cree una zona de balanceo de carga de DNS

Puede crear una zona de equilibrio de carga de DNS para facilitar la selección dinámica de una LIF en función de la carga, es decir, el número de clientes montados en una LIF. Puede crear una zona de equilibrio de carga mientras crea una LIF de datos.

Antes de empezar

El transportista DNS del servidor DNS del sitio debe estar configurado para reenviar todas las solicitudes de la zona de equilibrio de carga a las LIF configuradas.

El artículo de la base de conocimientos ["Cómo configurar el equilibrio de carga de DNS en Cluster-Mode"](#) En el sitio de soporte de NetApp contiene más información acerca de la configuración del equilibrio de carga de DNS mediante reenvío condicional.

Acerca de esta tarea

- Cualquier LIF de datos puede responder a consultas DNS para un nombre de zona de equilibrio de carga DNS.
- Una zona de equilibrio de carga DNS debe tener un nombre único en el clúster y el nombre de la zona debe cumplir los siguientes requisitos:
 - No debe superar los 256 caracteres.
 - Debe incluir al menos un período.
 - El primer carácter y el último no deben ser un punto ni ningún otro carácter especial.
 - No puede incluir espacios entre caracteres.
 - Cada etiqueta del nombre DNS no debe superar los 63 caracteres.

Una etiqueta es el texto que aparece antes o después del período. Por ejemplo, la zona DNS llamada `storage.company.com` tiene tres etiquetas.

Paso

Utilice la `network interface create` con el `dns-zone` Opción para crear una zona de equilibrio de carga DNS.

Si ya existe la zona de equilibrio de carga, se agrega el LIF. Para obtener más información acerca del comando, consulte ["Comandos de ONTAP 9"](#).

En el siguiente ejemplo se muestra cómo crear una zona de equilibrio de carga DNS llamada `storage.company.com` durante la creación de la LIF `lif1`:

```
network interface create -vserver vs0 -lif lif1 -home-node node1
-home-port e0c -address 192.0.2.129 -netmask 255.255.255.128 -dns-zone
storage.company.com
```

Añada o quite una LIF de una zona de equilibrio de carga

Puede agregar o quitar una LIF de la zona de equilibrio de carga DNS de una máquina virtual (SVM). También puede quitar todas las LIF al mismo tiempo de una zona de equilibrio de carga.

Antes de empezar

- Todas las LIF de una zona de equilibrio de carga deben pertenecer a la misma SVM.
- Un LIF puede ser parte de solo una zona de equilibrio de carga de DNS.
- Debe haber configurado los grupos de conmutación por error de cada subred si las LIF pertenecen a subredes diferentes.

Acerca de esta tarea

Una LIF en estado administrativo inactivo se quita temporalmente de la zona de equilibrio de carga de DNS. Cuando la LIF vuelve al estado administrativo up, la LIF se agrega automáticamente a la zona de balanceo de carga de DNS.

Paso

Añada una LIF a o quite una LIF de una zona de equilibrio de carga:

| Si desea... | Introduzca... |
|---------------------|--|
| Añada una LIF | <pre>network interface modify -vserver vs1 -lif lif_name -dns-zone zone_name</pre> <p>Ejemplo:</p> <pre>network interface modify -vserver vs1 -lif data1 -dns-zone cifs.company.com</pre> |
| Quite una única LIF | <pre>network interface modify -vserver vs1 -lif lif_name -dns-zone none</pre> <p>Ejemplo:</p> <pre>network interface modify -vserver vs1 -lif data1 -dns-zone none</pre> |
| Quite todas las LIF | <pre>network interface modify -vserver vs1 -lif * -dns-zone none</pre> <p>Ejemplo:</p> <pre>network interface modify -vserver vs0 -lif * -dns-zone none</pre> <p>Puede quitar una SVM de una zona de equilibrio de carga mediante la eliminación de todas las LIF de la SVM de esa zona.</p> |

Configurar servicios DNS (ONTAP 9,8 y versiones posteriores)

Debe configurar los servicios DNS para la SVM antes de crear un servidor NFS o SMB. Generalmente, los servidores de nombres DNS son los servidores DNS integrados de Active Directory para el dominio al que se unirá el servidor NFS o SMB.

Acerca de esta tarea

Los servidores DNS integrados en Active Directory contienen los registros de ubicación de servicio (SRV) para los servidores LDAP de dominio y controlador de dominio. Si la SVM no puede encontrar los servidores LDAP de Active Directory y las controladoras de dominio, se produce un error en la configuración del servidor NFS o SMB.

Las SVM utilizan la base de datos ns-switch de servicios de nombres de hosts para determinar qué servicios de nombres utilizar y en qué orden se debe buscar información sobre los hosts. Los dos servicios de nombre admitidos para la base de datos de hosts son archivos y dns.

Debe asegurarse de que dns sea uno de los orígenes antes de crear el servidor SMB.



Para ver las estadísticas de los servicios de nombre DNS para el proceso mgwd y el proceso SECD, use la interfaz de usuario de Statistics.

Pasos

1. Determine cuál es la configuración actual para la base de datos de servicios de nombre de host. En este ejemplo, la base de datos del servicio de nombres de host utiliza la configuración predeterminada.

```
vserver services name-service ns-switch show -vserver vs1 -database hosts
```

```
Vserver: vs1
Name Service Switch Database: hosts
Vserver: vs1 Name Service Switch Database: hosts
Name Service Source Order: files, dns
```

2. Si es necesario, realice las siguientes acciones.

- a. Agregue el servicio de nombres DNS a la base de datos del servicio de nombres de host en el orden deseado o reordene los orígenes.

En este ejemplo, la base de datos hosts está configurada para utilizar DNS y archivos locales en ese orden.

```
vserver services name-service ns-switch modify -vserver vs1 -database hosts
-sources dns,files
```

- b. Compruebe que la configuración del servicio de nombres es correcta.

```
vserver services name-service ns-switch show -vserver vs1 -database hosts
```

```
Vserver: vs1
Name Service Switch Database: hosts
Name Service Source Order: dns, files
```

3. Configure los servicios DNS.

```
vserver services name-service dns create -vserver vs1 -domains
example.com,example2.com -name-servers 10.0.0.50,10.0.0.51
```



El comando `vserver Services NAME-service dns create` realiza una validación de configuración automática e informa de un mensaje de error si ONTAP no puede contactar con el servidor de nombres.

4. Verifique que la configuración de DNS sea correcta y que el servicio esté habilitado.

```
Vserver: vs1
Domains: example.com, example2.com Name Servers: 10.0.0.50, 10.0.0.51
Enable/Disable DNS: enabled Timeout (secs): 2
Maximum Attempts: 1
```

5. Validar el estado de los servidores de nombres.

```
vserver services name-service dns check -vserver vs1
```

| Vserver | Name Server | Status | Status Details |
|---------|-------------|--------|-------------------------|
| vs1 | 10.0.0.50 | up | Response time (msec): 2 |
| vs1 | 10.0.0.51 | up | Response time (msec): 2 |

Configure el DNS dinámico en la SVM

Si desea que el servidor DNS integrado en Active Directory registre de forma dinámica los registros DNS de un servidor NFS o SMB en DNS, debe configurar el DNS dinámico (DDNS) en la SVM.

Antes de empezar

Los servicios de nombres DNS deben configurarse en la SVM. Si utiliza DDNS seguro, debe usar servidores de nombres DNS integrados en Active Directory y debe haber creado un servidor NFS o SMB o una cuenta de Active Directory para la SVM.

Acerca de esta tarea

El nombre de dominio completo (FQDN) especificado debe ser único:

El nombre de dominio completo (FQDN) especificado debe ser único:

- Para NFS, el valor especificado en `-vserver-fqdn` como parte de la `vserver services name-service dns dynamic-update` El comando se convierte en el FQDN registrado de los LIF.
- Para SMB, los valores especificados como el nombre de NetBIOS del servidor CIFS y el nombre de dominio completo del servidor CIFS se convierten en el FQDN registrado de los LIF. No se puede configurar en ONTAP. En la siguiente situación, el nombre de dominio completo del LIF es «CIFS_VS1.EXAMPLE.COM»:

```
cluster1::> cifs server show -vserver vs1
```

```

                                Vserver: vs1
                                CIFS Server NetBIOS Name: CIFS_VS1
                                NetBIOS Domain/Workgroup Name: EXAMPLE
                                Fully Qualified Domain Name: EXAMPLE.COM
                                Organizational Unit: CN=Computers
Default Site Used by LIFs Without Site Membership:
                                Workgroup Name: -
                                Kerberos Realm: -
                                Authentication Style: domain
                                CIFS Server Administrative Status: up
                                CIFS Server Description:
                                List of NetBIOS Aliases: -
```



Para evitar un error de configuración de un FQDN de SVM que no es compatible con las reglas RFC para las actualizaciones de DDNS, utilice un nombre FQDN que es compatible con RFC. Para obtener más información, consulte ["RFC 1123"](#).

Pasos

1. Configure DDNS en la SVM:

```
vserver services name-service dns dynamic-update modify -vserver vserver_name
-is- enabled true [-use-secure {true|false} -vserver-fqdn
FQDN_used_for_DNS_updates
```

```
vserver services name-service dns dynamic-update modify -vserver vs1 -is
-enabled true - use-secure true -vserver-fqdn vs1.example.com
```

Los asteriscos no se pueden utilizar como parte del FQDN personalizado. Por ejemplo: *.netapp.com no es válido.

2. Compruebe que la configuración DDNS es correcta:

```
vserver services name-service dns dynamic-update show
```

| Vserver | Is-Enabled | Use-Secure | Vserver FQDN | TTL |
|---------|------------|------------|-----------------|-------|
| ----- | ----- | ----- | ----- | ----- |
| vs1 | true | true | vs1.example.com | 24h |

Configurar servicios DNS (ONTAP 9,7 y versiones anteriores)

Debe configurar los servicios DNS para la SVM antes de crear un servidor NFS o SMB. Generalmente, los servidores de nombres DNS son los servidores DNS integrados de Active Directory para el dominio al que se unirá el servidor NFS o SMB.

Acerca de esta tarea

Los servidores DNS integrados en Active Directory contienen los registros de ubicación de servicio (SRV) para los servidores LDAP de dominio y controlador de dominio. Si la SVM no puede encontrar los servidores LDAP de Active Directory y las controladoras de dominio, se produce un error en la configuración del servidor NFS o SMB.

Las SVM utilizan la base de datos ns-switch de servicios de nombres de hosts para determinar qué servicios de nombres utilizar y en qué orden se debe buscar información sobre los hosts. Los dos servicios de nombre admitidos para la base de datos de hosts son `files` y `dns`.

Debe asegurarse de eso `dns` Es uno de los orígenes antes de crear el servidor SMB.



Para ver las estadísticas de los servicios de nombre DNS para el proceso `mgwd` y el proceso `SECD`, use la interfaz de usuario de `Statistics`.

Pasos

1. Determine cuál es la configuración actual para `hosts` base de datos de servicios de nombres.

En este ejemplo, la base de datos del servicio de nombres de host utiliza la configuración predeterminada.

```
vserver services name-service ns-switch show -vserver vs1 -database hosts
```

```
Vserver: vs1
Name Service Switch Database: hosts
Name Service Source Order: files, dns
```

2. Si es necesario, realice las siguientes acciones.

- a. Agregue el servicio de nombres DNS a la base de datos del servicio de nombres de host en el orden deseado o reordene los orígenes.

En este ejemplo, la base de datos `hosts` está configurada para utilizar DNS y archivos locales en ese orden.

```
vserver services name-service ns-switch modify -vserver vs1 -database hosts
-sources dns,files
```

- a. Compruebe que la configuración del servicio de nombres es correcta.

```
vserver services name-service ns-switch show -vserver vs1 -database hosts
```

3. Configure los servicios DNS.

```
vserver services name-service dns create -vserver vs1 -domains
example.com,example2.com -name-servers 10.0.0.50,10.0.0.51
```



Los servicios `Vserver name-service dns create` El comando realiza una validación automática de la configuración e informa de un mensaje de error si ONTAP no puede comunicarse con el servidor de nombres.

4. Verifique que la configuración de DNS sea correcta y que el servicio esté habilitado.

```
Vserver: vs1
Domains: example.com, example2.com Name
Servers: 10.0.0.50, 10.0.0.51
Enable/Disable DNS: enabled Timeout (secs): 2
Maximum Attempts: 1
```

5. Validar el estado de los servidores de nombres.

```
vserver services name-service dns check -vserver vs1
```

| Vserver | Name Server | Status | Status Details |
|---------|-------------|--------|-------------------------|
| vs1 | 10.0.0.50 | up | Response time (msec): 2 |
| vs1 | 10.0.0.51 | up | Response time (msec): 2 |

Configure el DNS dinámico en la SVM

Si desea que el servidor DNS integrado en Active Directory registre de forma dinámica los registros DNS de un servidor NFS o SMB en DNS, debe configurar el DNS dinámico (DDNS) en la SVM.

Antes de empezar

Los servicios de nombres DNS deben configurarse en la SVM. Si utiliza DDNS seguro, debe usar servidores de nombres DNS integrados en Active Directory y debe haber creado un servidor NFS o SMB o una cuenta de Active Directory para la SVM.

Acerca de esta tarea

El nombre de dominio completo (FQDN) especificado debe ser único:

- Para NFS, el valor especificado en `-vserver-fqdn` como parte de la `vserver services name-service dns dynamic-update` El comando se convierte en el FQDN registrado de los LIF.
- Para SMB, los valores especificados como el nombre de NetBIOS del servidor CIFS y el nombre de dominio completo del servidor CIFS se convierten en el FQDN registrado de los LIF. No se puede configurar en ONTAP. En la siguiente situación, el nombre de dominio completo del LIF es «CIFS_VS1.EXAMPLE.COM»:

```
cluster1::> cifs server show -vserver vs1
```

```

                                Vserver: vs1
                                CIFS Server NetBIOS Name: CIFS_VS1
                                NetBIOS Domain/Workgroup Name: EXAMPLE
                                Fully Qualified Domain Name: EXAMPLE.COM
                                Organizational Unit: CN=Computers
Default Site Used by LIFs Without Site Membership:
                                Workgroup Name: -
                                Kerberos Realm: -
                                Authentication Style: domain
                                CIFS Server Administrative Status: up
                                CIFS Server Description:
                                List of NetBIOS Aliases: -
```



Para evitar un error de configuración de un FQDN de SVM que no es compatible con las reglas RFC para las actualizaciones de DDNS, utilice un nombre FQDN que es compatible con RFC. Para obtener más información, consulte ["RFC 1123"](#).

Pasos

1. Configure DDNS en la SVM:

```
vserver services name-service dns dynamic-update modify -vserver vserver_name
-is- enabled true [-use-secure {true|false} -vserver-fqdn
FQDN_used_for_DNS_updates
```

```
vserver services name-service dns dynamic-update modify -vserver vs1 -is
-enabled true - use-secure true -vserver-fqdn vs1.example.com
```

Los asteriscos no se pueden utilizar como parte del FQDN personalizado. Por ejemplo: *.netapp.com no es válido.

2. Compruebe que la configuración DDNS es correcta:

```
vserver services name-service dns dynamic-update show
```

| Vserver | Is-Enabled | Use-Secure | Vserver FQDN | TTL |
|---------|------------|------------|-----------------|-------|
| ----- | ----- | ----- | ----- | ----- |
| vs1 | true | true | vs1.example.com | 24h |

Configure los servicios DNS dinámicos

Si desea que el servidor DNS integrado en Active Directory registre de forma dinámica los registros DNS de un servidor NFS o SMB en DNS, debe configurar el DNS dinámico (DDNS) en la SVM.

Antes de empezar

Los servicios de nombres DNS deben configurarse en la SVM. Si utiliza DDNS seguro, debe usar servidores de nombres DNS integrados en Active Directory y debe haber creado un servidor NFS o SMB o una cuenta de Active Directory para la SVM.

Acerca de esta tarea

El FQDN especificado debe ser único.



Para evitar un error de configuración de un FQDN de SVM que no es compatible con las reglas RFC para las actualizaciones de DDNS, utilice un nombre FQDN que es compatible con RFC.

Pasos

1. Configure DDNS en la SVM:

```
vserver services name-service dns dynamic-update modify -vserver vserver_name  
-is-enabled true [-use-secure {true|false}] -vserver-fqdn  
FQDN_used_for_DNS_updates
```

```
vserver services name-service dns dynamic-update modify -vserver vs1 -is-  
-enabled true - use-secure true -vserver-fqdn vs1.example.com
```

Los asteriscos no se pueden utilizar como parte del FQDN personalizado. Por ejemplo: *.netapp.com no es válido.

2. Compruebe que la configuración DDNS es correcta:

```
vserver services name-service dns dynamic-update show
```

| Vserver | Is-Enabled | Use-Secure | Vserver FQDN | TTL |
|---------|------------|------------|-----------------|-----|
| vs1 | true | true | vs1.example.com | 24h |

Resolución del nombre de host

Descripción general de la resolución de nombres de host

ONTAP debe poder traducir los nombres de host a direcciones IP numéricas para proporcionar acceso a los clientes y acceder a los servicios. Debe configurar máquinas virtuales de almacenamiento (SVM) para que utilicen servicios de nombres locales o externos para resolver la información del host. ONTAP admite la configuración de un servidor DNS externo o la configuración del archivo de hosts locales para la resolución del nombre de host.

Cuando utiliza un servidor DNS externo, puede configurar el DNS dinámico (DDNS), que envía automáticamente información DNS nueva o modificada del sistema de almacenamiento al servidor DNS. Sin las actualizaciones dinámicas de DNS, debe agregar manualmente la información DNS (nombre DNS y dirección IP) a los servidores DNS identificados cuando se conecta un sistema nuevo o cuando cambie la información de DNS existente. Este proceso es lento y propenso a errores. Durante la recuperación ante

desastres, la configuración manual puede provocar tiempos de inactividad prolongados.

Configure DNS para la resolución de nombres de host

Se usa DNS para acceder a orígenes locales o remotos para obtener información del host. Debe configurar DNS para acceder a uno o ambos orígenes.

ONTAP debe ser capaz de buscar la información del host para proporcionar un acceso adecuado a los clientes. Es necesario configurar los servicios de nombre para permitir que ONTAP acceda a los servicios DNS locales o externos para obtener la información del host.

ONTAP almacena información de configuración del servicio de nombres en una tabla que equivale a `/etc/nsswitch.conf` Fichero de sistemas UNIX.

Configurar una SVM y LIF de datos para la resolución de nombres de host mediante un servidor DNS externo

Puede utilizar el `vserver services name-service dns` Comando para habilitar DNS en una SVM y configurarlo para usar DNS en la resolución de nombres de host. Los nombres de host se resuelven mediante servidores DNS externos.

Antes de empezar

Un servidor DNS para todo el sitio debe estar disponible para las búsquedas de nombre de host.

Debe configurar más de un servidor DNS para evitar un único punto de error. La `vserver services name-service dns create` El comando emite una advertencia si introduce solo un nombre de servidor DNS.

Acerca de esta tarea

Consulte [Configure los servicios DNS dinámicos](#) Para obtener más información sobre la configuración de DNS dinámico en la SVM.

Pasos

1. Habilite DNS en la SVM:

```
vserver services name-service dns create -vserver <vserver_name>
-domains <domain_name> -name-servers <ip_addresses> -state enabled
```

El siguiente comando habilita los servidores DNS externos en la SVM vs1:

```
vserver services name-service dns create -vserver vs1.example.com
-domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
enabled
```



La `vserver services name-service dns create` El comando realiza una validación automática de la configuración e informa de un mensaje de error si ONTAP no puede ponerse en contacto con el servidor de nombres.

2. Valide el estado de los servidores de nombres utilizando `vserver services name-service dns`

check comando.

```
vserver services name-service dns check -vserver vs1.example.com
```

| Name Server | | | |
|-----------------|-------------|--------|-------------------------|
| Vserver | Name Server | Status | Status Details |
| vs1.example.com | 10.0.0.50 | up | Response time (msec): 2 |
| vs1.example.com | 10.0.0.51 | up | Response time (msec): 2 |

Para obtener información sobre las políticas de servicio relacionadas con DNS, consulte ["LIF y políticas de servicio en ONTAP 9.6 y posteriores"](#).

Configure la tabla de switches de servicio de nombres para la resolución de nombres de host

Debe configurar correctamente la tabla del conmutador de servicio de nombres para permitir que ONTAP consulte el servicio de nombres local o externo a fin de recuperar la información del host.

Antes de empezar

Debe haber decidido qué servicio de nombres debe utilizar para la asignación de hosts en el entorno.

Pasos

1. Agregue las entradas necesarias a la tabla de cambio de servicio de nombres:

```
vserver services name-service ns-switch modify -vserver <vserver_name>  
-database <database_name> -source <source_names>
```

2. Compruebe que la tabla de cambio de servicio de nombres contiene las entradas esperadas en el orden deseado:

```
vserver services name-service ns-switch show -vserver <vserver_name>
```

Ejemplo

En el siguiente ejemplo se modifica una entrada en la tabla del conmutador de servicio de nombres para SVM VS1 a fin de utilizar primero el archivo de hosts locales y, a continuación, un servidor DNS externo para resolver los nombres de host:

```
vserver services name-service ns-switch modify -vserver vs1 -database  
hosts -sources files,dns
```

Gestionar la tabla hosts (solo administradores del clúster)

Un administrador de clúster puede añadir, modificar, eliminar y ver las entradas del nombre de host en la tabla hosts de la máquina virtual de almacenamiento (SVM) de

administrador. Un administrador de SVM solo puede configurar las entradas del nombre de host para la SVM asignada.

Comandos para gestionar entradas de nombre de host local

Puede utilizar el `vserver services name-service dns hosts` Comando para crear, modificar o eliminar entradas de la tabla de hosts DNS.

Cuando va a crear o modificar las entradas de nombre de host DNS, puede especificar varias direcciones de alias separadas por comas.

| Si desea... | Se usa este comando... |
|---|---|
| Cree una entrada DNS host-name | <code>vserver services name-service dns hosts create</code> |
| Modifique una entrada de nombre de host DNS | <code>vserver services name-service dns hosts modify</code> |
| Eliminar una entrada de nombre de host DNS | <code>vserver services name-service dns hosts delete</code> |

Para obtener más información, consulte ["Comandos de ONTAP 9"](#) para la `vserver services name-service dns hosts` comandos.

Proteja su red

Configuración de la seguridad de red mediante estándares federales de procesamiento de información (FIPS)

ONTAP cumple con los estándares de procesamiento de información federal (FIPS) 140-2 para todas las conexiones SSL. Puede activar y desactivar el modo FIPS de SSL, establecer protocolos SSL a nivel global y desactivar todos los cifrados débiles, como RC4 dentro de ONTAP.

De forma predeterminada, SSL en ONTAP se establece con el cumplimiento FIPS deshabilitado y el protocolo SSL habilitado con lo siguiente:

- TLSv1.3 (a partir de ONTAP 9.11.1)
- TLSv1,2
- TLSv1,1
- TLSv1

Cuando el modo SSL FIPS está activado, la comunicación SSL desde ONTAP a componentes de cliente o servidor externos a ONTAP utilizará cifrado compatible con FIPS para SSL.

Si desea que las cuentas de administrador accedan a SVM con una clave pública SSH, debe asegurarse de que el algoritmo de clave de host sea compatible antes de habilitar el modo SSL FIPS.

Nota: la compatibilidad con el algoritmo de clave de host ha cambiado en ONTAP 9.11.1 y versiones posteriores.

| Versión de ONTAP | Tipos de clave admitidos | Tipos de claves no compatibles |
|---------------------|------------------------------------|---|
| 9.11.1 y posterior | ecdsa-sha2-nistp256 | rsa-sha2-512 rsa-sha2-256 ssh-ed25519 ssh-dss ssh-rsa |
| 9.10.1 y anteriores | ecdsa-sha2-nistp256 ssh-ed25519 | ssh-dss ssh-rsa |

Las cuentas de clave pública SSH existentes sin los algoritmos de clave admitidos deben volver a configurarse con un tipo de clave compatible antes de habilitar FIPS o la autenticación del administrador fallará.

Para obtener más información, consulte ["Habilite cuentas de clave pública de SSH"](#).

Para obtener más información acerca de la configuración del modo FIPS de SSL, consulte `security config modify` página de manual.

Habilite FIPS

Se recomienda que todos los usuarios seguros ajusten su configuración de seguridad inmediatamente después de instalar o actualizar el sistema. Cuando el modo SSL FIPS está activado, la comunicación SSL desde ONTAP a componentes de cliente o servidor externos a ONTAP utilizará cifrado compatible con FIPS para SSL.



Cuando FIPS está habilitada, no se puede instalar ni crear un certificado con una longitud de clave RSA de 4096.

Pasos

1. Cambie al nivel de privilegio avanzado:

```
set -privilege advanced
```

2. Habilitar FIPS:

```
security config modify -interface SSL -is-fips-enabled true
```

3. Cuando se le solicite continuar, introduzca `y`
4. Si ejecuta ONTAP 9.8 o versiones anteriores, reinicie manualmente cada nodo del clúster de uno en uno. A partir de ONTAP 9.9.1, no es necesario reiniciar.

Ejemplo

Si está ejecutando ONTAP 9.9.1 o posterior, no verá el mensaje de advertencia.

```
security config modify -interface SSL -is-fips-enabled true
```

Warning: This command will enable FIPS compliance and can potentially cause some non-compliant components to fail. MetroCluster and Vserver DR require FIPS to be enabled on both sites in order to be compatible.

Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster. This is necessary to prevent components from failing due to an inconsistent security configuration state in the cluster. To avoid a service outage, reboot one node at a time and wait for it to completely initialize before rebooting the next node. Run "security config status show" command to monitor the reboot status.

Do you want to continue? {y|n}: y

Deshabilite FIPS

Si sigue ejecutando una configuración de sistema anterior y desea configurar ONTAP con compatibilidad con versiones anteriores, solo puede activar SSLv3 cuando FIPS esté deshabilitado.

Pasos

1. Cambie al nivel de privilegio avanzado:

```
set -privilege advanced
```

2. Para deshabilitar FIPS, escriba:

```
security config modify -interface SSL -is-fips-enabled false
```

3. Cuando se le solicite continuar, introduzca y.
4. Si utiliza ONTAP 9.8 o una versión anterior, reinicie manualmente cada nodo del clúster. A partir de ONTAP 9.9.1, no es necesario reiniciar.

Ejemplo

Si está ejecutando ONTAP 9.9.1 o posterior, no verá el mensaje de advertencia.


```
security config modify -interface SSL -supported-protocols SSLv3
```

Warning: Enabling the SSLv3 protocol may reduce the security of the interface, and is not recommended.

Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster. This is necessary to prevent components from failing due to an inconsistent security configuration state in the cluster. To avoid a service outage, reboot one node at a time and wait for it to completely initialize before rebooting the next node. Run "security config status show" command to monitor the reboot status.

Do you want to continue? {y|n}: y

Ver el estado de cumplimiento de normativas FIPS

Puede ver si el clúster completo está ejecutando las opciones de configuración de seguridad actuales.

Pasos

1. De uno a uno, reinicie cada nodo del clúster.

No reinicie todos los nodos del clúster en simultáneo. Se requiere un reinicio para asegurarse de que todas las aplicaciones del clúster estén ejecutando la nueva configuración de seguridad y para todos los cambios en el modo de encendido/apagado, los protocolos y los cifrados de FIPS.

2. Ver el estado de cumplimiento actual:

```
security config show
```

```
security config show
```

| | Cluster | | Cluster |
|-----------|-----------|-------------------------|-------------------------------------|
| Security | | | |
| Interface | FIPS Mode | Supported Protocols | Supported Ciphers Config |
| Ready | | | |
| ----- | ----- | ----- | ----- |
| ----- | | | |
| SSL | false | TLsv1_2, TLsv1_1, TLsv1 | ALL:!LOW:!aNULL: yes !EXP:!eNULL |

Configurar la seguridad IP (IPsec) a través del cifrado de cable

ONTAP utiliza la seguridad del protocolo de Internet (IPsec) en el modo de transporte para garantizar que los datos estén protegidos y cifrados de forma continua, incluso durante el tránsito. IPSec ofrece cifrado de datos para todo el tráfico IP, incluidos los

protocolos NFS, iSCSI y SMB.

A partir de ONTAP 9.12.1, está disponible la compatibilidad con IPsec del protocolo de host de interfaz de usuario en las configuraciones con conexión a la estructura de MetroCluster IP y MetroCluster.

La compatibilidad con IPSec en clústeres de MetroCluster se limita al tráfico de host de front-end y no se admite en las LIF de interconexión de clústeres de MetroCluster.

A partir de ONTAP 9.10.1, puede utilizar claves precompartidas (PSK) o certificados para la autenticación con IPsec. Anteriormente, sólo PSK eran compatibles con IPsec.

A partir de ONTAP 9.9.1, los algoritmos de cifrado utilizados por IPsec están validados con FIPS 140-2-2. Los algoritmos los genera el módulo de criptografía de NetApp en ONTAP, que conlleva la validación FIPS 140-2-2.

A partir de ONTAP 9,8, ONTAP admite IPsec en modo de transporte.

Una vez configurado IPsec, el tráfico de red entre el cliente y ONTAP está protegido con medidas preventivas para combatir los ataques de repetición y de hombre en el medio (MITM).

Para el cifrado de tráfico de paridad de clústeres y SnapMirror de NetApp, se recomienda el cifrado de paridad de clústeres (CPE) y la seguridad de la capa de transporte (TLS) a través de IPsec para garantizar la seguridad en tránsito por el cable. Esto se debe a que TLS tiene mejor rendimiento que IPsec.

Aunque la capacidad IPsec está habilitada en el clúster, la red requiere una entrada de base de datos de directivas de seguridad (SPD) para que coincida con el tráfico a proteger y para especificar detalles de protección (como la suite de cifrado y el método de autenticación) antes de que pueda fluir el tráfico. También se necesita una entrada SPD correspondiente en cada cliente.

Habilite IPsec en el clúster

Puede habilitar IPsec en el clúster para asegurarse de que los datos están protegidos y cifrados de forma continua, incluso mientras están en tránsito.

Pasos

1. Detectar si IPsec está activada:

```
security ipsec config show
```

Si el resultado incluye `IPsec Enabled: false`, continúe con el próximo paso.

2. Habilitar IPsec:

```
security ipsec config modify -is-enabled true
```

3. Vuelva a ejecutar el comando Discovery:

```
security ipsec config show
```

El resultado ahora incluye `IPsec Enabled: true`.

Prepárese para la creación de directivas IPsec con autenticación de certificados

Puede omitir este paso si solo utiliza claves precompartidas (PSKs) para la autenticación y no utilizará la autenticación de certificados.

Antes de crear una política IPsec que utilice certificados para la autenticación, debe verificar que se cumplan los siguientes requisitos previos:

- Tanto ONTAP como el cliente deben tener instalado el certificado CA de la otra parte para que los certificados de la entidad final (ya sea ONTAP o el cliente) sean verificables por ambas partes
- Se instala un certificado para el LIF de ONTAP que participa en la política



Las LIF de ONTAP pueden compartir certificados. No es necesario realizar una asignación de uno a uno entre certificados y LIF.

Pasos

1. Instale todos los certificados de CA utilizados durante la autenticación mutua, incluidas las CA de ONTAP y del lado del cliente, en la gestión de certificados de ONTAP a menos que ya esté instalado (como es el caso de una CA raíz autofirmado de ONTAP).

Comando de ejemplo

```
cluster::> security certificate install -vserver svm_name -type server-ca  
-cert-name my_ca_cert
```

2. Para asegurarse de que la CA instalada se encuentra dentro de la ruta de búsqueda de la CA IPsec durante la autenticación, agregue las CA de gestión de certificados ONTAP al módulo IPsec mediante `security ipsec ca-certificate add` comando.

Comando de ejemplo

```
cluster::> security ipsec ca-certificate add -vserver svm_name -ca-certs  
my_ca_cert
```

3. Cree e instale un certificado para que lo utilice la LIF de ONTAP. La entidad emisora de certificados de este certificado ya debe estar instalada en ONTAP y agregada a IPsec.

Comando de ejemplo

```
cluster::> security certificate install -vserver svm_name -type server -cert  
-name my_nfs_server_cert
```

Para obtener más información sobre los certificados de ONTAP, consulte los comandos de certificado de seguridad en la documentación de ONTAP 9 .

Definir la base de datos de directivas de seguridad (SPD)

IPSec requiere una entrada SPD antes de permitir que el tráfico fluya por la red. Esto es cierto tanto si está utilizando un PSK como un certificado para la autenticación.

Pasos

1. Utilice la `security ipsec policy create` comando para:
 - a. Seleccione la dirección IP de ONTAP o la subred de direcciones IP para participar en el transporte IPsec.
 - b. Seleccione las direcciones IP del cliente que se conectarán a las direcciones IP de ONTAP.



El cliente debe admitir la versión 2 de Exchange de claves de Internet (IKEv2) con una clave compartida previamente (PSK).

- c. Opcional. Seleccione los parámetros de tráfico detallados, como los protocolos de capa superior (UDP, TCP, ICMP, etc.)), los números de puerto locales y los números de puerto remotos para proteger el tráfico. Los parámetros correspondientes son `protocols`, `local-ports` y `remote-ports` respectivamente.

Omita este paso para proteger todo el tráfico entre la dirección IP de ONTAP y la dirección IP del cliente. La protección de todo el tráfico es la opción predeterminada.

- d. Introduzca PSK o la infraestructura de clave pública (PKI) para el `auth-method` parámetro del método de autenticación deseado.
- i. Si introduce un PSK, incluya los parámetros y, a continuación, pulse <enter> para que el mensaje introduzca y verifique la clave precompartida.



`local-identity` y `remote-identity` Los parámetros son opcionales si tanto el host como el cliente utilizan strongSwan y no se ha seleccionado ninguna política de comodín para el host o el cliente.

- ii. Si introduce una PKI, deberá introducir también la `cert-name`, `local-identity`, `remote-identity` parámetros. Si la identidad del certificado del lado remoto es desconocida o si se esperan varias identidades de cliente, introduzca la identidad especial `ANYTHING`.

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32
Enter the preshared key for IPsec Policy _test34_ on Vserver _vs1_:
```

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32 -local-ports 2049
-protocols tcp -auth-method PKI -cert-name my_nfs_server_cert -local
-identity CN=netapp.ipsec.lif1.vs0 -remote-identity ANYTHING
```

El tráfico IP no puede fluir entre el cliente y el servidor hasta que ONTAP y el cliente hayan configurado las directivas IPsec coincidentes y las credenciales de autenticación (PSK o certificado) estén en su lugar en ambos lados. Para obtener más información, consulte la configuración de IPsec del lado del cliente.

Usar identidades IPsec

Para el método de autenticación de clave precompartida, las identidades locales y remotas son opcionales si tanto el host como el cliente utilizan strongSwan y no se selecciona ninguna política de comodín para el host o el cliente.

Para el método de autenticación PKI/certificado, las identidades locales y remotas son obligatorias. Las identidades especifican qué identidad está certificada dentro del certificado de cada lado y se utilizan en el proceso de verificación. Si la identidad remota es desconocida o si podría ser una identidad muy distinta, utilice la identidad especial `ANYTHING`.

Acerca de esta tarea

En ONTAP, las identidades se especifican modificando la entrada SPD o durante la creación de la política SPD. El SPD puede ser una dirección IP o un nombre de identidad con formato de cadena.

Paso

Para modificar una configuración de identidad SPD existente, utilice el siguiente comando:

```
security ipsec policy modify
```

Comando de ejemplo

```
security ipsec policy modify -vserver vs1 -name test34 -local-identity  
192.168.134.34 -remote-identity client.fooboo.com
```

Configuración de varios clientes IPSec

Cuando un pequeño número de clientes necesitan aprovechar IPsec, es suficiente utilizar una sola entrada SPD para cada cliente. Sin embargo, cuando cientos o incluso miles de clientes necesitan aprovechar IPsec, NetApp recomienda el uso de una configuración de varios clientes IPsec.

Acerca de esta tarea

ONTAP admite la conexión de varios clientes a través de varias redes a una única dirección IP de SVM con IPsec habilitada. Para ello, utilice uno de los siguientes métodos:

- **Configuración de subred**

Para permitir que todos los clientes de una subred determinada (por ejemplo, 192.168.134.0/24) se conecten a una única dirección IP de SVM mediante una única entrada de directiva SPD, debe especificar el `remote-ip-subnets` en formato de subred. Además, debe especificar el `remote-identity` campo con la identidad del cliente correcta.



Al utilizar una sola entrada de directiva en una configuración de subred, los clientes IPsec de esa subred comparten la identidad IPsec y la clave precompartida (PSK). Sin embargo, esto no es cierto con la autenticación de certificado. Cuando se utilizan certificados, cada cliente puede utilizar su propio certificado único o un certificado compartido para autenticarse. IPsec de ONTAP comprueba la validez del certificado en función de las CA instaladas en el almacén de confianza local. ONTAP también admite la comprobación de la lista de revocación de certificados (CRL).

- **Permitir la configuración de todos los clientes**

Para permitir que cualquier cliente, independientemente de su dirección IP de origen, se conecte a la dirección IP habilitada para IPsec de SVM, utilice `0.0.0.0/0` comodín al especificar `remote-ip-subnets` campo.

Además, debe especificar el `remote-identity` campo con la identidad del cliente correcta. Para la autenticación del certificado, puede introducir `ANYTHING`.

Además, cuando la `0.0.0.0/0` se utiliza el comodín, debe configurar un número de puerto local o remoto específico para utilizarlo. Por ejemplo: `NFS port 2049`.

Pasos

a. Utilice uno de los siguientes comandos para configurar IPsec para varios clientes.

i. Si está utilizando **configuración de subred** para admitir varios clientes IPsec:

```
security ipsec policy create -vserver vserver_name -name policy_name
```

```
-local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets
IP_address/subnet -local-identity local_id -remote-identity remote_id
```

Comando de ejemplo

```
security ipsec policy create -vserver vs1 -name subnet134 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.0/24 -local-identity
ontap_side_identity -remote-identity client_side_identity
```

- i. Si está utilizando **Permitir que todos los clientes configuren** para admitir múltiples clientes IPsec:

```
security ipsec policy create -vserver vserver_name -name policy_name
-local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local
-ports port_number -local-identity local_id -remote-identity remote_id
```

Comando de ejemplo

```
security ipsec policy create -vserver vs1 -name test35 -local-ip-subnets
IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local-ports 2049 -local
-identity ontap_side_identity -remote-identity client_side_identity
```

Estadísticas IPsec

A través de la negociación, se puede establecer un canal de seguridad denominado Asociación de seguridad IKE (SA) entre la dirección IP de la SVM de ONTAP y la dirección IP del cliente. Las unidades SAS IPsec se instalan en ambos extremos para que funcionen el cifrado y descifrado de datos.

Puede utilizar comandos de estadísticas para comprobar el estado de las unidades SAS IPsec y SAS IKE.

Comandos de ejemplo

Comando de ejemplo IKE SA:

```
security ipsec show-ikesa -node hosting_node_name_for_svm_ip
```

Ejemplo de comando SA IPsec y salida:

```
security ipsec show-ipseca -node hosting_node_name_for_svm_ip
```

```
cluster1::> security ipsec show-ikesa -node cluster1-node1
```

| | Policy | Local | Remote | | |
|---------|--------|----------------|----------------|------------------|-------------|
| Vserver | Name | Address | Address | Initiator-SPI | State |
| vs1 | test34 | 192.168.134.34 | 192.168.134.44 | c764f9ee020cec69 | ESTABLISHED |

Ejemplo de comando SA IPsec y salida:

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip

cluster1::> security ipsec show-ipsecsa -node cluster1-node1
      Policy  Local          Remote          Inbound  Outbound
Vserver  Name    Address          Address          SPI      SPI
State
-----
-----
vs1      test34
          192.168.134.34  192.168.134.44  c4c5b3d6  c2515559
INSTALLED
```

Configurar políticas de firewall para LIF

La configuración de un firewall mejora la seguridad del clúster y ayuda a evitar el acceso no autorizado al sistema de almacenamiento. De forma predeterminada, el firewall incorporado está configurado para permitir el acceso remoto a un conjunto específico de servicios IP para LIF de datos, gestión e interconexión de clústeres.

A partir de ONTAP 9.10.1:

- Las políticas de firewall quedan obsoletas y se reemplazan por las políticas de servicio de LIF. Anteriormente, el firewall incorporado se gestionaba mediante directivas de firewall. Esta funcionalidad ahora se logra usando una política de servicio de LIF.
- Todas las políticas de firewall están vacías y no abren ningún puerto en el firewall subyacente. En su lugar, se deben abrir todos los puertos con una política de servicio de LIF.
- No es necesario realizar ninguna acción después de una actualización a la versión 9.10.1 o posterior para pasar de políticas de firewall a políticas de servicio de LIF. El sistema crea automáticamente políticas de servicio de LIF coherentes con las políticas de firewall que se están usando en la versión anterior de ONTAP. Si utiliza scripts u otras herramientas que crean y gestionan políticas de firewall personalizadas, es posible que deba actualizar dichas secuencias de comandos para crear políticas de servicio personalizadas en su lugar.

Para obtener más información, consulte ["LIF y políticas de servicio en ONTAP 9.6 y posteriores"](#).

Las políticas de firewall se pueden utilizar para controlar el acceso a protocolos de servicio de gestión como SSH, HTTP, HTTPS, Telnet, NTP, NDMP, NDMPs, RSH, DNS o SNMP. No se pueden establecer políticas de firewall para protocolos de datos como NFS o SMB.

Puede administrar el servicio y las políticas de firewall de las siguientes maneras:

- Activación o desactivación del servicio de firewall
- Mostrar la configuración actual del servicio de firewall
- Creación de una nueva directiva de firewall con el nombre de directiva y los servicios de red especificados
- Aplicar una política de firewall a una interfaz lógica
- Crear una nueva directiva de firewall que sea una copia exacta de una directiva existente

Puede usar esto para realizar una política con características similares dentro de la misma SVM o para copiar la política en una SVM diferente.

- Mostrar información acerca de las directivas de firewall
- Modificar las direcciones IP y las máscaras de red que utiliza una directiva de firewall
- Eliminar una política de firewall que no esté en uso en una LIF

Políticas de firewall y LIF

Las políticas de firewall de LIF se utilizan para restringir el acceso al clúster en cada LIF. Debe entender cómo afecta la política de firewall predeterminada al acceso del sistema sobre cada tipo de LIF y cómo puede personalizar una política de firewall para aumentar o reducir la seguridad de una LIF.

Al configurar una LIF con la `network interface create` o `network interface modify` comando, el valor especificado para `-firewall-policy` El parámetro determina los protocolos de servicio y las direcciones IP a los que se permite el acceso a la LIF.

En muchos casos puede aceptar el valor predeterminado de la política de firewall. En otros casos, es posible que deba restringir el acceso a determinadas direcciones IP y ciertos protocolos de servicio de gestión. Los protocolos de servicio de gestión disponibles incluyen SSH, HTTP, HTTPS, Telnet, NTP, NDMP, NDMPS, RSH, DNS Y SNMP.

De forma predeterminada, la política de firewall para todas las LIF del clúster es "" y no se puede modificar.

En la siguiente tabla se describen las políticas de firewall predeterminadas que se asignan a cada LIF, en función de su rol (ONTAP 9.5 y versiones anteriores) o política de servicio (ONTAP 9.6 y versiones posteriores), al crear la LIF:

| Política de firewall | Protocolos de servicio predeterminados | Acceso predeterminado | LIF aplicadas a. |
|----------------------------|--|---------------------------------|---|
| gestión | dns, http, https, ndmp, ndmps, ntp, snmp, ssh | Cualquier dirección (0.0.0.0/0) | Gestión de clústeres, gestión de SVM y LIF de gestión de nodos |
| gestión de nfs | dns, http, https, ndmp, ndmps, ntp, portmap, snmp, ssh | Cualquier dirección (0.0.0.0/0) | LIF de datos que también admiten el acceso a la gestión de la SVM |
| interconexión de clústeres | https, ndmp, ndmps | Cualquier dirección (0.0.0.0/0) | Todas las LIF de interconexión de clústeres |
| sql server | dns, ndmp, ndmps, portmap | Cualquier dirección (0.0.0.0/0) | Todos los LIF de datos |

Configuración del servicio portmap

El servicio portmap asigna los servicios RPC a los puertos en los que escuchan.

El servicio portmap siempre se pudo acceder en ONTAP 9.3 y versiones anteriores, se pasó a configurar en ONTAP 9.4 a través de ONTAP 9.6 y se gestiona automáticamente empezando por ONTAP 9.7.

- En ONTAP 9.3 y anteriores, siempre se pudo acceder al servicio portmap (rpcbind) en el puerto 111 en configuraciones de red que dependían del firewall integrado de ONTAP en lugar de un firewall de terceros.
- Desde ONTAP 9.4 a ONTAP 9.6, puede modificar las políticas de firewall para controlar si el servicio portmap es accesible en determinadas LIF.
- A partir de ONTAP 9.7, se elimina el servicio de firewall de portmap. En su lugar, el puerto portmap se abre automáticamente para todos los LIF que admiten el servicio NFS.

El servicio Portmap se puede configurar en el firewall de ONTAP 9.4 a ONTAP 9.6.

En el resto de este tema se describe cómo configurar el servicio de firewall de portmap para versiones de ONTAP 9.4 a ONTAP 9.6.

En función de la configuración, es posible que no permita el acceso al servicio en tipos específicos de LIF, que suelen ser de gestión y LIF entre clústeres. En algunas circunstancias, puede que incluso no permita el acceso en las LIF de datos.

Qué comportamiento se puede esperar

El comportamiento de ONTAP 9.4 a ONTAP 9.6 está diseñado para proporcionar una transición fluida durante la actualización. Si ya se está accediendo al servicio portmap a través de tipos específicos de LIF, continuará siendo accesible mediante estos tipos de LIF. Al igual que en ONTAP 9.3 y versiones anteriores, puede especificar los servicios a los que se puede acceder dentro del firewall en la política de firewall para el tipo de LIF.

Para que el comportamiento surta efecto, todos los nodos del clúster deben ejecutar de ONTAP 9.4 a ONTAP 9.6. Sólo se ve afectado el tráfico entrante.

Las nuevas reglas son las siguientes:

- Tras la actualización al lanzamiento del 9.4 al 9.6, ONTAP agrega el servicio portmap a todas las políticas de firewall existentes, predeterminadas o personalizadas.
- Cuando crea un nuevo clúster o un nuevo espacio IP, ONTAP agrega el servicio portmap solo a la política de datos predeterminada, no a las políticas de gestión o interconexión de clústeres predeterminadas.
- Puede agregar el servicio portmap a las políticas predeterminadas o personalizadas según sea necesario y eliminar el servicio según sea necesario.

Cómo agregar o quitar el servicio portmap

Para agregar el servicio portmap a una política de firewall de SVM o clúster (hacer que sea accesible dentro del firewall), introduzca:

```
system services firewall policy create -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

Para quitar el servicio portmap de una política de firewall de SVM o clúster (hacer que sea inaccesible dentro del firewall), introduzca:

```
system services firewall policy delete -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

Puede usar el comando `network interface modify` para aplicar la política del firewall a una LIF existente. Para obtener una sintaxis completa del comando, consulte ["Comandos de ONTAP 9"](#).

Cree una política de firewall y asígnela a una LIF

Las políticas de firewall predeterminadas se asignan a cada LIF al crear la LIF. En muchos casos, la configuración predeterminada del firewall funciona bien y no es necesario modificarla. Si desea cambiar los servicios de red o las direcciones IP que pueden acceder a una LIF, puede crear una política de firewall personalizada y asignarla a la LIF.

Acerca de esta tarea

- No puede crear una directiva de firewall con `policy` nombre `data`, `intercluster`, `cluster`, o `mgmt`.

Estos valores se reservan para las políticas de firewall definidas por el sistema.

- No puede establecer ni modificar una política de firewall para las LIF del clúster.

La política de firewall para las LIF del clúster se establece en `0.0.0.0/0` para todos los tipos de servicios.

- Si necesita quitar un servicio de una política, debe eliminar la política de firewall existente y crear una nueva.
- Si IPv6 está habilitado en el clúster, puede crear políticas de firewall con direcciones IPv6.

Una vez que IPv6 está habilitado, `data`, `intercluster`, y `mgmt` Las políticas de firewall incluyen `::/0`, el comodín IPv6, en su lista de direcciones aceptadas.

- Cuando se usa System Manager para configurar la funcionalidad de protección de datos en todos los clústeres, se debe asegurarse de que las direcciones IP de LIF entre clústeres estén incluidas en la lista permitida y que el servicio HTTPS esté en las LIF entre clústeres y en los firewalls de propiedad de la empresa.

De forma predeterminada, la `intercluster` La directiva de firewall permite el acceso desde todas las direcciones IP (`0.0.0.0/0`, o `::/0` para IPv6) y habilita los servicios HTTPS, NDMP y NDMPs. Si modifica esta política predeterminada o crea su propia política de firewall para las LIF de interconexión de clústeres, debe añadir cada dirección IP de la LIF entre clústeres a la lista permitida y habilitar el servicio HTTPS.

- A partir de ONTAP 9.6, los servicios de firewall HTTPS y SSH no son compatibles.

En ONTAP 9.6, el `management-https` y `management-ssh` Los servicios LIF están disponibles para el acceso de gestión HTTPS y SSH.

Pasos

1. Cree una política de firewall que estará disponible para las LIF en una SVM específica:

```
system services firewall policy create -vserver vservice_name -policy
policy_name -service network_service -allow-list ip_address/mask
```

Puede usar este comando varias veces para agregar más de un servicio de red y una lista de direcciones IP permitidas para cada servicio de la directiva de firewall.

2. Compruebe que la directiva se ha agregado correctamente utilizando `system services firewall policy show` comando.
3. Aplique la política de firewall a una LIF:

```
network interface modify -vserver vservice_name -lif lif_name -firewall-policy
policy_name
```

4. Compruebe que la política se ha añadido correctamente a la LIF mediante el `network interface show -fields firewall-policy` comando.

Ejemplo de creación de una política de firewall y su aplicación a una LIF

El siguiente comando crea una política de firewall llamada `data_http` que permite el acceso al protocolo HTTP y HTTPS desde direcciones IP de la subred 10.10, aplica esa política a la LIF llamada `data1` en la SVM `vs1` y, a continuación, muestra todas las políticas de firewall del clúster:

```
system services firewall policy create -vserver vs1 -policy data_http  
-service http - allow-list 10.10.0.0/16
```

```
system services firewall policy show
```

| Vserver | Policy | Service | Allowed |
|-----------|--------------|---------|--------------|
| ----- | ----- | ----- | ----- |
| cluster-1 | | | |
| | data | | |
| | | dns | 0.0.0.0/0 |
| | | ndmp | 0.0.0.0/0 |
| | | ndmps | 0.0.0.0/0 |
| cluster-1 | | | |
| | intercluster | | |
| | | https | 0.0.0.0/0 |
| | | ndmp | 0.0.0.0/0 |
| | | ndmps | 0.0.0.0/0 |
| cluster-1 | | | |
| | mgmt | | |
| | | dns | 0.0.0.0/0 |
| | | http | 0.0.0.0/0 |
| | | https | 0.0.0.0/0 |
| | | ndmp | 0.0.0.0/0 |
| | | ndmps | 0.0.0.0/0 |
| | | ntp | 0.0.0.0/0 |
| | | snmp | 0.0.0.0/0 |
| | | ssh | 0.0.0.0/0 |
| vs1 | | | |
| | data_http | | |
| | | http | 10.10.0.0/16 |
| | | https | 10.10.0.0/16 |

```
network interface modify -vserver vs1 -lif data1 -firewall-policy  
data_http
```

```
network interface show -fields firewall-policy
```

| vserver | lif | firewall-policy |
|-----------|--------------|-----------------|
| ----- | ----- | ----- |
| Cluster | node1_clus_1 | |
| Cluster | node1_clus_2 | |
| Cluster | node2_clus_1 | |
| Cluster | node2_clus_2 | |
| cluster-1 | cluster_mgmt | mgmt |
| cluster-1 | node1_mgmt1 | mgmt |
| cluster-1 | node2_mgmt1 | mgmt |
| vs1 | data1 | data_http |
| vs3 | data2 | data |

Comandos para administrar el servicio y las políticas de firewall

Puede utilizar el `system services firewall` comandos para administrar el servicio de firewall, el `system services firewall policy` comandos para administrar las directivas de firewall y la `network interface modify` Comando para administrar la configuración del firewall de las LIF.

| Si desea... | Se usa este comando... |
|--|---|
| Active o desactive el servicio de firewall | <code>system services firewall modify</code> |
| Muestra la configuración actual del servicio de firewall | <code>system services firewall show</code> |
| Cree una política de firewall o agregue un servicio a una política de firewall existente | <code>system services firewall policy create</code> |
| Aplique una política de firewall a una LIF | <code>network interface modify -lif lifname -firewall-policy</code> |
| Modifique las direcciones IP y las máscaras de red asociadas a una directiva de firewall | <code>system services firewall policy modify</code> |
| Mostrar información acerca de las políticas de firewall | <code>system services firewall policy show</code> |
| Cree una nueva directiva de firewall que sea una copia exacta de una directiva existente | <code>system services firewall policy clone</code> |
| Eliminar una política de firewall que no esté usando una LIF | <code>system services firewall policy delete</code> |

Para obtener más información, consulte las páginas de manual de `system services firewall`, `system services firewall policy`, y `network interface modify` comandos de ["Comandos de ONTAP 9"](#).

Marcado de QoS (solo para administradores de clústeres)

Información general de QoS

El marcado de calidad de servicio (QoS) de la red le ayuda a priorizar los diferentes tipos de tráfico según las condiciones de la red para utilizar eficazmente los recursos de la red. Puede establecer el valor de punto de código de servicios diferenciados (DSCP) de los paquetes IP salientes para los tipos de tráfico admitidos por espacio IP.

Marcado DSCP para el cumplimiento de las UC

Puede habilitar el marcado de punto de código de servicios diferenciados (DSCP) en el tráfico de paquetes IP saliente (de salida) para un protocolo determinado con un código DSCP predeterminado o proporcionado por el usuario. El marcado DSCP es un mecanismo para clasificar y gestionar el tráfico de red y es un

componente de la conformidad de Unified Capability (UC).

El marcado DSCP (también conocido como *QoS marking* o *quality of service marking*) se habilita al proporcionar un valor de espacio IP, protocolo y DSCP. Los protocolos en los que se puede aplicar la Marca DSCP son NFS, SMB, iSCSI, SnapMirror, NDMP, FTP, HTTP/HTTPS, SSH, Telnet y SNMP.

Si no se proporciona un valor DSCP al habilitar el marcado DSCP para un protocolo determinado, se utiliza un valor predeterminado:

- El valor predeterminado para el tráfico y los protocolos de datos es 0x0A (10).
- El valor predeterminado para el tráfico y los protocolos de control es 0x30 (48).

Modifique los valores de marcado de QoS

Puede modificar los valores de marcado de calidad de servicio (QoS) de diferentes protocolos en cada espacio IP.

Antes de empezar

Todos los nodos del clúster deben ejecutar la misma versión de ONTAP.

Paso

Modifique los valores de marcado de QoS mediante el `network qos-marking modify` comando.

- La `-ipspace` El parámetro especifica el espacio IP para el que se va a modificar la entrada de marcado de QoS.
- La `-protocol` El parámetro especifica el protocolo para el que se va a modificar la entrada de marcado de QoS. La `network qos-marking modify` la página man describe los posibles valores del protocolo.
- La `-dscp` Parámetro especifica el valor de punto de código de servicios diferenciados (DSCP). Los valores posibles van de 0 a 63.
- La `-is-enabled` El parámetro se utiliza para habilitar o deshabilitar el marcado de calidad de servicio del protocolo especificado en el espacio IP que proporciona el `-ipspace` parámetro.

El siguiente comando habilita el marcado de calidad de servicio del protocolo NFS en el espacio IP predeterminado:

```
network qos-marking modify -ipspace Default -protocol NFS -is-enabled true
```

El siguiente comando establece el valor de DSCP en 20 para el protocolo NFS en el espacio IP predeterminado:

```
network qos-marking modify -ipspace Default -protocol NFS -dscp 20
```

Mostrar los valores de marcado de QoS

Puede mostrar los valores de marcado de la calidad de servicio de los diferentes protocolos, en cada espacio IP.

Paso

Muestra los valores de marcado de QoS mediante `network qos-marking show` comando.

El siguiente comando muestra el marcado de calidad de servicio de todos los protocolos en el espacio IP predeterminado:

```
network qos-marking show -ip space Default
IPspace          Protocol          DSCP    Enabled?
-----
Default
                CIFS                10      false
                FTP                  48      false
                HTTP-admin           48      false
                HTTP-filesrv         10      false
                NDMP                 10      false
                NFS                  10      true
                SNMP                 48      false
                SSH                   48      false
                SnapMirror            10      false
                Telnet                48      false
                iSCSI                 10      false
11 entries were displayed.
```

Gestionar SNMP (solo administradores de clústeres)

Información general de SNMP

Puede configurar SNMP para supervisar las SVM del clúster a fin de evitar los problemas antes de que se produzcan y responder a los problemas si se producen. La gestión de SNMP implica configurar usuarios SNMP y destinos de host de capturas de SNMP (estaciones de trabajo de gestión) para todos los eventos SNMP. SNMP está deshabilitado de forma predeterminada en las LIF de datos.

En la SVM de datos, se pueden crear y gestionar usuarios SNMP solo de lectura. Los LIF de datos deben configurarse para recibir solicitudes SNMP en la SVM.

Las estaciones de trabajo de gestión de redes SNMP, o los administradores, pueden consultar al agente SNMP de SVM para obtener información. El agente SNMP recopila información y la reenvía a los administradores SNMP. El agente SNMP también genera notificaciones de capturas siempre que se produzcan eventos específicos. El agente SNMP de la SVM tiene privilegios de solo lectura; no se puede utilizar para ninguna operación definida ni para realizar una acción correctiva en respuesta a una captura. ONTAP proporciona un agente SNMP compatible con las versiones v1, v2c y v3 de SNMP. SNMPv3 ofrece seguridad avanzada mediante passphrases y cifrado.

Para obtener más información sobre la compatibilidad de SNMP en sistemas ONTAP, consulte ["TR-4220: Compatibilidad con SNMP en Data ONTAP"](#).

Información general de MIB

Un MIB (base de datos de información de gestión) es un archivo de texto que describe los objetos y las capturas SNMP.

Los MIB describen la estructura de los datos de gestión del sistema de almacenamiento y utilizan un espacio de nombres jerárquico que contiene identificadores de objeto (OIDs). Cada OID identifica una variable que se puede leer mediante SNMP.

Dado que los MIB no son archivos de configuración y ONTAP no lee estos archivos, la función SNMP no se ve afectada por los MIB. ONTAP proporciona el siguiente archivo MIB:

- Una MIB personalizada de NetApp (`netapp.mib`)

ONTAP admite MIB de IPv6 (RFC 2465), TCP (RFC 4022), UDP (RFC 4113) e ICMP (RFC 2466), que muestran datos de IPv4 e IPv6.

ONTAP también proporciona una referencia cruzada corta entre identificadores de objeto (OIDs) y nombres cortos de objeto en la `traps.dat` archivo.



Las versiones más recientes de los archivos ONTAP MIBs y "traps.dat" están disponibles en el sitio de soporte de NetApp. Sin embargo, las versiones de estos archivos en el sitio de soporte no corresponden necesariamente a las capacidades SNMP de su versión de ONTAP. Estos archivos se proporcionan para ayudarle a evaluar las funciones SNMP en la última versión de ONTAP.

Capturas SNMP

Las capturas SNMP capturan información de supervisión del sistema que se envía como una notificación asíncrona desde el agente SNMP al administrador SNMP.

Hay tres tipos de capturas SNMP: Estándar, integrado y definido por el usuario. ONTAP no admite capturas definidas por el usuario.

Una captura se puede utilizar para comprobar periódicamente si existen umbrales o errores operativos definidos en el MIB. Si se alcanza un umbral o se detecta un fallo, el agente SNMP envía un mensaje (captura) a los hosts de capturas para alertarlos del evento.



ONTAP es compatible con las trampas SNMPv1 y, a partir de las trampas ONTAP 9.1 y SNMPv3. ONTAP no admite capturas SNMPv2c ni informa.

Capturas SNMP estándar

Estos solapamientos se definen en RFC 1215. Hay cinco capturas SNMP estándar que son compatibles con ONTAP: Coldstart, warwStart, linkdown, linkup y authenticationFailure.



La captura de autenticación por fallo está deshabilitada de forma predeterminada. Debe utilizar el `system snmp authtrap` comando para habilitar la captura. Para obtener más información, consulte las páginas de manual: ["Comandos de ONTAP 9"](#)

Capturas SNMP integradas

Las capturas integradas están predefinidas en ONTAP y se envían automáticamente a las estaciones de

administración de red en la lista de capturas si se produce un evento. Estas capturas, como `diskFailedShutdown`, `cpuTooBusy` y `volumeNearlyFull`, se definen en la MIB personalizada.

Cada captura integrada se identifica mediante un código de captura único.

Cree una comunidad SNMP y asígnela a una LIF

Es posible crear una comunidad SNMP que actúa como mecanismo de autenticación entre la estación de gestión y la máquina virtual de almacenamiento (SVM) cuando se usa SNMPv1 y SNMPv2c.

Al crear comunidades SNMP en una SVM de datos, puede ejecutar comandos como `snmpwalk` y `snmpget` en las LIF de datos.

Acerca de esta tarea

- En las nuevas instalaciones de ONTAP, SNMPv1 y SNMPv2c se desactivan de forma predeterminada.

Se habilitan SNMPv1 y SNMPv2c después de crear una comunidad SNMP.

- ONTAP admite comunidades de solo lectura.
- De forma predeterminada, la política de firewall "datos" asignada a las LIF de datos tiene el servicio SNMP establecido en `deny`.

Debe crear una nueva política de firewall con el servicio SNMP establecido en `allow` Cuando se crea un usuario SNMP para una SVM de datos.



A partir de ONTAP 9.10.1, las políticas de firewall están obsoletas y sustituidas por completo por políticas de servicios LIF. Para obtener más información, consulte ["Configurar políticas de firewall para LIF"](#).

- Es posible crear comunidades SNMP para los usuarios de SNMPv1 y SNMPv2c para la SVM admin y la SVM de datos.
- Puesto que una SVM no forma parte del estándar SNMP, las consultas sobre los LIF de datos deben incluir el OID raíz de NetApp (1.3.6.1.4.1.789), por ejemplo, `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`.

Pasos

1. Cree una comunidad SNMP mediante el `system snmp community add` comando. El siguiente comando muestra cómo crear una comunidad SNMP en la SVM de administrador cluster-1:

```
system snmp community add -type ro -community-name comty1 -vserver cluster-1
```

El siguiente comando muestra cómo crear una comunidad SNMP en la SVM de datos vs1:

```
system snmp community add -type ro -community-name comty2 -vserver vs1
```

2. Verifique que se hayan creado las comunidades mediante el comando `System snmp Community show`.

El siguiente comando muestra las dos comunidades creadas para SNMPv1 y SNMPv2c:

```
system snmp community show
cluster-1
rocomty1
vs1
rocomty2
```

3. Compruebe si se permite SNMP como un servicio en la política de firewall de "datos" mediante el `system services firewall policy show` comando.

El siguiente comando muestra que el servicio snmp no está permitido en la política de firewall predeterminada "data" (el servicio snmp se permite únicamente en la política de firewall "mgmt"):

```
system services firewall policy show
Vserver Policy      Service      Allowed
-----
cluster-1
  data
    dns          0.0.0.0/0
    ndmp         0.0.0.0/0
    ndmps        0.0.0.0/0
cluster-1
  intercluster
    https        0.0.0.0/0
    ndmp         0.0.0.0/0
    ndmps        0.0.0.0/0
cluster-1
  mgmt
    dns          0.0.0.0/0
    http         0.0.0.0/0
    https        0.0.0.0/0
    ndmp         0.0.0.0/0
    ndmps        0.0.0.0/0
    ntp          0.0.0.0/0
    snmp         0.0.0.0/0
    ssh          0.0.0.0/0
```

4. Cree una nueva directiva de firewall que permita el acceso mediante snmp servicio mediante el `system services firewall policy create` comando.

Los siguientes comandos crean una nueva política de firewall de datos denominada "data1" que permite el snmp

```
system services firewall policy create -policy data1 -service snmp
-vserver vs1 -allow-list 0.0.0.0/0
```

```
cluster-1::> system services firewall policy show -service snmp
```

| Vserver | Policy | Service | Allowed |
|-----------|--------|---------|-----------|
| ----- | | | |
| cluster-1 | | | |
| | mgmt | | |
| | | snmp | 0.0.0.0/0 |
| vs1 | | | |
| | data1 | | |
| | | snmp | 0.0.0.0/0 |

5. Aplicar la política de firewall a una LIF de datos mediante el comando "Network interface modify" con el parámetro -firewall-policy.

El siguiente comando asigna la nueva política de firewall "data1" a la LIF "datalif1":

```
network interface modify -vserver vs1 -lif datalif1 -firewall-policy
data1
```

Configure los usuarios de SNMPv3 en un clúster

SNMPv3 es un protocolo seguro en comparación con SNMPv1 y SNMPv2c. Para utilizar SNMPv3, debe configurar un usuario SNMPv3 para ejecutar las utilidades SNMP desde el administrador SNMP.

Paso

Utilice el "Security login create command" para crear un usuario SNMPv3.

Se le pedirá que introduzca la siguiente información:

- ID del motor: El valor predeterminado y recomendado es ID del motor local
- Protocolo de autenticación
- Contraseña de autenticación
- Protocolo de privacidad
- Contraseña del protocolo de privacidad

Resultado

El usuario SNMPv3 puede iniciar sesión desde el administrador SNMP mediante el nombre de usuario y la contraseña y ejecutar los comandos de la utilidad SNMP.

Parámetros de seguridad SNMPv3

SNMPv3 incluye una función de autenticación que, cuando se selecciona, requiere que los usuarios escriban

sus nombres, un protocolo de autenticación, una clave de autenticación y el nivel de seguridad deseado al invocar un comando.

En la siguiente tabla se enumeran los parámetros de seguridad de SNMPv3 :

| Parámetro | Opción de línea de comandos | Descripción |
|--|---|---|
| ID de motor | -E Ingeniería | ID de motor del agente SNMP. El valor predeterminado es EngineID local (recomendado). |
| SecurityName | -U Nombre | El nombre de usuario no debe superar los 32 caracteres. |
| Protocolo de autenticación | -A {none | MD5 |
| SHA | SHA-256} | El tipo de autenticación puede ser none, MD5, SHA o SHA-256. |
| Clave de autenticación | -UNA FRASE DE PASO | Frase de contraseña con un mínimo de ocho caracteres. |
| Nivel de seguridad | -L {authNoprivilegios | authpriv |
| noAuthprivilegios} | El nivel de seguridad puede ser autenticación, sin privacidad, autenticación, privacidad o sin autenticación, Sin privacidad. | PrivProtocol |
| -x { none | des | aes128} |
| El protocolo de privacidad puede ser none, des o aes 128 | PrivPassword | -X contraseña |

Ejemplos de diferentes niveles de seguridad

En este ejemplo se muestra cómo un usuario SNMPv3 creado con diferentes niveles de seguridad puede utilizar los comandos del cliente SNMP, como `snmpwalk`, para consultar los objetos del clúster.

Para obtener un mejor rendimiento, debe recuperar todos los objetos de una tabla en lugar de un solo objeto o algunos objetos de la tabla.



Debe usar `snmpwalk` 5.3.1 o posterior cuando el protocolo de autenticación es SHA.

Nivel de seguridad: Authpriv

El siguiente resultado muestra la creación de un usuario SNMPv3 con el nivel de seguridad authpriv.

```
security login create -user-or-group-name snmpv3user -application snmp
-authentication-method usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha, sha2-
256) [none]: md5

Enter the authentication protocol password (minimum 8 characters long):
Enter the authentication protocol password again:
Which privacy protocol do you want to choose (none, des, aes128) [none]:
des
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

Modo FIPS

```
security login create -username snmpv3user -application snmp -authmethod
usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (sha, sha2-256) [sha]

Enter authentication protocol password (minimum 8 characters long):
Enter authentication protocol password again:
Which privacy protocol do you want to choose (aes128) [aes128]:
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

Prueba snmpwalk

El siguiente resultado muestra al usuario SNMPv3 que ejecuta el comando snmpwalk:

Para obtener un mejor rendimiento, debe recuperar todos los objetos de una tabla en lugar de un solo objeto o algunos objetos de la tabla.

```
$ snmpwalk -v 3 -u snmpv3user -a SHA -A password1! -x DES -X password1! -l
authPriv 192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

Nivel de seguridad: AuthNoprivilegios

El siguiente resultado muestra la creación de un usuario SNMPv3 con el nivel de seguridad authNoprivilegios.

```
security login create -username snmpv3user1 -application snmp -authmethod
usm -role admin
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: md5
```

Modo FIPS

FIPS no le permite elegir **none** para el protocolo de privacidad. Como resultado, no es posible configurar un usuario authNoPriv SNMPv3 en modo FIPS.

Prueba snmpwalk

El siguiente resultado muestra al usuario SNMPv3 que ejecuta el comando snmpwalk:

Para obtener un mejor rendimiento, debe recuperar todos los objetos de una tabla en lugar de un solo objeto o algunos objetos de la tabla.

```
$ snmpwalk -v 3 -u snmpv3user1 -a MD5 -A password1! -l authNoPriv
192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

Nivel de seguridad: NoAuthNoprivilegios

El siguiente resultado muestra la creación de un usuario SNMPv3 con el nivel de seguridad noAuthNoprivilegios.

```
security login create -username snmpv3user2 -application snmp -authmethod
usm -role admin
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: none
```

Modo FIPS

FIPS no le permite elegir **none** para el protocolo de privacidad.

Prueba snmpwalk

El siguiente resultado muestra al usuario SNMPv3 que ejecuta el comando snmpwalk:

Para obtener un mejor rendimiento, debe recuperar todos los objetos de una tabla en lugar de un solo objeto o algunos objetos de la tabla.

```
$ snmpwalk -v 3 -u snmpv3user2 -l noAuthNoPriv 192.0.2.62
.1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

Configurar los hosts de capturas para recibir notificaciones SNMP

Puede configurar el host de capturas (administrador SNMP) para recibir notificaciones (PDU de captura SNMP) cuando se generan capturas SNMP en el clúster. Es posible especificar el nombre de host o la dirección IP (IPv4 o IPv6) del host de capturas de SNMP.

Antes de empezar

- Se debe habilitar SNMP y las capturas de SNMP en el clúster.



SNMP y las capturas de SNMP se habilitan de forma predeterminada.

- El DNS debe haberse configurado en el clúster para resolver los nombres de host de capturas.
- IPv6 debe estar habilitado en el clúster para configurar los hosts de capturas de SNMP mediante direcciones IPv6.
- Para ONTAP 9.1 y versiones posteriores, debe haber especificado la autenticación de un modelo de seguridad basado en usuario (USM) predefinido y las credenciales de privacidad al crear hosts de capturas.

Paso

Añada un host de capturas de SNMP:

```
system snmp traphost add
```



Las capturas solo se pueden enviar cuando se especifica al menos una estación de administración SNMP como un host de capturas.

El siguiente comando añade un nuevo host de capturas SNMPv3 llamado yyy.example.com con un usuario USM conocido:

```
system snmp traphost add -peer-address yyy.example.com -usm-username
MyUsmUser
```

El siguiente comando añade un host de capturas mediante la dirección IPv6 del host:

```
system snmp traphost add -peer-address 2001:0db8:1:1:209:6bff:feae:6d67
```

Comandos para gestionar SNMP

Puede utilizar el `system snmp` Comandos para gestionar SNMP, capturas y hosts de capturas. Puede utilizar el `security` Comandos para gestionar usuarios SNMP por SVM. Puede utilizar el `event` Comandos para gestionar eventos relacionados con capturas SNMP.

Comandos para configurar SNMP

| Si desea... | Se usa este comando... |
|--------------------------------|---|
| Habilite SNMP en el clúster | <pre>options -option-name snmp.enable -option-value on</pre> <p>Se debe permitir el servicio SNMP bajo la política del firewall de gestión (gestión). Puede verificar si se permite SNMP mediante el comando <code>system Services firewall policy show</code>.</p> |
| Deshabilite SNMP en el clúster | <pre>options -option-name snmp.enable -option-value off</pre> |

Comandos para gestionar usuarios de SNMP v1, v2c y v3

| Si desea... | Se usa este comando... |
|---|---|
| Configurar usuarios SNMP | <pre>security login create</pre> |
| Mostrar usuarios SNMP | <pre>security snmpusers and security login show -application snmp</pre> |
| Eliminar usuarios SNMP | <pre>security login delete</pre> |
| Modifique el nombre de rol de control de acceso de un método de inicio de sesión para los usuarios SNMP | <pre>security login modify</pre> |

Comandos para proporcionar información de contacto y ubicación

| Si desea... | Se usa este comando... |
|--|-----------------------------------|
| Mostrar o modificar los detalles de contacto del clúster | <code>system snmp contact</code> |
| Muestra o modifica los detalles de ubicación del clúster | <code>system snmp location</code> |

Comandos para gestionar comunidades SNMP

| Si desea... | Se usa este comando... |
|--|---|
| Añada una comunidad de solo lectura (ro) para una SVM o para todas las SVM del clúster | <code>system snmp community add</code> |
| Elimine una comunidad o todas las comunidades | <code>system snmp community delete</code> |
| Mostrar la lista de todas las comunidades | <code>system snmp community show</code> |

Dado que las SVM no forman parte del estándar SNMP, las consultas sobre los LIF de datos deben incluir el OID raíz de NetApp (1.3.6.1.4.1.789), por ejemplo, `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`.

Comando para mostrar valores de opciones de SNMP

| Si desea... | Se usa este comando... |
|---|-------------------------------|
| Mostrar los valores actuales de todas las opciones de SNMP, incluido el contacto del clúster, la ubicación de contacto, si el clúster está configurado para enviar capturas, la lista de hosts de capturas y la lista de comunidades y el tipo de control de acceso | <code>system snmp show</code> |

Comandos para gestionar las capturas y los hosts de capturas de SNMP

| Si desea... | Se usa este comando... |
|---|---------------------------------------|
| Habilite las capturas de SNMP que se envían desde el clúster | <code>system snmp init -init 1</code> |
| Deshabilite las capturas de SNMP enviadas desde el clúster | <code>system snmp init -init 0</code> |
| Añada un host de capturas que reciba notificaciones SNMP para eventos específicos en el clúster | <code>system snmp traphost add</code> |

| | |
|---------------------------------------|--|
| Eliminar un host de capturas | <code>system snmp traphost delete</code> |
| Mostrar la lista de hosts de capturas | <code>system snmp traphost show</code> |

Comandos para gestionar eventos relacionados con capturas SNMP

| Si desea... | Se usa este comando... |
|---|---|
| Mostrar los eventos para los que se generan capturas SNMP (integradas) | <code>event route show</code> Utilice la <code>-snmp-support true</code> Parámetro para ver únicamente eventos relacionados con SNMP. Utilice la <code>instance -messagename <message></code> parámetro para ver una descripción detallada por qué podría haber ocurrido un evento y cualquier acción correctiva. No se admite el enrutamiento de eventos de captura SNMP individuales a destinos de host de capturas específicos. Todos los eventos de captura SNMP se envían a todos los destinos de host de capturas. |
| Mostrar una lista de registros del historial de capturas SNMP, que son notificaciones de eventos que se han enviado a capturas SNMP | <code>event snmphistory show</code> |
| Elimine un registro del historial de capturas SNMP | <code>event snmphistory delete</code> |

Para obtener más información acerca de `system snmp`, `security`, y `event` consulte las páginas de manual: ["Comandos de ONTAP 9"](#)

Gestione el enrutamiento en una SVM

Información general sobre el enrutamiento de SVM

La tabla de enrutamiento de una SVM determina la ruta de red que la SVM utiliza para comunicarse con un destino. Es importante comprender cómo funcionan las tablas de enrutamiento para evitar problemas de red antes de que ocurran.

Las reglas de enrutamiento son las siguientes:

- ONTAP enruta el tráfico por la ruta disponible más específica.
- ONTAP enruta el tráfico por una ruta de puerta de enlace predeterminada (con 0 bits de máscara de red) como último recurso, cuando no hay más rutas específicas disponibles.

En el caso de rutas con el mismo destino, máscara de red y métrica, no hay garantía de que el sistema utilice la misma ruta después de un reinicio o después de una actualización. Esto es especialmente un problema si

ha configurado varias rutas predeterminadas.

Se recomienda configurar una ruta predeterminada solo para una SVM. Para evitar interrupciones, debe asegurarse de que la ruta predeterminada pueda llegar a cualquier dirección de red a la que no se pueda acceder mediante una ruta más específica. Para obtener más información, consulte el artículo de la base de conocimientos ["SU134: El acceso a la red puede verse interrumpido por una configuración de enrutamiento incorrecta en Clustered ONTAP"](#)

Cree una ruta estática

Puede crear rutas estáticas dentro de una máquina virtual de almacenamiento (SVM) para controlar cómo usan las LIF la red para el tráfico de salida.

Cuando se crea una entrada de ruta asociada a una SVM, todas las LIF son propiedad de la SVM especificada y que se encuentran en la misma subred que la puerta de enlace usarán.

Paso

Utilice la `network route create` comando para crear una ruta.

```
network route create -vserver vs0 -destination 0.0.0.0/0 -gateway
10.61.208.1
```

Habilite el enrutamiento multivía

Si varias rutas tienen la misma métrica para un destino, sólo se selecciona una de las rutas para el tráfico saliente. Esto lleva a que otras rutas no se utilicen para enviar tráfico saliente. Puede habilitar el enrutamiento multivía para equilibrar la carga y utilizar todas las rutas disponibles.

Pasos

1. Inicie sesión en el nivel de privilegio avanzado:

```
set -privilege advanced
```

2. Habilitar enrutamiento multivía:

```
network options multipath-routing modify -is-enabled true
```

El enrutamiento multivía está habilitado para todos los nodos del clúster.

```
network options multipath-routing modify -is-enabled true
```

Eliminar una ruta estática

Es posible eliminar una ruta estática innecesaria de una máquina virtual de almacenamiento (SVM).

Paso

Utilice la `network route delete` comando para eliminar una ruta estática.

Para obtener más información acerca de este comando, consulte `network route` página de manual: ["Comandos de ONTAP 9"](#).

En el ejemplo siguiente se elimina una ruta estática asociada a SVM vs0 con una puerta de enlace 10.63.0.1 y una dirección IP de destino 0.0.0.0/0:

```
network route delete -vserver vs0 -gateway 10.63.0.1 -destination
0.0.0.0/0
```

Mostrar información de ruta

Puede ver información sobre la configuración de enrutamiento de cada SVM del clúster. Esto puede ayudarle a diagnosticar problemas de enrutamiento relacionados con problemas de conectividad entre aplicaciones o servicios de cliente y una LIF en un nodo del clúster.

Pasos

1. Utilice la `network route show` Comando para mostrar las rutas dentro de una o varias SVM. En el siguiente ejemplo, se muestra una ruta configurada en la SVM vs0:

```
network route show
(network route show)
Vserver          Destination      Gateway          Metric
-----
vs0
                0.0.0.0/0       172.17.178.1    20
```

2. Utilice la `network route show-lifs` Comando para mostrar la asociación de las rutas y las LIF dentro de una o varias SVM.

En el ejemplo siguiente se muestran las LIF con rutas propiedad de la SVM vs0:

```
network route show-lifs
(network route show-lifs)

Vserver: vs0
Destination      Gateway          Logical Interfaces
-----
0.0.0.0/0        172.17.178.1    cluster_mgmt,
LIF-b-01_mgmt1,
LIF-b-02_mgmt1
```

3. Utilice la `network route active-entry show` Comando para mostrar las rutas instaladas en uno o más nodos, SVM, subredes o rutas con destinos especificados.

En el siguiente ejemplo, se muestran todas las rutas instaladas en una SVM específica:

```
network route active-entry show -vserver Data0
```

```
Vserver: Data0
```

```
Node: node-1
```

```
Subnet Group: 0.0.0.0/0
```

| Destination | Gateway | Interface | Metric | Flags |
|-------------|------------|-----------|--------|-------|
| 127.0.0.1 | 127.0.0.1 | lo | 10 | UHS |
| 127.0.10.1 | 127.0.20.1 | losk | 10 | UHS |
| 127.0.20.1 | 127.0.20.1 | losk | 10 | UHS |

```
Vserver: Data0
```

```
Node: node-1
```

```
Subnet Group: fd20:8b1e:b255:814e::/64
```

| Destination | Gateway | Interface | Metric | Flags |
|--------------------------|------------------------|-----------|--------|-------|
| default | fd20:8b1e:b255:814e::1 | e0d | 20 | UGS |
| fd20:8b1e:b255:814e::/64 | link#4 | e0d | 0 | UC |

```
Vserver: Data0
```

```
Node: node-2
```

```
Subnet Group: 0.0.0.0/0
```

| Destination | Gateway | Interface | Metric | Flags |
|-------------|-----------|-----------|--------|-------|
| 127.0.0.1 | 127.0.0.1 | lo | 10 | UHS |

```
Vserver: Data0
```

```
Node: node-2
```

```
Subnet Group: 0.0.0.0/0
```

| Destination | Gateway | Interface | Metric | Flags |
|-------------|------------|-----------|--------|-------|
| 127.0.10.1 | 127.0.20.1 | losk | 10 | UHS |
| 127.0.20.1 | 127.0.20.1 | losk | 10 | UHS |

```
Vserver: Data0
```

```
Node: node-2
```

```
Subnet Group: fd20:8b1e:b255:814e::/64
```

| Destination | Gateway | Interface | Metric | Flags |
|-------------|---------|-----------|--------|-------|
|-------------|---------|-----------|--------|-------|

```

default          fd20:8b1e:b255:814e::1
                                e0d          20    UGS
fd20:8b1e:b255:814e::/64
                                link#4      e0d          0    UC
fd20:8b1e:b255:814e::1  link#4      e0d          0    UHL
11 entries were displayed.

```

Quitar rutas dinámicas de las tablas de enrutamiento

Cuando se reciben redirecciones ICMP para IPv4 e IPv6, se agregan rutas dinámicas a la tabla de enrutamiento. De forma predeterminada, las rutas dinámicas se eliminan tras 300 segundos. Si desea mantener rutas dinámicas durante un período de tiempo diferente, puede cambiar el valor de tiempo de espera.

Acerca de esta tarea

Puede ajustar el valor del tiempo de espera de 0 a 65,535 segundos. Si establece el valor en 0, las rutas nunca caducan. La eliminación de rutas dinámicas evita la pérdida de conectividad causada por la persistencia de rutas no válidas.

Pasos

1. Muestra el valor de tiempo de espera actual.

- Para IPv4:

```
network tuning icmp show
```

- Para IPv6:

```
network tuning icmp6 show
```

2. Modifique el valor del tiempo de espera.

- Para IPv4:

```
network tuning icmp modify -node node_name -redirect-timeout
timeout_value
```

- Para IPv6:

```
network tuning icmp6 modify -node node_name -redirect-v6-timeout
timeout_value
```

3. Compruebe que el valor del tiempo de espera se ha modificado correctamente.

- Para IPv4:

```
network tuning icmp show
```

- Para IPv6:

```
network tuning icmp6 show
```

Ver información de red

Ver información general de la red

Mediante la CLI, puede ver información relacionada con los puertos, las LIF, las rutas, las reglas de conmutación por error, los grupos de conmutación por error, reglas de firewall, DNS, NIS y conexiones. A partir de ONTAP 9.8, también puede descargar los datos que se muestran en System Manager sobre su red.

Esta información puede ser útil en situaciones como volver a configurar la configuración de red o al solucionar problemas del clúster.

Si es un administrador de clúster, puede ver toda la información de redes disponible. Si es un administrador de SVM, puede ver solo la información relacionada con las SVM que tiene asignadas.

En System Manager, cuando se muestra información en una *Vista de lista*, puede hacer clic en **Descargar** y se descarga la lista de objetos que se muestra.

- La lista se descarga en formato de valores separados por comas (CSV).
- Sólo se descargan los datos de las columnas visibles.
- El nombre de archivo CSV tiene formato con el nombre del objeto y una Marca de hora.

Muestra información del puerto de red

Puede ver información sobre un puerto específico o acerca de todos los puertos de todos los nodos del clúster.

Acerca de esta tarea

Se muestra la siguiente información:

- Nombre del nodo
- Nombre de puerto
- Nombre del espacio IP
- Nombre de dominio de retransmisión
- Estado del enlace (activo o inactivo)
- Configuración de MTU
- Configuración de velocidad del puerto y estado operativo (1 Gigabit o 10 gigabits por segundo)

- Configuración de negociación automática (verdadero o falso)
- Modo doble y estado operativo (mitad o completo)
- El grupo de interfaces del puerto, si corresponde
- La información de etiqueta de VLAN del puerto, si corresponde
- Estado del puerto (estado o degradado)
- Motivos para que un puerto se marque como degradado

Si los datos de un campo no están disponibles (por ejemplo, la dúplex operativa y la velocidad de un puerto inactivo no están disponibles), el valor del campo se muestra como -.

Paso

Muestra información del puerto de red mediante el `network port show` comando.

Puede mostrar información detallada de cada puerto especificando el `-instance` parámetro o obtenga información específica especificando nombres de campo mediante el `-fields` parámetro.


```
network port show
```

```
Node: node1
```

```
Ignore
```

| | | | | | | Speed(Mbps) | Health |
|--------|---------|-----------|--------|------|------|-------------|----------|
| Health | | | | | | | |
| Port | IPspace | Broadcast | Domain | Link | MTU | Admin/Oper | Status |
| Status | | | | | | | |
| ----- | ----- | ----- | ---- | ---- | ---- | ----- | ----- |
| ----- | | | | | | | |
| e0a | Cluster | Cluster | | up | 9000 | auto/1000 | healthy |
| false | | | | | | | |
| e0b | Cluster | Cluster | | up | 9000 | auto/1000 | healthy |
| false | | | | | | | |
| e0c | Default | Default | | up | 1500 | auto/1000 | degraded |
| false | | | | | | | |
| e0d | Default | Default | | up | 1500 | auto/1000 | degraded |
| true | | | | | | | |

```
Node: node2
```

```
Ignore
```

| | | | | | | Speed(Mbps) | Health |
|--------|---------|-----------|--------|------|------|-------------|---------|
| Health | | | | | | | |
| Port | IPspace | Broadcast | Domain | Link | MTU | Admin/Oper | Status |
| Status | | | | | | | |
| ----- | ----- | ----- | ---- | ---- | ---- | ----- | ----- |
| ----- | | | | | | | |
| e0a | Cluster | Cluster | | up | 9000 | auto/1000 | healthy |
| false | | | | | | | |
| e0b | Cluster | Cluster | | up | 9000 | auto/1000 | healthy |
| false | | | | | | | |
| e0c | Default | Default | | up | 1500 | auto/1000 | healthy |
| false | | | | | | | |
| e0d | Default | Default | | up | 1500 | auto/1000 | healthy |
| false | | | | | | | |

```
8 entries were displayed.
```

Mostrar información sobre una VLAN (solo administradores de clúster)

Puede ver información sobre una VLAN específica o sobre todas las VLAN del clúster.

Acerca de esta tarea

Puede mostrar información detallada de cada VLAN especificando el `-instance` parámetro. Puede mostrar información específica especificando los nombres de campo mediante el `-fields` parámetro.

Paso

Muestra información acerca de las VLAN mediante `network port vlan show` comando. El siguiente comando muestra información sobre todas las VLAN del clúster:

```
network port vlan show
```

| Node | VLAN Name | Port | Network VLAN ID | Network MAC Address |
|--------------|-----------|------|--------------------|------------------------|
| cluster-1-01 | | | | |
| | a0a-10 | a0a | 10 | 02:a0:98:06:10:b2 |
| | a0a-20 | a0a | 20 | 02:a0:98:06:10:b2 |
| | a0a-30 | a0a | 30 | 02:a0:98:06:10:b2 |
| | a0a-40 | a0a | 40 | 02:a0:98:06:10:b2 |
| | a0a-50 | a0a | 50 | 02:a0:98:06:10:b2 |
| cluster-1-02 | | | | |
| | a0a-10 | a0a | 10 | 02:a0:98:06:10:ca |
| | a0a-20 | a0a | 20 | 02:a0:98:06:10:ca |
| | a0a-30 | a0a | 30 | 02:a0:98:06:10:ca |
| | a0a-40 | a0a | 40 | 02:a0:98:06:10:ca |
| | a0a-50 | a0a | 50 | 02:a0:98:06:10:ca |

Mostrar información del grupo de interfaces (solo administradores de clúster)

Puede mostrar información sobre un grupo de interfaces para determinar su configuración.

Acerca de esta tarea

Se muestra la siguiente información:

- Nodo en el que está ubicado el grupo de interfaces
- Lista de puertos de red que se incluyen en el grupo de interfaces
- Nombre del grupo de interfaces
- Función de distribución (MAC, IP, puerto o secuencial)
- La dirección Media Access Control (MAC) del grupo de interfaces
- Estado de la actividad portuaria; es decir, si todos los puertos agregados están activos (participación completa), si algunos están activos (participación parcial) o si ninguno está activo

Paso

Se muestra información sobre los grupos de interfaces mediante el `network port ifgrp show` comando.

Puede mostrar información detallada de cada nodo especificando el `-instance` parámetro. Puede mostrar información específica especificando los nombres de campo mediante el `-fields` parámetro.

El siguiente comando muestra información sobre todos los grupos de interfaces del clúster:

```

network port ifgrp show

```

| Node | Port IfGrp | Distribution Function | MAC Address | Active Ports | Ports |
|--------------|---------------|--------------------------|-------------------|-----------------|----------|
| cluster-1-01 | a0a | ip | 02:a0:98:06:10:b2 | full | e7a, e7b |
| cluster-1-02 | a0a | sequential | 02:a0:98:06:10:ca | full | e7a, e7b |
| cluster-1-03 | a0a | port | 02:a0:98:08:5b:66 | full | e7a, e7b |
| cluster-1-04 | a0a | mac | 02:a0:98:08:61:4e | full | e7a, e7b |

El siguiente comando muestra información detallada del grupo de interfaces de un solo nodo:

```

network port ifgrp show -instance -node cluster-1-01

Node: cluster-1-01
Interface Group Name: a0a
Distribution Function: ip
Create Policy: multimode
MAC Address: 02:a0:98:06:10:b2
Port Participation: full
Network Ports: e7a, e7b
Up Ports: e7a, e7b
Down Ports: -

```

Mostrar la información de LIF

Puede ver información detallada sobre una LIF para determinar su configuración.

También puede que desee ver esta información para diagnosticar problemas básicos de LIF, como la comprobación de direcciones IP duplicadas o la comprobación de si el puerto de red pertenece a la subred correcta. Los administradores de máquinas virtuales de almacenamiento (SVM) solo pueden ver la información acerca de las LIF asociadas con la SVM.

Acerca de esta tarea

Se muestra la siguiente información:

- La dirección IP asociada con la LIF
- Estado administrativo de la LIF
- Estado operativo de la LIF

El estado operativo de los LIF de datos viene determinado por el estado de la SVM con la que están asociadas los LIF de datos. Cuando se detiene la SVM, el estado operativo de la LIF cambia a inactivo. Cuando se inicia de nuevo la SVM, el estado operativo cambia a up

- Y el puerto en el que reside el LIF

Si los datos de un campo no están disponibles (por ejemplo, si no hay información de estado ampliada), el valor del campo se muestra como –.

Paso

Muestra la información de la LIF mediante el comando `network interface show`.

Puede ver la información detallada de cada LIF especificando el parámetro `-instance` o obtener información específica especificando nombres de campo con el parámetro `-fields`.

El siguiente comando muestra información general acerca de todas las LIF de un clúster:

network interface show

| Vserver | Logical Interface | Status Admin/Oper | Network Address/Mask | Current Node | Current Is Port |
|---------|-------------------|-------------------|----------------------|--------------|-----------------|
| Home | | | | | |
| ----- | ----- | ----- | ----- | ----- | ----- |
| example | | | | | |
| | lif1 | up/up | 192.0.2.129/22 | node-01 | e0d |
| false | | | | | |
| node | cluster_mgmt | up/up | 192.0.2.3/20 | node-02 | e0c |
| false | | | | | |
| node-01 | clus1 | up/up | 192.0.2.65/18 | node-01 | e0a |
| true | | | | | |
| | clus2 | up/up | 192.0.2.66/18 | node-01 | e0b |
| true | | | | | |
| | mgmt1 | up/up | 192.0.2.1/20 | node-01 | e0c |
| true | | | | | |
| node-02 | clus1 | up/up | 192.0.2.67/18 | node-02 | e0a |
| true | | | | | |
| | clus2 | up/up | 192.0.2.68/18 | node-02 | e0b |
| true | | | | | |
| | mgmt2 | up/up | 192.0.2.2/20 | node-02 | e0d |
| true | | | | | |
| vs1 | d1 | up/up | 192.0.2.130/21 | node-01 | e0d |
| false | | | | | |
| | d2 | up/up | 192.0.2.131/21 | node-01 | e0d |
| true | | | | | |
| | data3 | up/up | 192.0.2.132/20 | node-02 | e0c |
| true | | | | | |

El siguiente comando muestra información detallada sobre una única LIF:

```
network interface show -lif data1 -instance

Vserver Name: vs1
Logical Interface Name: data1
Role: data
Data Protocol: nfs,cifs
Home Node: node-01
Home Port: e0c
Current Node: node-03
Current Port: e0c
Operational Status: up
Extended Status: -
Is Home: false
Network Address: 192.0.2.128
Netmask: 255.255.192.0
Bits in the Netmask: 18
IPv4 Link Local: -
Subnet Name: -
Administrative Status: up
Failover Policy: local-only
Firewall Policy: data
Auto Revert: false
Fully Qualified DNS Zone Name: xxx.example.com
DNS Query Listen Enable: false
Failover Group Name: Default
FCP WWPN: -
Address family: ipv4
Comment: -
IPspace of LIF: Default
```

Mostrar información de ruta

Puede mostrar información sobre las rutas dentro de una SVM.

Paso

En función del tipo de información de enrutamiento que desee ver, introduzca el comando correspondiente:

| Para ver información acerca de... | Introduzca... |
|-----------------------------------|-------------------------|
| Rutas estáticas, por SVM | network route show |
| LIF en cada ruta, por SVM | network route show-lifs |

Puede mostrar información detallada de cada ruta especificando el `-instance` parámetro. El siguiente comando muestra las rutas estáticas dentro de las SVM en cluster- 1:

```
network route show
Vserver          Destination      Gateway          Metric
-----
Cluster
0.0.0.0/0        10.63.0.1       10
cluster-1
0.0.0.0/0        198.51.9.1      10
vs1
0.0.0.0/0        192.0.2.1       20
vs3
0.0.0.0/0        192.0.2.1       20
```

El siguiente comando muestra la asociación de rutas estáticas e interfaces lógicas (LIF) dentro de todas las SVM del clúster-1:

```
network route show-lifs
Vserver: Cluster
Destination      Gateway          Logical Interfaces
-----
0.0.0.0/0        10.63.0.1       -

Vserver: cluster-1
Destination      Gateway          Logical Interfaces
-----
0.0.0.0/0        198.51.9.1      cluster_mgmt,
cluster-1_mgmt1,

Vserver: vs1
Destination      Gateway          Logical Interfaces
-----
0.0.0.0/0        192.0.2.1       data1_1, data1_2

Vserver: vs3
Destination      Gateway          Logical Interfaces
-----
0.0.0.0/0        192.0.2.1       data2_1, data2_2
```

Mostrar entradas de la tabla de hosts DNS (solo administradores de clúster)

Las entradas de la tabla de hosts DNS asignan nombres de host a direcciones IP. Puede mostrar los nombres de host y los nombres de alias, y la dirección IP a la que se asignan para todas las SVM de un clúster.

Paso

Visualice las entradas de nombre de host de todas las SVM mediante el comando `vserver Services NAME-service dns hosts show`.

En el ejemplo siguiente se muestran las entradas de la tabla de hosts:

```
vserver services name-service dns hosts show
Vserver      Address      Hostname      Aliases
-----
cluster-1
10.72.219.36  lnx219-36    -
vs1
10.72.219.37  lnx219-37    lnx219-37.example.com
```

Puede utilizar el `vserver services name-service dns` Comando para habilitar DNS en una SVM y configurarlo para usar DNS en la resolución de nombres de host. Los nombres de host se resuelven mediante servidores DNS externos.

Mostrar configuraciones de dominio DNS

Puede mostrar la configuración de dominios DNS de una o varias máquinas virtuales de almacenamiento (SVM) en el clúster para verificar que está configurada correctamente.

Paso

Ver las configuraciones de dominio DNS mediante `vserver services name-service dns show` comando.

El siguiente comando muestra las configuraciones de DNS de todas las SVM del clúster:

```
vserver services name-service dns show
Vserver      State      Domains      Name
-----
cluster-1    enabled    xyz.company.com  192.56.0.129,
192.56.0.130
vs1           enabled    xyz.company.com  192.56.0.129,
192.56.0.130
vs2           enabled    xyz.company.com  192.56.0.129,
192.56.0.130
vs3           enabled    xyz.company.com  192.56.0.129,
192.56.0.130
```

El siguiente comando muestra información detallada de la configuración de DNS para SVM vs1:


```
vserver services name-service dns show -vserver vs1
      Vserver: vs1
      Domains: xyz.company.com
      Name Servers: 192.56.0.129, 192.56.0.130
      Enable/Disable DNS: enabled
      Timeout (secs): 2
      Maximum Attempts: 1
```

Mostrar información acerca de los grupos de conmutación por error

Puede ver información acerca de los grupos de conmutación por error, incluida la lista de nodos y puertos de cada grupo de conmutación por error, tanto si la conmutación por error está habilitada como deshabilitada, así como el tipo de política de conmutación por error que se aplica a cada LIF.

Pasos

1. Muestre los puertos de destino de cada grupo de conmutación por error mediante el `network interface failover-groups show` comando.

El siguiente comando muestra información sobre todos los grupos de conmutación al nodo de respaldo en un clúster de dos nodos:

```
network interface failover-groups show
      Vserver      Group      Failover
      -----      -
      Cluster
      vs1          Cluster
                        cluster1-01:e0a, cluster1-01:e0b,
                        cluster1-02:e0a, cluster1-02:e0b
      vs1          Default
                        cluster1-01:e0c, cluster1-01:e0d,
                        cluster1-01:e0e, cluster1-02:e0c,
                        cluster1-02:e0d, cluster1-02:e0e
```

2. Muestre los puertos de destino y el dominio de retransmisión para un grupo de conmutación al nodo de respaldo específico mediante el `network interface failover-groups show` comando.

El siguiente comando muestra información detallada acerca de los datos del grupo de conmutación al nodo de respaldo 12 para SVM vs4:

```
network interface failover-groups show -vserver vs4 -failover-group data12
```

```
Vserver Name: vs4
Failover Group Name: data12
Failover Targets: cluster1-01:e0f, cluster1-01:e0g, cluster1-02:e0f,
                  cluster1-02:e0g
Broadcast Domain: Default
```

3. Muestra la configuración de recuperación tras fallos utilizada por todas las LIF mediante el `network interface show` comando.

El siguiente comando muestra la política de conmutación por error y el grupo de conmutación por error que utiliza cada LIF:

```
network interface show -vserver * -lif * -fields failover-
group,failover-policy
```

| vserver | lif | failover-policy | failover-group |
|----------|--------------------|-----------------------|----------------|
| ----- | ----- | ----- | ----- |
| Cluster | cluster1-01_clus_1 | local-only | Cluster |
| Cluster | cluster1-01_clus_2 | local-only | Cluster |
| Cluster | cluster1-02_clus_1 | local-only | Cluster |
| Cluster | cluster1-02_clus_2 | local-only | Cluster |
| cluster1 | cluster_mgmt | broadcast-domain-wide | Default |
| cluster1 | cluster1-01_mgmt1 | local-only | Default |
| cluster1 | cluster1-02_mgmt1 | local-only | Default |
| vs1 | data1 | disabled | Default |
| vs3 | data2 | system-defined | group2 |

Mostrar los destinos de conmutación por error de LIF

Puede tener que comprobar si las políticas de conmutación por error y los grupos de conmutación por error de una LIF están configurados correctamente. Para evitar la configuración incorrecta de las reglas de conmutación al nodo de respaldo, puede mostrar los destinos de conmutación por error para una única LIF o para todas las LIF.

Acerca de esta tarea

Mostrar los destinos de conmutación por error de LIF permite comprobar lo siguiente:

- Si los LIF están configurados con el grupo de conmutación por error y la normativa de recuperación tras fallos correctos
- Si la lista resultante de puertos de destino de conmutación por error es adecuada para cada LIF
- Si el destino de conmutación al nodo de respaldo de una LIF de datos no es un puerto de gestión (e0M)

Paso

Muestre los destinos de conmutación por error de una LIF mediante `failover` opción de `network interface show` comando.

El siguiente comando muestra información acerca de los destinos de conmutación por error para todas las LIF de un clúster de dos nodos. La `Failover Targets` La fila muestra la lista (priorizada) de combinaciones de puertos-nodo para una LIF determinada.

```
network interface show -failover
```

| Vserver | Logical Interface | Home Node:Port | Failover Policy | Failover Group |
|----------|-------------------|---|-----------------------|----------------|
| Cluster | | | | |
| | node1_clus1 | node1:e0a | local-only | Cluster |
| | | Failover Targets: node1:e0a, node1:e0b | | |
| | node1_clus2 | node1:e0b | local-only | Cluster |
| | | Failover Targets: node1:e0b, node1:e0a | | |
| | node2_clus1 | node2:e0a | local-only | Cluster |
| | | Failover Targets: node2:e0a, node2:e0b | | |
| | node2_clus2 | node2:e0b | local-only | Cluster |
| | | Failover Targets: node2:e0b, node2:e0a | | |
| cluster1 | | | | |
| | cluster_mgmt | node1:e0c | broadcast-domain-wide | Default |
| | | Failover Targets: node1:e0c, node1:e0d, node2:e0c, node2:e0d | | |
| | node1_mgmt1 | node1:e0c | local-only | Default |
| | | Failover Targets: node1:e0c, node1:e0d | | |
| | node2_mgmt1 | node2:e0c | local-only | Default |
| | | Failover Targets: node2:e0c, node2:e0d | | |
| vs1 | | | | |
| | data1 | node1:e0e | system-defined | bcast1 |
| | | Failover Targets: node1:e0e, node1:e0f, node2:e0e, node2:e0f | | |

Muestre los LIF en una zona de equilibrio de carga

Puede verificar si una zona de equilibrio de carga está configurada correctamente mostrando todas las LIF que pertenecen a ella. También puede ver la zona de equilibrio de carga de una LIF determinada o las zonas de equilibrio de carga de todas las LIF.

Paso

Muestre las LIF y los detalles de equilibrio de carga que desee mediante uno de los comandos siguientes

| Para mostrar... | Introduzca... |
|---|---|
| LIF en una zona de equilibrio de carga en particular | <code>network interface show -dns-zone zone_name</code> <code>zone_name</code> especifica el nombre de la zona de equilibrio de carga. |
| La zona de equilibrio de carga de una LIF determinada | <code>network interface show -lif lif_name -fields dns-zone</code> |
| Las zonas de equilibrio de carga de todas las LIF | <code>network interface show -fields dns-zone</code> |

Ejemplos de mostrar zonas de equilibrio de carga para las LIF

El siguiente comando muestra los detalles de todas las LIF de la zona de equilibrio de carga `storage.company.com` para SVM `vs0`:

```
net int show -vserver vs0 -dns-zone storage.company.com
```

| Vserver | Logical Interface | Status Admin/Oper | Network Address/Mask | Current Node | Current Port | Is Home |
|---------|-------------------|-------------------|----------------------|--------------|--------------|---------|
| vs0 | lif3 | up/up | 10.98.226.225/20 | ndeux-11 | e0c | true |
| | lif4 | up/up | 10.98.224.23/20 | ndeux-21 | e0c | true |
| | lif5 | up/up | 10.98.239.65/20 | ndeux-11 | e0c | true |
| | lif6 | up/up | 10.98.239.66/20 | ndeux-11 | e0c | true |
| | lif7 | up/up | 10.98.239.63/20 | ndeux-21 | e0c | true |
| | lif8 | up/up | 10.98.239.64/20 | ndeux-21 | e0c | true |

El siguiente comando muestra los detalles de la zona DNS de los datos de la LIF.3:

```
network interface show -lif data3 -fields dns-zone
Vserver  lif    dns-zone
-----  ----  -
vs0      data3  storage.company.com
```

El siguiente comando muestra la lista de todas las LIF del clúster y sus zonas DNS correspondientes:

```
network interface show -fields dns-zone
Vserver      lif          dns-zone
-----
cluster      cluster_mgmt none
ndeux-21     clus1        none
ndeux-21     clus2        none
ndeux-21     mgmt1        none
vs0          data1        storage.company.com
vs0          data2        storage.company.com
```

Mostrar las conexiones del clúster

Puede mostrar todas las conexiones activas del clúster o un recuento de conexiones activas en el nodo por cliente, interfaz lógica, protocolo o servicio. También puede mostrar todas las conexiones de escucha en el clúster.

Mostrar conexiones activas por cliente (solo administradores de clúster)

Puede ver las conexiones activas por cliente para verificar el nodo que está utilizando un cliente específico y para ver los posibles desequilibrios entre el número de clientes por nodo.

Acerca de esta tarea

El número de conexiones activas por cliente es útil en las siguientes situaciones:

- Búsqueda de un nodo ocupado o sobrecargado.
- Determinar por qué el acceso de un cliente en particular a un volumen es lento.

Puede ver detalles sobre el nodo al que accede el cliente y después compararlo con el nodo en el que reside el volumen. Si acceder al volumen requiere recorrer la red del clúster, es posible que los clientes experimenten una reducción del rendimiento debido al acceso remoto al volumen en un nodo remoto sobresuscritos.

- Comprobación de que todos los nodos se están utilizando igualmente para el acceso a los datos.
- Búsqueda de clientes que tienen un número alto de conexiones inesperadamente.
- Comprobar si determinados clientes tienen conexiones a un nodo.

Paso

Muestre un recuento de las conexiones activas por parte del cliente en un nodo mediante el `network connections active show-clients` comando.

Para obtener más información sobre este comando, consulte la página man: "[Comandos de ONTAP 9](#)"

```

network connections active show-clients
Node      Vserver Name      Client IP Address      Count
-----
node0     vs0                192.0.2.253            1
          vs0                192.0.2.252            2
          Cluster        192.10.2.124           5
node1     vs0                192.0.2.250            1
          vs0                192.0.2.252            3
          Cluster        192.10.2.123           4
node2     vs1                customer.example.com    1
          vs1                192.0.2.245            3
          Cluster        192.10.2.122           4
node3     vs1                customer.example.org    1
          vs1                customer.example.net    3
          Cluster        192.10.2.121           4

```

Mostrar las conexiones activas por protocolo (solo administradores de clúster)

Puede mostrar un recuento de las conexiones activas por protocolo (TCP o UDP) en un nodo para comparar el uso de protocolos dentro del clúster.

Acerca de esta tarea

El número de conexiones activas por protocolo es útil en las siguientes situaciones:

- Encontrar los clientes UDP que están perdiendo su conexión.

Si un nodo está cerca de su límite de conexión, los clientes UDP son los primeros en caer.

- Comprobando que no se está utilizando ningún otro protocolo.

Paso

Muestre un recuento de las conexiones activas por protocolo en un nodo mediante el `network connections active show-protocols` comando.

Para obtener más información sobre este comando, consulte la página man.

```

network connections active show-protocols
Node      Vserver Name  Protocol  Count
-----
node0
      vs0      UDP      19
      Cluster  TCP      11
node1
      vs0      UDP      17
      Cluster  TCP      8
node2
      vs1      UDP      14
      Cluster  TCP      10
node3
      vs1      UDP      18
      Cluster  TCP      4

```

Mostrar conexiones activas por servicio (sólo administradores de clúster)

Puede mostrar un recuento de las conexiones activas por tipo de servicio (por ejemplo, por NFS, SMB, montaje, etc.) para cada nodo de un clúster. Esto resulta útil para comparar el uso de los servicios del clúster, lo que ayuda a determinar la carga de trabajo principal de un nodo.

Acerca de esta tarea

El recuento de conexiones activas por servicio es útil en los siguientes casos:

- Comprobar que todos los nodos se están utilizando para los servicios adecuados y que el equilibrio de carga de ese servicio está funcionando.
- Verificando que no se está utilizando ningún otro servicio. Muestra un recuento de las conexiones activas por servicio en un nodo mediante el `network connections active show-services` comando.

Para obtener más información sobre este comando, consulte la página man: ["Comandos de ONTAP 9"](#)

```

network connections active show-services
Node      Vserver Name      Service      Count
-----
node0
    vs0          mount          3
    vs0          nfs            14
    vs0          nlm_v4         4
    vs0          cifs_srv       3
    vs0          port_map       18
    vs0          rclopcp        27
    Cluster      ctlopcp        60
node1
    vs0          cifs_srv       3
    vs0          rclopcp        16
    Cluster      ctlopcp        60
node2
    vs1          rclopcp        13
    Cluster      ctlopcp        60
node3
    vs1          cifs_srv       1
    vs1          rclopcp        17
    Cluster      ctlopcp        60

```

Muestre las conexiones activas por LIF en un nodo y una SVM

Puede mostrar un número de conexiones activas para cada LIF, por nodo y máquina virtual de almacenamiento (SVM), para ver los desequilibrios de conexión entre las LIF dentro del clúster.

Acerca de esta tarea

El número de conexiones activas por LIF es útil en las siguientes situaciones:

- Buscar un LIF sobrecargado mediante la comparación del número de conexiones en cada LIF.
- Comprobar que el equilibrio de carga de DNS funciona en todos los LIF de datos.
- Comparación del número de conexiones con las distintas SVM para encontrar las SVM que más se usan.

Paso

Muestre un recuento de conexiones activas para cada LIF mediante SVM y el nodo mediante el `network connections active show-lifs` comando.

Para obtener más información sobre este comando, consulte la página man: ["Comandos de ONTAP 9"](#)


```

network connections active show-lifs
Node      Vserver Name  Interface Name  Count
-----
node0
    vs0        datalif1        3
    Cluster    node0_clus_1    6
    Cluster    node0_clus_2    5
node1
    vs0        datalif2        3
    Cluster    node1_clus_1    3
    Cluster    node1_clus_2    5
node2
    vs1        datalif2        1
    Cluster    node2_clus_1    5
    Cluster    node2_clus_2    3
node3
    vs1        datalif1        1
    Cluster    node3_clus_1    2
    Cluster    node3_clus_2    2

```

Muestra las conexiones activas en un clúster

Puede mostrar información acerca de las conexiones activas de un clúster para ver la LIF, el puerto, el host remoto, el servicio, las máquinas virtuales de almacenamiento (SVM) y el protocolo que utilizan las conexiones individuales.

Acerca de esta tarea

Ver las conexiones activas en un clúster es útil en las siguientes situaciones:

- Verificar que los clientes individuales están usando el protocolo y el servicio correctos en el nodo correcto.
- Si un cliente tiene problemas para acceder a los datos mediante una cierta combinación de nodo, protocolo y servicio, puede utilizar este comando para encontrar un cliente similar para la comparación de la configuración o el seguimiento de paquetes.

Paso

Muestre las conexiones activas de un clúster mediante el `network connections active show` comando.

Para obtener más información sobre este comando, consulte la página man: ["Comandos de ONTAP 9"](#)

El siguiente comando muestra las conexiones activas del nodo 1:

```
network connections active show -node node1
```

| Vserver | Interface | Remote | |
|-------------|--------------------|--------------------|------------------|
| Name | Name:Local Port | Host:Port | Protocol/Service |
| ----- | ----- | ----- | ----- |
| Node: node1 | | | |
| Cluster | node1_clus_1:50297 | 192.0.2.253:7700 | TCP/ctlopcp |
| Cluster | node1_clus_1:13387 | 192.0.2.253:7700 | TCP/ctlopcp |
| Cluster | node1_clus_1:8340 | 192.0.2.252:7700 | TCP/ctlopcp |
| Cluster | node1_clus_1:42766 | 192.0.2.252:7700 | TCP/ctlopcp |
| Cluster | node1_clus_1:36119 | 192.0.2.250:7700 | TCP/ctlopcp |
| vs1 | data1:111 | host1.aa.com:10741 | UDP/port-map |
| vs3 | data2:111 | host1.aa.com:10741 | UDP/port-map |
| vs1 | data1:111 | host1.aa.com:12017 | UDP/port-map |
| vs3 | data2:111 | host1.aa.com:12017 | UDP/port-map |

El siguiente comando muestra las conexiones activas en la SVM vs1:

```
network connections active show -vserver vs1
```

| Vserver | Interface | Remote | |
|-------------|-----------------|--------------------|------------------|
| Name | Name:Local Port | Host:Port | Protocol/Service |
| ----- | ----- | ----- | ----- |
| Node: node1 | | | |
| vs1 | data1:111 | host1.aa.com:10741 | UDP/port-map |
| vs1 | data1:111 | host1.aa.com:12017 | UDP/port-map |

Muestra las conexiones de escucha en un clúster

Puede mostrar información acerca de las conexiones de escucha en un clúster para ver las LIF y los puertos que aceptan conexiones para un protocolo y un servicio dados.

Acerca de esta tarea

Ver las conexiones de escucha en un clúster es útil en las siguientes situaciones:

- Verificación de que el protocolo o servicio deseado están escuchando en una LIF si las conexiones de cliente con esta LIF fallan de forma consistente.
- Comprobar que se abre un listener de UDP/rclopcp en cada LIF de clúster si se produce un error en el acceso remoto a datos a un volumen de un nodo a través de una LIF en otro nodo.
- Comprobación de que se abre un agente de escucha UDP/rclopcp en cada LIF del clúster si se producen errores en las transferencias de SnapMirror entre dos nodos del mismo clúster.
- Comprobar que se ha abierto un agente de escucha TCP/ctlopcp en cada LIF de interconexión de clústeres si se producen fallos en las transferencias de SnapMirror entre dos nodos en clústeres diferentes.

Paso

Muestre las conexiones de escucha por nodo mediante el `network connections listening show` comando.

```

network connections listening show
Vserver Name      Interface Name:Local Port      Protocol/Service
-----
Node: node0
Cluster           node0_clus_1:7700              TCP/ctlopcp
vs1               data1:4049                    UDP/unknown
vs1               data1:111                     TCP/port-map
vs1               data1:111                     UDP/port-map
vs1               data1:4046                    TCP/sm
vs1               data1:4046                    UDP/sm
vs1               data1:4045                    TCP/nlm-v4
vs1               data1:4045                    UDP/nlm-v4
vs1               data1:2049                    TCP/nfs
vs1               data1:2049                    UDP/nfs
vs1               data1:635                     TCP/mount
vs1               data1:635                     UDP/mount
Cluster           node0_clus_2:7700              TCP/ctlopcp

```

Comandos para diagnosticar problemas de red

Puede diagnosticar problemas en la red con comandos como `ping`, `traceroute`, `ndp`, y.. `tcpdump`. También puede utilizar comandos como `ping6` y.. `traceroute6` Para diagnosticar problemas IPv6.

| Si desea... | Introduzca este comando... |
|--|---|
| Compruebe si el nodo puede llegar a otros hosts de su red | <code>network ping</code> |
| Probar si el nodo puede llegar a otros hosts en su red IPv6 | <code>network ping6</code> |
| Siga la ruta que llevan los paquetes IPv4 a un nodo de red | <code>network traceroute</code> |
| Rastree la ruta que los paquetes IPv6 toman a un nodo de red | <code>network traceroute6</code> |
| Gestión del protocolo de descubrimiento cercano (NDP) | <code>network ndp</code> |
| Mostrar estadísticas sobre los paquetes que se reciben y se envían en una interfaz de red especificada o en todas las interfaces de red | <code>run -node <i>node_name</i> ifstat</code> Nota: Este comando está disponible desde el nodeshell. |
| Muestra información sobre los dispositivos vecinos que se detectan de cada nodo y puerto del clúster, incluido el tipo de dispositivo remoto y la plataforma de dispositivos | <code>network device-discovery show</code> |

| | |
|--|--|
| Ver los vecinos de CDP del nodo (ONTAP solo admite anuncios de CDPv1) | <pre>run -node <i>node_name</i> cdpd show-neighbors</pre> <p>Nota: Este comando está disponible desde el nodeshell.</p> |
| Realice el seguimiento de los paquetes que se envían y se reciben en la red | <pre>network tcpdump start -node <i>node-name</i> -port <i>port_name</i></pre> <p>Nota: Este comando está disponible desde el nodeshell.</p> |
| Mida la latencia y el rendimiento entre nodos entre clústeres o dentro del clúster | <pre>network test -path -source-node <i>source_nodename</i> local -destination -cluster <i>destination_clustername</i> -destination-node <i>destination_nodename</i> -session-type <i>Default, AsyncMirrorLocal, AsyncMirrorRemote, SyncMirrorRemote, or RemoteDataTransfer</i></pre> <p>Para obtener más información, consulte "Gestión del rendimiento".</p> |

Para obtener más información sobre estos comandos, consulte las páginas de manual correspondientes: ["Comandos de ONTAP 9"](#)

Mostrar conectividad de red con protocolos de descubrimiento de vecinos

Mostrar conectividad de red con protocolos de descubrimiento de vecinos

En un centro de datos, puede utilizar protocolos de descubrimiento de vecinos para ver la conectividad de red entre un par de sistemas físicos o virtuales y sus interfaces de red. ONTAP admite dos protocolos de detección de vecinos: El protocolo de descubrimiento de Cisco (CDP) y el protocolo de detección de nivel de enlace (LLDP).

Los protocolos de detección de vecinos permiten detectar y ver automáticamente información sobre los dispositivos habilitados para protocolos conectados directamente en una red. Cada dispositivo anuncia la identificación, las capacidades y la información de conectividad. Esta información se transmite en tramas Ethernet a una dirección MAC de multidifusión y la reciben todos los dispositivos vecinos habilitados por protocolo.

Para que dos dispositivos se conviertan en vecinos, cada uno debe tener un protocolo activado y configurado correctamente. La funcionalidad del protocolo de detección se limita a redes conectadas directamente. Los vecinos pueden incluir dispositivos habilitados para protocolos, como switches, routers, puentes, etc. ONTAP admite dos protocolos de detección de vecinos, que se pueden utilizar por separado o juntos.

Cisco Discovery Protocol (CDP)

CDP es un protocolo de capa de enlace patentado desarrollado por Cisco Systems. Está habilitado de forma predeterminada en ONTAP para los puertos de clúster, pero debe habilitarse explícitamente para los puertos de datos.

Protocolo de detección de nivel de enlace (LLDP)

LLDP es un protocolo neutral en cuanto a proveedores especificado en el documento estándar IEEE 802.1AB. Debe habilitarse explícitamente para todos los puertos.

Utilice CDP para detectar la conectividad de red

El uso de CDP para detectar la conectividad de red consiste en revisar las consideraciones de implementación, habilitarlo en puertos de datos, ver dispositivos vecinos y ajustar los valores de configuración de CDP según sea necesario. De forma predeterminada, CDP está habilitado en los puertos de clúster.

CDP también debe estar habilitado en cualquier switch y router antes de poder mostrar la información sobre los dispositivos vecinos.

| Versión de ONTAP | Descripción |
|---------------------|---|
| 9.10.1 y anteriores | El monitor de estado del switch de clúster también utiliza el CDP para detectar automáticamente los switches de red de gestión y clúster. |
| 9.11.1 y posterior | El monitor de estado del switch de clúster también utiliza el CDP para detectar automáticamente los switches de red de clúster, almacenamiento y gestión. |

Información relacionada

["Administración del sistema"](#)

Consideraciones para usar CDP

De forma predeterminada, los dispositivos compatibles con CDP envían anuncios de CDPv2. Los dispositivos compatibles con CDP envían anuncios de CDPv1 sólo cuando reciben anuncios de CDPv1. ONTAP solo es compatible con CDPv1. Por lo tanto, cuando un nodo ONTAP envía anuncios de CDPv1, los dispositivos vecinos que cumplen con CDP devuelven anuncios de CDPv1.

Debe considerar la siguiente información antes de habilitar CDP en un nodo:

- CDP es compatible con todos los puertos.
- Los anuncios de CDP son enviados y recibidos por los puertos que están en el estado up.
- CDP debe estar activado en los dispositivos de transmisión y recepción para enviar y recibir anuncios de CDP.
- Los anuncios de CDP se envían a intervalos regulares y puede configurar el intervalo de tiempo.
- Cuando cambian las direcciones IP de una LIF, el nodo envía la información actualizada en el siguiente anuncio de CDP.
- ONTAP 9.10.1 y anteriores:
 - CDP está siempre habilitado en los puertos de clúster.
 - De forma predeterminada, CDP está deshabilitado en todos los puertos que no son de clúster.
- ONTAP 9.11.1 y posteriores:
 - CDP está siempre habilitado en los puertos de clúster y de almacenamiento.
 - De forma predeterminada, CDP está deshabilitado en todos los puertos que no son de clúster y que no están relacionados con el almacenamiento.



A veces, cuando se cambian las LIF en el nodo, la información de CDP no se actualiza en el lado del dispositivo receptor (por ejemplo, un switch). Si encuentra este problema, debe configurar la interfaz de red del nodo con el estado inactivo y, a continuación, con el estado activo.

- Sólo las direcciones IPv4 están anunciadas en los anuncios de CDP.
- Para los puertos de red físicos con VLAN, se anuncian todas las LIF configuradas en las VLAN de ese puerto.
- Para los puertos físicos que forman parte de un grupo de interfaces, todas las direcciones IP configuradas en ese grupo de interfaces se anuncian en cada puerto físico.
- Para un grupo de interfaces que aloja VLAN, todas las LIF configuradas en el grupo de interfaces y las VLAN se anuncian en cada uno de los puertos de red.
- Debido a que los paquetes CDP se restringen a no más de 1500 bytes en los puertos configurados con un gran número de LIF, solo un subconjunto de estas direcciones IP puede notificarse en el switch adyacente.

Activa o desactiva CDP

Para detectar y enviar anuncios a dispositivos vecinos compatibles con CDP, CDP debe estar habilitado en cada nodo del clúster.

De manera predeterminada en ONTAP 9.10.1 y versiones anteriores, CDP está habilitado en todos los puertos de clúster de un nodo y está deshabilitado en todos los puertos que no son de clúster de un nodo.

De forma predeterminada en ONTAP 9.11.1 y versiones posteriores, CDP está habilitado en todos los puertos de clúster y almacenamiento de un nodo, y está deshabilitado en todos los puertos que no son de clúster y que no son de almacenamiento de un nodo.

Acerca de esta tarea

La `cdpd.enable` Option controla si CDP está habilitado o deshabilitado en los puertos de un nodo:

- Para ONTAP 9.10.1 y versiones anteriores, en habilita CDP en puertos que no son de clúster.
- Para ONTAP 9.11.1 y versiones posteriores, el habilita CDP en puertos que no son de clúster y que no son de almacenamiento.
- Para ONTAP 9.10.1 y versiones anteriores, OFF deshabilita CDP en puertos que no son de clúster; no puede deshabilitar CDP en los puertos de clúster.
- Para ONTAP 9.11.1 y versiones posteriores, OFF deshabilita CDP en puertos que no son de clúster y que no son de almacenamiento; no puede deshabilitar CDP en puertos de clúster.

Cuando CDP está desactivado en un puerto conectado a un dispositivo compatible con CDP, es posible que el tráfico de red no esté optimizado.

Pasos

1. Muestre la configuración actual de CDP para un nodo o para todos los nodos de un clúster:

| | |
|-------------------------------------|---|
| Para ver la configuración CDP de... | Introduzca... |
| Un nodo | <code>run - node <node_name> options cdpd.enable</code> |

| | |
|-------------------------------|----------------------------------|
| Todos los nodos de un clúster | <code>options cdpd.enable</code> |
|-------------------------------|----------------------------------|

2. Habilite o deshabilite CDP en todos los puertos de un nodo, o en todos los puertos de todos los nodos de un clúster:

| | |
|---|--|
| Para habilitar o deshabilitar CDP en... | Introduzca... |
| Un nodo | <code>run -node node_name options cdpd.enable {on or off}</code> |
| Todos los nodos de un clúster | <code>options cdpd.enable {on or off}</code> |

Ver la información de CDP vecino

Puede ver información acerca de los dispositivos vecinos que están conectados a cada puerto de los nodos del clúster, siempre que el puerto esté conectado a un dispositivo compatible con CDP. Puede utilizar el `network device-discovery show -protocol cdp` para ver la información de vecinos.

Acerca de esta tarea

En ONTAP 9.10.1 y versiones anteriores, como el CDP siempre está habilitado para los puertos de clúster, la información de vecinos CDP siempre se muestra para esos puertos. CDP debe estar habilitado en puertos que no son de clúster para que aparezca la información de cercanía para esos puertos.

En ONTAP 9.11.1 y versiones posteriores, como el CDP está siempre habilitado para el clúster y los puertos de almacenamiento, la información de vecino de CDP siempre se muestra para esos puertos. Para que aparezca la información relacionada con los puertos, CDP debe estar habilitado en puertos que no sean de clúster y que no sean de almacenamiento.

Paso

Muestra información acerca de todos los dispositivos compatibles con CDP que están conectados a los puertos de un nodo del clúster:

```
network device-discovery show -node node -protocol cdp
```

El siguiente comando muestra los vecinos que están conectados a los puertos en el nodo sti2650-212:

```

network device-discovery show -node sti2650-212 -protocol cdp
Node/          Local  Discovered
Protocol      Port   Device (LLDP: ChassisID)  Interface      Platform
-----
sti2650-212/cdp
              e0M    RTP-LF810-510K37.gdl.eng.netapp.com(SAL1942R8JS)
                                Ethernet1/14    N9K-
C93120TX
              e0a    CS:RTP-CS01-510K35        0/8            CN1610
              e0b    CS:RTP-CS01-510K36        0/8            CN1610
              e0c    RTP-LF350-510K34.gdl.eng.netapp.com(FDO21521S76)
                                Ethernet1/21    N9K-
C93180YC-FX
              e0d    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                Ethernet1/22    N9K-
C93180YC-FX
              e0e    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                Ethernet1/23    N9K-
C93180YC-FX
              e0f    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                Ethernet1/24    N9K-
C93180YC-FX

```

El resultado enumera los dispositivos Cisco que están conectados a cada puerto del nodo especificado.

Configure el tiempo de espera para los mensajes CDP

El tiempo de espera es el período de tiempo durante el cual los anuncios de CDP se almacenan en la caché en los dispositivos vecinos que cumplen con CDP. El tiempo de mantenimiento se anuncia en cada paquete CDPv1 y se actualiza cada vez que un nodo recibe un paquete CDPv1.

- El valor de `cdpd.holdtime` Esta opción debe definirse con el mismo valor en ambos nodos de una pareja de alta disponibilidad.
- El valor de tiempo de espera predeterminado es de 180 segundos, pero puede introducir valores que oscilan entre 10 segundos y 255 segundos.
- Si se elimina una dirección IP antes de que caduque el tiempo de retención, la información CDP se almacena en caché hasta que caduque el tiempo de retención.

Pasos

1. Muestre el tiempo de espera actual de CDP para un nodo o para todos los nodos de un clúster:

| | |
|------------------------------------|--|
| Para ver el tiempo de espera de... | Introduzca... |
| Un nodo | <code>run -node node_name options cdpd.holdtime</code> |

| | |
|-------------------------------|------------------------------------|
| Todos los nodos de un clúster | <code>options cdpd.holdtime</code> |
|-------------------------------|------------------------------------|

- Configure el tiempo de retención de CDP en todos los puertos de un nodo o en todos los puertos de todos los nodos de un clúster:

| | |
|---|---|
| Para establecer el tiempo de espera activado: | Introduzca... |
| Un nodo | <code>run -node node_name options cdpd.holdtime holdtime</code> |
| Todos los nodos de un clúster | <code>options cdpd.holdtime holdtime</code> |

Establezca el intervalo para enviar anuncios CDP

Los anuncios de CDP se envían a los vecinos de CDP a intervalos periódicos. Puede aumentar o disminuir el intervalo para enviar anuncios CDP dependiendo del tráfico de red y de los cambios en la topología de la red.

- El valor de `cdpd.interval` Esta opción debe definirse con el mismo valor en ambos nodos de una pareja de alta disponibilidad.
- El intervalo predeterminado es de 60 segundos, pero puede introducir un valor entre 5 segundos y 900 segundos.

Pasos

- Muestre el intervalo de tiempo de anuncio de CDP actual para un nodo, o bien para todos los nodos de un clúster:

| | |
|-------------------------------|--|
| Para ver el intervalo de... | Introduzca... |
| Un nodo | <code>run -node node_name options cdpd.interval</code> |
| Todos los nodos de un clúster | <code>options cdpd.interval</code> |

- Configure el intervalo para enviar anuncios CDP para todos los puertos de un nodo o para todos los puertos de todos los nodos de un clúster:

| | |
|--------------------------------------|---|
| Para establecer el intervalo para... | Introduzca... |
| Un nodo | <code>run -node node_name options cdpd.interval interval</code> |
| Todos los nodos de un clúster | <code>options cdpd.interval interval</code> |

Ver o borrar las estadísticas de CDP

Es posible ver las estadísticas de CDP para los puertos del clúster y que no son del clúster en cada nodo para detectar posibles problemas de conectividad de red. Las estadísticas de CDP son acumulativas desde la última vez que se borraron.

Acerca de esta tarea

En ONTAP 9.10.1 y versiones anteriores, como CDP está siempre habilitado para los puertos, las estadísticas de CDP siempre se muestran para el tráfico de esos puertos. CDP debe estar habilitado en los puertos para que aparezcan las estadísticas para esos puertos.

En ONTAP 9.11.1 y versiones posteriores, como el CDP está siempre habilitado para los puertos de clúster y de almacenamiento, las estadísticas de CDP siempre se muestran para el tráfico de esos puertos. CDP debe estar habilitado en puertos que no sean de clúster o que no sean de almacenamiento para que las estadísticas aparezcan para esos puertos.

Paso

Muestra o borra las estadísticas actuales de CDP para todos los puertos de un nodo:

| Si desea... | Introduzca... |
|----------------------------------|--|
| Consulte las estadísticas de CDP | <code>run -node node_name cdpd show-stats</code> |
| Borre las estadísticas de CDP | <code>run -node node_name cdpd zero-stats</code> |

Ejemplo de mostrar y borrar estadísticas

El siguiente comando muestra las estadísticas de CDP antes de que se borren. El resultado muestra el número total de paquetes que se enviaron y recibieron desde la última vez que se borraron las estadísticas.

```
run -node nodel cdpd show-stats
```

RECEIVE

| | | | | | | | |
|-----------------|------|--|-----------------|---|--|-------------------|------|
| Packets: | 9116 | | Csum Errors: | 0 | | Unsupported Vers: | 4561 |
| Invalid length: | 0 | | Malformed: | 0 | | Mem alloc fails: | 0 |
| Missing TLVs: | 0 | | Cache overflow: | 0 | | Other errors: | 0 |

TRANSMIT

| | | | | | | | |
|-------------------|------|--|------------------|---|--|---------------|---|
| Packets: | 4557 | | Xmit fails: | 0 | | No hostname: | 0 |
| Packet truncated: | 0 | | Mem alloc fails: | 0 | | Other errors: | 0 |

OTHER

| | |
|----------------|---|
| Init failures: | 0 |
|----------------|---|

El siguiente comando borra las estadísticas de CDP:

```
run -node nodel cdpd zero-stats
```

```
run -node nodel cdpd show-stats
```

RECEIVE

| | | | | | |
|-----------------|---|-----------------|---|-------------------|---|
| Packets: | 0 | Csum Errors: | 0 | Unsupported Vers: | 0 |
| Invalid length: | 0 | Malformed: | 0 | Mem alloc fails: | 0 |
| Missing TLVs: | 0 | Cache overflow: | 0 | Other errors: | 0 |

TRANSMIT

| | | | | | |
|-------------------|---|------------------|---|---------------|---|
| Packets: | 0 | Xmit fails: | 0 | No hostname: | 0 |
| Packet truncated: | 0 | Mem alloc fails: | 0 | Other errors: | 0 |

OTHER

| | |
|----------------|---|
| Init failures: | 0 |
|----------------|---|

Después de borrar las estadísticas, comienzan a acumularse después de que se envíe o reciba el próximo anuncio de CDP.

Use LLDP para detectar la conectividad de red

El uso de LLDP para detectar la conectividad de red consiste en revisar consideraciones de implementación, habilitarlo en todos los puertos, ver dispositivos vecinos y ajustar los valores de configuración de LLDP según sea necesario.

También es necesario habilitar LLDP en cualquier switch y enrutador para poder mostrar la información acerca de los dispositivos vecinos.

ONTAP informa actualmente de las siguientes estructuras de longitud de valor de tipo (TLV):

- Identificador del chasis
- Identificador del puerto
- Tiempo de vida (TTL)
- Nombre del sistema

El TLV del nombre del sistema no se envía en los dispositivos CNA.

Ciertos adaptadores de red convergentes (CNA), como el adaptador X1143 y los puertos UTA2 integrados, contienen compatibilidad con la descarga para LLDP:

- La descarga de LLDP se utiliza para la creación de puentes en centros de datos (DCB).
- La información mostrada podría diferir entre el clúster y el switch.

Los datos del identificador del chasis y del identificador del puerto que muestra el switch podrían ser diferentes para los puertos CNA y no CNA.

Por ejemplo:

- Para puertos que no son CNA:

- El identificador de chasis es una dirección MAC fija de uno de los puertos en el nodo
- Port ID es el nombre de puerto del puerto correspondiente en el nodo
- Para puertos CNA:
 - Los identificadores de chasis y de puerto son las direcciones MAC de los respectivos puertos en el nodo.

Sin embargo, los datos que muestra el clúster son consistentes para estos tipos de puerto.



La especificación LLDP define el acceso a la información recogida a través de una MIB SNMP. Sin embargo, ONTAP no admite actualmente la MIB de LLDP.

Habilite o deshabilite LLDP

Para detectar y enviar anuncios a dispositivos vecinos compatibles con LLDP, es necesario habilitar LLDP en cada nodo del clúster. A partir de ONTAP 9.7, LLDP está habilitado en todos los puertos de un nodo de manera predeterminada.

Acerca de esta tarea

Para ONTAP 9.10.1 y versiones anteriores, la `lldp.enable` La opción controla si LLDP está habilitada o deshabilitada en los puertos de un nodo:

- `on` Habilita LLDP en todos los puertos.
- `off` Deshabilita LLDP en todos los puertos.

Para ONTAP 9.11.1 y posteriores, el `lldp.enable` La opción controla si LLDP está habilitada o deshabilitada en los puertos no-clúster y no-almacenamiento de un nodo:

- `on` Permite LLDP en todos los puertos que no son de clúster y que no son de almacenamiento.
- `off` Deshabilita LLDP en todos los puertos que no son de clúster y que no son de almacenamiento.

Pasos

1. Muestra la configuración actual de LLDP para un nodo o para todos los nodos de un clúster:
 - Un solo nodo: `run -node node_name options lldp.enable`
 - Todos los nodos: Opciones `lldp.enable`
2. Habilite o deshabilite LLDP en todos los puertos de un nodo o en todos los puertos de todos los nodos de un clúster:

| | |
|--|---|
| Para habilitar o deshabilitar LLDP en... | Introduzca... |
| Un nodo | <code>`run -node node_name options lldp.enable {on</code> |
| <code>off}`</code> | Todos los nodos de un clúster |
| <code>`options lldp.enable {on</code> | <code>off}`</code> |

- Un solo nodo:

```
run -node node_name options lldp.enable {on|off}
```

- Todos los nodos:

```
options lldp.enable {on|off}
```

Consulte la información sobre vecinos de LLDP

Puede ver información sobre los dispositivos vecinos que están conectados a cada puerto de los nodos del clúster, siempre y cuando el puerto esté conectado a un dispositivo compatible con LLDP. Puede utilizar el comando `network device-discovery show` para ver información de los vecinos.

Paso

1. Muestra información sobre todos los dispositivos compatibles con LLDP que están conectados a los puertos de un nodo del clúster:

```
network device-discovery show -node node -protocol lldp
```

El siguiente comando muestra los vecinos que están conectados a los puertos en el nodo `cluster-1_01`. La salida enumera los dispositivos habilitados para LLDP que están conectados a cada puerto del nodo especificado. Si la `-protocol` Se omite la opción, la salida también enumera los dispositivos habilitados para CDP.

```
network device-discovery show -node cluster-1_01 -protocol lldp
Node/          Local  Discovered
Protocol      Port   Device
-----
cluster-1_01/lldp
                e2a    0013.c31e.5c60    GigabitEthernet1/36
                e2b    0013.c31e.5c60    GigabitEthernet1/35
                e2c    0013.c31e.5c60    GigabitEthernet1/34
                e2d    0013.c31e.5c60    GigabitEthernet1/33
```

Ajuste el intervalo para la transmisión de anuncios de LLDP

Los anuncios de LLDP se envían a intervalos periódicos. Es posible aumentar o reducir el intervalo para enviar anuncios de LLDP en función del tráfico de red y los cambios en la topología de red.

Acerca de esta tarea

El intervalo predeterminado recomendado por IEEE es de 30 segundos, pero puede introducir un valor de 5 segundos a 300 segundos.

Pasos

1. Muestre el intervalo de tiempo de anuncio de LLDP actual para un nodo o para todos los nodos de un clúster:

- Un solo nodo:

```
run -node <node_name> options lldp.xmit.interval
```

- Todos los nodos:

```
options lldp.xmit.interval
```

2. Ajuste el intervalo para enviar anuncios de LLDP para todos los puertos de un nodo o para todos los puertos de todos los nodos de un clúster:

- Un solo nodo:

```
run -node <node_name> options lldp.xmit.interval <interval>
```

- Todos los nodos:

```
options lldp.xmit.interval <interval>
```

Ajuste el tiempo de respuesta de los anuncios de LLDP

El tiempo de vida (TTL) es el período de tiempo durante el cual los anuncios de LLDP se almacenan en la caché en dispositivos vecinos compatibles con LLDP. TTL se anuncia en cada paquete LLDP y se actualiza cada vez que un nodo recibe un paquete LLDP. TTL puede modificarse en tramas LLDP salientes.

Acerca de esta tarea

- TTL es un valor calculado, el producto del intervalo de transmisión (`lldp.xmit.interval`) y el multiplicador de retención (`lldp.xmit.hold`) más uno.
- El valor predeterminado del multiplicador de retención es 4, pero puede introducir valores que oscilen entre 1 y 100.
- Por lo tanto, el valor predeterminado TTL es de 121 segundos, como recomienda el IEEE, pero al ajustar el intervalo de transmisión y mantener los valores multiplicadores, puede especificar un valor para los fotogramas salientes de 6 segundos a 30001 segundos.
- Si se elimina una dirección IP antes de que caduque el TTL, la información de LLDP se almacena en caché hasta que caduque el TTL.

Pasos

1. Muestre el valor actual de contener multiplicador para un nodo o para todos los nodos de un clúster:

- Un solo nodo:

```
run -node <node_name> options lldp.xmit.hold
```

- Todos los nodos:

```
options lldp.xmit.hold
```

2. Ajuste el valor de multiplicador de mantenimiento en todos los puertos de un nodo o en todos los puertos de todos los nodos de un clúster:

- Un solo nodo:

```
run -node <node_name> options lldp.xmit.hold <hold_value>
```

- Todos los nodos:

```
options lldp.xmit.hold <hold_value>
```

Ver o borrar estadísticas de LLDP

Es posible ver las estadísticas de LLDP de los puertos de clúster y no de clúster en cada nodo para detectar posibles problemas de conectividad de red. Las estadísticas de LLDP son acumulativas a partir del momento en que se borraron por última vez.

Acerca de esta tarea

Para ONTAP 9.10.1 y versiones anteriores, como LLDP siempre están habilitadas para puertos del clúster, siempre se muestran las estadísticas de LLDP para el tráfico de esos puertos. LLDP debe estar habilitado en puertos que no son del clúster para que se muestren estadísticas de esos puertos.

Para ONTAP 9.11.1 y versiones posteriores, como LLDP siempre está habilitado para los puertos de clúster y de almacenamiento, siempre se muestran las estadísticas de LLDP para el tráfico de esos puertos. LLDP deben estar habilitadas en puertos que no sean del clúster y en puertos del almacenamiento para que se muestren estadísticas de esos puertos.

Paso

Muestre o borre las estadísticas actuales de LLDP para todos los puertos en un nodo:

| Si desea... | Introduzca... |
|-----------------------------------|--|
| Consulte las estadísticas de LLDP | <code>run -node node_name lldp stats</code> |
| Borre las estadísticas de LLDP | <code>run -node node_name lldp stats -z</code> |

Ejemplo de estadísticas show y clear

El siguiente comando muestra las estadísticas de LLDP antes de borrarlas. El resultado muestra el número total de paquetes que se enviaron y recibieron desde la última vez que se borraron las estadísticas.

```
cluster-1::> run -node vsim1 lldp stats
```

RECEIVE

```
  Total frames:      190k | Accepted frames:  190k | Total drops:
0
```

TRANSMIT

```
  Total frames:      5195 | Total failures:      0
```

OTHER

```
  Stored entries:      64
```

El siguiente comando borra las estadísticas de LLDP.

```
cluster-1::> The following command clears the LLDP statistics:
```

```
run -node vsim1 lldp stats -z
```

```
run -node node1 lldp stats
```

RECEIVE

```
  Total frames:      0 | Accepted frames:  0 | Total drops:
0
```

TRANSMIT

```
  Total frames:      0 | Total failures:      0
```

OTHER

```
  Stored entries:      64
```

Una vez borradas las estadísticas, comienzan a acumularse después de que se envía o recibe el próximo anuncio de LLDP.

Gestión del almacenamiento nas

Gestione protocolos NAS con System Manager

Información general de la gestión de NAS con System Manager

Los temas de esta sección muestran cómo configurar y gestionar entornos NAS con System Manager en ONTAP 9.7 y versiones posteriores.

Si utiliza la versión clásica de System Manager (disponible solo en ONTAP 9.7 y versiones anteriores), consulte los temas siguientes:

- ["Información general de la configuración de NFS"](#)
- ["Información general de la configuración de SMB"](#)

System Manager admite flujos de trabajo para:

- Configuración inicial de los clústeres que pretende utilizar para los servicios de archivos NAS.
- Aprovisionamiento de volúmenes adicional para las necesidades de almacenamiento cambiantes.
- Configuración y mantenimiento de las instalaciones de seguridad y autenticación estándar del sector.

Mediante System Manager, puede gestionar servicios NAS en el nivel de componentes:

- Protocolos: NFS, SMB o ambos (NAS multiprotocolo)
- Servicios de nombres: DNS, LDAP y NIS
- Cambio de servicio de nombres
- Seguridad Kerberos
- Exportaciones y acciones
- Qtrees
- Asignación de nombres de usuarios y grupos

Aprovisione almacenamiento NFS para almacenes de datos de VMware

Antes de usar Virtual Storage Console para VMware vSphere (VSC) para aprovisionar volúmenes NFS en un sistema de almacenamiento basado en ONTAP para hosts ESXi, habilite NFS mediante System Manager para ONTAP 9.7 o una versión posterior.

Después de crear un ["Máquina virtual de almacenamiento compatible con NFS"](#) En System Manager, entonces debe aprovisionar volúmenes de NFS y gestionar almacenes de datos mediante VSC.

A partir de VSC 7.0, VSC forma parte del ["Herramientas de ONTAP para el dispositivo virtual de VMware vSphere"](#), Que incluye las funcionalidades VSC, vStorage APIs for Storage Awareness (VASA) Provider y Storage Replication Adapter (SRA) para VMware vSphere.

Asegúrese de comprobar el ["Matriz de interoperabilidad de NetApp"](#) Para confirmar la compatibilidad entre sus versiones actuales de ONTAP y VSC.

Para configurar el acceso NFS para hosts ESXi a almacenes de datos con System Manager Classic (para

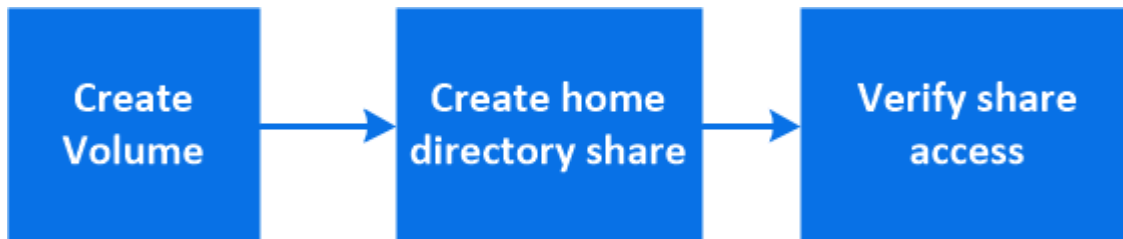
ONTAP 9.7 y versiones anteriores), consulte ["Configuración de NFS para ESXi mediante información general de VSC"](#)

Para obtener más información, consulte ["TR-4597: VMware vSphere para ONTAP"](#) Y la documentación de su versión de VSC.

Aprovisionar almacenamiento NAS para directorios iniciales

Cree volúmenes para proporcionar almacenamiento para directorios iniciales mediante el protocolo SMB.

Este procedimiento crea nuevos volúmenes para directorios iniciales en un ["Máquinas virtuales de almacenamiento habilitadas para SMB existentes"](#). Puede aceptar los valores predeterminados del sistema al configurar volúmenes o especificar configuraciones personalizadas.



Es posible crear volúmenes FlexVol o, para sistemas de archivos de gran tamaño con requisitos de alto rendimiento, se pueden crear volúmenes FlexGroup. Consulte también ["Aprovisione almacenamiento NAS para sistemas de archivos de gran tamaño con volúmenes FlexGroup"](#).

También puede guardar las especificaciones de este volumen en un libro de aplicaciones de Ansible. Para obtener más información, visite ["Utilice libros de aplicaciones Ansible para añadir o editar volúmenes o LUN"](#).

Pasos

1. Añadir un volumen nuevo en una máquina virtual de almacenamiento habilitada para SMB.
 - a. Seleccione **Almacenamiento > Volúmenes** y, a continuación, haga clic en **Agregar**.
 - b. Introduzca un nombre, seleccione la máquina virtual de almacenamiento e introduzca un tamaño.

Solo se enumeran las máquinas virtuales de almacenamiento configuradas con el protocolo SMB. Si solo hay disponible una VM de almacenamiento configurada con el protocolo SMB, no se muestra el campo **Storage VM**.

- Si hace clic en **Guardar** en este momento, System Manager utiliza valores predeterminados del sistema para crear y agregar un volumen FlexVol.
 - Puede hacer clic en **más opciones** para personalizar la configuración del volumen y activar servicios como autorización, calidad de servicio y protección de datos. Consulte [Personalice la configuración del volumen](#), a continuación, vuelva aquí para completar los pasos siguientes.
2. haga clic en **almacenamiento > recursos compartidos**, haga clic en **Agregar** y seleccione **Directorio inicial**.
 3. En un cliente Windows, haga lo siguiente para verificar que se puede acceder al recurso compartido.
 - a. En el Explorador de Windows, asigne una unidad al recurso compartido con el siguiente formato:
_SMB_Server_Name__Share_Name_

Si el nombre del recurso compartido se creó con variables (%w, %d o %u), asegúrese de probar el

acceso con un nombre resuelto.

- b. En la unidad recién creada, cree un archivo de prueba y, a continuación, elimine el archivo.

Personalice la configuración del volumen

Se puede personalizar la configuración del volumen cuando se añaden volúmenes en lugar de aceptar los valores predeterminados del sistema.

Procedimiento

Después de hacer clic en **más opciones**, seleccione la funcionalidad que necesite e introduzca los valores necesarios.

- Caché para volumen remoto.
- Nivel de servicio de rendimiento (calidad de servicio, calidad de servicio).

A partir de ONTAP 9.8, puede especificar una política de calidad de servicio personalizada o deshabilitar la calidad de servicio, además de la selección de valor predeterminada.

- Para desactivar QoS, seleccione **personalizado, existente y ninguno**.
- Si selecciona **personalizado** y especifica un nivel de servicio existente, se seleccionará automáticamente un nivel local.
- A partir de ONTAP 9.9.1, si decide crear un nivel de servicio de rendimiento personalizado, puede utilizar System Manager para seleccionar manualmente el nivel local (**colocación manual**) en el que desea colocar el volumen que está creando.

Esta opción no está disponible si selecciona las opciones de caché remota o volumen FlexGroup.

- FlexGroup Volumes (seleccione **distribuir datos de volumen en el clúster**).

Esta opción no está disponible si ha seleccionado previamente **colocación manual** en **nivel de servicio de rendimiento**. De lo contrario, el volumen que va a añadir se convierte en volumen FlexVol de forma predeterminada.

- Permisos de acceso para los protocolos para los que se configuró el volumen.
- Protección de datos con SnapMirror (local o remoto) y, a continuación, especifique la política de protección y la configuración para el clúster de destino desde las listas desplegables.
- Seleccione **Guardar** para crear el volumen y agregarlo al clúster y a la VM de almacenamiento.



Después de guardar el volumen, vuelva a. [Paso 2 en el flujo de trabajo](#) para completar el aprovisionamiento de directorios iniciales.

Aprovisionar almacenamiento NAS para servidores Linux mediante NFS

Cree volúmenes para proporcionar almacenamiento para servidores Linux mediante el protocolo NFS con el Administrador del sistema de ONTAP (9.7 y posterior).

En este procedimiento, se crean nuevos volúmenes en un ["Máquina virtual de almacenamiento compatible con NFS existente"](#). Puede aceptar los valores predeterminados del sistema al configurar volúmenes o especificar configuraciones personalizadas.

Es posible crear volúmenes FlexVol o, para sistemas de archivos de gran tamaño con requisitos de alto rendimiento, se pueden crear volúmenes FlexGroup. Consulte también ["Aprovisione almacenamiento NAS para sistemas de archivos de gran tamaño con volúmenes FlexGroup"](#).

También puede guardar las especificaciones de este volumen en un libro de aplicaciones de Ansible. Para obtener más información, visite ["Utilice libros de aplicaciones Ansible para añadir o editar volúmenes o LUN"](#).

Si desea obtener detalles acerca del rango de funcionalidades del protocolo NFS de ONTAP, consulte ["Información general de referencia de NFS"](#).

Pasos

1. Añadir un volumen nuevo en una máquina virtual de almacenamiento habilitada para NFS
 - a. Haga clic en **almacenamiento > volúmenes** y, a continuación, haga clic en **Agregar**.
 - b. Introduzca un nombre, seleccione la máquina virtual de almacenamiento e introduzca un tamaño.

Solo se muestran las máquinas virtuales de almacenamiento configuradas con el protocolo NFS. Si solo hay disponible una VM de almacenamiento configurada con el protocolo SMB, no se muestra el campo **Storage VM**.

- Si hace clic en **Guardar** en este momento, System Manager utiliza valores predeterminados del sistema para crear y agregar un volumen FlexVol.



La política de exportación predeterminada concede acceso completo a todos los usuarios.

- Puede hacer clic en **más opciones** para personalizar la configuración del volumen y activar servicios como autorización, calidad de servicio y protección de datos. Consulte [Personalice la configuración del volumen](#), a continuación, vuelva aquí para completar los pasos siguientes.
2. [[paso 2-Complete-prov,paso 2 en el flujo de trabajo]] en un cliente Linux, haga lo siguiente para verificar el acceso.
 - a. Cree y monte el volumen con la interfaz de red de la máquina virtual de almacenamiento.
 - b. En el volumen recién montado, cree un archivo de prueba, escriba texto y, a continuación, elimine el archivo.

Después de verificar el acceso, puede ["restrinja el acceso de los clientes con la política de exportación del volumen"](#) Y establezca la propiedad de UNIX y los permisos que desee en el volumen montado.

Personalice la configuración del volumen

Se puede personalizar la configuración del volumen cuando se añaden volúmenes en lugar de aceptar los valores predeterminados del sistema.

Procedimiento

Después de hacer clic en **más opciones**, seleccione la funcionalidad que necesite e introduzca los valores necesarios.

- Caché para volumen remoto.
- Nivel de servicio de rendimiento (calidad de servicio, calidad de servicio).

A partir de ONTAP 9,8, puede especificar una política de calidad de servicio personalizada o deshabilitar la calidad de servicio, además de la selección de valor predeterminada.

- Para desactivar QoS, seleccione **personalizado, existente y ninguno**.
- Si selecciona **personalizado** y especifica un nivel de servicio existente, se seleccionará automáticamente un nivel local.
- A partir de ONTAP 9.9.1, si decide crear un nivel de servicio de rendimiento personalizado, puede utilizar System Manager para seleccionar manualmente el nivel local (**colocación manual**) en el que desea colocar el volumen que está creando.

Esta opción no está disponible si selecciona las opciones de caché remota o volumen FlexGroup.

- FlexGroup Volumes (seleccione **distribuir datos de volumen en el clúster**).

Esta opción no está disponible si ha seleccionado previamente **colocación manual** en **nivel de servicio de rendimiento**. De lo contrario, el volumen que va a añadir se convierte en volumen FlexVol de forma predeterminada.

- Permisos de acceso para los protocolos para los que se configuró el volumen.
- Protección de datos con SnapMirror (local o remoto) y, a continuación, especifique la política de protección y la configuración para el clúster de destino desde las listas desplegables.
- Seleccione **Guardar** para crear el volumen y agregarlo al clúster y a la VM de almacenamiento.



Después de guardar el volumen, vuelva a [\[step2-complete-prov\]](#) Para completar el aprovisionamiento de servidores Linux mediante NFS.

Otras maneras de hacerlo en ONTAP

| Para realizar esta tarea con... | Consulte... |
|---|---|
| System Manager Classic (ONTAP 9.7 y anterior) | "Información general de la configuración de NFS" |
| La interfaz de línea de comandos (CLI) de ONTAP | "Información general de la configuración de NFS con la interfaz de línea de comandos" |

Gestione el acceso mediante políticas de exportación

Habilite el acceso del cliente Linux a servidores NFS mediante políticas de exportación.

Este procedimiento crea o modifica las políticas de exportación de un ["Máquina virtual de almacenamiento compatible con NFS existente"](#).

Pasos

1. En System Manager, haga clic en **almacenamiento > volúmenes**.
2. Haga clic en un volumen con NFS activado y haga clic en **más**.
3. Haga clic en **Editar directiva de exportación** y, a continuación, haga clic en **Seleccionar una directiva existente** o **Agregar una nueva directiva**.

Aprovisionar almacenamiento NAS para servidores de Windows mediante SMB

Cree volúmenes para proporcionar almacenamiento para servidores Windows mediante el protocolo SMB mediante System Manager, que está disponible con ONTAP 9.7 y versiones posteriores.

En este procedimiento, se crean nuevos volúmenes en un ["Máquinas virtuales de almacenamiento habilitadas para SMB existentes"](#) y crea un recurso compartido para el directorio raíz del volumen (/). Puede aceptar los valores predeterminados del sistema al configurar volúmenes o especificar configuraciones personalizadas. Después de la configuración inicial de SMB, también puede crear recursos compartidos adicionales y modificar sus propiedades.

Es posible crear volúmenes FlexVol o, para sistemas de archivos de gran tamaño con requisitos de alto rendimiento, se pueden crear volúmenes FlexGroup. Consulte también ["Aprovisione almacenamiento NAS para sistemas de archivos de gran tamaño con volúmenes FlexGroup"](#).

También puede guardar las especificaciones de este volumen en un libro de aplicaciones de Ansible. Para obtener más información, visite ["Utilice libros de aplicaciones Ansible para añadir o editar volúmenes o LUN"](#).

Si desea obtener detalles acerca del rango de funcionalidades del protocolo SMB de ONTAP, consulte la ["Información general sobre la referencia de SMB"](#).

Antes de empezar

- A partir de ONTAP 9.13.1, puede habilitar los análisis de capacidad y el seguimiento de actividades de forma predeterminada en volúmenes nuevos. En System Manager, puede gestionar la configuración predeterminada en el nivel del clúster o de máquina virtual de almacenamiento. Para obtener más información, consulte [Active File System Analytics](#).

Pasos

1. Añadir un volumen nuevo en una máquina virtual de almacenamiento habilitada para SMB.

- a. Haga clic en **almacenamiento > volúmenes** y, a continuación, haga clic en **Agregar**.
- b. Introduzca un nombre, seleccione la máquina virtual de almacenamiento e introduzca un tamaño.

Solo se enumeran las máquinas virtuales de almacenamiento configuradas con el protocolo SMB. Si solo hay disponible una VM de almacenamiento configurada con el protocolo SMB, no se muestra el campo **Storage VM**.

- Si selecciona **Guardar** en este punto, System Manager utiliza los valores predeterminados del sistema para crear y añadir un volumen de FlexVol.
- Puede seleccionar **Más opciones** para personalizar la configuración del volumen y habilitar servicios como autorización, calidad de servicio y protección de datos. Consulte [Personalice la configuración del volumen](#), a continuación, vuelva aquí para completar los pasos siguientes.

2. cambie a un cliente de Windows para verificar que el recurso compartido esté accesible.

- a. En el Explorador de Windows, asigne una unidad al recurso compartido con el siguiente formato:
`_SMB_Server_Name__Share_Name__`
- b. En la unidad recién creada, cree un archivo de prueba, escriba texto y, a continuación, elimine el archivo.

Después de verificar el acceso, puede restringir el acceso de cliente con la ACL compartida y establecer las propiedades de seguridad deseadas en la unidad asignada. Consulte ["Cree un recurso compartido de SMB"](#) si quiere más información.

Añadir o modificar recursos compartidos

Puede añadir recursos compartidos adicionales después de la configuración inicial de SMB. Los recursos compartidos se crean con los valores predeterminados y las propiedades que se seleccionan. Estos se pueden modificar más adelante.

Puede establecer las siguientes propiedades de uso compartido al configurar un recurso compartido:


- Permisos de acceso
- Comparta propiedades
 - Habilitar la disponibilidad continua de los recursos compartidos que contienen Hyper-V y SQL Server en datos de SMB (empezando por ONTAP 9.10.1). Consulte también:
 - ["Disponibilidad continua de los requisitos de recursos compartidos para Hyper-V en SMB"](#)
 - ["Requisitos de recursos compartidos disponibles de forma continua para SQL Server en SMB"](#)
 - Cifre datos con SMB 3.0 al acceder al recurso compartido.

Después de la configuración inicial, también es posible modificar estas propiedades:

- Enlaces simbólicos
 - Activa o desactiva los enlaces simbólicos y las tintas alámbrica
- Comparta propiedades
 - Permitir a los clientes acceder al directorio de copias snapshot.
 - Habilite los bloqueos oportunistas, lo que permite a los clientes bloquear archivos y almacenar el contenido en la caché localmente (predeterminado).
 - Habilite la enumeración basada en acceso (ABE) para que muestre recursos compartidos basados en los permisos de acceso del usuario.

Procedimientos

Para añadir un nuevo recurso compartido en un volumen habilitado para SMB, haga clic en **almacenamiento > recursos compartidos**, haga clic en **Agregar** y seleccione **Compartir**.

Para modificar un recurso compartido existente, haga clic en **almacenamiento > Recursos compartidos** y, a continuación, haga clic en  Y seleccione **Editar**.

Personalice la configuración del volumen

Se puede personalizar la configuración del volumen cuando se añaden volúmenes en lugar de aceptar los valores predeterminados del sistema.

Procedimiento

Después de hacer clic en **más opciones**, seleccione la funcionalidad que necesite e introduzca los valores necesarios.

- Caché para volumen remoto.
- Nivel de servicio de rendimiento (calidad de servicio, calidad de servicio).

A partir de ONTAP 9.8, puede especificar una política de calidad de servicio personalizada o deshabilitar la calidad de servicio, además de la selección de valor predeterminada.

- Para desactivar QoS, seleccione **personalizado, existente y ninguno**.
- Si selecciona **personalizado** y especifica un nivel de servicio existente, se seleccionará automáticamente un nivel local.
- A partir de ONTAP 9.9.1, si decide crear un nivel de servicio de rendimiento personalizado, puede utilizar System Manager para seleccionar manualmente el nivel local (**colocación manual**) en el que desea colocar el volumen que está creando.

Esta opción no está disponible si selecciona las opciones de caché remota o volumen FlexGroup.

- FlexGroup Volumes (seleccione **distribuir datos de volumen en el clúster**).

Esta opción no está disponible si ha seleccionado previamente **colocación manual** en **nivel de servicio de rendimiento**. De lo contrario, el volumen que va a añadir se convierte en volumen FlexVol de forma predeterminada.

Esta opción no está disponible si ha seleccionado previamente *colocación manual en nivel de servicio de rendimiento. De lo contrario, el volumen que va a añadir se convierte en volumen FlexVol de forma predeterminada.

Permiso de acceso para los protocolos para los que está configurado el volumen.

***Protección de datos con SnapMirror (local o remoto) y, a continuación, especifique la política de protección y la configuración del clúster de destino desde las listas desplegables.**

***Haga clic en *Guardar** para crear el volumen y añadirlo al cluster y al equipo virtual de almacenamiento.

Se puede personalizar la configuración del volumen cuando se añaden volúmenes en lugar de aceptar los valores predeterminados del sistema.

Procedimiento

Después de hacer clic en **más opciones**, seleccione la funcionalidad que necesite e introduzca los valores necesarios.

- Caché para volumen remoto.
- Nivel de servicio de rendimiento (calidad de servicio, calidad de servicio).

A partir de ONTAP 9,8, puede especificar una política de calidad de servicio personalizada o deshabilitar la calidad de servicio, además de la selección de valor predeterminada.

- Para desactivar QoS, seleccione **personalizado, existente y ninguno**.
- Si selecciona **personalizado** y especifica un nivel de servicio existente, se seleccionará automáticamente un nivel local.
- A partir de ONTAP 9.9.1, si decide crear un nivel de servicio de rendimiento personalizado, puede utilizar System Manager para seleccionar manualmente el nivel local (**colocación manual**) en el que desea colocar el volumen que está creando.

Esta opción no está disponible si selecciona las opciones de caché remota o volumen FlexGroup.

- FlexGroup Volumes (seleccione **distribuir datos de volumen en el clúster**).

Esta opción no está disponible si ha seleccionado previamente **colocación manual** en **nivel de servicio de rendimiento**. De lo contrario, el volumen que va a añadir se convierte en volumen FlexVol de forma predeterminada.

- Permisos de acceso para los protocolos para los que se configuró el volumen.
- Protección de datos con SnapMirror (local o remoto) y, a continuación, especifique la política de protección y la configuración para el clúster de destino desde las listas desplegables.
- Seleccione **Guardar** para crear el volumen y agregarlo al clúster y a la VM de almacenamiento.



Después de guardar el volumen, vuelva a. [\[step2-compl-prov-win\]](#) Para completar el aprovisionamiento de servidores Windows mediante SMB.

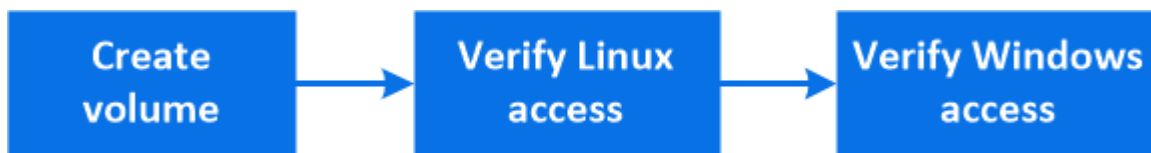
Otras maneras de hacerlo en ONTAP

| Para realizar esta tarea con... | Consulte... |
|---|--|
| System Manager Classic (ONTAP 9.7 y anterior) | "Información general de la configuración de SMB" |
| La interfaz de línea de comandos de ONTAP | "Información general de configuración de SMB con la CLI" |

Aprovisione almacenamiento NAS para Windows y Linux usando NFS y SMB

Cree volúmenes para proporcionar almacenamiento a los clientes mediante el protocolo NFS o SMB.

En este procedimiento, se crean nuevos volúmenes en un ["Máquinas virtuales de almacenamiento existentes habilitadas para los protocolos NFS y SMB"](#).



El protocolo NFS se utiliza con frecuencia en entornos Linux. El protocolo SMB se utiliza generalmente en entornos Windows. Sin embargo, tanto NFS como SMB pueden usarse tanto con Linux como con Windows.

Es posible crear volúmenes FlexVol o, para sistemas de archivos de gran tamaño con requisitos de alto rendimiento, se pueden crear volúmenes FlexGroup. Consulte ["Aprovisione almacenamiento NAS para sistemas de archivos de gran tamaño con volúmenes FlexGroup"](#).

También puede guardar las especificaciones de este volumen en un libro de aplicaciones de Ansible. Para obtener más información, visite ["Utilice libros de aplicaciones Ansible para añadir o editar volúmenes o LUN"](#).

Pasos

1. Añadir un nuevo volumen en una máquina virtual de almacenamiento habilitada para NFS y SMB.

- Haga clic en **almacenamiento > volúmenes** y, a continuación, haga clic en **Agregar**.
- Introduzca un nombre, seleccione la máquina virtual de almacenamiento e introduzca un tamaño.

Solo se muestran las máquinas virtuales de almacenamiento configuradas con los protocolos NFS y SMB. Si sólo está disponible un equipo virtual de almacenamiento configurado con los protocolos NFS y SMB, no se muestra el campo **Storage VM**.

- Haga clic en **Más opciones** y seleccione **Exportar a través de NFS**.

El valor predeterminado concede acceso total a todos los usuarios. Si lo desea, puede añadir más reglas restrictivas a la política de exportación.

- Seleccione **Compartir a través de SMB/CIFS**.

El recurso compartido se crea con una lista predeterminada de control de acceso (ACL) establecida en "Control total" para el grupo **Everyone**. Puede agregar restricciones a la ACL más adelante.

- e. Si hace clic en **Guardar** en este momento, System Manager utiliza valores predeterminados del sistema para crear y agregar un volumen FlexVol.

También puede continuar habilitando cualquier servicio necesario adicional, como la autorización, la calidad del servicio y la protección de datos. Consulte [Personalice la configuración del volumen](#), a continuación, vuelva aquí para completar los pasos siguientes.

2. en un cliente Linux, verifique que se pueda acceder a la exportación.
 - a. Cree y monte el volumen con la interfaz de red de la máquina virtual de almacenamiento.
 - b. En el volumen recién montado, cree un archivo de prueba, escriba texto y, a continuación, elimine el archivo.
3. En un cliente Windows, haga lo siguiente para verificar que se puede acceder al recurso compartido.
 - a. En el Explorador de Windows, asigne una unidad al recurso compartido con el siguiente formato:
_SMB_Server_Name__Share_Name_
 - b. En la unidad recién creada, cree un archivo de prueba, escriba texto y, a continuación, elimine el archivo.

Después de verificar el acceso, puede "[Restringir el acceso de los clientes con la política de exportación del volumen, restringir el acceso de los clientes con la ACL de uso compartido](#)" y establezca la propiedad y los permisos deseados en el volumen exportado y compartido.

Personalice la configuración del volumen

Se puede personalizar la configuración del volumen cuando se añaden volúmenes en lugar de aceptar los valores predeterminados del sistema.

Procedimiento

Después de hacer clic en **más opciones**, seleccione la funcionalidad que necesite e introduzca los valores necesarios.

- Caché para volumen remoto.
- Nivel de servicio de rendimiento (calidad de servicio, calidad de servicio).

A partir de ONTAP 9.8, puede especificar una política de calidad de servicio personalizada o deshabilitar la calidad de servicio, además de la selección de valor predeterminada.

- Para desactivar QoS, seleccione **personalizado, existente y ninguno**.
- Si selecciona **personalizado** y especifica un nivel de servicio existente, se seleccionará automáticamente un nivel local.
- A partir de ONTAP 9.9.1, si decide crear un nivel de servicio de rendimiento personalizado, puede utilizar System Manager para seleccionar manualmente el nivel local (**colocación manual**) en el que desea colocar el volumen que está creando.

Esta opción no está disponible si selecciona las opciones de caché remota o volumen FlexGroup.

- FlexGroup Volumes (seleccione **distribuir datos de volumen en el clúster**).

Esta opción no está disponible si ha seleccionado previamente **colocación manual** en **nivel de servicio de rendimiento**. De lo contrario, el volumen que va a añadir se convierte en volumen FlexVol de forma predeterminada.

- Permisos de acceso para los protocolos para los que se configuró el volumen.
- Protección de datos con SnapMirror (local o remoto) y, a continuación, especifique la política de protección y la configuración para el clúster de destino desde las listas desplegables.
- Seleccione **Guardar** para crear el volumen y agregarlo al clúster y a la VM de almacenamiento.

Después de guardar el volumen, vuelva a. [\[step2-compl-prov-nfs-smb\]](#) A un aprovisionamiento multiprotocolo completo para servidores Windows y Linux.

Otras maneras de hacerlo en ONTAP

| Para ejecutar estas tareas con... | Ver este contenido... |
|---|--|
| System Manager Classic (ONTAP 9.7 y anterior) | "Información general de la configuración de varios protocolos de SMB y NFS" |
| La interfaz de línea de comandos de ONTAP | "Información general de configuración de SMB con la CLI" "Información general de la configuración de NFS con la interfaz de línea de comandos" "Cuáles son los estilos de seguridad y sus efectos" "Distinción entre mayúsculas y minúsculas de nombres de archivos y directorios en un entorno multiprotocolo" |

Acceso de cliente seguro con Kerberos

Active Kerberos para garantizar el acceso al almacenamiento seguro para clientes NAS.

Este procedimiento configura Kerberos en una máquina virtual de almacenamiento existente habilitada para "NFS" o. "SMB".

Antes de empezar, debe haber configurado DNS, NTP y. "LDAP" en el sistema de almacenamiento.



Pasos

1. En la línea de comandos de ONTAP, establezca permisos UNIX para el volumen raíz de la máquina virtual de almacenamiento.
 - a. Visualice los permisos relevantes en el volumen raíz de la máquina virtual de almacenamiento:
`volume show -volume root_vol_name-fields user,group,unix-permissions`

El volumen raíz del equipo virtual de almacenamiento debe tener la siguiente configuración:

| Nombre... | Estableciendo... |
|---------------|------------------|
| UID | Raíz o ID 0 |
| GID | Raíz o ID 0 |
| Permisos UNIX | 755 |

a. Si no se muestran estos valores, utilice `volume modify` comando para actualizarlos.

2. Configure los permisos de usuario para el volumen raíz de la máquina virtual de almacenamiento.

a. Mostrar los usuarios UNIX locales: `vserver services name-service unix-user show -vserver vserver_name`

El equipo virtual de almacenamiento debe tener configurados los siguientes usuarios UNIX:

| Nombre de usuario | ID de usuario | ID del grupo principal |
|-------------------|---------------|------------------------|
| nfs | 500 | 0 |
| raíz | 0 | 0 |

+

Nota: el usuario NFS no es necesario si existe una asignación de nombres Kerberos-UNIX para el SPN del usuario cliente NFS; consulte el paso 5.

a. Si no se muestran estos valores, utilice `vserver services name-service unix-user modify` comando para actualizarlos.

3. Configure permisos de grupo para el volumen raíz de la máquina virtual de almacenamiento.

a. Mostrar los grupos UNIX locales: `vserver services name-service unix-group show -vserver vserver_name`

El equipo virtual de almacenamiento debe tener configurados los siguientes grupos UNIX:

| Nombre del grupo | ID de grupo |
|------------------|-------------|
| daemon | 1 |
| raíz | 0 |

a. Si no se muestran estos valores, utilice `vserver services name-service unix-group modify` comando para actualizarlos.

4. Cambie a System Manager para configurar Kerberos

5. En System Manager, haga clic en **almacenamiento > Storage VMs** y seleccione la VM de almacenamiento.

6. Haga clic en **Configuración**.

7. Haga clic en [→](#) En Kerberos.

8. Haga clic en **Agregar** en Kerberos Realm y complete las siguientes secciones:


- Añada Kerberos Realm

Introduzca los detalles de configuración según el proveedor de KDC.

- Agregue interfaz de red a Realm

Haga clic en **Agregar** y seleccione una interfaz de red.

9. Si lo desea, agregue asignaciones de nombres principales de Kerberos a nombres de usuario locales.

- Haga clic en **Almacenamiento > Storage VMs** y seleccione la VM de almacenamiento.
- Haga clic en **Configuración** y, a continuación, haga clic en  En **asignación de nombres**.
- En **Kerberos a UNIX**, agregue patrones y reemplazos usando expresiones regulares.



Proporcionar a los clientes acceso con servicios de nombres

Habilite ONTAP para que busque información de host, usuario, grupo o grupo de red mediante LDAP o NIS para autenticar clientes NAS.

Este procedimiento crea o modifica las configuraciones de LDAP o NIS en una máquina virtual de almacenamiento existente habilitada para "NFS" o "SMB".

Para las configuraciones LDAP, debe tener los detalles de configuración LDAP necesarios en el entorno y debe usar un esquema LDAP de ONTAP predeterminado.

Pasos

- Configure el servicio requerido: Haga clic en **almacenamiento > Storage VMs**.
- Seleccione la VM de almacenamiento, haga clic en **Configuración** y, a continuación, haga clic en  Para LDAP o NIS.
- Incluya cualquier cambio en el modificador de servicios de nombre: Haga clic en  En Cambio de servicios de nombres.

Gestionar directorios y archivos

Expanda la visualización de volumen de System Manager para ver y eliminar directorios y archivos.

A partir de ONTAP 9.9.1, se eliminan directorios con la funcionalidad de eliminación rápida de directorios y baja latencia.

Para obtener más información sobre cómo ver sistemas de archivos en ONTAP 9.9.1 y versiones posteriores, consulte "[Descripción general de File System Analytics](#)".

Paso

- Seleccione **almacenamiento > volúmenes**. Expanda un volumen para ver su contenido.

Gestione usuarios y grupos específicos de host con System Manager

A partir de ONTAP 9.10.1, puede utilizar System Manager para gestionar usuarios y grupos específicos de un host UNIX o Windows.

Puede realizar los siguientes procedimientos:

| Windows | UNIX |
|---|---|
| <ul style="list-style-type: none"> • Ver usuarios y grupos de Windows • [add-edit-delete-Windows] • [manage-windows-users] | <ul style="list-style-type: none"> • Ver usuarios y grupos UNIX • [add-edit-delete-UNIX] • [manage-unix-users] |



Ver usuarios y grupos de Windows

En System Manager, puede ver una lista de usuarios y grupos de Windows.

Pasos

1. En System Manager, haga clic en **almacenamiento > Storage VMs**.
2. Seleccione el equipo virtual de almacenamiento y, a continuación, seleccione la ficha **Configuración**.
3. Desplácese hasta el área **usuarios de host y grupos**.

La sección **Windows** muestra un resumen del número de usuarios de cada grupo asociado con el equipo virtual de almacenamiento seleccionado.





4. Haga clic en  En la sección **Windows**.
5. Haga clic en la ficha **grupos** y, a continuación, haga clic en  junto a un nombre de grupo para ver los detalles sobre ese grupo.
6. Para ver los usuarios de un grupo, seleccione el grupo y, a continuación, haga clic en la ficha **usuarios**.

Agregar, editar o eliminar un grupo Windows

En System Manager, puede gestionar grupos de Windows añadiendo, editando o eliminando grupos.

Pasos

1. En System Manager, consulte la lista de grupos de Windows. Consulte [Ver usuarios y grupos de Windows](#).
2. En la ficha **grupos**, puede administrar grupos con las siguientes tareas:


| Para realizar esta acción... | Realice estos pasos... |
|------------------------------|---|
| Agregar un grupo | <ol style="list-style-type: none">1. Haga clic en  Add.2. Introduzca la información del grupo.3. Especifique los privilegios.4. Especificar miembros de grupo (agregar usuarios locales, usuarios de dominio o grupos de dominio). |
| Editar un grupo | <ol style="list-style-type: none">1. Junto al nombre del grupo, haga clic en . A continuación, haga clic en Editar.2. Modifique la información del grupo. |
| Eliminar un grupo | <ol style="list-style-type: none">1. Marque la casilla situada junto al grupo o grupos que desee eliminar.2. Haga clic en  Delete. <p>Nota: También puede eliminar un solo grupo haciendo clic  Junto al nombre del grupo, haga clic en Eliminar.</p> |

Administrar usuarios de Windows

En System Manager, puede gestionar usuarios de Windows añadiendo, editando, eliminando, habilitando o deshabilitando. También puede cambiar la contraseña de un usuario de Windows.

Pasos

1. En System Manager, puede ver la lista de usuarios del grupo. Consulte [Ver usuarios y grupos de Windows](#).
2. En la ficha **usuarios**, puede administrar usuarios con las siguientes tareas:

| Para realizar esta acción... | Realice estos pasos... |
|-------------------------------|--|
| Agregar un usuario | <ol style="list-style-type: none">1. Haga clic en  Add.2. Introduzca la información del usuario. |
| Editar un usuario | <ol style="list-style-type: none">1. Junto al nombre de usuario, haga clic en , A continuación, haga clic en Editar.2. Modifique la información del usuario. |
| Eliminar un usuario | <ol style="list-style-type: none">1. Active la casilla situada junto al usuario o usuarios que desee eliminar.2. Haga clic en  Delete. <p>Nota: también puede eliminar un solo usuario haciendo clic en  Junto al nombre de usuario, haga clic en Eliminar.</p> |
| Cambiar contraseña de usuario | <ol style="list-style-type: none">1. Junto al nombre de usuario, haga clic en , A continuación, haga clic en Cambiar contraseña.2. Introduzca la nueva contraseña y confírmela. |
| Habilitar un usuario | <ol style="list-style-type: none">1. Marque la casilla situada junto a cada usuario deshabilitado que desee activar.2. Haga clic en  Enable. |
| Desactivar usuarios | <ol style="list-style-type: none">1. Marque la casilla junto a cada usuario habilitado que desee deshabilitar.2. Haga clic en  Disable. |

Ver usuarios y grupos UNIX

En System Manager, puede ver una lista de usuarios y grupos de UNIX.

Pasos

1. En System Manager, haga clic en **almacenamiento > Storage VMs**.
2. Seleccione el equipo virtual de almacenamiento y, a continuación, seleccione la ficha **Configuración**.
3. Desplácese hasta el área **usuarios de host y grupos**.

La sección **UNIX** muestra un resumen del número de usuarios de cada grupo asociado al VM de almacenamiento seleccionado.

4. Haga clic en [→](#) En la sección **UNIX**.
5. Haga clic en la ficha **grupos** para ver los detalles de ese grupo.
6. Para ver los usuarios de un grupo, seleccione el grupo y, a continuación, haga clic en la ficha **usuarios**.

Agregar, editar o eliminar un grupo UNIX

En System Manager, puede gestionar grupos UNIX agregándolos, editándolos o eliminarlos.

Pasos

1. En System Manager, consulte la lista de grupos UNIX. Consulte [Ver usuarios y grupos UNIX](#).
2. En la ficha **grupos**, puede administrar grupos con las siguientes tareas:

| Para realizar esta acción... | Realice estos pasos... |
|------------------------------|---|
| Agregar un grupo | <ol style="list-style-type: none">1. Haga clic en + Add .2. Introduzca la información del grupo.3. (Opcional) indique los usuarios asociados. |
| Editar un grupo | <ol style="list-style-type: none">1. Seleccione el grupo.2. Haga clic en ✎ Edit .3. Modifique la información del grupo.4. (Opcional) Añada o elimine usuarios. |
| Eliminar un grupo | <ol style="list-style-type: none">1. Seleccione el grupo o los grupos que desea eliminar.2. Haga clic en 🗑 Delete . |



Gestionar usuarios UNIX

En System Manager, puede gestionar usuarios de Windows añadiendo, editando o eliminando usuarios.

Pasos

1. En System Manager, puede ver la lista de usuarios del grupo. Consulte [Ver usuarios y grupos UNIX](#).
2. En la ficha **usuarios**, puede administrar usuarios con las siguientes tareas:

| Para realizar esta acción... | Realice estos pasos... |
|------------------------------|---|
| Agregar un usuario | <ol style="list-style-type: none">1. Haga clic en + Add .2. Introduzca la información del usuario. |

| | |
|---------------------|---|
| Editar un usuario | <ol style="list-style-type: none"> 1. Seleccione el usuario que desea editar. 2. Haga clic en  Edit . 3. Modifique la información del usuario. |
| Eliminar un usuario | <ol style="list-style-type: none"> 1. Seleccione el usuario o los usuarios que desee eliminar. 2. Haga clic en  Delete . |

Supervisar los clientes activos NFS

A partir de ONTAP 9.8, System Manager muestra qué conexiones de cliente NFS están activas cuando se otorga una licencia para NFS en un clúster.

Esto le permite verificar rápidamente qué clientes NFS se conectan de forma activa con una máquina virtual de almacenamiento, que está conectada pero inactiva, y que está desconectada.

Para cada dirección IP del cliente NFS, la pantalla **Clientes NFS** muestra:

- * Hora del último acceso
- * Dirección IP de interfaz de red
- * Versión de conexión NFS
- * Nombre de VM de almacenamiento

Además, una lista de clientes NFS activos en las últimas 48 horas también se muestra en la pantalla **Storage>Volumes** y un recuento de clientes NFS se incluye en la pantalla **Dashboard**.

Paso

1. Mostrar la actividad del cliente NFS: Haga clic en **hosts > clientes NFS**.

Habilitar el almacenamiento NAS

Almacenamiento NAS para servidores Linux mediante NFS

Crear o modificar equipos virtuales de almacenamiento para permitir que los servidores NFS sirva datos a clientes Linux.

Este procedimiento habilita una máquina virtual de almacenamiento nueva o existente para el protocolo NFS. Se asume que los detalles de la configuración están disponibles para cualquier servicio de red, autenticación o seguridad que requiera el entorno.




Pasos

1. Activación de NFS en una máquina virtual de almacenamiento.
 - a. Para los nuevos equipos virtuales de almacenamiento: Haga clic en **almacenamiento > Storage VMs**, haga clic en **Agregar**, introduzca un nombre de VM de almacenamiento y, en la ficha **SMB/CIFS, NFS**,

S3, seleccione **Activar NFS**.

- Confirme el idioma predeterminado.
- Agregue interfaces de red.
- Actualizar la información de cuenta del administrador de máquinas virtuales de almacenamiento (opcional).

b. Para las VM de almacenamiento existentes: Haga clic en **almacenamiento > Storage VMs**, seleccione una VM de almacenamiento, haga clic en **Configuración** y, a continuación, haga clic en  En **NFS**.

2. Abra la política de exportación del volumen raíz del equipo virtual de almacenamiento:


a. Haga clic en **almacenamiento > volúmenes**, seleccione el volumen raíz de la VM de almacenamiento (que por defecto es *volume-name_root*) y, a continuación, haga clic en la directiva que aparece en **Política de exportación**.


b. Haga clic en **Agregar** para agregar una regla.

- Especificación del cliente = 0.0.0.0/0
- Protocolos de acceso = NFS
- Detalles de acceso = solo lectura de UNIX

3. Configure DNS para la resolución de nombres de host: Haga clic en **almacenamiento > Storage VMs**, seleccione la VM de almacenamiento, haga clic en **Configuración** y, a continuación, haga clic en  En **DNS**.


4. Configure los servicios de nombres como corresponda.

a. Haga clic en **almacenamiento > Storage VMs**, seleccione la VM de almacenamiento, haga clic en **Configuración** y, a continuación, haga clic en para  LDAP o NIS.

b. Incluya cualquier cambio en el archivo de cambio de servicios de nombre: Haga clic en  En el icono Cambio de servicios de nombre.

5. Configure Kerberos si es necesario:

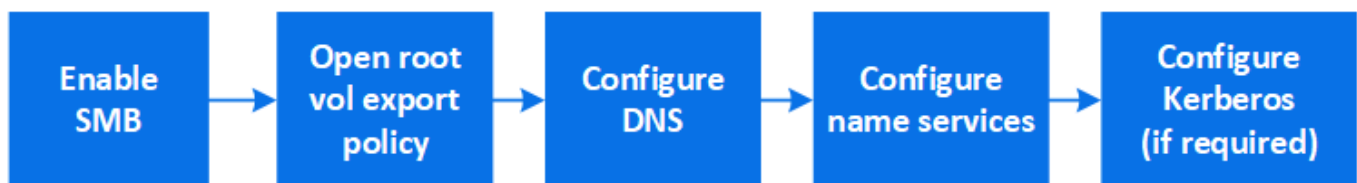
a. Haga clic en **almacenamiento > Storage VMs**, seleccione la VM de almacenamiento y, a continuación, haga clic en **Configuración**.

b. Haga clic en  En el mosaico Kerberos y, a continuación, haga clic en **Agregar**.





Habilite el almacenamiento NAS para servidores de Windows mediante SMB

Cree o modifique máquinas virtuales de almacenamiento para permitir que los servidores SMB sirviendo datos a clientes Windows.

Este procedimiento habilita una VM de almacenamiento nueva o existente para el protocolo SMB. Se asume que los detalles de la configuración están disponibles para cualquier servicio de red, autenticación o seguridad que requiera el entorno.



Pasos

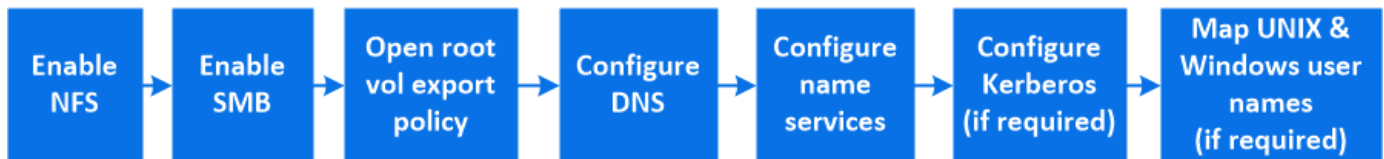
1. Habilite SMB en una máquina virtual de almacenamiento.
 - a. Para los nuevos equipos virtuales de almacenamiento: Haga clic en **almacenamiento > Storage VMs**, haga clic en **Agregar**, escriba un nombre de VM de almacenamiento y, en la ficha **SMB/CIFS, NFS, S3**, seleccione **Activar SMB/CIFS**.
 - Introduzca la siguiente información:
 - Nombre y contraseña del administrador
 - Nombre del servidor
 - Dominio de Active Directory
 - Confirme la unidad organizativa.
 - Confirme los valores DNS.
 - Confirme el idioma predeterminado.
 - Agregue interfaces de red.
 - Actualizar la información de cuenta del administrador de máquinas virtuales de almacenamiento (opcional).
 - b. Para las VM de almacenamiento existentes: Haga clic en **almacenamiento > Storage VMs**, seleccione una VM de almacenamiento, haga clic en **Configuración** y, a continuación, haga clic en  En **SMB**.
2. Abra la política de exportación del volumen raíz del equipo virtual de almacenamiento:
 - a. Haga clic en **almacenamiento > volúmenes**, seleccione el volumen raíz de la VM de almacenamiento (que por defecto es *volume-name_root*) y, a continuación, haga clic en la directiva que aparece en **Política de exportación**.
 - b. Haga clic en **Agregar** para agregar una regla.
 - Especificación del cliente = 0.0.0.0/0
 - Protocolos de acceso = bloque de mensajes del servidor
 - Detalles de acceso = sólo lectura NTFS
3. Configure DNS para la resolución de nombres de host:
 - a. Haga clic en **almacenamiento > Storage VMs**, seleccione la VM de almacenamiento, haga clic en **Configuración** y, a continuación, haga clic en  En **DNS**.
 - b. Cambie al servidor DNS y asigne el servidor SMB.
 - Cree entradas de búsqueda hacia delante (a - Registro de dirección) e inversa (PTR - Registro de puntero) para asignar el nombre del servidor SMB a la dirección IP de la interfaz de red de datos.
 - Si utiliza alias NetBIOS, cree una entrada de búsqueda de nombre canónico (registro de recursos CNAME) de alias para asignar cada alias a la dirección IP de la interfaz de red de datos del servidor SMB.
4. Configure los servicios de nombres como corresponda
 - a. Haga clic en **almacenamiento > Storage VMs**, seleccione la VM de almacenamiento, haga clic en **Configuración** y, a continuación, haga clic en  Bajo **LDAP** o **NIS**.
 - b. Incluya cualquier cambio en el archivo de cambio de servicios de nombre: Haga clic en  En **Cambio de servicios de nombres**.
5. Configure Kerberos si es necesario:
 - a. Haga clic en **almacenamiento > Storage VMs**, seleccione la VM de almacenamiento y, a continuación, haga clic en **Configuración**.

- b. Haga clic en ➔ En **Kerberos** y, a continuación, haga clic en **Agregar**.



Habilite el almacenamiento NAS para Windows y Linux usando NFS y SMB






Crear o modificar máquinas virtuales de almacenamiento para permitir que los servidores NFS y SMB proporcionen datos a clientes de Linux y Windows.

Este procedimiento permite que una máquina virtual de almacenamiento nueva o existente proporcione los protocolos NFS y SMB. Se asume que los detalles de la configuración están disponibles para cualquier servicio de red, autenticación o seguridad que requiera el entorno.



Pasos

1. Habilite NFS y SMB en una máquina virtual de almacenamiento.
 - a. Para los nuevos equipos virtuales de almacenamiento: Haga clic en **almacenamiento > Storage VMs**, haga clic en **Agregar**, escriba el nombre de un equipo virtual de almacenamiento y, en la ficha **SMB/CIFS, NFS, S3**, seleccione **Activar SMB/CIFS** y **Activar NFS**.
 - Introduzca la siguiente información:
 - Nombre y contraseña del administrador
 - Nombre del servidor
 - Dominio de Active Directory
 - Confirme la unidad organizativa.
 - Confirme los valores DNS.
 - Confirme el idioma predeterminado.
 - Agregue interfaces de red.
 - Actualizar la información de cuenta del administrador de máquinas virtuales de almacenamiento (opcional).
 - b. Para las VM de almacenamiento existentes: Haga clic en **almacenamiento > Storage VMs**, seleccione una VM de almacenamiento y, a continuación, haga clic en **Configuración**. Complete los siguientes subpasos si NFS o SMB todavía no está habilitado.
 - Haga clic en  En **NFS**.
 - Haga clic en  En **SMB**.
2. Abra la política de exportación del volumen raíz del equipo virtual de almacenamiento:
 - a. Haga clic en **almacenamiento > volúmenes**, seleccione el volumen raíz de la VM de almacenamiento (que por defecto es *volume-name_root*) y, a continuación, haga clic en la directiva que aparece en **Política de exportación**.
 - b. Haga clic en **Agregar** para agregar una regla.
 - Especificación del cliente = 0.0.0.0/0
 - Protocolos de acceso = NFS
 - Detalles de acceso = solo lectura para NFS

3. Configure DNS para la resolución de nombres de host:
 - a. Haga clic en **almacenamiento > Storage VMs**, seleccione la VM de almacenamiento, haga clic en **Configuración** y, a continuación, haga clic en  En **DNS**.
 - b. Cuando se complete la configuración de DNS, cambie al servidor DNS y asigne el servidor SMB.
 - Cree entradas de búsqueda hacia delante (a - Registro de dirección) e inversa (PTR - Registro de puntero) para asignar el nombre del servidor SMB a la dirección IP de la interfaz de red de datos.
 - Si utiliza alias NetBIOS, cree una entrada de búsqueda de nombre canónico (registro de recursos CNAME) de alias para asignar cada alias a la dirección IP de la interfaz de red de datos del servidor SMB.
4. Configure los servicios de nombres según sea necesario:
 - a. Haga clic en **almacenamiento > Storage VMs**, seleccione la VM de almacenamiento, haga clic en **Configuración** y, a continuación, haga clic en  Para LDAP o NIS.
 - b. Incluya cualquier cambio en el archivo de cambio de servicios de nombre: Haga clic en  En **Cambio de servicios de nombres**.
5. Configure Kerberos si es necesario: Haga clic en  En el mosaico Kerberos y, a continuación, haga clic en **Agregar**.
6. Asignar nombres de usuario de UNIX y Windows si es necesario: Haga clic en  En **asignación de nombres** y, a continuación, haga clic en **Agregar**.

Debe utilizar este procedimiento sólo si el sitio tiene cuentas de usuario de Windows y UNIX que no se asignan implícitamente, que es cuando la versión en minúscula de cada nombre de usuario de Windows coincide con el nombre de usuario de UNIX. Este procedimiento se puede realizar utilizando usuarios LDAP, NIS o locales. Si tiene dos conjuntos de usuarios que no coinciden, debe configurar la asignación de nombres.

Configure NFS con la CLI

Información general de la configuración de NFS con la interfaz de línea de comandos

Puede usar comandos de la CLI de ONTAP 9 para configurar el acceso del cliente de NFS a los archivos ubicados en un volumen o un qtree de una máquina virtual de almacenamiento (SVM) nueva o existente.

Use estos procedimientos si desea configurar el acceso a un volumen o qtree de la siguiente forma:

- Desea utilizar cualquier versión de NFS compatible actualmente con ONTAP: NFSv3, NFSv4, NFSv4.1, NFSv4.2 o NFSv4.1 con pNFS.
- Desea usar la interfaz de línea de comandos (CLI), no System Manager ni una herramienta de secuencias de comandos automatizadas.

Para usar System Manager para configurar el acceso multiprotocolo NAS, consulte ["Aprovisione almacenamiento NAS para Windows y Linux usando NFS y SMB"](#).

- Quiere utilizar las prácticas recomendadas, no explorar todas las opciones disponibles.

Puede obtener más detalles acerca de la sintaxis de los comandos en la ayuda de la CLI y en las páginas de manual de ONTAP.

- Se utilizarán permisos de archivos UNIX para proteger el nuevo volumen.
- Tiene privilegios de administrador de clúster, no de administrador de SVM.

Si desea obtener detalles acerca del rango de funcionalidades del protocolo NFS de ONTAP, consulte ["Información general de referencia de NFS"](#).

Otras maneras de hacerlo en ONTAP

| Para ejecutar estas tareas con... | Consulte... |
|--|--|
| System Manager rediseñado (disponible con ONTAP 9.7 y versiones posteriores) | "Aprovisionar almacenamiento NAS para servidores Linux mediante NFS" |
| System Manager Classic (disponible con ONTAP 9.7 y versiones anteriores) | "Información general de la configuración de NFS" |

Flujo de trabajo de configuración de NFS

La configuración de NFS implica la evaluación de los requisitos de almacenamiento físico y de red, y la selección de un flujo de trabajo específico para el objetivo; entre otras, la configuración del acceso NFS a una SVM nueva o existente, o la adición de un volumen o un qtree a una SVM existente que ya esté completamente configurada para el acceso NFS.

Preparación

Evaluar los requisitos de almacenamiento físico

Antes de aprovisionar almacenamiento NFS para clientes, debe asegurarse de que haya espacio suficiente en un agregado existente para el nuevo volumen. Si no lo hay, puede añadir discos a un agregado existente o crear uno nuevo con el tipo deseado.

Pasos

1. Mostrar el espacio disponible en los agregados existentes:

```
storage aggregate show
```

Si hay un agregado con suficiente espacio, registre su nombre en la hoja de cálculo.

```
cluster::> storage aggregate show
```

| Aggregate | Size | Available | Used% | State | #Vols | Nodes | RAID | Status |
|-----------|---------|-----------|-------|--------|-------|-------|----------|--------|
| aggr_0 | 239.0GB | 11.13GB | 95% | online | 1 | node1 | raid_dp, | normal |
| aggr_1 | 239.0GB | 11.13GB | 95% | online | 1 | node1 | raid_dp, | normal |
| aggr_2 | 239.0GB | 11.13GB | 95% | online | 1 | node2 | raid_dp, | normal |
| aggr_3 | 239.0GB | 11.13GB | 95% | online | 1 | node2 | raid_dp, | normal |
| aggr_4 | 239.0GB | 238.9GB | 95% | online | 5 | node3 | raid_dp, | normal |
| aggr_5 | 239.0GB | 239.0GB | 95% | online | 4 | node4 | raid_dp, | normal |

6 entries were displayed.

- Si no hay agregados con espacio suficiente, añada discos a un agregado existente mediante el `storage aggregate add-disks` o cree un nuevo agregado con el `storage aggregate create` comando.

Información relacionada

["Conceptos de ONTAP"](#)

Evaluar los requisitos de red

Antes de proporcionar almacenamiento NFS a los clientes, debe verificar que la red esté correctamente configurada para cumplir los requisitos de aprovisionamiento de NFS.

Lo que necesitará

Deben configurarse los siguientes objetos de red de clúster:

- Puertos físicos y lógicos
- Dominios de retransmisión
- Subredes (si es necesario)
- Espacios IP (según se requiera, además del espacio IP predeterminado)
- Grupos de conmutación por error (según sea necesario, además del grupo de conmutación por error predeterminado para cada dominio de retransmisión).
- Firewalls externos

Pasos

- Mostrar los puertos físicos y virtuales disponibles:

```
network port show
```

- Cuando sea posible, debe utilizar el puerto con la velocidad más alta para la red de datos.
- Todos los componentes de la red de datos deben tener la misma configuración de MTU para obtener

el mejor rendimiento.

2. Si tiene pensado utilizar un nombre de subred para asignar la dirección IP y el valor de máscara de red para una LIF, compruebe que la subred existe y que tenga suficientes direcciones disponibles: +

```
network subnet show
```

Las subredes contienen un grupo de direcciones IP que pertenecen a la misma subred de capa 3. Las subredes se crean mediante la `network subnet create` comando.

3. Mostrar espacios IP disponibles:

```
network ipspace show
```

Puede usar el espacio IP predeterminado o un espacio IP personalizado.

4. Si desea usar direcciones IPv6, compruebe que IPv6 esté habilitado en el clúster:

```
network options ipv6 show
```

Si es necesario, puede habilitar IPv6 con el `network options ipv6 modify` comando.

Decidir dónde provisionar la nueva capacidad de almacenamiento NFS

Antes de crear un volumen o qtree de NFS nuevo, debe decidir si colocarlo en una SVM nueva o existente y cuánta configuración necesita la SVM. Esta decisión determina su flujo de trabajo.

Opciones

- Si desea aprovisionar un volumen o qtree en una SVM nueva o en una SVM existente con NFS habilitado pero no configurado, complete los pasos de "Configuración del acceso NFS a una SVM" y "adición de almacenamiento NFS a una SVM habilitada para NFS".

[Configure el acceso NFS a una SVM](#)

[Añada almacenamiento NFS a una SVM habilitada para NFS](#)

Puede optar por crear una nueva SVM si se cumple alguna de las siguientes condiciones:

- Es la primera vez que habilita NFS en un clúster.
- Tiene SVM existentes en un clúster en el que no desea habilitar la compatibilidad con NFS.
- Tiene una o varias SVM habilitadas para NFS en un clúster y desea otro servidor NFS en un espacio de nombres aislado (escenario multi-tenancy).
También debe elegir esta opción para aprovisionar almacenamiento en una SVM existente con NFS habilitado pero no configurado. Este puede ser el caso si se creó la SVM para el acceso SAN o si no se habilitó ningún protocolo cuando se creó la SVM.

Después de habilitar NFS en la SVM, proceda a aprovisionar un volumen o un qtree.

- Si desea aprovisionar un volumen o un qtree en una SVM existente que esté completamente configurada para el acceso NFS, complete los pasos descritos en "Cómo añadir almacenamiento NFS a una SVM habilitada para NFS".

[Adición de almacenamiento NFS a una SVM habilitada para NFS](#)

Hoja de trabajo para recopilar información sobre la configuración de NFS

La hoja de datos de configuración de NFS le permite recopilar la información necesaria para configurar el acceso NFS para los clientes.

Debe rellenar una o ambas secciones de la hoja de datos en función de la decisión que haya tomado sobre dónde aprovisionar almacenamiento:

Si va a configurar el acceso NFS a una SVM, debe completar ambas secciones.

- Configuración del acceso NFS a una SVM
- Adición de capacidad de almacenamiento a una SVM habilitada para NFS

Si va a añadir capacidad de almacenamiento a una SVM habilitada para NFS, solo debe completar:

- Adición de capacidad de almacenamiento a una SVM habilitada para NFS

Consulte las páginas manuales de comandos para obtener más detalles sobre los parámetros.

Configure el acceso NFS a una SVM

Parámetros para crear una SVM

Proporcione estos valores con `vserver create` Si va a crear una SVM nueva.


| Campo | Descripción | Su valor |
|---|--|----------------------|
| <code>-vserver</code> | Un nombre que se proporciona para la SVM nueva que es un nombre de dominio completo (FQDN) o sigue otra convención que aplica nombres de SVM únicos en un clúster. | |
| <code>-aggregate</code> | El nombre de un agregado del clúster con espacio suficiente para la nueva capacidad de almacenamiento NFS. | |
| <code>-rootvolume</code> | Un nombre único que se proporciona para el volumen raíz de SVM. | |
| <code>-rootvolume-security-style</code> | Use el estilo de seguridad UNIX para la SVM. | <code>unix</code> |
| <code>-language</code> | Utilice la configuración de idioma predeterminada en este flujo de trabajo. | <code>C.UTF-8</code> |

| | | |
|---------|---|--|
| ipSPACE | Los espacios IP son espacios de direcciones IP distintos en los que residen (máquinas virtuales de almacenamiento (SVM)). | |
|---------|---|--|

Parámetros para crear un servidor NFS

Proporcione estos valores con `vserver nfs create` Comando cuando crea un servidor NFS nuevo y especifica las versiones NFS compatibles.

Si habilita NFSv4 o posterior, debe utilizar LDAP para mejorar la seguridad.

| Campo | Descripción | Su valor |
|-------------------------------|---|----------|
| -v3, -v4.0, -v4.1, -v4.1-pnfs | <p>Habilite las versiones de NFS según sea necesario.</p> <div>  <p>La versión 4.2 también es compatible con ONTAP 9.8 y versiones posteriores si v4.1 está habilitado.</p> </div> | |
| -v4-id-domain | ID asignando nombre de dominio. | |
| -v4-numeric-ids | Compatibilidad con ID de propietario numéricos (activado o desactivado). | |

Parámetros para crear una LIF

Proporcione estos valores con `network interface create` Comando cuando crea las LIF.

Si utiliza Kerberos, debe habilitar Kerberos en varias LIF.

| Campo | Descripción | Su valor |
|----------------|--|----------|
| -lif | Nombre que se proporciona para la nueva LIF. | |
| -role | Utilice el rol de LIF de datos en este flujo de trabajo. | data |
| -data-protocol | Utilice solo el protocolo NFS en este flujo de trabajo. | nfs |

| | | |
|------------------|--|------|
| -home-node | El nodo al que devuelve el LIF cuando el <code>network interface revert</code> El comando se ejecuta en la LIF. | |
| -home-port | El puerto o el grupo de interfaces al que devuelve la LIF cuando el <code>network interface revert</code> El comando se ejecuta en la LIF. | |
| -address | La dirección IPv4 o IPv6 del clúster que se usará para el acceso a los datos mediante la nueva LIF. | |
| -netmask | La máscara de red y la puerta de enlace para la LIF. | |
| -subnet | Un conjunto de direcciones IP. En lugar de <code>-address</code> y <code>-netmask</code> para asignar direcciones y máscaras de red automáticamente. | |
| -firewall-policy | Utilice la política de firewall de datos predeterminada en este flujo de trabajo. | data |

Parámetros para la resolución del nombre de host DNS

Proporcione estos valores con `vserver services name-service dns create` Comando cuando está configurando DNS.

| Campo | Descripción | Su valor |
|---------------|--|----------|
| -domains | Hasta cinco nombres de dominio DNS. | |
| -name-servers | Hasta tres direcciones IP para cada servidor de nombres DNS. | |

Información del servicio de nombres

Parámetros para crear usuarios locales

Estos valores se proporcionan si se crean usuarios locales mediante el `vserver services name-service unix-user create` comando. Si va a configurar usuarios locales cargando un archivo que contiene usuarios UNIX de un identificador de recursos uniforme (URI), no es necesario especificar estos valores manualmente.

| | Nombre de usuario (-user) | ID de usuario (-id) | ID de grupo (-primary-gid) | Nombre completo (-full-name) |
|---------|---------------------------|---------------------|----------------------------|------------------------------|
| Ejemplo | javier martínez | 123 | 100 | John Miller |
| 1 | | | | |
| 2 | | | | |
| 3 | | | | |
| ... | | | | |
| n | | | | |

Parámetros para crear grupos locales

Estos valores se proporcionan si está creando grupos locales mediante el `vserver services name-service unix-group create` comando. Si va a configurar grupos locales cargando un archivo que contiene grupos UNIX de un URI, no es necesario especificar estos valores manualmente.

| | Nombre del grupo (-name) | ID de grupo (-id) |
|---------|--------------------------|-------------------|
| Ejemplo | Ingeniería | 100 |
| 1 | | |
| 2 | | |
| 3 | | |
| ... | | |
| n | | |

Parámetros para NIS

Proporcione estos valores con `vserver services name-service nis-domain create` comando.



A partir de ONTAP 9.2, el campo `-nis-servers` reemplaza el campo `-servers`. Este nuevo campo puede tomar un nombre de host o una dirección IP para el servidor NIS.

| Campo | Descripción | Su valor |
|----------------------|--|----------|
| <code>-domain</code> | El dominio NIS que utilizará la SVM para las búsquedas de nombres. | |

| | | |
|--------------|---|---------------|
| -active | El servidor de dominio NIS activo. | true o. false |
| -servers | ONTAP 9.0, 9.1: Una o más direcciones IP de servidores NIS utilizadas por la configuración de dominio NIS. | |
| -nis-servers | ONTAP 9.2: Lista separada por comas de direcciones IP y nombres de host para los servidores NIS utilizados por la configuración de dominio. | |

Parámetros para LDAP

Proporcione estos valores con `vserver services name-service ldap client create` comando.

También se necesita un certificado de CA raíz autofirmado .pem archivo.



A partir de ONTAP 9.2, el campo `-ldap-servers` reemplaza el campo `-servers`. Este nuevo campo puede tomar un nombre de host o una dirección IP para el servidor LDAP.

| Campo | Descripción | Su valor |
|----------------|---|----------|
| -vserver | El nombre de la SVM para la cual se creará la configuración de cliente LDAP. | |
| -client-config | El nombre que se asigna para la nueva configuración de cliente LDAP. | |
| -servers | ONTAP 9.0, 9.1: Uno o varios servidores LDAP por dirección IP en una lista separada por comas. | |
| -ldap-servers | ONTAP 9.2: Lista separada por comas de direcciones IP y nombres de host para los servidores LDAP. | |
| -query-timeout | Utilice el valor predeterminado 3 segundos para este flujo de trabajo. | 3 |

| Campo | Descripción | Su valor |
|------------------------------------|--|----------|
| <code>-min-bind-level</code> | El nivel de autenticación de enlace mínimo. El valor predeterminado es <code>anonymous</code> . Debe definirse como <code>sasl</code> si está configurada la firma y el sellado. | |
| <code>-preferred-ad-servers</code> | Uno o varios servidores de Active Directory preferidos por dirección IP en una lista delimitada por comas. | |
| <code>-ad-domain</code> | El dominio de Active Directory. | |
| <code>-schema</code> | La plantilla de esquema que se va a utilizar. Puede utilizar un esquema predeterminado o personalizado. | |
| <code>-port</code> | Utilice el puerto predeterminado del servidor LDAP 389 para este flujo de trabajo. | 389 |
| <code>-bind-dn</code> | El nombre distintivo del usuario Bind. | |
| <code>-base-dn</code> | El nombre distintivo de la base. El valor predeterminado es <code>"</code> (raíz). | |
| <code>-base-scope</code> | Utilizar el ámbito de búsqueda base predeterminado <code>subnet</code> para este flujo de trabajo. | subnet |
| <code>-session-security</code> | Habilita la firma, firma y sellado LDAP. El valor predeterminado es <code>none</code> . | |
| <code>-use-start-tls</code> | Habilita LDAP sobre TLS. El valor predeterminado es <code>false</code> . | |

Parámetros para la autenticación Kerberos

Proporcione estos valores con `vserver nfs kerberos realm create` comando. Algunos de los valores variarán dependiendo de si utiliza Microsoft Active Directory como servidor de Key Distribution Center (KDC), o MIT u otro servidor UNIX KDC.

| Campo | Descripción | Su valor |
|-------|-------------|----------|
|-------|-------------|----------|

| | | |
|-----------------------------------|---|-------------------------------|
| <code>-vserver</code> | La SVM que se comunicará con el KDC. | |
| <code>-realm</code> | El dominio Kerberos. | |
| <code>-clock-skew</code> | Desfase de reloj permitido entre clientes y servidores. | |
| <code>-kdc-ip</code> | Dirección IP de KDC. | |
| <code>-kdc-port</code> | Número de puerto KDC. | |
| <code>-adserver-name</code> | Sólo Microsoft KDC: Nombre DEL servidor DE ANUNCIOS. | |
| <code>-adserver-ip</code> | Sólo Microsoft KDC: Dirección IP del servidor DE ANUNCIOS. | |
| <code>-adminserver-ip</code> | Sólo UNIX KDC: Dirección IP del servidor de administración. | |
| <code>-adminserver-port</code> | Sólo UNIX KDC: Número de puerto del servidor de administración. | |
| <code>-passwordserver-ip</code> | Sólo UNIX KDC: Dirección IP del servidor de contraseñas. | |
| <code>-passwordserver-port</code> | Sólo UNIX KDC: Puerto del servidor de contraseñas. | |
| <code>-kdc-vendor</code> | Proveedor KDC. | { Microsoft |
| Other } | <code>-comment</code> | Cualquier comentario deseado. |

Proporcione estos valores con `vserver nfs kerberos interface enable` comando.

| Campo | Descripción | Su valor |
|-----------------------|--|----------|
| <code>-vserver</code> | El nombre de la SVM para la cual desea crear una configuración de Kerberos. | |
| <code>-lif</code> | La LIF de datos en la que activará Kerberos. Puede habilitar Kerberos en varias LIF. | |

| | | |
|----------------------|---|--|
| -spn | El nombre del principio de servicio (SPN) | |
| -permitted-enc-types | Los tipos de cifrado permitidos para Kerberos a través de NFS; aes-256 se recomienda, dependiendo de las capacidades del cliente. | |
| -admin-username | Las credenciales de administrador de KDC para recuperar la clave secreta SPN directamente del KDC. Se requiere una contraseña | |
| -keytab-uri | El archivo keytab del KDC que contiene la clave SPN si no tiene credenciales de administrador KDC. | |
| -ou | La unidad organizativa (OU) en la que se creará la cuenta de servidor de Microsoft Active Directory al habilitar Kerberos mediante un Reino para Microsoft KDC. | |

Adición de capacidad de almacenamiento a una SVM habilitada para NFS

Parámetros para crear políticas y reglas de exportación

Proporcione estos valores con `vserver export-policy create` comando.

| Campo | Descripción | Su valor |
|-------------|---|----------|
| -vserver | El nombre de la SVM que alojará el nuevo volumen. | |
| -policyname | Nombre que se proporciona para una nueva política de exportación. | |

Puede proporcionar estos valores para cada regla con `vserver export-policy rule create` comando.

| Campo | Descripción | Su valor |
|--------------|--|----------|
| -clientmatch | Especificación de coincidencia del cliente. | |
| -ruleindex | Posición de la regla de exportación en la lista de reglas. | |

| | | |
|------------|---|-----|
| -protocol | Utilice NFS en este flujo de trabajo. | nfs |
| -rorule | Método de autenticación de acceso de solo lectura. | |
| -rwrule | Método de autenticación para acceso de lectura/escritura. | |
| -superuser | Método de autenticación para acceso de superusuario. | |
| -anon | ID de usuario al que se asignan usuarios anónimos. | |

Debe crear una o varias reglas para cada política de exportación.

| -ruleindex | -clientmatch | -rorule | -rwrule | -superuser | -anon |
|------------|--------------------------------|------------|---------|------------|-------|
| Ejemplos | 0.0.0.0/0,@rootaccess_netgroup | cualquiera | krb5 | act | 65534 |
| 1 | | | | | |
| 2 | | | | | |
| 3 | | | | | |
| ... | | | | | |
| n | | | | | |

Parámetros para crear un volumen

Proporcione estos valores con `volume create` comando si crea un volumen en lugar de un qtree.

| Campo | Descripción | Su valor |
|----------|--|----------|
| -vserver | El nombre de una SVM nueva o existente que alojará el nuevo volumen. | |
| -volume | Se suministra un nombre descriptivo único para el volumen nuevo. | |

| | | |
|------------------|--|------|
| -aggregate | El nombre de un agregado del clúster de con espacio suficiente para el nuevo volumen NFS. | |
| -size | Se proporciona un entero para el tamaño del nuevo volumen. | |
| -user | Nombre o ID del usuario que se establece como el propietario de la raíz del volumen. | |
| -group | Nombre o ID del grupo que se establece como el propietario de la raíz del volumen. | |
| --security-style | Utilice el estilo de seguridad UNIX para este flujo de trabajo. | unix |
| -junction-path | Ubicación bajo la raíz (/) donde se va a montar el nuevo volumen. | |
| -export-policy | Si tiene pensado utilizar una política de exportación existente, puede introducir su nombre al crear el volumen. | |

Parámetros para crear un qtree

Proporcione estos valores con `volume qtree create` comando si va a crear un qtree en lugar de un volumen.

| Campo | Descripción | Su valor |
|----------|---|----------|
| -vserver | El nombre de la SVM en la que reside el volumen que contiene el qtree. | |
| -volume | El nombre del volumen que contendrá el nuevo qtree. | |
| -qtree | Nombre descriptivo único que se proporciona para el nuevo qtree, con 64 caracteres o menos. | |

| | | |
|--------------------------------|--|--|
| <code>-qtree-path</code> | El argumento de ruta de qtree en el formato <code>/vol/volume_name/qtree_name\></code> se puede especificar en lugar de especificar el volumen y qtree como argumentos independientes. | |
| <code>-unix-permissions</code> | Optional: Los permisos de UNIX para el qtree. | |
| <code>-export-policy</code> | Si tiene pensado usar una política de exportación existente, puede introducir su nombre al crear el qtree. | |

Configure el acceso NFS a una SVM

Cree una SVM

Si no tiene al menos una SVM en un clúster para proporcionar acceso a los datos a los clientes NFS, debe crear una.

Antes de empezar

- A partir de ONTAP 9.13.1, puede establecer una capacidad máxima para una máquina virtual de almacenamiento. También puede configurar alertas cuando la SVM se acerca a un nivel de umbral de capacidad. Para obtener más información, consulte [Gestionar la capacidad de SVM](#).

Pasos

1. Cree una SVM:

```
vserver create -vserver vserver_name -rootvolume root_volume_name -aggregate
aggregate_name -rootvolume-security-style unix -language C.UTF-8 -ipspace
ipspace_name
```

- Utilice el valor UNIX del `-rootvolume-security-style` opción.
- Utilice el C.UTF-8 predeterminado `-language` opción.
- La `ipspace` el ajuste es opcional.

2. Compruebe la configuración y el estado de la SVM recién creada:

```
vserver show -vserver vserver_name
```

La Allowed Protocols El campo debe incluir NFS. Puede editar esta lista más tarde.

La Vserver Operational State el campo debe mostrar la `running` estado. Si muestra la `initializing` estado, significa que hubo un error en algunas operaciones intermedias, como la creación del volumen raíz, y que debe eliminarse la SVM y volver a crearla.

Ejemplos

El siguiente comando crea una SVM para acceder a los datos en el espacio IP ipspaceA:

```
cluster1::> vservers create -vservers vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style unix -language C.UTF-8 -ipspace ipspaceA
```

```
[Job 2059] Job succeeded:
Vserver creation completed
```

El siguiente comando muestra que se creó una SVM con un volumen raíz de 1 GB, y se inició automáticamente y está en `running` estado. El volumen raíz tiene una política de exportación predeterminada que no incluye reglas, por lo que el volumen raíz no se exporta tras la creación.

```
cluster1::> vservers show -vservers vs1.example.com
Vserver: vs1.example.com
Vserver Type: data
Vserver Subtype: default
Vserver UUID: b8375669-19b0-11e5-b9d1-00a0983d9736
Root Volume: root_vs1
Aggregate: aggr1
NIS Domain: -
Root Volume Security Style: unix
LDAP Client: -
Default Volume Language Code: C.UTF-8
Snapshot Policy: default
Comment:
Quota Policy: default
List of Aggregates Assigned: -
Limit on Maximum Number of Volumes allowed: unlimited
Vserver Admin State: running
Vserver Operational State: running
Vserver Operational State Stopped Reason: -
Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
Disallowed Protocols: -
QoS Policy Group: -
Config Lock: false
IPspace Name: ipspaceA
```



A partir de ONTAP 9.13.1, puede establecer una plantilla de grupo de políticas de calidad de servicio adaptativa, aplicando un límite máximo y mínimo de rendimiento a los volúmenes en la SVM. Solo puede aplicar esta política después de crear la SVM. Para obtener más información sobre este proceso, consulte [Defina una plantilla de grupo de políticas adaptativas](#).

Compruebe que el protocolo NFS está habilitado en la SVM

Antes de poder configurar y utilizar NFS en las SVM, debe comprobar que el protocolo esté habilitado.

Acerca de esta tarea

Esto suele hacerse durante la configuración de la SVM, pero si no ha habilitar el protocolo durante la configuración, puede habilitarla más adelante mediante el `vserver add-protocols` comando.



Una vez creado, no puede agregar ni quitar un protocolo de una LIF.

También puede deshabilitar protocolos en las SVM mediante el `vserver remove-protocols` comando.

Pasos

1. Compruebe qué protocolos están habilitados y deshabilitados actualmente para la SVM:

```
vserver show -vserver vserver_name -protocols
```

También puede utilizar el `vserver show-protocols` Comando para ver los protocolos habilitados actualmente en todas las SVM del clúster.

2. Si es necesario, habilite o deshabilite un protocolo:

- Para habilitar el protocolo NFS:

```
vserver add-protocols -vserver vserver_name -protocols nfs
```

- Para desactivar un protocolo:

```
vserver remove-protocols -vserver vserver_name -protocols protocol_name  
[,protocol_name,...]
```

3. Confirme que los protocolos activados y deshabilitados se han actualizado correctamente:

```
vserver show -vserver vserver_name -protocols
```

Ejemplo

El siguiente comando muestra qué protocolos están habilitados y deshabilitados actualmente (permitidos y deshabilitados) en la SVM llamada vs1:

```
vs1::> vserver show -vserver vs1.example.com -protocols
```

| Vserver | Allowed Protocols | Disallowed Protocols |
|-----------------|-------------------|------------------------|
| vs1.example.com | nfs | cifs, fcp, iscsi, ndmp |

El siguiente comando permite acceder a través de NFS mediante una adición `nfs` A la lista de protocolos habilitados en la SVM llamada vs1:

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols nfs
```

Abra la política de exportación del volumen raíz de la SVM

La política de exportación predeterminada del volumen raíz de la SVM debe incluir una regla para permitir que todos los clientes abran el acceso mediante NFS. Sin esa regla, todos los clientes NFS se ven privados del acceso a la SVM y sus volúmenes.

Acerca de esta tarea

Cuando se crea una SVM nueva, se crea automáticamente una política de exportación predeterminada (denominada predeterminada) para el volumen raíz de la SVM. Debe crear una o varias reglas para la política de exportación predeterminada para que los clientes puedan acceder a los datos de la SVM.

Debe verificar que el acceso está abierto a todos los clientes NFS de la política de exportación predeterminada y, más adelante, restringir el acceso a volúmenes individuales mediante la creación de políticas de exportación personalizadas para volúmenes o qtrees individuales.

Pasos

1. Si va a utilizar una SVM existente, compruebe la política de exportación de volumen raíz predeterminada:

```
vserver export-policy rule show
```

El resultado del comando debe ser similar a lo siguiente:

```
cluster::> vserver export-policy rule show -vserver vs1.example.com
-policyname default -instance

Vserver: vs1.example.com
Policy Name: default
Rule Index: 1
Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
RO Access Rule: any
RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
Superuser Security Types: any
Honor SetUID Bits in SETATTR: true
Allow Creation of Devices: true
```

Si existe una regla de este tipo que permite el acceso abierto, esta tarea se completa. De lo contrario, continúe con el siguiente paso.

2. Cree una regla de exportación para el volumen raíz de la SVM:

```
vserver export-policy rule create -vserver vserver_name -policyname default
-ruleindex 1 -protocol nfs -clientmatch 0.0.0.0/0 -rorule any -rwrule any
-superuser any
```

Si la SVM solo contendrá volúmenes protegidos por Kerberos, puede configurar las opciones de reglas de exportación `-rorule`, `-rwrule`, y `-superuser` para el volumen raíz a `krb5` o `krb5i`. Por ejemplo:

```
-rorule krb5i -rwrule krb5i -superuser krb5i
```

3. Compruebe la creación de reglas mediante `vserver export-policy rule show` comando.

Resultado

Cualquier cliente de NFS ahora puede acceder a cualquier volumen o qtree creado en la SVM.

Cree un servidor NFS

Tras comprobar que NFS tiene licencia en el clúster, puede utilizar la `vserver nfs create` Para crear un servidor NFS en la SVM y especificar las versiones de NFS que admite.

Acerca de esta tarea

Es posible configurar SVM para que admita una o varias versiones de NFS. Si admite NFSv4 o posteriores:

- El nombre de dominio de asignación del ID de usuario de NFSv4 debe ser igual en el servidor NFSv4 y en los clientes de destino.

No necesariamente debe ser el mismo que un nombre de dominio LDAP o NIS siempre que el servidor NFSv4 y los clientes utilicen el mismo nombre.

- Los clientes de destino deben admitir la configuración de ID numérico de NFSv4.
- Por motivos de seguridad, debe utilizar LDAP para los servicios de nombres en las puestas en marcha de NFSv4.

Antes de empezar

Debe haber configurado la SVM para permitir el protocolo NFS.

Pasos

1. Compruebe que NFS tiene licencia en el clúster:

```
system license show -package nfs
```

Si no lo está, póngase en contacto con su representante de ventas.

2. Cree un servidor NFS:

```
vserver nfs create -vserver vserver_name -v3 {enabled|disabled} -v4.0  
{enabled|disabled} -v4-id-domain nfsv4_id_domain -v4-numeric-ids  
{enabled|disabled} -v4.1 {enabled|disabled} -v4.1-pnfs {enabled|disabled}
```

Puede optar por habilitar cualquier combinación de versiones de NFS. Si desea admitir pNFS, debe habilitar ambos `-v4.1` y `-v4.1-pnfs` opciones.

Si activa v4 o posterior, también debe estar seguro de que las siguientes opciones están configuradas correctamente:

- `-v4-id-domain`

Este parámetro opcional especifica la parte de dominio del formulario de cadena de nombres de usuario y de grupo, tal como lo define el protocolo NFSv4. De forma predeterminada, ONTAP utiliza el

dominio NIS si se establece uno; si no es así, se utiliza el dominio DNS. Debe proporcionar un valor que coincida con el nombre de dominio utilizado por los clientes de destino.

° `-v4-numeric-ids`

Este parámetro opcional especifica si la compatibilidad con identificadores de cadena numéricos en los atributos de propietario de NFSv4 está habilitada. La configuración predeterminada está habilitada, pero debe verificar que los clientes de destino lo admitan.

Puede habilitar las funciones NFS adicionales más adelante mediante la `vserver nfs modify` comando.

3. Compruebe que NFS está ejecutando:

```
vserver nfs status -vserver vserver_name
```

4. Compruebe que NFS está configurado como se desea:

```
vserver nfs show -vserver vserver_name
```

Ejemplos

El siguiente comando crea un servidor NFS en la SVM llamada `vs1` con NFSv3 y NFSv4.0 habilitado:

```
vs1::> vserver nfs create -vserver vs1 -v3 enabled -v4.0 enabled -v4-id  
-domain my_domain.com
```

Los siguientes comandos verifican el estado y los valores de configuración del nuevo servidor NFS llamado `vs1`:

```
vs1::> vserver nfs status -vserver vs1  
The NFS server is running on Vserver "vs1".  
  
vs1::> vserver nfs show -vserver vs1  
  
                Vserver: vs1  
        General NFS Access: true  
                NFS v3: enabled  
                NFS v4.0: enabled  
        UDP Protocol: enabled  
        TCP Protocol: enabled  
    Default Windows User: -  
        NFSv4.0 ACL Support: disabled  
    NFSv4.0 Read Delegation Support: disabled  
    NFSv4.0 Write Delegation Support: disabled  
        NFSv4 ID Mapping Domain: my_domain.com  
...
```


Cree una LIF

Una LIF es una dirección IP asociada con un puerto físico o lógico. Si hay un fallo de un componente, un LIF puede conmutar al respaldo o migrarse a un puerto físico diferente, lo que continúa comunicándose con la red.

Lo que necesitará

- El puerto de red físico o lógico subyacente debe haber sido configurado para el administrador `up` estado.
- Si tiene pensado utilizar un nombre de subred para asignar la dirección IP y el valor de máscara de red para una LIF, la subred ya debe existir.

Las subredes contienen un grupo de direcciones IP que pertenecen a la misma subred de capa 3. Se crean mediante la `network subnet create` comando.

- El mecanismo para especificar el tipo de tráfico que maneja una LIF ha cambiado. Para ONTAP 9.5 y versiones anteriores, LIF usaba funciones para especificar el tipo de tráfico que gestionaría. A partir de ONTAP 9.6, los LIF utilizan políticas de servicio para especificar el tipo de tráfico que manejaría.

Acerca de esta tarea

- Puede crear tanto LIF IPv4 como IPv6 en el mismo puerto de red.
- Si utiliza la autenticación de Kerberos, habilite Kerberos en varias LIF.
- Si tiene un gran número de LIF en su clúster, puede verificar la capacidad de LIF admitida en el clúster mediante el `network interface capacity show` Comando y la capacidad de LIF admitida en cada nodo mediante el `network interface capacity details show` (en el nivel de privilegio avanzado).
- A partir de ONTAP 9.7, si ya existen otras LIF para la SVM en la misma subred, no es necesario especificar el puerto de inicio de la LIF. ONTAP elige automáticamente un puerto aleatorio en el nodo raíz especificado en el mismo dominio de retransmisión que las otras LIF ya configuradas en la misma subred.

A partir de la versión 9.4 de ONTAP, se admite FC-NVMe. Si crea una LIF FC-NVMe, debe tener en cuenta lo siguiente:

- El protocolo NVMe debe ser compatible con el adaptador de FC en el que se crea la LIF.
- FC-NVMe puede ser el único protocolo de datos en las LIF de datos.
- Debe configurarse un LIF que gestiona el tráfico de gestión para cada máquina virtual de almacenamiento (SVM) compatible con SAN.
- Las LIF y los espacios de nombres de NVMe deben alojarse en el mismo nodo.
- Solo se puede configurar una LIF NVMe que gestiona el tráfico de datos por SVM

Pasos

1. Cree una LIF:

```
network interface create -vserver vservice_name -lif lif_name -role data -data
-protocol nfs -home-node node_name -home-port port_name {-address IP_address
-netmask IP_address | -subnet-name subnet_name} -firewall-policy data -auto
-revert {true|false}
```

| Opción | Descripción |
|--------|-------------|
|--------|-------------|

| | |
|---|--|
| ONTAP 9.5 y anteriores | <code>`network interface create -vserver vservice_name -lif lif_name -role data -data-protocol nfs -home-node node_name -home-port port_name {-address IP_address -netmask IP_address</code> |
| <code>-subnet-name subnet_name} -firewall-policy data -auto-revert {true</code> | <code>false}`</code> |
| ONTAP 9.6 y posterior | <code>`network interface create -vserver vservice_name -lif lif_name -role data -data-protocol nfs -home-node node_name -home-port port_name {-address IP_address -netmask IP_address</code> |
| <code>-subnet-name subnet_name} -firewall-policy data -auto-revert {true</code> | <code>false}`</code> |

- La `-role` No es necesario parámetro cuando se crea una LIF con una política de servicio (a partir de ONTAP 9.6).
- La `-data-protocol` Debe especificarse el parámetro cuando se crea el LIF y no se puede modificar más adelante sin destruir ni volver a crear la LIF de datos.

La `-data-protocol` No se requiere el parámetro al crear una LIF con una política de servicio (a partir de ONTAP 9.6).

- `-home-node` Es el nodo al que devuelve el LIF cuando el `network interface revert` El comando se ejecuta en la LIF.

También puede especificar si el LIF debería volver automáticamente al nodo raíz y al puerto raíz con el `-auto-revert` opción.

- `-home-port` Es el puerto físico o lógico al que devuelve la LIF cuando el `network interface revert` El comando se ejecuta en la LIF.
- Puede especificar una dirección IP con el `-address` y.. `-netmask` o puede habilitar la asignación desde una subred con `-subnet_name` opción.
- Al usar una subred para suministrar la dirección IP y la máscara de red, si la subred se definió con una puerta de enlace, se añadirá automáticamente a la SVM una ruta predeterminada a esa puerta de enlace cuando se cree una LIF con dicha subred.
- Si asigna direcciones IP manualmente (sin una subred), es posible que deba configurar una ruta predeterminada para una puerta de enlace si hay clientes o controladores de dominio en una subred IP diferente. La `network route create` La página man contiene información sobre la creación de una ruta estática dentro de una SVM.
- Para la `-firewall-policy` opción, utilice el mismo valor predeterminado `data` Como el rol de LIF.

Si lo desea, puede crear y agregar una política de firewall personalizada más adelante.



A partir de ONTAP 9.10.1, las políticas de firewall están obsoletas y sustituidas por completo por políticas de servicios LIF. Para obtener más información, consulte ["Configurar políticas de firewall para LIF"](#).

- `-auto-revert` Permite especificar si un LIF de datos se revierte automáticamente a su nodo

principal en circunstancias como el inicio, los cambios en el estado de la base de datos de gestión o el momento en que se realiza la conexión de red. El valor predeterminado es `false`, pero puede establecerlo en `false` según las políticas de administración de red del entorno.

2. Compruebe que la LIF se ha creado correctamente mediante el `network interface show` comando.
3. Compruebe que se pueda acceder a la dirección IP configurada:

| Para verificar una... | Usar... |
|-----------------------|----------------------------|
| Dirección IPv4 | <code>network ping</code> |
| Dirección IPv6 | <code>network ping6</code> |

4. Si utiliza Kerberos, repita los pasos 1 a 3 para crear LIF adicionales.

Kerberos debe habilitarse por separado en cada uno de estos LIF.

Ejemplos

El siguiente comando crea una LIF y especifica la dirección IP y los valores de máscara de red mediante el `-address` y.. `-netmask` parámetros:

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol nfs -home-node node-4 -home-port elc -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

El siguiente comando crea una LIF y asigna valores de dirección IP y máscara de red a partir de la subred especificada (denominada `cliente1_sub`):

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol nfs -home-node node-3 -home-port elc -subnet-name
cliente1_sub -firewall-policy data -auto-revert true
```

El siguiente comando muestra todas las LIF del clúster-1. Data LIF `datalif1` y `datalif3` están configurados con direcciones IPv4, y `datalif4` está configurado con una dirección IPv6:

```
network interface show
```

| Vserver | Logical Interface | Status Admin/Oper | Network Address/Mask | Current Node | Current Port | Is |
|---------------------------|-------------------|-------------------|----------------------|--------------|--------------|-------|
| Home | | | | | | |
| ----- | ----- | ----- | ----- | ----- | ----- | ----- |
| cluster-1 | | | | | | |
| true | cluster_mgmt | up/up | 192.0.2.3/24 | node-1 | e1a | |
| node-1 | | | | | | |
| true | clus1 | up/up | 192.0.2.12/24 | node-1 | e0a | |
| true | clus2 | up/up | 192.0.2.13/24 | node-1 | e0b | |
| true | mgmt1 | up/up | 192.0.2.68/24 | node-1 | e1a | |
| node-2 | | | | | | |
| true | clus1 | up/up | 192.0.2.14/24 | node-2 | e0a | |
| true | clus2 | up/up | 192.0.2.15/24 | node-2 | e0b | |
| true | mgmt1 | up/up | 192.0.2.69/24 | node-2 | e1a | |
| vs1.example.com | | | | | | |
| true | datalif1 | up/down | 192.0.2.145/30 | node-1 | e1c | |
| vs3.example.com | | | | | | |
| true | datalif3 | up/up | 192.0.2.146/30 | node-2 | e0c | |
| true | datalif4 | up/up | 2001::2/64 | node-2 | e0c | |
| 5 entries were displayed. | | | | | | |

El siguiente comando muestra cómo crear una LIF de datos NAS asignada con default-data-files política de servicio:

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport e0d -service-policy default-data-files -subnet-name ipspace1
```

Habilite DNS para la resolución de nombres de host

Puede utilizar el `vserver services name-service dns` Comando para habilitar DNS en una SVM y configurarlo para usar DNS en la resolución de nombres de host. Los

nombres de host se resuelven mediante servidores DNS externos.

Lo que necesitará

Un servidor DNS para todo el sitio debe estar disponible para las búsquedas de nombre de host.

Debe configurar más de un servidor DNS para evitar un único punto de error. La `vserver services name-service dns create` El comando emite una advertencia si introduce solo un nombre de servidor DNS.

Acerca de esta tarea

La *Network Management Guide* contiene información acerca de la configuración de DNS dinámico en la SVM.

Pasos

- 1. Habilite DNS en la SVM:

```
vserver services name-service dns create -vserver vserver_name -domains
domain_name -name-servers ip_addresses -state enabled
```

El siguiente comando habilita los servidores DNS externos en la SVM vs1:

```
vserver services name-service dns create -vserver vs1.example.com
-domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
enabled
```



A partir de ONTAP 9.2, el `vserver services name-service dns create` El comando realiza una validación automática de la configuración e informa de un mensaje de error si ONTAP no puede ponerse en contacto con el servidor de nombres.

- 2. Muestre las configuraciones del dominio DNS mediante `vserver services name-service dns show` comando.

El siguiente comando muestra las configuraciones de DNS de todas las SVM del clúster:

```
vserver services name-service dns show
```

| Vserver | State | Domains | Name Servers |
|-----------------|---------|-------------|-----------------------------|
| cluster1 | enabled | example.com | 192.0.2.201, 192.0.2.202 |
| vs1.example.com | enabled | example.com | 192.0.2.201, 192.0.2.202 |

El siguiente comando muestra información detallada de la configuración de DNS para SVM vs1:

```
vserver services name-service dns show -vserver vs1.example.com
Vserver: vs1.example.com
Domains: example.com
Name Servers: 192.0.2.201, 192.0.2.202
Enable/Disable DNS: enabled
Timeout (secs): 2
Maximum Attempts: 1
```

3. Valide el estado de los servidores de nombres utilizando `vserver services name-service dns check` comando.

La `vserver services name-service dns check` El comando está disponible a partir de ONTAP 9.2.

```
vserver services name-service dns check -vserver vs1.example.com
```

| Vserver | Name Server | Status | Status Details |
|-----------------|-------------|--------|-------------------------|
| ----- | ----- | ----- | |
| vs1.example.com | 10.0.0.50 | up | Response time (msec): 2 |
| vs1.example.com | 10.0.0.51 | up | Response time (msec): 2 |

Configure los servicios de nombres

Información general de configure los servicios de nombres

Según la configuración del sistema de almacenamiento, ONTAP debe poder buscar la información del host, usuario, grupo o grupo de red para proporcionar un acceso adecuado a los clientes. Es necesario configurar los servicios de nombres para permitir que ONTAP acceda a los servicios de nombres locales o externos para obtener esta información.

Debe utilizar un servicio de nombres como NIS o LDAP para facilitar las búsquedas de nombres durante la autenticación del cliente. Se recomienda utilizar LDAP siempre que sea posible para obtener una mayor seguridad, especialmente cuando se pone en marcha NFSv4 o posteriores. También debe configurar usuarios y grupos locales en caso de que los servidores de nombres externos no estén disponibles.

La información del servicio de nombres debe mantenerse sincronizada en todas las fuentes.

Configure la tabla de cambio de servicio de nombres

Debe configurar correctamente la tabla del conmutador del servicio de nombres para permitir que ONTAP consulte servicios de nombres locales o externos para recuperar información de asignación de hosts, usuarios, grupos, netgroup o nombres.

Lo que necesitará

Debe haber decidido qué servicios de nombre desea utilizar para la asignación de host, usuario, grupo, netgroup o nombre según corresponda a su entorno.

Si planea utilizar netgroups, todas las direcciones IPv6 especificadas en netgroups deben acortarse y comprimirse según se especifica en RFC 5952.

Acerca de esta tarea

No incluya fuentes de información que no se estén utilizando. Por ejemplo, si NIS no se está utilizando en su entorno, no especifique el `-sources nis` opción.

Pasos

1. Agregue las entradas necesarias a la tabla de cambio de servicio de nombres:

```
vserver services name-service ns-switch create -vserver vserver_name -database database_name -sources source_names
```

2. Compruebe que la tabla de cambio de servicio de nombres contiene las entradas esperadas en el orden deseado:

```
vserver services name-service ns-switch show -vserver vserver_name
```

Si desea realizar alguna corrección, debe utilizar el `vserver services name-service ns-switch modify` o `vserver services name-service ns-switch delete` comandos.

Ejemplo

En el siguiente ejemplo se crea una entrada nueva en la tabla de switches del servicio de nombres para la SVM vs1 para utilizar el archivo de netgroup local y un servidor NIS externo para buscar información de netgroup en ese orden:

```
cluster::> vserver services name-service ns-switch create -vserver vs1  
-database netgroup -sources files,nis
```

Después de terminar

- Debe configurar los servicios de nombres que haya especificado para la SVM a fin de proporcionar acceso a los datos.
- Si elimina cualquier servicio de nombres para la SVM, también debe quitarlo de la tabla de switch de servicio de nombres.

Es posible que el acceso del cliente al sistema de almacenamiento no funcione como se espera, si no puede eliminar el servicio de nombres de la tabla de switches de servicio de nombres.

Configurar usuarios y grupos UNIX locales

Descripción general de la configuración de usuarios y grupos UNIX locales

Se pueden usar usuarios y grupos UNIX locales en la SVM para fines de autenticación y asignaciones de nombres. Puede crear usuarios y grupos de UNIX manualmente, o bien cargar un archivo que contenga usuarios o grupos de UNIX a partir de un identificador de recursos (URI) uniforme.

Hay un límite máximo predeterminado de 32,768 grupos de usuarios UNIX locales y miembros de grupo combinados en el clúster. El administrador del clúster puede modificar este límite.

Cree un usuario UNIX local

Puede utilizar el `vserver services name-service unix-user create` Comando para crear usuarios UNIX locales. Un usuario UNIX local es un usuario de UNIX que se crea en la SVM como una opción de servicios de nombres UNIX que se va a utilizar en el procesamiento de asignaciones de nombres.

Paso

1. Crear un usuario local de UNIX:

```
vserver services name-service unix-user create -vserver vserver_name -user
user_name -id integer -primary-gid integer -full-name full_name
```

`-user user_name` especifica el nombre de usuario. La longitud del nombre de usuario debe ser de 64 caracteres o menos.

`-id integer` Especifica el ID de usuario que asigna.

`-primary-gid integer` Especifica el ID del grupo principal. Esto agrega el usuario al grupo principal. Después de crear el usuario, puede agregar manualmente el usuario a cualquier grupo adicional deseado.

Ejemplo

El siguiente comando crea un usuario local de UNIX llamado johnm (nombre completo "John Miller") en la SVM llamada vs1. El usuario tiene el ID 123 y el ID 100 del grupo principal.

```
node::> vserver services name-service unix-user create -vserver vs1 -user
johnm -id 123
-primary-gid 100 -full-name "John Miller"
```

Cargar usuarios UNIX locales desde un URI

Como alternativa a la creación manual de usuarios de UNIX locales individuales en SVM, puede simplificar la tarea cargando una lista de usuarios de UNIX locales en SVM a partir de un identificador de recurso uniforme (URI) (`vserver services name-service unix-user load-from-uri`).

Pasos

1. Cree un archivo que contenga la lista de usuarios UNIX locales que desee cargar.

El archivo debe contener información del usuario en UNIX `/etc/passwd` formato:

```
user_name: password: user_ID: group_ID: full_name
```

El comando descarta el valor de `password` y los valores de los campos después del `full_name` campo (`home_directory` y `shell`).

El tamaño máximo de archivo admitido es de 2.5 MB.

2. Compruebe que la lista no contiene ninguna información duplicada.

Si la lista contiene entradas duplicadas, se produce un error al cargar la lista.

3. Copie el archivo en un servidor.

El sistema de almacenamiento debe acceder al servidor a través de HTTP, HTTPS, FTP o FTPS.

4. Determine cuál es el URI del archivo.

El URI es la dirección que se proporciona al sistema de almacenamiento para indicar dónde se encuentra el archivo.

5. Cargue el archivo que contiene la lista de usuarios UNIX locales en SVM desde el URI:

```
vserver services name-service unix-user load-from-uri -vserver vserver_name  
-uri {ftp|http|ftps|https}://uri -overwrite {true|false}
```

`-overwrite {true false}` especifica si se sobrescribirán las entradas. El valor predeterminado es `false`.

Ejemplo

El siguiente comando carga una lista de usuarios UNIX locales desde el URI

`ftp://ftp.example.com/passwd` En la SVM denominada `vs1`. Los usuarios existentes del SVM no se sobrescriben por información del URI.

```
node::> vserver services name-service unix-user load-from-uri -vserver vs1  
-uri ftp://ftp.example.com/passwd -overwrite false
```

Cree un grupo UNIX local

Puede utilizar el `vserver services name-service unix-group create`

Comando para crear grupos UNIX que son locales a la SVM. Los grupos UNIX locales se utilizan con usuarios UNIX locales.

Paso

1. Crear un grupo UNIX local:

```
vserver services name-service unix-group create -vserver vserver_name -name  
group_name -id integer
```

`-name group_name` especifica el nombre del grupo. La longitud del nombre del grupo debe ser de 64 caracteres o menos.

`-id integer` Especifica el ID de grupo que asigna.

Ejemplo

El siguiente comando crea un grupo local llamado `eng` en la SVM llamada `vs1`. El grupo tiene el ID 101.

```
vs1::> vserver services name-service unix-group create -vserver vs1 -name
eng -id 101
```

Agregar un usuario a un grupo UNIX local

Puede utilizar el `vserver services name-service unix-group adduser` Comando para agregar un usuario a un grupo UNIX suplementario local de la SVM.

Paso

1. Agregar un usuario a un grupo UNIX local:

```
vserver services name-service unix-group adduser -vserver vserver_name -name
group_name -username user_name
```

`-name group_name` Especifica el nombre del grupo UNIX al que se agregará el usuario además del grupo principal del usuario.

Ejemplo

El siguiente comando agrega un usuario llamado max a un grupo UNIX local llamado eng en la SVM llamada vs1:

```
vs1::> vserver services name-service unix-group adduser -vserver vs1 -name
eng
-username max
```

Cargar grupos UNIX locales desde un URI

Como alternativa a la creación manual de grupos UNIX locales individuales, puede cargar una lista de grupos UNIX locales en SVM desde un identificador de recurso (URI) uniforme mediante el `vserver services name-service unix-group load-from-uri` comando.

Pasos

1. Cree un archivo que contenga la lista de grupos UNIX locales que desee cargar.

El archivo debe contener información de grupo en UNIX `/etc/group` formato:

```
group_name: password: group_ID: comma_separated_list_of_users
```

El comando descarta el valor de `password` campo.

El tamaño máximo de archivo admitido es de 1 MB.

La longitud máxima de cada línea del archivo de grupo es de 32,768 caracteres.

2. Compruebe que la lista no contiene ninguna información duplicada.

La lista no debe contener entradas duplicadas o, de lo contrario, se producirá un error al cargar la lista. Si

ya hay entradas en la SVM, debe establecer el `-overwrite` parámetro a `true` para sobrescribir todas las entradas existentes con el nuevo archivo o asegurarse de que el nuevo archivo no contenga ninguna entrada que duplique las entradas existentes.

3. Copie el archivo en un servidor.

El sistema de almacenamiento debe acceder al servidor a través de HTTP, HTTPS, FTP o FTPS.

4. Determine cuál es el URI del archivo.

El URI es la dirección que se proporciona al sistema de almacenamiento para indicar dónde se encuentra el archivo.

5. Cargue el archivo que contiene la lista de grupos UNIX locales en la SVM desde el URI:

```
vserver services name-service unix-group load-from-uri -vserver vserver_name  
-uri {ftp|http|ftps|https}://uri -overwrite {true|false}
```

`-overwrite true false` especifica si se sobrescribirán las entradas. El valor predeterminado es `false`. Si especifica este parámetro como `true`, ONTAP reemplaza toda la base de datos de grupos UNIX locales existente de la SVM especificada por las entradas del archivo que se está cargando.

Ejemplo

El siguiente comando carga una lista de grupos UNIX locales del URI `ftp://ftp.example.com/group` En la SVM denominada `vs1`. Los grupos existentes de la SVM no se sobrescriben por información del URI.

```
vs1::> vserver services name-service unix-group load-from-uri -vserver vs1  
-uri ftp://ftp.example.com/group -overwrite false
```

Trabajar con netgroups

Información general sobre cómo trabajar con grupos de red

Puede utilizar netgroups para la autenticación de usuarios y para que coincida con los clientes en las reglas de directiva de exportación. Es posible proporcionar acceso a los grupos de red de servidores de nombres externos (LDAP o NIS), o puede cargar grupos de redes desde un identificador de recurso uniforme (URI) a las SVM mediante el `vserver services name-service netgroup load` comando.

Lo que necesitará

Antes de trabajar con netgroups, debe asegurarse de que se cumplen las siguientes condiciones:

- Todos los hosts de los grupos de red, independientemente del origen (NIS, LDAP o archivos locales), deben tener registros DNS tanto de reenvío (A) como de retroceso (PTR) para proporcionar búsquedas DNS de reenvío e inversa coherentes.

Además, si una dirección IP de un cliente tiene varios registros PTR, todos esos nombres de host deben ser miembros del netgroup y tener registros Correspondientes.

- Los nombres de todos los hosts de netgroups, independientemente de su origen (NIS, LDAP o archivos locales), deben estar escritos correctamente y utilizar el caso correcto. Las incoherencias de los casos en

los nombres de host utilizados en los grupos de redes pueden dar lugar a un comportamiento inesperado, como las comprobaciones de exportación fallidas.

- Todas las direcciones IPv6 especificadas en los grupos de red deben acortarse y comprimirse como se especifica en RFC 5952.

Por ejemplo, 2011:hu9:0:0:0:0:3:1 debe acortarse a 2011:hu9::3:1.

Acerca de esta tarea

Al trabajar con netgroups, puede realizar las siguientes operaciones:

- Puede utilizar el `vserver export-policy netgroup check-membership` Comando para ayudar a determinar si una IP de cliente es miembro de un determinado netgroup.
- Puede utilizar el `vserver services name-service getxxbyyy netgrp` comando para comprobar si un cliente forma parte de un netgroup.

El servicio subyacente para realizar la búsqueda se selecciona según el orden de cambio de servicio de nombres configurado.

Cargue grupos de redes en SVM

Uno de los métodos que se pueden utilizar para hacer coincidir clientes en las reglas de directiva de exportación es utilizando los hosts enumerados en netgroups. Puede cargar grupos de red de un identificador de recursos uniforme (URI) en las SVM como alternativa al uso de grupos de red almacenados en servidores de nombres externos (`vserver services name-service netgroup load`).

Lo que necesitará

Los archivos de grupos de red deben cumplir los siguientes requisitos antes de cargarlos en una SVM:

- El archivo debe utilizar el mismo formato de archivo de texto de netgroup adecuado que se utiliza para rellenar NIS.

ONTAP comprueba el formato del archivo de texto del grupo de red antes de cargarlo. Si el archivo contiene errores, no se cargará y se mostrará un mensaje que indique las correcciones que debe realizar en el archivo. Después de corregir los errores, puede volver a cargar el archivo netgroup en la SVM especificada.

- Los caracteres alfabéticos en los nombres de host del archivo netgroup deben ser en minúscula.
- El tamaño máximo de archivo admitido es de 5 MB.
- El nivel máximo admitido para los grupos de red de anidamiento es 1000.
- Sólo se pueden utilizar nombres de host DNS primarios al definir nombres de host en el archivo de grupo de red.

Para evitar problemas de acceso a la exportación, los nombres de host no deben definirse mediante registros CNAME o round robin de DNS.

- Las porciones de triples del usuario y del dominio en el archivo de netgroup deben mantenerse vacías porque ONTAP no las admite.

Solo se admite la parte host/IP.

Acerca de esta tarea

ONTAP admite búsquedas netgroup-by-host para el archivo de netgroup local. Después de cargar el archivo netgroup, ONTAP crea automáticamente un mapa netgroup.byhost para habilitar búsquedas netgroup-by-host. Esto puede acelerar significativamente las búsquedas de grupos de red locales al procesar reglas de políticas de exportación para evaluar el acceso de los clientes.

Paso

1. Cargue los grupos de redes en SVM desde un URI:

```
vserver services name-service netgroup load -vserver vserver_name -source {ftp|http|https|https}://uri
```

La carga del archivo de netgroup y la creación del mapa netgroup.byhost pueden tardar varios minutos.

Si desea actualizar los grupos de red, puede editar el archivo y cargar el archivo de netgroup actualizado en la SVM.

Ejemplo

El siguiente comando carga las definiciones de netgroup en la SVM denominada vs1 desde la URL HTTP `http://intranet/downloads/corp-netgroup`:

```
vs1::> vserver services name-service netgroup load -vserver vs1  
-source http://intranet/downloads/corp-netgroup
```

Compruebe el estado de las definiciones de netgroup

Después de cargar grupos de red en la SVM, puede usar la `vserver services name-service netgroup status` comando para verificar el estado de las definiciones de netgroup. Esto permite determinar si las definiciones de grupos de red son consistentes en todos los nodos que forman parte de la SVM.

Pasos

1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Compruebe el estado de las definiciones de netgroup:

```
vserver services name-service netgroup status
```

Puede visualizar información adicional en una vista más detallada.

3. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

Ejemplo

Una vez establecido el nivel de privilegio, el siguiente comando muestra el estado de netgroup para todas las SVM:

```
vs1::> set -privilege advanced
```

Warning: These advanced commands are potentially dangerous; use them only when

directed to do so by technical support.

Do you wish to continue? (y or n): y

```
vs1::*> vserver services name-service netgroup status
```

Virtual

| Server | Node | Load Time | Hash Value |
|--------|------|-----------|------------|
|--------|------|-----------|------------|

| | | | |
|-------|-------|-------|-------|
| ----- | ----- | ----- | ----- |
| ----- | ----- | ----- | ----- |

vs1

| | | | |
|--|-------|--------------------|--|
| | node1 | 9/20/2006 16:04:53 | |
|--|-------|--------------------|--|

e6cb38ec1396a280c0d2b77e3a84eda2

| | | | |
|--|-------|--------------------|--|
| | node2 | 9/20/2006 16:06:26 | |
|--|-------|--------------------|--|

e6cb38ec1396a280c0d2b77e3a84eda2

| | | | |
|--|-------|--------------------|--|
| | node3 | 9/20/2006 16:08:08 | |
|--|-------|--------------------|--|

e6cb38ec1396a280c0d2b77e3a84eda2

| | | | |
|--|-------|--------------------|--|
| | node4 | 9/20/2006 16:11:33 | |
|--|-------|--------------------|--|

e6cb38ec1396a280c0d2b77e3a84eda2

Cree una configuración de dominio NIS

Si se utiliza un Servicio de información de red (NIS) en el entorno para servicios de nombres, debe crear una configuración de dominio NIS para la SVM mediante el `vserver services name-service nis-domain create` comando.

Lo que necesitará

Todos los servidores NIS configurados deben estar disponibles y accesibles antes de configurar el dominio NIS en la SVM.

Si tiene previsto utilizar NIS para búsquedas en directorios, los mapas de sus servidores NIS no pueden tener más de 1,024 caracteres para cada entrada. No especifique el servidor NIS que no cumpla con este límite. De lo contrario, es posible que se produzca un error en el acceso del cliente que depende de las entradas NIS.

Acerca de esta tarea

Puede crear varios dominios NIS. Sin embargo, sólo puede utilizar una que esté establecida en `active`.

Si la base de datos NIS contiene un `netgroup.byhost` Map, ONTAP puede utilizarlo para realizar búsquedas más rápidas. La `netgroup.byhost` y `netgroup` los mapas del directorio deben mantenerse sincronizados en todo momento para evitar problemas de acceso de los clientes. A partir de ONTAP 9.7, NIS `netgroup.byhost` las entradas se pueden almacenar en caché mediante `vserver services name-service nis-domain netgroup-database` comandos.

No se admite el uso de NIS para la resolución del nombre de host.

Pasos

1. Cree una configuración de dominio NIS:

```
vserver services name-service nis-domain create -vserver vs1 -domain  
domain_name -active true -servers IP_addresses
```

Puede especificar hasta 10 servidores NIS.



A partir de ONTAP 9.2, el campo `-nis-servers` reemplaza el campo `-servers`. Este nuevo campo puede tomar un nombre de host o una dirección IP para el servidor NIS.

2. Compruebe que se ha creado el dominio:

```
vserver services name-service nis-domain show
```

Ejemplo

El siguiente comando crea y realiza una configuración de dominio NIS activa para un dominio NIS llamado nisdomain en la SVM denominada vs1 con un servidor NIS en la dirección IP 192.0.2.180:

```
vs1::> vserver services name-service nis-domain create -vserver vs1  
-domain nisdomain -active true -nis-servers 192.0.2.180
```

Utilice LDAP

Información general sobre cómo usar LDAP

Si se utiliza LDAP en su entorno para servicios de nombre, debe trabajar con el administrador de LDAP para determinar los requisitos y las configuraciones del sistema de almacenamiento adecuadas, habilitar la SVM como cliente LDAP.

A partir de ONTAP 9.10.1, el enlace de canal LDAP se admite de forma predeterminada tanto para las conexiones LDAP de los servicios de nombres como de Active Directory. ONTAP intentará establecer la vinculación de canal con las conexiones LDAP solo si Start-TLS o LDAPS está habilitado junto con la seguridad de la sesión establecida en Sign o Seal. Para deshabilitar o volver a habilitar el enlace de canal LDAP con servidores de nombres, utilice `-try-channel-binding` con el `ldap client modify` comando.

Para obtener más información, consulte

["2020 requisitos de enlace de canal LDAP y firma LDAP para Windows"](#).

- Antes de configurar LDAP para ONTAP, debe verificar que la implementación del sitio cumple las prácticas recomendadas para la configuración del cliente y el servidor LDAP. En particular, deben cumplirse las siguientes condiciones:
 - El nombre de dominio del servidor LDAP debe coincidir con la entrada del cliente LDAP.
 - Los tipos hash de contraseña de usuario LDAP compatibles con el servidor LDAP deben incluir los compatibles con ONTAP:
 - CRIPTA (todos los tipos) y SHA-1 (SHA, SSHA).
 - A partir de los valores hash de ONTAP 9.8, SHA-2 (SHA-256, SSH-384, SHA-512, SSHA-256, También se admiten SSHA-384 y SSHA-512).

- Si el servidor LDAP requiere medidas de seguridad de la sesión, debe configurarlas en el cliente LDAP.

Están disponibles las siguientes opciones de seguridad de la sesión:

- La firma LDAP (proporciona comprobación de la integridad de los datos) y la firma y el sellado LDAP (proporciona cifrado y comprobación de la integridad de los datos).
- INICIE TLS
- LDAPS (LDAP sobre TLS o SSL)
- Para habilitar consultas LDAP firmadas y selladas, se deben configurar los siguientes servicios:
 - Los servidores LDAP deben ser compatibles con el mecanismo SASL GSSAPI (Kerberos).
 - Los servidores LDAP deben tener registros DNS A/AAAA, así como registros PTR configurados en el servidor DNS.
 - Los servidores Kerberos deben tener registros SRV presentes en el servidor DNS.
- Para habilitar el INICIO de TLS o LDAPS, se deben tener en cuenta los siguientes puntos.
 - Se trata de una práctica recomendada de NetApp para usar Start TLS en lugar de LDAPS.
 - Si se usa LDAPS, el servidor LDAP debe habilitar para TLS o SSL en ONTAP 9.5 y versiones posteriores. SSL no es compatible con ONTAP 9.0-9.4.
 - Ya debe configurarse un servidor de certificados en el dominio.
- Para habilitar la búsqueda de referencias LDAP (en ONTAP 9.5 y posterior), se deben cumplir las siguientes condiciones:
 - Ambos dominios deben configurarse con una de las siguientes relaciones de confianza:
 - Bidireccional
 - Unidireccional, donde la primaria confía en el dominio de referencia
 - Padre-hijo
 - El DNS debe configurarse de modo que resuelva todos los nombres de servidor a los que se hace referencia.
 - Las contraseñas de dominio deben coincidir para autenticarse cuando `--bind-as-cifs-Server` se establece en `true`.

Las siguientes configuraciones no son compatibles con la búsqueda de referencias LDAP.



- Para todas las versiones de ONTAP:
 - Clientes LDAP en una SVM de administrador
- Para ONTAP 9.8 y versiones anteriores (se admiten en la versión 9.9.1 y posteriores):
 - Firma y sellado LDAP (la `-session-security` opción)
 - Conexiones TLS cifradas (la `-use-start-tls` opción)
 - Comunicaciones por puerto LDAPS 636 (el `-use-ldaps-for-ad-ldap` opción)

- Debe introducir un esquema de LDAP al configurar el cliente LDAP en la SVM.

En la mayoría de los casos, uno de los esquemas ONTAP predeterminados será apropiado. Sin embargo, si el esquema LDAP del entorno difiere de éste, debe crear un nuevo esquema de cliente LDAP para ONTAP antes de crear el cliente LDAP. Consulte a su administrador LDAP sobre los requisitos de su

entorno.

- No se admite el uso de LDAP para la resolución de nombres de host.

Si quiere más información

- ["Informe técnico de NetApp 4835: Cómo configurar LDAP en ONTAP"](#)
- ["Instale el certificado de CA raíz autofirmado en la SVM"](#)

Cree un nuevo esquema de cliente LDAP

Si el esquema LDAP del entorno difiere de los valores predeterminados de ONTAP, debe crear un nuevo esquema de cliente LDAP para ONTAP antes de crear la configuración de cliente LDAP.

Acerca de esta tarea

La mayoría de los servidores LDAP pueden utilizar los esquemas predeterminados proporcionados por ONTAP:

- MS-AD-BIS (el esquema preferido para la mayoría de los servidores AD de Windows 2012 y posteriores)
- AD-IDMU (servidores AD de Windows 2008, Windows 2012 y posteriores)
- AD-SFU (servidores Windows 2003 y anteriores de AD)
- RFC-2307 (SERVIDORES UNIX LDAP)

Si necesita utilizar un esquema LDAP no predeterminado, debe crearlo antes de crear la configuración del cliente LDAP. Consulte con el administrador LDAP antes de crear un nuevo esquema.

Los esquemas LDAP predeterminados proporcionados por ONTAP no se pueden modificar. Para crear un nuevo esquema, cree una copia y, a continuación, modifique la copia en consecuencia.

Pasos

1. Mostrar las plantillas de esquema de cliente LDAP existentes para identificar la que desea copiar:

```
vserver services name-service ldap client schema show
```

2. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

3. Haga una copia de un esquema de cliente LDAP existente:

```
vserver services name-service ldap client schema copy -vserver vserver_name  
-schema existing_schema_name -new-schema-name new_schema_name
```

4. Modifique el nuevo esquema y personalícelo para su entorno:

```
vserver services name-service ldap client schema modify
```

5. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

Cree una configuración de cliente LDAP

Si desea que ONTAP acceda a los servicios LDAP o Active Directory externos en el entorno, primero debe configurar un cliente LDAP en el sistema de almacenamiento.

Lo que necesitará

Uno de los tres primeros servidores de la lista de dominios resueltos de Active Directory debe estar activo y servir datos. De lo contrario, esta tarea falla.



Hay varios servidores, de los cuales más de dos servidores están inactivos en cualquier momento.

Pasos

1. Consulte con el administrador LDAP para determinar los valores de configuración adecuados para `vserver services name-service ldap client create` comando:

- a. Especifique una conexión basada en dominio o en dirección a los servidores LDAP.

La `-ad-domain` y `-servers` las opciones son mutuamente excluyentes.

- Utilice la `-ad-domain` Opción para habilitar la detección de servidores LDAP en el dominio de Active Directory.
 - Puede utilizar el `-restrict-discovery-to-site` Opción para restringir la detección del servidor LDAP al sitio predeterminado de CIFS para el dominio especificado. Si usa esta opción, también debe especificar el sitio predeterminado de CIFS con `-default-site`.
- Puede utilizar el `-preferred-ad-servers` Opción para especificar uno o varios servidores de Active Directory preferidos por dirección IP en una lista delimitada por comas. Una vez creado el cliente, puede modificar esta lista mediante el `vserver services name-service ldap client modify` comando.
- Utilice la `-servers` Opción para especificar uno o más servidores LDAP (Active Directory o UNIX) por dirección IP en una lista delimitada por comas.



La `-servers` La opción está en desuso en ONTAP 9.2. A partir de ONTAP 9.2, el `-ldap-servers` el campo sustituye al `-servers` campo. Este campo puede tomar un nombre de host o una dirección IP para el servidor LDAP.

- b. Especifique un esquema LDAP predeterminado o personalizado.

La mayoría de los servidores LDAP pueden utilizar los esquemas de sólo lectura predeterminados que proporciona ONTAP. Lo mejor es utilizar esos esquemas predeterminados a menos que haya un requisito para hacer lo contrario. Si es así, puede crear su propio esquema copiando un esquema predeterminado (son de sólo lectura) y modificando la copia.

Esquemas predeterminados:

- MS-AD-BIS

Basado en RFC-2307bis, este es el esquema LDAP preferido para la mayoría de implementaciones LDAP estándar de Windows 2012 y posteriores.

- AD-IDMU

Basado en Administración de identidades de Active Directory para UNIX, este esquema es apropiado para la mayoría de servidores AD de Windows 2008, Windows 2012 y posteriores.

- AD-SFU

Basado en los Servicios de Active Directory para UNIX, este esquema es apropiado para la mayoría de servidores de AD anteriores y Windows 2003.

- RFC-2307

Basado en RFC-2307 (*an Approach for using LDAP as a Network Information Service*), este esquema es apropiado para la mayoría de servidores UNIX AD.

c. Seleccione valores de enlace.

- `-min-bind-level {anonymous|simple|sasl}` especifica el nivel de autenticación de enlace mínimo.

El valor predeterminado es **anonymous**.

- `-bind-dn LDAP_DN` especifica el usuario de enlace.

Para los servidores de Active Directory, debe especificar el usuario en el formulario de cuenta (DOMINIO\usuario) o principal ([user@domain.com](#)). De lo contrario, debe especificar el usuario en el formulario Nombre completo (CN=user,DC=domain,DC=com).

- `-bind-password password` especifica la contraseña de enlace.

d. Seleccione las opciones de seguridad de la sesión, si es necesario.

Puede habilitar la firma y el sellado LDAP o LDAP over TLS si lo requiere el servidor LDAP.

- `--session-security {none|sign|seal}`

Puede habilitar la firma (`sign`, integridad de los datos), firma y sellado (`seal`, integridad y cifrado de los datos), o ninguno de los dos `none`, sin firma ni sellado). El valor predeterminado es `none`.

También debe configurar `-min-bind-level {sasl}` a menos que desee que la autenticación de enlace vuelva a estar en **anonymous** o **simple** si la firma y el enlace de sellado fallan.

- `-use-start-tls {true|false}`

Si se establece en **true** Además, el servidor LDAP lo admite, el cliente LDAP utiliza una conexión TLS cifrada con el servidor. El valor predeterminado es **false**. Debe instalar un certificado de CA raíz autofirmado del servidor LDAP para usar esta opción.



Si la máquina virtual de almacenamiento tiene un servidor SMB añadido a un dominio y el servidor LDAP es uno de los controladores de dominio del dominio inicial del servidor SMB, podrá modificar el `-session-security-for-ad-ldap` mediante el `vserver cifs security modify` comando.

e. Seleccione los valores de puerto, consulta y base.

Se recomiendan los valores predeterminados, pero debe verificar con el administrador de LDAP que

son adecuados para su entorno.

- `-port port` Especifica el puerto del servidor LDAP.

El valor predeterminado es 389.

Si tiene pensado utilizar Start TLS para proteger la conexión LDAP, debe utilizar el puerto predeterminado 389. Start TLS comienza como una conexión de texto sin formato sobre el puerto 389 predeterminado LDAP y esa conexión se actualiza a TLS. Si cambia el puerto, Start TLS falla.

- `-query-timeout integer` especifica el tiempo de espera de la consulta en segundos.

El intervalo permitido es de 1 a 10 segundos. El valor predeterminado es 3 segundos.

- `-base-dn LDAP_DN` Especifica el DN base.

Se pueden introducir varios valores si es necesario (por ejemplo, si la búsqueda de referencias LDAP está activada). El valor predeterminado es "" (raíz).

- `-base-scope {base|onelevel|subtree}` especifica el ámbito de búsqueda base.

El valor predeterminado es `subtree`.

- `-referral-enabled {true|false}` Especifica si la búsqueda de referencias LDAP está activada.

A partir de ONTAP 9.5, esto permite al cliente LDAP de ONTAP remitir solicitudes de búsqueda a otros servidores LDAP si el servidor LDAP principal devuelve una respuesta de referencia LDAP que indica que los registros deseados están presentes en los servidores LDAP remitidos. El valor predeterminado es **false**.

Para buscar registros presentes en los servidores LDAP a los que se hace referencia, se debe agregar la base-dn de los registros referidos a la base-dn como parte de la configuración del cliente LDAP.

2. Cree una configuración de cliente LDAP en la máquina virtual de almacenamiento:

```
vserver services name-service ldap client create -vserver vserver_name -client
-config client_config_name {-servers LDAP_server_list | -ad-domain ad_domain}
-preferred-ad-servers preferred_ad_server_list -restrict-discovery-to-site
{true|false} -default-site CIFS_default_site -schema schema -port 389 -query
-timeout 3 -min-bind-level {anonymous|simple|sasl} -bind-dn LDAP_DN -bind
-password password -base-dn LDAP_DN -base-scope subtree -session-security
{none|sign|seal} [-referral-enabled {true|false}]
```



Debe proporcionar el nombre de la máquina virtual de almacenamiento al crear una configuración de cliente LDAP.

3. Compruebe que la configuración del cliente LDAP se ha creado correctamente:

```
vserver services name-service ldap client show -client-config
client_config_name
```

Ejemplos

El siguiente comando crea una nueva configuración de cliente LDAP llamada ldap1 para que la máquina virtual de almacenamiento VS1 funcione con un servidor de Active Directory para LDAP:

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level simple -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100
```

El siguiente comando crea una nueva configuración de cliente LDAP denominada ldap1 para la máquina virtual de almacenamiento VS1 con el fin de funcionar con un servidor de Active Directory para LDAP en el que se requiere firma y sellado, y la detección del servidor LDAP está restringida a un sitio determinado para el dominio especificado:

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -restrict
-discovery-to-site true -default-site cifsdefaultsite.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100 -session-security seal
```

El siguiente comando crea una nueva configuración de cliente LDAP denominada ldap1 para que la máquina virtual de almacenamiento VS1 funcione con un servidor de Active Directory para LDAP en el que se requiere la búsqueda de referencias de LDAP:

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
"DC=adbasedomain,DC=example1,DC=com; DC=adrefdomain,DC=example2,DC=com"
-base-scope subtree -preferred-ad-servers 172.17.32.100 -referral-enabled
true
```

El siguiente comando modifica la configuración de cliente LDAP llamada ldap1 para la máquina virtual de almacenamiento VS1 especificando el DN base:

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn CN=Users,DC=addomain,DC=example,DC=com
```

El siguiente comando modifica la configuración de cliente LDAP denominada ldap1 para la máquina virtual de almacenamiento VS1 habilitando la búsqueda de referencias:

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn "DC=adbasedomain,DC=example1,DC=com;
DC=adrefdomain,DC=example2,DC=com" -referral-enabled true
```

Asocie la configuración del cliente LDAP con las SVM

Para habilitar LDAP en una SVM, debe usar el `vserver services name-service ldap create` Comando para asociar una configuración de cliente LDAP con la SVM.

Lo que necesitará

- Debe haber un dominio de LDAP dentro de la red y estar accesible para el clúster en el que está ubicada la SVM.
- Debe haber una configuración de cliente LDAP en la SVM.

Pasos

1. Habilite LDAP en la SVM:

```
vserver services name-service ldap create -vserver vserver_name -client-config
client_config_name
```



A partir de ONTAP 9.2, el `vserver services name-service ldap create` El comando realiza una validación automática de la configuración e informa de un mensaje de error si ONTAP no puede comunicarse con el servidor de nombres.

El siguiente comando habilita LDAP en el SVM "vs1" SVM y lo configura para utilizar la configuración del cliente LDAP "ldap1":

```
cluster1::> vserver services name-service ldap create -vserver vs1
-client-config ldap1 -client-enabled true
```

2. Validar el estado de los servidores de nombres mediante el comando `vserver Services NAME-service ldap check`.

El siguiente comando valida los servidores LDAP en la SVM VS1.

```
cluster1::> vserver services name-service ldap check -vserver vs1

| Vserver: vs1 |
| Client Configuration Name: cl |
| LDAP Status: up |
| LDAP Status Details: Successfully connected to LDAP server |
"10.11.12.13". |
```

El comando `name service check` está disponible a partir de ONTAP 9.2.

Compruebe los orígenes LDAP en la tabla de cambio de servicio de nombres

Debe comprobar que los orígenes LDAP para servicios de nombres figuran correctamente en la tabla de switches de servicio de nombres para la SVM.

Pasos

- 1. Mostrar el contenido de la tabla de cambio de servicio de nombres actual:

```
vserver services name-service ns-switch show -vserver svm_name
```

El siguiente comando muestra los resultados de la SVM My_SVM:

```
ie3220-a::> vserver services name-service ns-switch show -vserver My_SVM
Source
Vserver      Database      Order
-----
My_SVM       hosts         files,
              dns
My_SVM       group         files,ldap
My_SVM       passwd        files,ldap
My_SVM       netgroup      files
My_SVM       namemap       files
5 entries were displayed.
```

namemap especifica las fuentes en las que buscar información de asignación de nombres y en qué orden. En un entorno únicamente UNIX, esta entrada no es necesaria. La asignación de nombres sólo es necesaria en un entorno mixto que utilice UNIX y Windows.

- 2. Actualice el ns-switch entrada según corresponda:

| Si desea actualizar la entrada del interruptor ns para... | Introduzca el comando... |
|---|---|
| Información del usuario | vserver services name-service ns-switch modify -vserver vserver_name -database passwd -sources ldap,files |
| Información de grupo | vserver services name-service ns-switch modify -vserver vserver_name -database group -sources ldap,files |
| Información de netgroup | vserver services name-service ns-switch modify -vserver vserver_name -database netgroup -sources ldap,files |

Utilice Kerberos con NFS para una mayor seguridad

Información general sobre cómo utilizar Kerberos con NFS para una mayor seguridad

Si se utiliza Kerberos en su entorno para autenticación segura, debe trabajar con el administrador de Kerberos para determinar requisitos y configuraciones del sistema de almacenamiento apropiadas y, a continuación, habilitar la SVM como cliente Kerberos.

Su entorno debe cumplir las siguientes directrices:

- La implementación de su sitio debe seguir las prácticas recomendadas para la configuración del servidor Kerberos y del cliente antes de configurar Kerberos para ONTAP.
- Si es posible, utilice NFSv4 o posteriores si es necesaria la autenticación de Kerberos.

NFSv3 se puede utilizar con Kerberos. Sin embargo, todas las ventajas de seguridad de Kerberos solo se materializan en puestas en marcha de ONTAP de NFSv4 o posteriores.

- Para promover el acceso redundante al servidor, se debe habilitar Kerberos en varias LIF de datos en varios nodos del clúster mediante el mismo SPN.
- Cuando se habilita Kerberos en la SVM, debe especificarse uno de los siguientes métodos de seguridad en las reglas de exportación para volúmenes o qtrees en función de la configuración del cliente NFS.
 - `krb5` (Protocolo Kerberos v5)
 - `krb5i` (Protocolo Kerberos v5 con comprobación de integridad con sumas de comprobación)
 - `krb5p` (Protocolo Kerberos v5 con servicio de privacidad)

Además del servidor Kerberos y los clientes, para ONTAP se deben configurar los siguientes servicios externos con el fin de admitir Kerberos:

- Servicio de directorio

Debe utilizar un servicio de directorio seguro en su entorno, como Active Directory u OpenLDAP, que esté configurado para usar LDAP sobre SSL/TLS. No utilice NIS, cuyas solicitudes se envían en texto claro y, por lo tanto, no son seguras.

- NTP

Debe tener un servidor de tiempo de trabajo que ejecute NTP. Esto es necesario para evitar errores de autenticación de Kerberos debido a una desviación de tiempo.

- Resolución de nombres de dominio (DNS)

Cada cliente UNIX y cada LIF de SVM deben tener un registro de servicio (SRV) adecuado registrado con el KDC en zonas de búsqueda inversa y de reenvío. Todos los participantes deben poder resolverse correctamente a través de DNS.

Verifique los permisos para la configuración de Kerberos

Kerberos requiere que se establezcan determinados permisos de UNIX para el volumen raíz de la SVM y para los usuarios y grupos locales.

Pasos

1. Visualice los permisos relevantes en el volumen raíz de la SVM:

```
volume show -volume root_vol_name-fields user,group,unix-permissions
```

El volumen raíz de la SVM debe tener la siguiente configuración:

| Nombre... | Estableciendo... |
|---------------|------------------|
| UID | Raíz o ID 0 |
| GID | Raíz o ID 0 |
| Permisos UNIX | 755 |

Si no se muestran estos valores, utilice `volume modify` comando para actualizarlos.

2. Mostrar los usuarios UNIX locales:

```
vserver services name-service unix-user show -vserver vserver_name
```

La SVM debe tener configurados los siguientes usuarios de UNIX:

| Nombre de usuario | ID de usuario | ID del grupo principal | Comentar |
|-------------------|---------------|------------------------|---|
| nfs | 500 | 0 | <p>Necesario para la fase DE INICIALIZACIÓN de GSS.</p> <p>El primer componente del SPN de usuario del cliente NFS se utiliza como usuario.</p> <p>El usuario nfs no es necesario si existe una asignación de nombre Kerberos-UNIX para el SPN del usuario cliente NFS.</p> |
| raíz | 0 | 0 | Necesario para el montaje. |

Si no se muestran estos valores, puede usar `vserver services name-service unix-user modify` comando para actualizarlos.

3. Mostrar los grupos UNIX locales:

```
vserver services name-service unix-group show -vserver vserver_name
```

La SVM debe tener configurados los siguientes grupos UNIX:

| Nombre del grupo | ID de grupo |
|------------------|-------------|
| daemon | 1 |
| raíz | 0 |

Si no se muestran estos valores, puede usar `vserver services name-service unix-group modify` comando para actualizarlos.

Cree una configuración de dominio de Kerberos para NFS

Si desea que ONTAP acceda a servidores Kerberos externos en su entorno, primero debe configurar la SVM para que utilice un Reino de Kerberos existente. Para ello, necesita recopilar valores de configuración para el servidor Kerberos KDC y, a continuación, utilizar `vserver nfs kerberos realm create` Comando para crear la configuración de dominio de Kerberos en una SVM.

Lo que necesitará

El administrador del clúster debe haber configurado NTP en el sistema de almacenamiento, el cliente y el servidor KDC para evitar problemas de autenticación. Las diferencias de tiempo entre un cliente y un servidor (desfase de reloj) son una causa común de fallos de autenticación.

Pasos

1. Consulte con su administrador Kerberos para determinar los valores de configuración adecuados para suministrar con `vserver nfs kerberos realm create` comando.
2. Cree una configuración de dominio de Kerberos en la SVM:

```
vserver nfs kerberos realm create -vserver vserver_name -realm realm_name
{AD_KDC_server_values |AD_KDC_server_values} -comment "text"
```

3. Compruebe que la configuración de dominio Kerberos se ha creado correctamente:

```
vserver nfs kerberos realm show
```

Ejemplos

El siguiente comando crea una configuración de dominio Kerberos para NFS para la SVM vs1 que utiliza un servidor de Microsoft Active Directory como servidor KDC. El dominio Kerberos es AUTH.EXAMPLE.COM. El servidor de Active Directory se denomina ad-1 y su dirección IP es 10.10.8.14. La desviación del reloj permitida es de 300 segundos (valor predeterminado). La dirección IP del servidor KDC es 10.10.8.14 y su número de puerto es 88 (el valor predeterminado). "Microsoft Kerberos config" es el comentario.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
AUTH.EXAMPLE.COM -adserver-name ad-1
-adserver-ip 10.10.8.14 -clock-skew 300 -kdc-ip 10.10.8.14 -kdc-port 88
-kdc-vendor Microsoft
-comment "Microsoft Kerberos config"
```

El siguiente comando crea una configuración de dominio de Kerberos para NFS para la SVM vs1 que utiliza un MIT KDC. El dominio Kerberos es SECURITY.EXAMPLE.COM. La desviación del reloj permitida es de 300 segundos. La dirección IP del servidor KDC es 10.10.9.1 y su número de puerto es 88. El proveedor de KDC es otro que indica un proveedor de UNIX. La dirección IP del servidor de administración es 10.10.9.1 y su número de puerto es 749 (el valor predeterminado). La dirección IP del servidor de contraseñas es 10.10.9.1 y su número de puerto es 464 (el valor predeterminado). "UNIX Kerberos config" es el comentario.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
SECURITY.EXAMPLE.COM. -clock-skew 300
-kdc-ip 10.10.9.1 -kdc-port 88 -kdc-vendor Other -adminserver-ip 10.10.9.1
-adminserver-port 749
-passwordserver-ip 10.10.9.1 -passwordserver-port 464 -comment "UNIX
Kerberos config"
```

Configurar los tipos de cifrado permitidos de Kerberos para NFS

De forma predeterminada, ONTAP admite los siguientes tipos de cifrado para NFS Kerberos: DES, 3DES, AES-128 y AES-256. Puede configurar los tipos de cifrado permitidos para cada SVM para adaptarse a los requisitos de seguridad de su entorno concreto mediante el `vserver nfs modify` con el `-permitted-enc-types` parámetro.

Acerca de esta tarea

Para obtener la mayor compatibilidad del cliente, ONTAP admite de forma predeterminada tanto el cifrado des débil como el AES sólido. Esto significa, por ejemplo, que si desea aumentar la seguridad y su entorno lo admite, puede utilizar este procedimiento para deshabilitar DES y 3DES y requerir que los clientes utilicen sólo el cifrado AES.

Debería utilizar el cifrado más potente disponible. Para ONTAP, esto es AES-256. Debe confirmar con el administrador de KDC que este nivel de cifrado es compatible con su entorno.

- Habilitar o deshabilitar completamente AES (tanto AES-128 como AES-256) en las SVM es disruptivo porque destruye el archivo ORIGINAL DE DES principal/keytab, lo que requiere que se deshabilite la configuración de Kerberos en todos los LIF para la SVM.

Antes de realizar este cambio, debe comprobar que los clientes NFS no utilizan el cifrado AES en la SVM.

- La habilitación o deshabilitación DE DES o 3DES no requiere ningún cambio en la configuración de Kerberos en las LIF.

Paso

1. Habilite o deshabilite el tipo de cifrado permitido que desee:

| Si desea habilitar o deshabilitar... | Siga estos pasos... |
|--------------------------------------|---|
| DES o 3DES | <p>a. Configure los tipos de cifrado de la SVM permitidos por NFS Kerberos:</p> <pre data-bbox="889 268 1442 367">vserver nfs modify -vserver vserver_name -permitted-enc-types encryption_types</pre> <p>Separe varios tipos de cifrado con una coma.</p> <p>b. Compruebe que el cambio se ha realizado correctamente:</p> <pre data-bbox="889 577 1474 676">vserver nfs show -vserver vserver_name -fields permitted-enc- types</pre> |

| Si desea habilitar o deshabilitar... | Siga estos pasos... |
|--------------------------------------|---|
| AES-128 o AES-256 | <p>a. Identificar en qué SVM y Kerberos de LIF están habilitados:</p> <pre>vserver nfs kerberos interface show</pre> <p>b. Deshabilite Kerberos en todas las LIF de la SVM cuyo NFS Kerberos permitió el tipo de cifrado que desea modificar:</p> <pre>vserver nfs kerberos interface disable -lif lif_name</pre> <p>c. Configure los tipos de cifrado de la SVM permitidos por NFS Kerberos:</p> <pre>vserver nfs modify -vserver vserver_name -permitted-enc-types encryption_types</pre> <p>Separe varios tipos de cifrado con una coma.</p> <p>d. Compruebe que el cambio se ha realizado correctamente:</p> <pre>vserver nfs show -vserver vserver_name -fields permitted-enc-types</pre> <p>e. Vuelva a habilitar Kerberos en todas las LIF en la SVM:</p> <pre>vserver nfs kerberos interface enable -lif lif_name -spn service_principal_name</pre> <p>f. Compruebe que Kerberos está habilitado en todas las LIF:</p> <pre>vserver nfs kerberos interface show</pre> |

Habilite Kerberos en una LIF de datos

Puede utilizar el `vserver nfs kerberos interface enable` Comando para habilitar Kerberos en una LIF de datos. Esto permite que la SVM utilice servicios de seguridad Kerberos para NFS.

Acerca de esta tarea

Si utiliza un KDC de Active Directory, los primeros 15 caracteres de los SPN utilizados deben ser únicos entre las SVM dentro de un dominio o dominio.

Pasos

1. Cree la configuración de Kerberos NFS:

```
vserver nfs kerberos interface enable -vserver vserver_name -lif
logical_interface -spn service_principal_name
```

ONTAP requiere la clave secreta del SPN desde el KDC para habilitar la interfaz Kerberos.

Para los KDC de Microsoft, se contacta con el KDC y se emite un mensaje de nombre de usuario y contraseña en la CLI para obtener la clave secreta. Si necesita crear el SPN en una unidad organizativa diferente del dominio Kerberos, puede especificar el opcional `-ou` parámetro.

Para los KDC que no son de Microsoft, la clave secreta se puede obtener utilizando uno de los dos métodos:

| Si... | También debe incluir el siguiente parámetro con el comando... |
|---|---|
| Tenga las credenciales de administrador de KDC para recuperar la clave directamente desde el KDC | <code>-admin-username kdc_admin_username</code> |
| No tiene las credenciales de administrador de KDC, pero tiene un archivo keytab del KDC que contiene la clave | <code>-keytab-uri {ftp</code> |

2. Compruebe que Kerberos estaba habilitado en la LIF:

```
vserver nfs kerberos-config show
```

3. Repita los pasos 1 y 2 para habilitar Kerberos en varios LIF.

Ejemplo

El siguiente comando crea y verifica una configuración Kerberos de NFS para la SVM denominada vs1 en la interfaz lógica ves03-d1, con el SPN `nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM` en la OU `lab2ou`:

```
vs1::> vserver nfs kerberos interface enable -lif ves03-d1 -vserver vs2
-spnn nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM -ou "ou=lab2ou"

vs1::>vserver nfs kerberos-config show
      Logical
Vserver Interface Address      Kerberos  SPN
-----
vs0      ves01-a1
          10.10.10.30 disabled -
vs2      ves01-d1
          10.10.10.40 enabled  nfs/ves03-
d1.lab.example.com@TEST.LAB.EXAMPLE.COM
2 entries were displayed.
```

Añadir capacidad de almacenamiento a una SVM habilitada para NFS

Añadir capacidad de almacenamiento a una información general de SVM habilitada para NFS

Para añadir capacidad de almacenamiento a una SVM habilitada para NFS, debe crear un volumen o un qtree para proporcionar un contenedor de almacenamiento y crear o modificar una política de exportación para ese contenedor. Después, puede verificar el acceso del cliente NFS desde el clúster y probar el acceso desde los sistemas cliente.

Lo que necesitará

- NFS debe estar configurado por completo en la SVM.
- La política de exportación predeterminada del volumen raíz de la SVM debe contener una regla que permita el acceso a todos los clientes.
- Se debe completar cualquier actualización de la configuración de los servicios de nombres.
- Deben completarse todas las adiciones o modificaciones que se realicen en una configuración de Kerberos.

Cree una política de exportación

Antes de crear reglas de exportación, debe crear una política de exportación para mantenerlas. Puede utilizar el `vserver export-policy create` comando para crear una política de exportación.

Pasos

1. Cree una política de exportación:

```
vserver export-policy create -vserver vserver_name -policyname policy_name
```

El nombre de la política puede tener hasta 256 caracteres.

2. Compruebe que se ha creado la política de exportación:

```
vserver export-policy show -policyname policy_name
```

Ejemplo

Los siguientes comandos crean y verifican la creación de una política de exportación llamada `exp1` en la SVM llamada `vs1`:

```
vs1::> vserver export-policy create -vserver vs1 -policyname exp1

vs1::> vserver export-policy show -policyname exp1
Vserver          Policy Name
-----
vs1              exp1
```

Añada una regla a una política de exportación

Sin reglas, la política de exportación no puede ofrecer a los clientes acceso a los datos. Para crear una nueva regla de exportación, debe identificar los clientes y seleccionar un formato de coincidencia de cliente, seleccionar los tipos de acceso y seguridad, especificar una asignación de ID de usuario anónimo, seleccionar un número de índice de regla y seleccionar el protocolo de acceso. A continuación, puede utilizar la `vserver export-policy rule create` comando para añadir la nueva regla a una política de exportación.

Lo que necesitará

- La política de exportación a la que desea añadir las reglas de exportación ya debe existir.
- DNS debe haberse configurado correctamente en la SVM de datos y los servidores DNS deben tener entradas correctas para los clientes NFS.

Esto se debe a que ONTAP realiza búsquedas de DNS mediante la configuración de DNS de la SVM de datos para determinados formatos de coincidencia del cliente. Además, si se produce un error en la coincidencia de reglas de política de exportación, se puede evitar el acceso a los datos del cliente.

- Si va a autenticarse con Kerberos, debe haber determinado cuál de los siguientes métodos de seguridad se utiliza en sus clientes NFS:
 - `krb5` (Protocolo Kerberos V5)
 - `krb5i` (Protocolo Kerberos V5 con comprobación de integridad mediante sumas de comprobación)
 - `krb5p` (Protocolo Kerberos V5 con servicio de privacidad)

Acercas de esta tarea

No es necesario crear una nueva regla si una regla existente en una política de exportación cubre las coincidencias del cliente y los requisitos de acceso.

Si va a autenticarse con Kerberos y si se accede a todos los volúmenes de la SVM a través de Kerberos, puede configurar las opciones de regla de exportación `-rorule`, `-rwrule`, y, `-superuser` para el volumen raíz a. `krb5`, `krb5i`, o. `krb5p`.

Pasos

1. Identifique los clientes y el formato de coincidencia del cliente para la nueva regla.

La `-clientmatch` opción especifica los clientes a los que se aplica la regla. Se pueden especificar valores de coincidencia de clientes individuales o múltiples; las especificaciones de varios valores deben estar separadas por comas. Puede especificar la coincidencia en cualquiera de los siguientes formatos:

| Formato de coincidencia del cliente | Ejemplo |
|--|--|
| Nombre de dominio precedido por "." carácter | <code>.example.com</code> o. <code>.example.com,.example.net,...</code> |
| Nombre de host | <code>host1</code> o. <code>host1,host2, ...</code> |
| Dirección IPv4 | <code>10.1.12.24</code> o. <code>10.1.12.24,10.1.12.25, ...</code> |

| Formato de coincidencia del cliente | Ejemplo |
|---|---|
| Dirección IPv4 con una máscara de subred expresada como un número de bits | 10.1.12.10/4 o. 10.1.12.10/4,10.1.12.11/4,... |
| La dirección IPv4 con una máscara de red | 10.1.16.0/255.255.255.0 o. 10.1.16.0/255.255.255.0,10.1.17.0/255.255.255.0,... |
| Dirección IPv6 en formato punteado | ::1.2.3.4 o. ::1.2.3.4,::1.2.3.5,... |
| Dirección IPv6 con una máscara de subred expresada como un número de bits | ff::00/32 o. ff::00/32,ff::01/32,... |
| Un solo netgroup con el nombre del netgroup precedido por el carácter @ | @netgroup1 o. @netgroup1,@netgroup2,... |

También puede combinar tipos de definiciones de cliente; por ejemplo, .example.com,@netgroup1.

Al especificar direcciones IP, tenga en cuenta lo siguiente:

- No se permite introducir un rango de direcciones IP, como 10.1.12.10-10.1.12.70.

Las entradas con este formato se interpretan como cadenas de texto y se consideran nombres de host.

- Al especificar direcciones IP individuales en reglas de exportación para la gestión granular del acceso a clientes, no especifique direcciones IP que se encuentren asignadas de forma dinámica (por ejemplo, DHCP) o temporalmente (por ejemplo, IPv6).

De lo contrario, el cliente pierde el acceso cuando cambia su dirección IP.

- No se permite introducir una dirección IPv6 con una máscara de red, como ff::12/ff::00.

2. Seleccione los tipos de acceso y seguridad de las coincidencias del cliente.

Puede especificar uno o varios de los siguientes modos de acceso a los clientes que se autentican con los tipos de seguridad especificados:

- -rorule (acceso de solo lectura)
- -rwrule (acceso de lectura y escritura)
- -superuser (acceso raíz)



Un cliente solo puede obtener acceso de lectura y escritura para un tipo de seguridad específico si la regla de exportación permite también el acceso de solo lectura para ese tipo de seguridad. Si el parámetro de solo lectura es más restrictivo para un tipo de seguridad que el parámetro de lectura y escritura, es posible que el cliente no obtenga acceso de lectura/escritura. Lo mismo es cierto para el acceso de superusuario.

Puede especificar una lista separada por comas de varios tipos de seguridad para una regla. Si

especifica el tipo de seguridad como `any` o `never`, no especifique ningún otro tipo de seguridad. Elija entre los siguientes tipos de seguridad válidos:

| Cuando el tipo de seguridad se establece en... | Un cliente coincidente puede acceder a los datos exportados... |
|--|---|
| <code>any</code> | Siempre, independientemente del tipo de seguridad entrante. |
| <code>none</code> | Si se enumera solo, a los clientes con cualquier tipo de seguridad se les concede acceso como anónimos. Si se enumera con otros tipos de seguridad, se concede acceso a los clientes con un tipo de seguridad especificado y se concede acceso como anónimos a los clientes con cualquier otro tipo de seguridad. |
| <code>never</code> | Nunca, independientemente del tipo de seguridad entrante. |
| <code>krb5</code> | Si está autenticada por Kerberos 5. Sólo autenticación: El encabezado de cada solicitud y respuesta está firmado. |
| <code>krb5i</code> | Si se autentica con Kerberos 5i. Autenticación e integridad: Se firma el encabezado y el cuerpo de cada solicitud y respuesta. |
| <code>krb5p</code> | Si está autenticada por Kerberos 5p. Autenticación, integridad y privacidad: Se firma el encabezado y el cuerpo de cada solicitud y respuesta, y la carga útil de datos NFS está cifrada. |
| <code>ntlm</code> | Si se autentica con CIFS NTLM. |
| <code>sys</code> | Si se autentica mediante NFS AUTH_SYS. |

El tipo de seguridad recomendado es `sys`, O si se utiliza Kerberos, `krb5`, `krb5i`, o `krb5p`.

Si utiliza Kerberos con NFSv3, la regla de política de exportación debe permitir `-rorule y.. -rwrule` acceso a `sys` además de `krb5`. Esto se debe a la necesidad de permitir el acceso de Network Lock Manager (NLM) a la exportación.

3. Especifique una asignación de ID de usuario anónimo.

La `-anon` La opción especifica un ID de usuario o nombre de usuario de UNIX que se asigna a las solicitudes de cliente que llegan con un ID de usuario de 0 (cero), que normalmente se asocia con el nombre de usuario `root`. El valor predeterminado es `65534`. Los clientes NFS normalmente asocian el ID de usuario `65534` con el nombre de usuario `nobody` (también conocido como *root squashing*). En ONTAP,

este ID de usuario está asociado con el usuario pcuser. Para desactivar el acceso por parte de cualquier cliente con un ID de usuario de 0, especifique un valor de 65535.

4. Seleccione el orden de índice de reglas.

La `-ruleindex` opción especifica el número de índice de la regla. Las reglas se evalúan según su orden en la lista de números de índice; las reglas con números de índice más bajos se evalúan primero. Por ejemplo, la regla con el número de índice 1 se evalúa antes que la regla con el número de índice 2.

| Si va a añadir... | Realice lo siguiente... |
|--|---|
| La primera regla a una política de exportación | Introduzca 1. |
| Reglas adicionales a una política de exportación | <p>a. Mostrar reglas existentes en la política:</p> <pre>vserver export-policy rule show -instance -policyname <i>your_policy</i></pre> <p>b. Seleccione un número de índice para la nueva regla dependiendo de la orden en la que se debe evaluar.</p> |

5. Seleccione el valor de acceso de NFS aplicable: {nfs|nfs3|nfs4}.

`nfs` coincide con cualquier versión, `nfs3` y.. `nfs4` coincidir sólo con aquellas versiones específicas.

6. Cree la regla de exportación y añádala a una política de exportación existente:

```
vserver export-policy rule create -vserver vserver_name -policyname  
policy_name -ruleindex integer -protocol {nfs|nfs3|nfs4} -clientmatch { text |  
"text,text,..." } -rorule security_type -rwrule security_type -superuser  
security_type -anon user_ID
```

7. Muestre las reglas de la política de exportación para verificar que la nueva regla esté presente:

```
vserver export-policy rule show -policyname policy_name
```

El comando muestra un resumen de esa política de exportación, incluida una lista de reglas aplicadas a esa política. ONTAP asigna a cada regla un número de índice de regla. Una vez que conozca el número de índice de regla, puede utilizarlo para mostrar información detallada acerca de la regla de exportación especificada.

8. Compruebe que las reglas aplicadas a la política de exportación se han configurado correctamente:

```
vserver export-policy rule show -policyname policy_name -vserver vserver_name  
-ruleindex integer
```

Ejemplos

Los siguientes comandos crean y verifican la creación de una regla de exportación en la SVM con el nombre `vs1` en una política de exportación denominada `rs1`. La regla tiene el número de índice 1. La regla coincide con cualquier cliente del dominio `eng.company.com` y el `netgroup @netgroup1`. La regla habilita todo el acceso NFS. Permite el acceso de solo lectura y de lectura y escritura a los usuarios autenticados con `AUTH_SYS`.

Los clientes con el ID de usuario de UNIX 0 (cero) se anóniman a menos que se autenticuen con Kerberos.

```
vs1::> vserver export-policy rule create -vserver vs1 -policyname expl
-ruleindex 1 -protocol nfs
-clientmatch .eng.company.com,@netgoup1 -rorule sys -rwrule sys -anon
65534 -superuser krb5
```

```
vs1::> vserver export-policy rule show -policyname nfs_policy
```

| Virtual Server | Policy Name | Rule Index | Access Protocol | Client Match | RO Rule |
|-------------------|----------------|---------------|--------------------|--------------------------------|------------|
| vs1 | expl | 1 | nfs | eng.company.com, @netgroup1 | sys |

```
vs1::> vserver export-policy rule show -policyname expl -vserver vs1
-ruleindex 1
```

```

Vserver: vs1
Policy Name: expl
Rule Index: 1
Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
eng.company.com,@netgroup1
RO Access Rule: sys
RW Access Rule: sys
User ID To Which Anonymous Users Are Mapped: 65534
Superuser Security Types: krb5
Honor SetUID Bits in SETATTR: true
Allow Creation of Devices: true
```

Los siguientes comandos crean y verifican la creación de una regla de exportación en la SVM llamada vs2 en una política de exportación llamada expol2. La regla tiene el número de índice 21. La regla coincide con los clientes con los miembros del netgroup dev_netgroup_main. La regla habilita todo el acceso NFS. Permite el acceso de solo lectura para los usuarios que se autentican con AUTH_SYS y requiere autenticación de Kerberos para acceso de lectura/escritura y raíz. A los clientes con el ID de usuario de UNIX 0 (cero) se les deniega el acceso raíz a menos que se autenticuen con Kerberos.

```
vs2::> vsserver export-policy rule create -vsserver vs2 -policyname expol2
-ruleindex 21 -protocol nfs
-clientmatch @dev_netgroup_main -rorule sys -rwrule krb5 -anon 65535
-superuser krb5
```

```
vs2::> vsserver export-policy rule show -policyname nfs_policy
```

| Virtual Server | Policy Name | Rule Index | Access Protocol | Client Match | RO Rule |
|----------------|-------------|------------|-----------------|--------------------|---------|
| vs2 | expol2 | 21 | nfs | @dev_netgroup_main | sys |

```
vs2::> vsserver export-policy rule show -policyname expol2 -vsserver vs1
-ruleindex 21
```

```

Vserver: vs2
Policy Name: expol2
Rule Index: 21
Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
                                         @dev_netgroup_main
RO Access Rule: sys
RW Access Rule: krb5
User ID To Which Anonymous Users Are Mapped: 65535
Superuser Security Types: krb5
Honor SetUID Bits in SETATTR: true
Allow Creation of Devices: true

```

Cree un volumen o un contenedor de almacenamiento Qtree

Cree un volumen

Puede crear un volumen y especificar su punto de unión y otras propiedades mediante la `volume create` comando.

Acerca de esta tarea

Un volumen debe incluir una *ruta de unión* para que sus datos estén disponibles para los clientes. Puede especificar la ruta de unión cuando cree un nuevo volumen. Si crea un volumen sin especificar una ruta de unión, debe *Mount* el volumen en el espacio de nombres de la SVM mediante el `volume mount` comando.

Antes de empezar

- NFS debe estar configurado y en ejecución.
- El estilo de seguridad de la SVM debe ser UNIX.
- A partir de ONTAP 9.13.1, se pueden crear volúmenes con análisis de capacidad y seguimiento de actividades habilitados. Para activar la capacidad o el seguimiento de actividades, emita el `volume create` comando con `-analytics-state on`. `-activity-tracking-state` establezca en `on`.

Para obtener más información sobre el análisis de capacidad y el seguimiento de actividades, consulte [Active File System Analytics](#).

Pasos

1. Cree el volumen con un punto de unión:

```
volume create -vserver svm_name -volume volume_name -aggregate aggregate_name
-size {integer[KB|MB|GB|TB|PB]} -security-style unix -user user_name_or_number
-group group_name_or_number -junction-path junction_path [-policy
export_policy_name]
```

Las opciones para `-junction-path` son las siguientes:

- Directamente bajo la raíz, por ejemplo, `/new_vol`

Puede crear un nuevo volumen y especificar que se monte directamente en el volumen raíz de SVM.

- En un directorio existente, por ejemplo, `/existing_dir/new_vol`

Puede crear un nuevo volumen y especificar que se monte en un volumen existente (en una jerarquía existente), expresado como un directorio.

Si desea crear un volumen en un nuevo directorio (en una nueva jerarquía debajo de un nuevo volumen), por ejemplo, `/new_dir/new_vol`, Entonces debe crear primero un nuevo volumen principal que se junte al volumen raíz de la SVM. A continuación, creará el nuevo volumen secundario en la ruta de unión del nuevo volumen principal (nuevo directorio).

Si piensa utilizar una política de exportación existente, puede especificarla al crear el volumen. También puede añadir una política de exportación más adelante con el `volume modify` comando.

2. Compruebe que el volumen se ha creado con el punto de unión deseado:

```
volume show -vserver svm_name -volume volume_name -junction
```

Ejemplos

El siguiente comando crea un nuevo volumen denominado `user1` en la SVM `vs1.example.com` y el agregado `aggr1`. El nuevo volumen está disponible en `/users`. El tamaño del volumen es de 750 GB y su garantía de volumen es del tipo volumen (de forma predeterminada).

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction
```

| Vserver | Volume | Active | Junction Path | Junction Path Source |
|-----------------|--------|--------|---------------|----------------------|
| vs1.example.com | users1 | true | /users | RW_volume |

El siguiente comando crea un nuevo volumen llamado «home4» en la SVM "vs1.example.com" y el agregado

«aggr1». El directorio /eng/ Ya existe en el espacio de nombres para el SVM vs1 y el nuevo volumen estará disponible en /eng/home, que se convierte en el directorio principal de /eng/ espacio de nombres. El volumen tiene un tamaño de 750 GB y su garantía de volumen es de tipo `volume` (de forma predeterminada).

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
```

| | | Junction | | Junction |
|-----------------|--------|----------|---------------|-------------|
| Vserver | Volume | Active | Junction Path | Path Source |
| vs1.example.com | home4 | true | /eng/home | RW_volume |

Cree un qtree

Puede crear un qtree para que contenga datos y especificar sus propiedades mediante la `volume qtree create` comando.

Lo que necesitará

- La SVM y el volumen que contendrán el nuevo qtree ya deben existir.
- El estilo de seguridad de SVM debe ser UNIX y NFS debe configurarse y ejecutarse.

Pasos

1. Cree el qtree:

```
volume qtree create -vserver vserver_name { -volume volume_name -qtree
qtree_name | -qtree-path qtree path } -security-style unix [-policy
export_policy_name]
```

Puede especificar el volumen y el qtree como argumentos independientes o especificar el argumento de la ruta de qtree en el formato `/vol/volume_name/_qtree_name`.

De forma predeterminada, los qtrees heredan las políticas de exportación de su volumen principal, pero se pueden configurar para que utilicen las suyas propias. Si piensa utilizar una política de exportación existente, puede especificarla al crear el qtree. También puede añadir una política de exportación más adelante con el `volume qtree modify` comando.

2. Compruebe que el qtree se ha creado con la ruta de unión que desee:

```
volume qtree show -vserver vserver_name { -volume volume_name -qtree
qtree_name | -qtree-path qtree path }
```

Ejemplo

En el siguiente ejemplo se crea un qtree llamado qt01 ubicado en la SVM vs1.example.com que tiene una ruta de unión `/vol/data1:`

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path  
/vol/data1/qt01 -security-style unix  
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume qtree show -vserver vs1.example.com -qtree-path  
/vol/data1/qt01
```

```
          Vserver Name: vs1.example.com  
          Volume Name: data1  
          Qtree Name: qt01  
Actual (Non-Junction) Qtree Path: /vol/data1/qt01  
          Security Style: unix  
          Oplock Mode: enable  
          Unix Permissions: ---rwxr-xr-x  
          Qtree Id: 2  
          Qtree Status: normal  
          Export Policy: default  
Is Export Policy Inherited: true
```

Acceso NFS seguro mediante políticas de exportación

Acceso NFS seguro mediante políticas de exportación

Puede utilizar las políticas de exportación para restringir el acceso de NFS a volúmenes o qtrees a clientes que coincidan con parámetros específicos. Al aprovisionar almacenamiento nuevo, puede usar una política y reglas existentes, agregar reglas a una política existente o crear una nueva política y reglas. También puede comprobar la configuración de las políticas de exportación



A partir de ONTAP 9.3, puede habilitar la comprobación de la configuración de la política de exportación como un trabajo en segundo plano que registra cualquier infracción de reglas en una lista de reglas de error. La `vserver export-policy config-checker` Los comandos invocan el comprobador y muestran los resultados, que se pueden utilizar para verificar la configuración y eliminar reglas erróneas de la directiva. Los comandos sólo validan la configuración de exportación para los nombres de host, grupos de red y usuarios anónimos.

Gestionar la orden de procesamiento de las reglas de exportación

Puede utilizar el `vserver export-policy rule setindex` comando para establecer manualmente el número de índice de una regla de exportación existente. Esto le permite especificar la prioridad mediante la cual ONTAP aplica reglas de exportación a las solicitudes de clientes.

Acerca de esta tarea

Si el nuevo número de índice ya está en uso, el comando inserta la regla en el punto especificado y vuelve a ordenar la lista en consecuencia.

Paso

1. Modifique el número de índice de una regla de exportación especificada:

```
vserver export-policy rule setindex -vserver virtual_server_name -policyname  
policy_name -ruleindex integer -newruleindex integer
```

Ejemplo

El siguiente comando cambia el número de índice de una regla de exportación en el número de índice 3 al número de índice 2 de una política de exportación denominada r1 en la SVM denominada vs1:

```
vs1::> vserver export-policy rule setindex -vserver vs1  
-policyname rs1 -ruleindex 3 -newruleindex 2
```

Asignar una política de exportación a un volumen

Cada volumen incluido en la SVM debe estar asociado a una política de exportación que contenga reglas de exportación para que los clientes accedan a los datos del volumen.

Acerca de esta tarea

Es posible asociar una política de exportación a un volumen cuando se crea el volumen o en cualquier momento después de crearlo. Es posible asociar una política de exportación al volumen, aunque otra se puede asociar a muchos volúmenes.

Pasos

1. Si no se especificó una política de exportación cuando se creó el volumen, asigne una política de exportación al volumen:

```
volume modify -vserver vserver_name -volume volume_name -policy  
export_policy_name
```

2. Compruebe que la política se haya asignado al volumen:

```
volume show -volume volume_name -fields policy
```

Ejemplo

Los siguientes comandos asignan la política de exportación `nfs_policy` al volumen `vol1` en la SVM `vs1` y verifican la asignación:

```
cluster::> volume modify -vserver vs1 -volume vol1 -policy nfs_policy  
  
cluster::> volume show -volume vol -fields policy  
vserver volume      policy  
-----  
vs1      vol1      nfs_policy
```

Asigne una política de exportación a un qtree

En lugar de exportar un volumen completo, también puede exportar un qtree concreto de un volumen para que los clientes puedan acceder a él directamente. Puede asignar una política de exportación a un qtree para exportarlo. Puede asignar la política de exportación al crear un qtree nuevo o al modificar un qtree existente.

Lo que necesitará

Debe existir la política de exportación.

Acerca de esta tarea

De forma predeterminada, los qtrees heredan la política de exportación principal del volumen que contiene si no se especifica de otro modo en el momento de la creación.

Puede asociar una política de exportación a un qtree al crear el qtree o en cualquier momento después de crearlo. Puede asociar una política de exportación al qtree, aunque otra se puede asociar con muchos qtrees.

Pasos

1. Si no se especificó una política de exportación al crear el qtree, asigne una política de exportación al qtree:

```
volume qtree modify -vserver vs1 -qtree-path /vol/vol1/qtree_name -export-policy export_policy_name
```

2. Compruebe que la política se ha asignado al qtree:

```
volume qtree show -qtree qtree_name -fields export-policy
```

Ejemplo

Los siguientes comandos asignan la política de exportación `nfs_policy` al qtree `qt1` en la SVM `vs1` y verifican la asignación:

```
cluster::> volume modify -vserver vs1 -qtree-path /vol/vol1/qt1 -policy nfs_policy

cluster::>volume qtree show -volume vol1 -fields export-policy
vserver volume qtree export-policy
-----
vs1      data1  qt01  nfs_policy
```

Compruebe el acceso del cliente NFS desde el clúster

Para proporcionar acceso a un recurso compartido a clientes seleccionados, debe establecer permisos de archivo UNIX en un host de administración UNIX. Puede comprobar el acceso del cliente mediante el `vserver export-policy check-access` ajuste las reglas de exportación según sea necesario.

Pasos

1. En el clúster, compruebe el acceso del cliente a las exportaciones mediante el `vserver export-policy check-access` comando.

El siguiente comando comprueba el acceso de lectura/escritura de un cliente NFSv3 con la dirección IP 1.2.3.4 en el volumen home2. El resultado del comando muestra que el volumen utiliza la política de exportación `exp-home-dir` y ese acceso es denegado.

```
cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
1.2.3.4 -volume home2 -authentication-method sys -protocol nfs3 -access
-type read-write
```

| Path | Policy | Policy Owner | Policy Owner Type | Rule Index | Access |
|------------|--------------|-----------------|----------------------|---------------|--------|
| / | default | vs1_root | volume | 1 | read |
| /eng | default | vs1_root | volume | 1 | read |
| /eng/home2 | exp-home-dir | home2 | volume | 1 | denied |

3 entries were displayed.

2. Examine el resultado para determinar si la política de exportación funciona según lo previsto y el acceso al cliente se comporta como se espera.

Específicamente, debe comprobar qué política de exportación usa el volumen o el qtree y el tipo de acceso al cliente como resultado.

3. Si es necesario, vuelva a configurar las reglas de política de exportación.

Probar el acceso NFS desde los sistemas cliente

Después de verificar el acceso de NFS al nuevo objeto de almacenamiento, debe probar la configuración iniciando sesión en un host de administración NFS y leyendo datos desde y escribiendo datos en la SVM. A continuación, debe repetir el proceso como usuario que no sea raíz en un sistema cliente.

Lo que necesitará

- El sistema cliente debe tener una dirección IP permitida por la regla de exportación especificada anteriormente.
- Debe tener la información de inicio de sesión para el usuario raíz.

Pasos

1. En el clúster, compruebe la dirección IP de la LIF que aloja el nuevo volumen:

```
network interface show -vserver svm_name
```

2. Inicie sesión como usuario raíz en el sistema cliente host de administración.
3. Cambie el directorio a la carpeta de montaje:

```
cd /mnt/
```

4. Cree y monte una nueva carpeta con la dirección IP de la SVM:

a. Crear una nueva carpeta:

```
mkdir /mnt/folder
```

b. Monte el volumen nuevo en este directorio nuevo:

```
mount -t nfs -o hard IPAddress:/volume_name /mnt/folder
```

c. Cambie el directorio a la nueva carpeta:

```
cd folder
```

Los siguientes comandos crean una carpeta llamada test1, montan el volumen vol1 en la dirección IP 192.0.2.130 de la carpeta de montaje test1 y cambian al nuevo directorio test1:

```
host# mkdir /mnt/test1
host# mount -t nfs -o hard 192.0.2.130:/vol1 /mnt/test1
host# cd /mnt/test1
```

5. Cree un archivo nuevo, compruebe que existe y escriba texto en él:

a. Cree un archivo de prueba:

```
touch filename
```

b. Compruebe que el archivo existe.:

```
ls -l filename
```

c. Introduzca:

```
cat > filename
```

Escriba algún texto y, a continuación, presione Ctrl+D para escribir texto en el archivo de prueba.

d. Muestra el contenido del archivo de prueba.

```
cat filename
```

e. Elimine el archivo de prueba:

```
rm filename
```

f. Vuelva al directorio principal:

```
cd ..
```

```
host# touch myfile1
host# ls -l myfile1
-rw-r--r-- 1 root root 0 Sep 18 15:58 myfile1
host# cat >myfile1
This text inside the first file
host# cat myfile1
This text inside the first file
host# rm -r myfile1
host# cd ..
```

6. Como raíz, se pueden establecer los permisos y la propiedad de UNIX que se desee en el volumen montado.
7. En un sistema cliente UNIX identificado en las reglas de exportación, inicie sesión como uno de los usuarios autorizados que ahora tienen acceso al nuevo volumen y repita los procedimientos descritos en los pasos 3 a 5 para verificar que puede montar el volumen y crear un archivo.

Dónde encontrar información adicional

Una vez que haya probado correctamente el acceso al cliente NFS, puede realizar una configuración de NFS adicional o añadir acceso SAN. Cuando se completa el acceso al protocolo, debe proteger el volumen raíz de la máquina virtual de almacenamiento (SVM).

Configuración de NFS

El acceso a NFS se puede configurar más utilizando la siguiente información e informes técnicos:

- ["Gestión de NFS"](#)

Describe cómo configurar y gestionar el acceso a archivos mediante NFS.

- ["Informe técnico de NetApp 4067: Guía de prácticas recomendadas e implementación de NFS"](#)

Sirve de guía de funcionamiento de NFSv3 y NFSv4 y ofrece una descripción general del sistema operativo de ONTAP haciendo hincapié en NFSv4.

- ["Informe técnico de NetApp 4073: Autenticación unificada segura"](#)

Explica cómo configurar ONTAP para su uso con los servidores Kerberos versión 5 (krb5) basados en UNIX para la autenticación de almacenamiento NFS y Active Directory de Windows Server (AD) como proveedor de identidades KDC y Lightweight Directory Access Protocol (LDAP).

- ["Informe técnico de NetApp 3580: Guía de mejoras y prácticas recomendadas de NFSv4: Implementación de Data ONTAP"](#)

Describe las prácticas recomendadas que se deben seguir mientras implementa componentes de NFSv4 en clientes AIX, Linux o Solaris conectados a sistemas que ejecutan ONTAP.

Configuración de redes

Además, puede configurar las funciones de red y los servicios de nombres mediante los siguientes informes técnicos e informati:

- ["Gestión de NFS"](#)

Describe cómo configurar y gestionar las redes de ONTAP.

- ["Informe técnico de NetApp 4182: Consideraciones de diseño y prácticas recomendadas de almacenamiento Ethernet para las configuraciones de Data ONTAP en clúster"](#)

Describe la implementación de las configuraciones de red de ONTAP, y proporciona escenarios comunes de puesta en marcha de redes y recomendaciones de prácticas recomendadas.

- ["Informe técnico de NetApp 4668: Guía de prácticas recomendadas de servicios de nombres"](#)

Explica cómo configurar la configuración de LDAP, NIS, DNS y archivos locales con fines de autenticación.

Configuración del protocolo SAN

Si desea proporcionar o modificar el acceso SAN a la SVM nueva, puede usar la información de configuración de FC o iSCSI, que está disponible para varios sistemas operativos host.

Protección de volúmenes raíz

Después de configurar los protocolos en la SVM, debe asegurarse de que su volumen raíz esté protegido:

- ["Protección de datos"](#)

Describe cómo crear un reflejo de uso compartido de carga para proteger el volumen raíz de SVM, que es una práctica recomendada por NetApp para SVM habilitadas para NAS. También describe cómo recuperarse rápidamente de fallos o pérdidas de volúmenes mediante la promoción del volumen raíz de SVM desde un reflejo de uso compartido de carga.

En qué se diferencian las exportaciones de ONTAP de las exportaciones de 7-Mode

En qué se diferencian las exportaciones de ONTAP de las exportaciones de 7-Mode

Si no está familiarizado con cómo ONTAP implementa exportaciones NFS, puede comparar las herramientas de configuración de exportación de 7-Mode y ONTAP, así como las herramientas de ejemplo de 7-Mode `/etc/exports` archivos con reglas y políticas en clúster.

En ONTAP no hay `/etc/exports` archivo y no `exportfs` comando. En su lugar, debe definir una política de exportación. Las políticas de exportación le permiten controlar el acceso de los clientes de la misma forma que en 7-Mode, pero le proporcionan funcionalidades adicionales como la capacidad de reutilizar la misma política de exportación para varios volúmenes.

Información relacionada


["Gestión de NFS"](#)

["Informe técnico de NetApp 4067: Guía de prácticas recomendadas e implementación de NFS"](#)

Comparación de exportaciones en 7-Mode y ONTAP

Las exportaciones en ONTAP se definen y utilizan de forma diferente a las que se utilizan en entornos de 7-Mode.

| Áreas de diferencia | 7-Mode | ONTAP |
|---|---|--|
| Cómo se definen las exportaciones | Las exportaciones se definen en la <code>/etc/exports</code> archivo. | Las exportaciones se definen mediante la creación de una política de exportación dentro de una SVM. Una SVM puede incluir más de una política de exportación. |
| Ámbito de exportación | <ul style="list-style-type: none">• Las exportaciones se aplican a una ruta de archivo o qtree especificados.• Debe crear una entrada independiente en <code>/etc/exports</code> para cada qtree o ruta de archivo.• Las exportaciones sólo son persistentes si se definen en la <code>/etc/exports</code> archivo. | <ul style="list-style-type: none">• Las políticas de exportación se aplican a un volumen completo, incluidos todos los qtrees y rutas de archivos contenidos en el volumen.• Las políticas de exportación se pueden aplicar a más de un volumen si se desea.• Todas las políticas de exportación son persistentes a través de reinicios del sistema. |
| Cercado (especificando un acceso diferente para clientes específicos a los mismos recursos) | Para proporcionar a clientes específicos un acceso diferente a un recurso exportado único, debe enumerar cada cliente y su acceso permitido en el <code>/etc/exports</code> archivo. | Las políticas de exportación están compuestas por varias reglas individuales de exportación. Cada regla de exportación define permisos de acceso específicos para un recurso y enumera los clientes que tienen dichos permisos. Para especificar un acceso diferente para clientes específicos, debe crear una regla de exportación para cada conjunto específico de permisos de acceso, enumerar los clientes que tienen esos permisos y, a continuación, agregar las reglas a la directiva de exportación. |

| | | |
|-----------------|---|--|
| Alias de nombre | Al definir una exportación, puede elegir que el nombre de la exportación sea diferente del nombre de la ruta de acceso del archivo. Debe utilizar el <code>-actual</code> parámetro al definir dicha exportación en la <code>/etc/exports</code> archivo. | <p>Es posible optar por que el nombre del volumen exportado sea diferente del nombre del volumen real. Para ello, debe montar el volumen con un nombre de ruta de unión personalizado dentro del espacio de nombres de la SVM.</p> <div>  <p>De manera predeterminada, los volúmenes se montan con su nombre de volumen. Para personalizar el nombre de ruta de unión de un volumen, debe desmontarlo, cambiarle el nombre y, a continuación, volver a montarlo.</p> </div> |
|-----------------|---|--|

Ejemplos de políticas de exportación de ONTAP

Puede revisar el ejemplo de políticas de exportación para comprender mejor cómo funcionan las políticas de exportación en ONTAP.

Implementación de ONTAP de ejemplo para una exportación de 7-Mode

En el siguiente ejemplo se muestra una exportación de 7-Mode tal como aparece en la `/etc/export` archivo:

```
/vol/vol1 -sec=sys,ro=@readonly_netgroup,rw=@readwrite_netgroup1:
@readwrite_netgroup2:@rootaccess_netgroup,root=@rootaccess_netgroup
```

Para reproducir esta exportación como una política de exportación en clúster, debe crear una política de exportación con tres reglas de exportación y, a continuación, asignar la política de exportación al volumen `vol1`.

| Regla | Elemento | Valor |
|---|--|---|
| Artículo 1 | <code>-clientmatch</code> (especificación del cliente) | <code>@readonly_netgroup</code> |
| <code>-ruleindex</code> (posición de la regla de exportación en la lista de reglas) | 1 | <code>-protocol</code> |
| <code>nfs</code> | <code>-rorule</code> (permitir acceso de solo lectura) | <code>sys</code> (Cliente autenticado con <code>AUTH_SYS</code>) |

| Regla | Elemento | Valor |
|---|---|---|
| -rwrule(permitir acceso de lectura/escritura) | never | -superuser(permitir acceso de superusuario) |
| none(root <i>squashed</i> a anon) | Regla 2 | -clientmatch |
| @rootaccess_netgroup | -ruleindex | 2 |
| -protocol | nfs | -rorule |
| sys | -rwrule | sys |
| -superuser | sys | Regla 3 |
| -clientmatch | @readwrite_netgroup1,@readwrite_netgroup2 | -ruleindex |
| 3 | -protocol | nfs |
| -rorule | sys | -rwrule |
| sys | -superuser | none |

1. Cree una política de exportación denominada exp_vol1:

```
vserver export-policy create -vserver NewSVM -policyname exp_vol1
```

2. Cree tres reglas con los siguientes parámetros en el comando base:

° Comando base:

```
vserver export-policy rule create -vserver NewSVM -policyname exp_vol1
```

° Parámetros de regla:

```
-clientmatch @readonly_netgroup -ruleindex 1 -protocol nfs -rorule sys
-rwrule never -superuser none
```

```
-clientmatch @rootaccess_netgroup -ruleindex 2 -protocol nfs -rorule sys
-rwrule sys -superuser sys
```

```
-clientmatch @readwrite_netgroup1,@readwrite_netgroup2 -ruleindex 3
-protocol nfs -rorule sys -rwrule sys -superuser none
```

3. Asigne la política al volumen vol1:

```
volume modify -vserver NewSVM -volume vol1 -policy exp_vol1
```

Consolidación de muestras de exportaciones de 7-Mode

En el siguiente ejemplo se muestra un modelo 7-Mode `/etc/export` archivo que incluye una línea para cada 10 qtrees:

```
/vol/vol1/q_1472 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1471 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1473 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1570 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1571 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_2237 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2238 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2239 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2240 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2241 -sec=sys,rw=host2057s,root=host2057s
```

En ONTAP, se necesita una de estas dos políticas para cada qtree: Una con una regla incluida `-clientmatch host1519s`, o una con una regla incluida `-clientmatch host2057s`.

1. Cree dos políticas de exportación llamadas `exp_vol1q1` y `exp_vol1q2`:

- `vserver export-policy create -vserver NewSVM -policyname exp_vol1q1`
- `vserver export-policy create -vserver NewSVM -policyname exp_vol1q2`

2. Crear una regla para cada política:

- `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1q1 -clientmatch host1519s -rwrule sys -superuser sys`
- `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1q2 -clientmatch host1519s -rwrule sys -superuser sys`

3. Aplique las políticas a los qtrees:

- `volume qtree modify -vserver NewSVM -qtree-path /vol/vol1/q_1472 -export -policy exp_vol1q1`
- [4 qtrees siguientes...]
- `volume qtree modify -vserver NewSVM -qtree-path /vol/vol1/q_2237 -export -policy exp_vol1q2`
- [4 qtrees siguientes...]

Si posteriormente necesita añadir qtrees adicionales para esos hosts, deberá usar las mismas políticas de exportación.

Gestione NFS con la interfaz de línea de comandos

Información general de referencia de NFS

ONTAP incluye funciones de acceso a archivos disponibles para el protocolo NFS. Puede habilitar un servidor NFS y exportar volúmenes o qtrees.

Este procedimiento se realiza en las siguientes circunstancias:

- Desea comprender la gama de funcionalidades del protocolo NFS de ONTAP.
- Desea realizar tareas de configuración y mantenimiento menos comunes, no una configuración NFS básica.
- Desea usar la interfaz de línea de comandos (CLI), no System Manager ni una herramienta de secuencias de comandos automatizadas.

Comprender el acceso a archivos NAS

Espacios de nombres y puntos de unión

Descripción general de los espacios de nombres y puntos de unión

Un NAS *Namespace* es una agrupación lógica de volúmenes Unidos en *Junction points* para crear una única jerarquía de sistemas de archivos. Un cliente con permisos suficientes puede acceder a los archivos del espacio de nombres sin especificar la ubicación de los archivos en el almacenamiento. Los volúmenes que se han Unido pueden residir en cualquier parte del clúster.

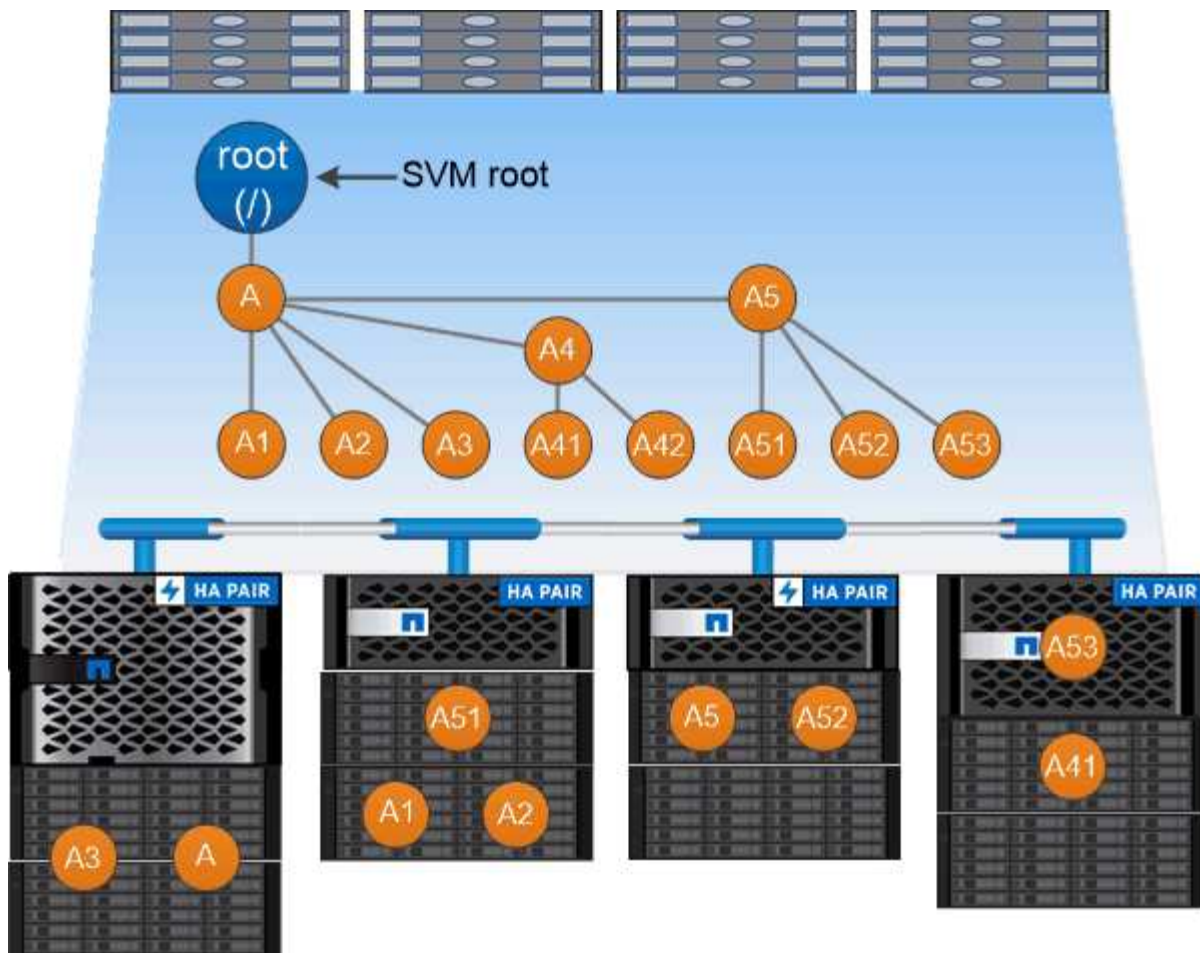
En lugar de montar cada volumen que contenga un archivo de interés, los clientes NAS montan un NFS *export* o acceden a un SMB *share*. La exportación o el recurso compartido representan todo el espacio de nombres o una ubicación intermedia dentro del espacio de nombres. El cliente solo accede a los volúmenes montados por debajo de su punto de acceso.

Es posible añadir volúmenes al espacio de nombres según sea necesario. Puede crear puntos de unión directamente debajo de una unión de volumen principal o en un directorio dentro de un volumen. Puede ser una ruta a una unión de volumen para un volumen denominado «'vol3'» `/vol1/vol2/vol3`, o `/vol1/dir2/vol3`, o incluso `/dir1/dir2/vol3`. La ruta se llama la *ruta de unión*.

Cada SVM tiene un espacio de nombres único. El volumen raíz de la SVM es el punto de entrada de la jerarquía del espacio de nombres.



Para garantizar que los datos sigan estando disponibles en caso de que se produzca una interrupción o conmutación al nodo de respaldo, debe crear una copia *mirror* de uso compartido de la carga para el volumen raíz de la SVM.



A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.

Ejemplo

En el siguiente ejemplo se crea un volumen denominado «'home4'» ubicado en la SVM vs1 que tiene una ruta de unión /eng/home:

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

Cuáles son las arquitecturas de espacio de nombres NAS típicas

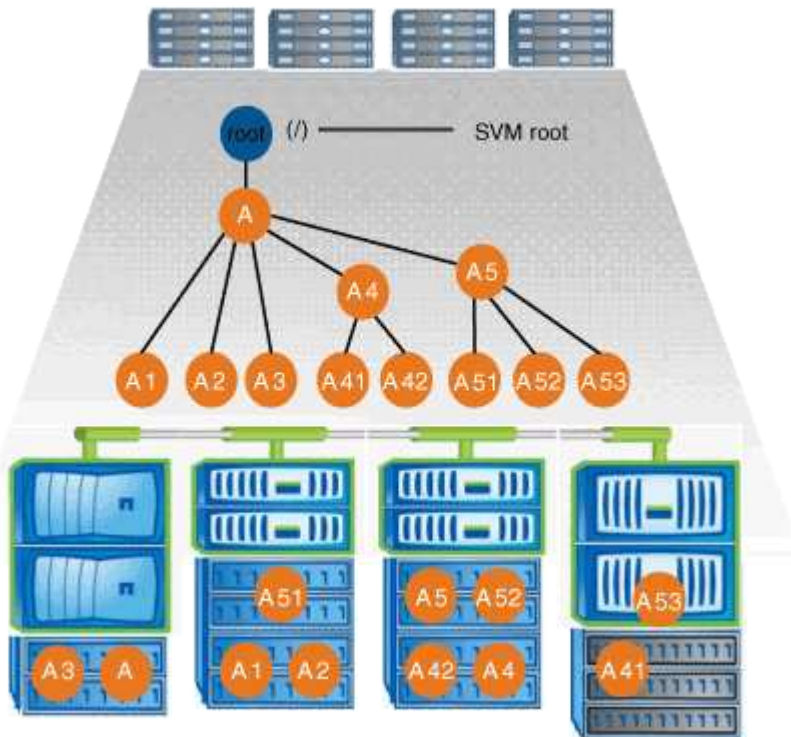
Existen varias arquitecturas de espacio de nombres NAS típicas que se pueden usar a medida que se crea el espacio de nombres de la SVM. Puede elegir la arquitectura de espacio de nombres que se ajuste a sus necesidades empresariales y de flujos de trabajo.

El principio del espacio de nombres siempre es el volumen raíz, que se representa mediante una barra diagonal (/). La arquitectura del espacio de nombres en la raíz se divide en tres categorías básicas:

- Un árbol ramificado único, con una única unión a la raíz del espacio de nombres
- Múltiples árboles ramificados, con varios puntos de unión en la raíz del espacio de nombres
- Varios volúmenes independientes, cada uno con un punto de unión separado en la raíz del espacio de nombres

Espacio de nombres con árbol ramificado único

Una arquitectura con un único árbol ramificado tiene un único punto de inserción en la raíz del espacio de nombres de SVM. El único punto de inserción puede ser un volumen juntado o un directorio debajo de la raíz. Los demás volúmenes se montan en puntos de unión debajo del punto de inserción único (que puede ser un volumen o un directorio).

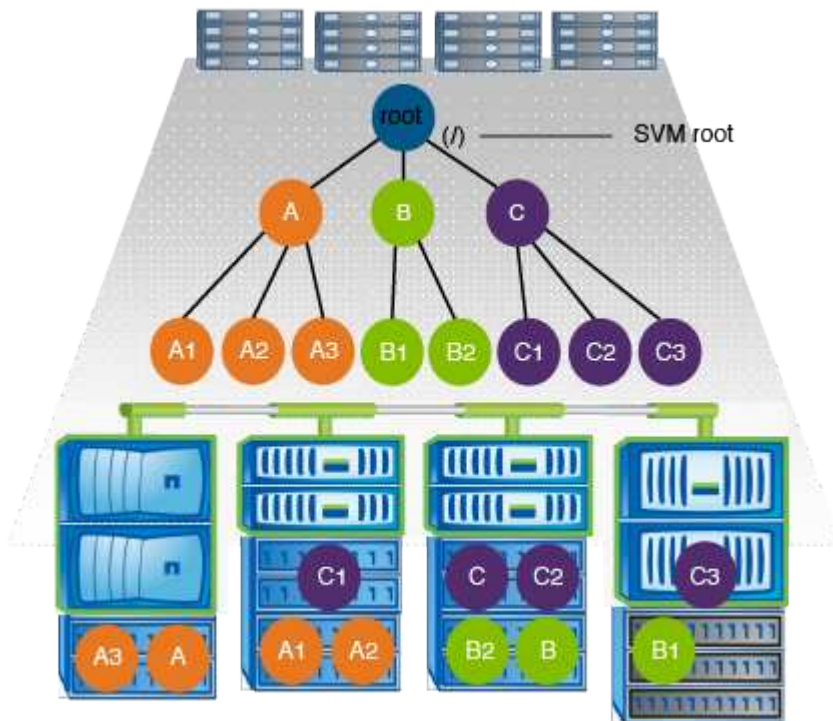


Por ejemplo, una configuración de unión de volúmenes típica con la arquitectura de espacio de nombres anterior podría tener el aspecto de la siguiente configuración, donde todos los volúmenes se unen por debajo del punto de inserción único, que es un directorio denominado «data»:

| Vserver | Volume | Junction Active | Junction Path | Junction Path Source |
|---------|----------|-----------------|-------------------|----------------------|
| vs1 | corp1 | true | /data/dir1/corp1 | RW_volume |
| vs1 | corp2 | true | /data/dir1/corp2 | RW_volume |
| vs1 | data1 | true | /data/data1 | RW_volume |
| vs1 | eng1 | true | /data/data1/eng1 | RW_volume |
| vs1 | eng2 | true | /data/data1/eng2 | RW_volume |
| vs1 | sales | true | /data/data1/sales | RW_volume |
| vs1 | vol1 | true | /data/vol1 | RW_volume |
| vs1 | vol2 | true | /data/vol2 | RW_volume |
| vs1 | vol3 | true | /data/vol3 | RW_volume |
| vs1 | vs1_root | - | / | - |

Espacio de nombres con varios árboles ramificados

Una arquitectura con varios árboles ramificados tiene varios puntos de inserción en la raíz del espacio de nombres de la SVM. Los puntos de inserción pueden ser volúmenes de juntados o directorios debajo de la raíz. Los demás volúmenes se montan en puntos de unión debajo de los puntos de inserción (que pueden ser volúmenes o directorios).

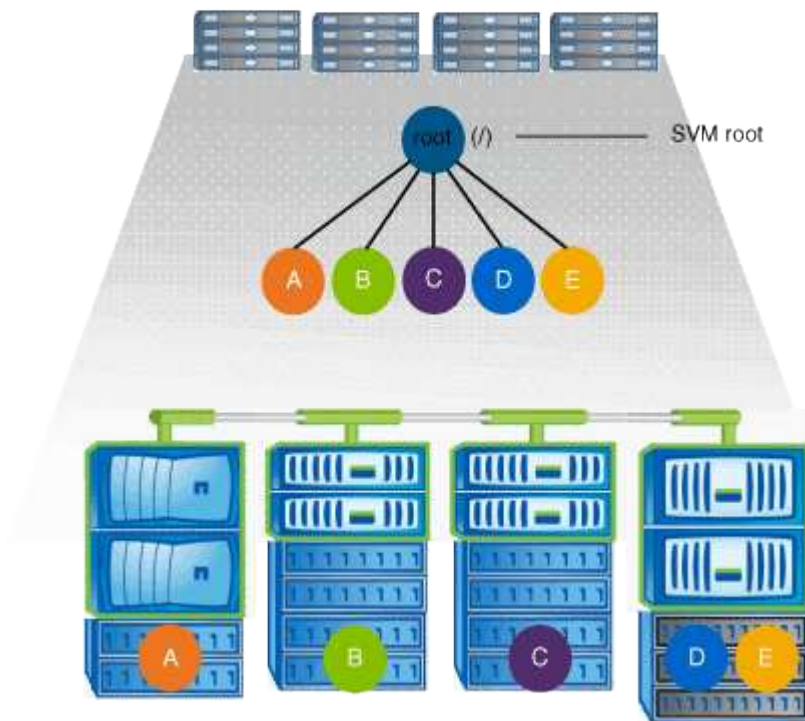


Por ejemplo, una configuración típica de unión de volúmenes con la arquitectura anterior del espacio de nombres puede parecer la siguiente configuración, donde hay tres puntos de inserción en el volumen raíz de la SVM. Dos puntos de inserción son directorios denominados «dé» y «proyectos». Un punto de inserción es un volumen Unido denominado «audit»:

| Vserver | Volume | Junction Active | Junction Path | Junction Path Source |
|---------|-------------|-----------------|--------------------|----------------------|
| vs1 | audit | true | /audit | RW_volume |
| vs1 | audit_logs1 | true | /audit/logs1 | RW_volume |
| vs1 | audit_logs2 | true | /audit/logs2 | RW_volume |
| vs1 | audit_logs3 | true | /audit/logs3 | RW_volume |
| vs1 | eng | true | /data/eng | RW_volume |
| vs1 | mktg1 | true | /data/mktg1 | RW_volume |
| vs1 | mktg2 | true | /data/mktg2 | RW_volume |
| vs1 | project1 | true | /projects/project1 | RW_volume |
| vs1 | project2 | true | /projects/project2 | RW_volume |
| vs1 | vs1_root | - | / | - |

Espacio de nombres con varios volúmenes independientes

En una arquitectura con volúmenes independientes, cada volumen tiene un punto de inserción en la raíz del espacio de nombres de SVM; sin embargo, el volumen no se ha Unido por debajo de otro volumen. Cada volumen tiene una ruta única y se conecta directamente debajo de la raíz o se conecta bajo un directorio debajo de la raíz.



Por ejemplo, una configuración típica de unión de volúmenes con la arquitectura anterior del espacio de nombres puede parecer la siguiente configuración, donde hay cinco puntos de inserción en el volumen raíz de la SVM, donde cada punto de inserción representa una ruta a un volumen.

| Vserver | Volume | Junction | | Junction Path | Junction Source |
|---------|----------|----------|-----------|---------------|-----------------|
| | | Active | | | |
| vs1 | eng | true | /eng | | RW_volume |
| vs1 | mktg | true | /vol/mktg | | RW_volume |
| vs1 | project1 | true | /project1 | | RW_volume |
| vs1 | project2 | true | /project2 | | RW_volume |
| vs1 | sales | true | /sales | | RW_volume |
| vs1 | vs1_root | - | / | | - |

Cómo ONTAP controla el acceso a los archivos

Información general sobre cómo ONTAP controla el acceso a los archivos

ONTAP controla el acceso a los archivos de acuerdo con las restricciones basadas en archivos y en autenticación que especifique.

Cuando un cliente se conecta al sistema de almacenamiento para acceder a los archivos, ONTAP debe realizar dos tareas:

- Autenticación

ONTAP debe autenticar el cliente verificando la identidad con un origen de confianza. Además, el tipo de autenticación del cliente es un método que puede utilizarse para determinar si un cliente puede acceder a los datos al configurar políticas de exportación (opcional para CIFS).

- Autorización

ONTAP tiene que autorizar al usuario comparando las credenciales del usuario con los permisos configurados en el archivo o directorio y determinando qué tipo de acceso, si hubiera, proporcionar.

Para administrar correctamente el control de acceso a archivos, ONTAP debe comunicarse con servicios externos como servidores NIS, LDAP y Active Directory. La configuración de un sistema de almacenamiento para el acceso a archivos mediante CIFS o NFS requiere configurar los servicios adecuados en función de su entorno en ONTAP.

Restricciones basadas en autenticación

Con las restricciones basadas en la autenticación, puede especificar qué máquinas cliente y qué usuarios se pueden conectar a la máquina virtual de almacenamiento (SVM).

ONTAP es compatible con la autenticación Kerberos desde servidores UNIX y Windows.

Restricciones basadas en archivos

ONTAP evalúa tres niveles de seguridad para determinar si una entidad está autorizada para realizar una acción solicitada sobre archivos y directorios que residen en una SVM. El acceso está determinado por los permisos efectivos después de la evaluación de los

tres niveles de seguridad.

Cualquier objeto de almacenamiento puede contener hasta tres tipos de capas de seguridad:

- Seguridad de exportación (NFS) y uso compartido (SMB)

La seguridad de exportación y uso compartido se aplica al acceso de los clientes a una exportación NFS o un recurso compartido de SMB dado. Los usuarios con privilegios administrativos pueden gestionar la seguridad de exportación y nivel de recurso compartido desde clientes SMB y NFS.

- Seguridad de directorio y archivos del protector de acceso a nivel de almacenamiento

La seguridad de protección de acceso a nivel de almacenamiento se aplica al acceso de clientes SMB y NFS a volúmenes de SVM. Sólo se admiten permisos de acceso NTFS. Para que ONTAP realice comprobaciones de seguridad en los usuarios de UNIX con el fin de acceder a los datos de los volúmenes para los que se ha aplicado la protección de acceso a nivel de almacenamiento, el usuario de UNIX debe asignar a un usuario de Windows en la SVM propietaria del volumen.



Si ve la configuración de seguridad en un archivo o un directorio desde un cliente NFS o SMB, no verá la seguridad de Access Guard a nivel de almacenamiento. La seguridad de protección de acceso a nivel de almacenamiento no se puede revocar de un cliente, ni siquiera por un administrador de sistema (Windows o UNIX).

- Seguridad nativa a nivel de archivo de NTFS, UNIX y NFSv4

Existe una seguridad nativa a nivel de archivo en el archivo o directorio que representa el objeto de almacenamiento. Puede establecer la seguridad a nivel de archivo desde un cliente. Los permisos de archivos son efectivos independientemente de si se utiliza SMB o NFS para acceder a los datos.

Cómo gestiona ONTAP la autenticación del cliente NFS

Cómo maneja ONTAP la información general sobre autenticación de clientes NFS

Los clientes de NFS deben autenticarse correctamente antes de poder acceder a los datos en la SVM. ONTAP autentica a los clientes al comprobar sus credenciales de UNIX con los servicios de nombres que se configuran.

Cuando un cliente NFS se conecta con la SVM, ONTAP obtiene las credenciales de UNIX del usuario comprobando diferentes servicios de nombre, en función de la configuración de los servicios de nombres de la SVM. ONTAP puede comprobar credenciales para cuentas UNIX locales, dominios NIS y dominios LDAP. Debe haber al menos uno de ellos configurado para que ONTAP pueda autenticar correctamente al usuario. Puede especificar varios servicios de nombres y el orden en el que ONTAP los busca.

En un entorno NFS puro con estilos de seguridad de volúmenes UNIX, esta configuración es suficiente para autenticar y proporcionar el acceso adecuado a los archivos para que los usuarios que se conecten desde un cliente NFS.

Si utiliza estilos de seguridad de volúmenes mixtos, NTFS o unificados, ONTAP debe obtener un nombre de usuario SMB para el usuario UNIX para la autenticación con un controlador de dominio de Windows. Esto puede suceder mediante la asignación de usuarios individuales mediante cuentas de UNIX locales o dominios LDAP, o bien mediante un usuario de SMB predeterminado. Puede especificar los servicios de nombres que ONTAP busca en qué orden, o bien especificar un usuario de SMB predeterminado.

Cómo utiliza ONTAP los servicios de nombres

ONTAP utiliza los servicios de nombres para obtener información acerca de los usuarios y los clientes. ONTAP usa esta información para autenticar a los usuarios que acceden a los datos o administran el sistema de almacenamiento, y para asignar las credenciales de usuario en un entorno mixto.

Al configurar el sistema de almacenamiento, debe especificar los servicios de nombres que desea que ONTAP utilice para obtener credenciales de usuario con fines de autenticación. ONTAP admite los siguientes servicios de nombres:

- Usuarios locales (archivo)
- Dominios NIS externos (NIS)
- Dominios LDAP externos (LDAP)

Utilice la `vserver services name-service ns-switch` Familia de comandos de para configurar SVM con los orígenes para buscar información de red y el orden en el que realizar búsquedas. Estos comandos proporcionan la funcionalidad equivalente del `/etc/nsswitch.conf` Fichero de sistemas UNIX.

Cuando un cliente NFS se conecta a la SVM, ONTAP comprueba los servicios de nombre especificados para obtener las credenciales de UNIX del usuario. Si los servicios de nombres están configurados correctamente y ONTAP puede obtener las credenciales de UNIX, ONTAP autentica correctamente el usuario.

En un entorno con estilos de seguridad mixtos, es posible que ONTAP tenga que asignar credenciales de usuario. Debe configurar los servicios de nombres según sea necesario para el entorno de a fin de permitir que ONTAP asigne correctamente las credenciales de usuario.

ONTAP también utiliza servicios de nombres para autenticar cuentas de administrador de SVM. Debe tener esto en cuenta al configurar o modificar el switch del servicio de nombres para evitar deshabilitar accidentalmente la autenticación de las cuentas de administrador de SVM. Para obtener más información sobre los usuarios de administración de SVM, consulte ["Autenticación de administrador y RBAC"](#).

Cómo ONTAP otorga acceso a archivos SMB desde los clientes NFS

ONTAP utiliza la semántica de seguridad del sistema de archivos de Windows NT (NTFS) para determinar si un usuario de UNIX, en un cliente NFS, tiene acceso a un archivo con permisos NTFS.

Para ello, ONTAP convierte el identificador de usuario de UNIX (UID) del usuario en una credencial de SMB y, a continuación, utiliza la credencial de SMB para verificar que el usuario tiene derechos de acceso al archivo. Una credencial SMB consta de un identificador de seguridad principal (SID), normalmente el nombre de usuario de Windows del usuario y uno o más SID de grupo que corresponden a los grupos Windows de los que el usuario es miembro.

El tiempo que tarda ONTAP en convertir el UID de UNIX en una credencial SMB puede ser de decenas de milisegundos a cientos de milisegundos, dado que el proceso implica contactar a un controlador de dominio. ONTAP asigna el UID a la credencial SMB e introduce la asignación en una caché de credenciales para reducir el tiempo de verificación debido a la conversión.

Cómo funciona la caché de credenciales NFS

Cuando un usuario de NFS solicita acceso a exportaciones NFS en el sistema de

almacenamiento de, ONTAP debe recuperar las credenciales de usuario desde servidores de nombres externos o desde archivos locales para autenticar el usuario. ONTAP después almacena estas credenciales en la caché de credenciales internas para futuras referencias. Comprender el funcionamiento de la caché de credenciales NFS le permite manejar los posibles problemas de rendimiento y acceso.

Sin la caché de credenciales, ONTAP tendría que consultar los servicios de nombres cada vez que un usuario NFS solicitara acceso. En un sistema de almacenamiento de mucha actividad al que acceden muchos usuarios, se pueden producir rápidamente problemas de rendimiento graves, que provocan retrasos no deseados o incluso la denegación del acceso del cliente NFS.

Con la caché de credenciales, ONTAP recupera las credenciales de usuario y las almacena durante un periodo predeterminado de tiempo para obtener un acceso rápido y sencillo en caso de que el cliente NFS envíe otra solicitud. Este método ofrece las siguientes ventajas:

- Facilita la carga en el sistema de almacenamiento al manejar menos solicitudes a servidores de nombres externos (como NIS o LDAP).
- Facilita la carga de los servidores de nombres externos enviando menos solicitudes.
- Acelera el acceso del usuario al eliminar el tiempo de espera para obtener credenciales de fuentes externas antes de que el usuario pueda autenticarse.

ONTAP almacena las credenciales positivas y negativas en la caché de credenciales. Las credenciales positivas significan que el usuario se ha autenticado y se le ha concedido acceso. Las credenciales negativas indican que el usuario no se ha autenticado y se le ha denegado el acceso.

De forma predeterminada, ONTAP almacena credenciales positivas durante 24 horas, es decir, tras autenticar inicialmente al usuario, ONTAP utiliza las credenciales en caché para cualquier solicitud de acceso por parte de ese usuario durante 24 horas. Si el usuario solicita acceso después de 24 horas, el ciclo se vuelve a iniciar: ONTAP descarta las credenciales en caché y obtiene de nuevo las credenciales del origen del servicio de nombres adecuado. Si las credenciales cambiaron en el servidor de nombres durante las 24 horas anteriores, ONTAP almacenará las credenciales actualizadas para utilizarlas en las próximas 24 horas.

De forma predeterminada, ONTAP almacena credenciales negativas durante dos horas; es decir, después de denegar inicialmente el acceso a un usuario, ONTAP continúa negando cualquier solicitud de acceso por ese usuario durante dos horas. Si el usuario solicita acceso después de 2 horas, el ciclo se inicia de nuevo: ONTAP obtiene las credenciales de nuevo del origen de servicio de nombres apropiado. Si las credenciales cambiaron en el servidor de nombres durante las dos horas anteriores, ONTAP almacena en caché las credenciales actualizadas para utilizarlas en las siguientes dos horas.

Cree y gestione volúmenes de datos en espacios de nombres NAS

Cree volúmenes de datos con puntos de unión especificados

Puede especificar el punto de unión cuando crea un volumen de datos. El volumen resultante se monta automáticamente en el punto de unión y se puede configurar inmediatamente para el acceso NAS.

Antes de empezar

- El agregado en el que desea crear el volumen ya debe existir.
- A partir de ONTAP 9.13.1, se pueden crear volúmenes con análisis de capacidad y seguimiento de actividades habilitados. Para activar la capacidad o el seguimiento de actividades, emita el `volume`

create comando con `-analytics-state` o. `-activity-tracking-state` establezca en on.

Para obtener más información sobre el análisis de capacidad y el seguimiento de actividades, consulte [Active File System Analytics](#).



Los siguientes caracteres no se pueden utilizar en la ruta de unión: * # " > < | ? \

+

Además, la longitud de la ruta de unión no puede ser superior a 255 caracteres.

Pasos

1. Cree el volumen con un punto de unión:

```
volume create -vserver vs1 -volume volume_name -aggregate  
aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style  
{ntfs|unix|mixed} -junction-path junction_path
```

La ruta de unión debe comenzar con la raíz (/) y puede contener tanto directorios como volúmenes con conexiones. No es necesario que la ruta de unión contenga el nombre del volumen. Las rutas de unión son independientes del nombre del volumen.

Es opcional especificar un estilo de seguridad del volumen. Si no se especifica un estilo de seguridad, ONTAP crea el volumen con el mismo estilo de seguridad que se aplica al volumen raíz de la máquina virtual de almacenamiento (SVM). Sin embargo, es posible que el estilo de seguridad del volumen raíz no sea el estilo de seguridad que se desea aplicar al volumen de datos que se crea. La recomendación es especificar el estilo de seguridad al crear el volumen para minimizar los problemas de acceso a archivos difíciles de solucionar.

La ruta de unión no distingue mayúsculas y minúsculas; /ENG es igual que /eng. Si crea un recurso compartido CIFS, Windows trata la ruta de unión como si fuera sensible a mayúsculas de minúsculas. Por ejemplo, si la unión es /ENG, La ruta de acceso de un recurso compartido SMB debe comenzar por /ENG, no /eng.

Existen muchos parámetros opcionales que se pueden usar para personalizar un volumen de datos. Para aprender más sobre ellos, consulte las páginas de manual de `volume create` comando.

2. Compruebe que el volumen se ha creado con el punto de unión deseado:

```
volume show -vserver vs1 -volume volume_name -junction
```

Ejemplo

En el siguiente ejemplo se crea un volumen denominado «'home4'» ubicado en la SVM vs1 que tiene una ruta de unión /eng/home:

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1 -volume home4 -junction
```

| Vserver | Volume | Active | Junction Path | Junction Path Source |
|---------|--------|--------|---------------|----------------------|
| vs1 | home4 | true | /eng/home | RW_volume |

Cree volúmenes de datos sin especificar puntos de unión

Puede crear un volumen de datos sin especificar un punto de unión. El volumen resultante no se monta automáticamente y no se puede configurar para acceso NAS. Debe montar el volumen para poder configurar los recursos compartidos de SMB o las exportaciones de NFS de ese volumen.

Antes de empezar

- El agregado en el que desea crear el volumen ya debe existir.
- A partir de ONTAP 9.13.1, se pueden crear volúmenes con análisis de capacidad y seguimiento de actividades habilitados. Para activar la capacidad o el seguimiento de actividades, emita el `volume create` comando con `-analytics-state on`. `-activity-tracking-state` establezca en `on`.

Para obtener más información sobre el análisis de capacidad y el seguimiento de actividades, consulte [Active File System Analytics](#).

Pasos

1. Cree el volumen sin un punto de unión mediante el siguiente comando:

```
volume create -vserver vserver_name -volume volume_name -aggregate
aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style
{ntfs|unix|mixed}
```

Es opcional especificar un estilo de seguridad del volumen. Si no se especifica un estilo de seguridad, ONTAP crea el volumen con el mismo estilo de seguridad que se aplica al volumen raíz de la máquina virtual de almacenamiento (SVM). Sin embargo, es posible que el estilo de seguridad del volumen raíz no sea el estilo de seguridad que se desea aplicar al volumen de datos. La recomendación es especificar el estilo de seguridad al crear el volumen para minimizar los problemas de acceso a archivos difíciles de solucionar.

Existen muchos parámetros opcionales que se pueden usar para personalizar un volumen de datos. Para aprender más sobre ellos, consulte las páginas de manual de `volume create` comando.

2. Compruebe que el volumen se ha creado sin un punto de unión:

```
volume show -vserver vserver_name -volume volume_name -junction
```

Ejemplo

En el siguiente ejemplo se crea un volumen denominado «números» ubicado en la SVM vs1 que no se monta en un punto de unión:

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1 -junction
```

| Vserver | Volume | Junction | | Junction Path | Junction Path Source |
|---------|----------|----------|--|---------------|----------------------|
| | | Active | | | |
| vs1 | data | true | | /data | RW_volume |
| vs1 | home4 | true | | /eng/home | RW_volume |
| vs1 | vs1_root | - | | / | - |
| vs1 | sales | - | | - | - |

Monte o desmonte volúmenes existentes en el espacio de nombres NAS

Un volumen se debe montar en el espacio de nombres NAS para poder configurar el acceso de clientes NAS a los datos contenidos en los volúmenes de la máquina virtual de almacenamiento (SVM). Puede montar un volumen en un punto de unión si no está montado actualmente. También es posible desmontar volúmenes.

Acerca de esta tarea

Si desmonta y desconecta un volumen, los clientes NAS no pueden acceder a todos los datos dentro del punto de unión, incluidos los datos en los volúmenes con puntos de unión ubicados en el espacio de nombres del volumen sin montar.



Para interrumpir el acceso de un cliente NAS a un volumen, no basta con desmontar el volumen. Debe desconectar el volumen o realizar otros pasos para garantizar que las cachés del identificador de archivos del cliente se invaliden. Para obtener más información, consulte el siguiente artículo de la base de conocimientos:

["Los clientes NFSv3 siguen teniendo acceso a un volumen después de eliminarse del espacio de nombres de ONTAP"](#)

Al desmontar y desconectar un volumen, no se pierden datos dentro del volumen. Además, se conservan las políticas de exportación de volúmenes existentes y los recursos compartidos de SMB creados en el volumen o en directorios y puntos de unión dentro del volumen desmontado. Si vuelve a montar el volumen desmontado, los clientes NAS pueden acceder a los datos contenidos en el volumen mediante políticas de exportación y recursos compartidos SMB existentes.

Pasos

1. Realice la acción deseada:

| Si desea... | Introduzca los comandos... |
|----------------------|---|
| Montar un volumen | <pre>volume mount -vserver svm_name -volume volume_name -junction-path junction_path</pre> |
| Desmontar un volumen | <pre>volume unmount -vserver svm_name -volume volume_name volume offline -vserver svm_name -volume volume_name</pre> |

2. Compruebe que el volumen esté en el estado de montaje deseado:

```
volume show -vserver svm_name -volume volume_name -fields state,junction-
path,junction-active
```

Ejemplos

El siguiente ejemplo monta un volumen llamado “sales” ubicado en SVM “VS1” al punto de unión “/sales”:

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active
```

| vserver | volume | state | junction-path | junction-active |
|---------|--------|--------|---------------|-----------------|
| vs1 | data | online | /data | true |
| vs1 | home4 | online | /eng/home | true |
| vs1 | sales | online | /sales | true |

El siguiente ejemplo desmonta y desconecta un volumen llamado “data” ubicado en la SVM “VS1”:

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active
```

| vserver | volume | state | junction-path | junction-active |
|---------|--------|---------|---------------|-----------------|
| vs1 | data | offline | - | - |
| vs1 | home4 | online | /eng/home | true |
| vs1 | sales | online | /sales | true |

Muestra información sobre el montaje del volumen y los puntos de unión

Puede ver información sobre los volúmenes montados para las máquinas virtuales de almacenamiento (SVM) y los puntos de unión a los que están montados los volúmenes. También puede determinar qué volúmenes no están montados en un punto de unión. Esta información se puede usar para comprender y gestionar el espacio de nombres de la SVM.

Paso

- 1. Realice la acción deseada:

| | |
|---|---|
| Si desea mostrar... | Introduzca el comando... |
| Información resumida sobre los volúmenes montados y desmontados en la SVM | <code>volume show -vserver vserver_name -junction</code> |
| Información detallada sobre los volúmenes montados y desmontados en la SVM | <code>volume show -vserver vserver_name -volume volume_name -instance</code> |
| Información específica sobre los volúmenes montados y desmontados en la SVM | <div>a. Si es necesario, puede mostrar campos válidos para <code>-fields</code> parámetro con el comando siguiente: <code>volume show -fields ?</code></div> <div>b. Muestre la información deseada mediante <code>-fields</code> parámetro: <code>volume show -vserver vserver_name -fields fieldname,...</code></div> |

Ejemplos

En el siguiente ejemplo, se muestra un resumen de los volúmenes montados y desmontados en la SVM vs1:

```
cluster1::> volume show -vserver vs1 -junction
Vserver    Volume      Junction
-----
vs1        data        true      /data      RW_volume
vs1        home4       true      /eng/home  RW_volume
vs1        vs1_root    -         /          -
vs1        sales       true      /sales     RW_volume
```

En el siguiente ejemplo, se muestra información sobre campos especificados para los volúmenes ubicados en la SVM vs2:


```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume    aggregate size state  type security-style junction-path
junction-parent node
-----
vs2      data1      aggr3      2GB  online RW    unix          -          -
node3
vs2      data2      aggr3      1GB  online RW    ntfs          /data2
vs2_root node3
vs2      data2_1    aggr3      8GB  online RW    ntfs          /data2/d2_1
data2     node3
vs2      data2_2    aggr3      8GB  online RW    ntfs          /data2/d2_2
data2     node3
vs2      pubs      aggr1      1GB  online RW    unix          /publications
vs2_root node1
vs2      images    aggr3      2TB  online RW    ntfs          /images
vs2_root node3
vs2      logs      aggr1      1GB  online RW    unix          /logs
vs2_root node1
vs2      vs2_root  aggr3      1GB  online RW    ntfs          /          -
node3
```

Configurar estilos de seguridad

Cómo afectan los estilos de seguridad al acceso a los datos

Cuáles son los estilos de seguridad y sus efectos

Hay cuatro estilos de seguridad diferentes: UNIX, NTFS, mixto y unificado. Cada estilo de seguridad tiene un efecto diferente sobre cómo se gestionan los permisos para los datos. Debe comprender los diferentes efectos para asegurarse de que selecciona el estilo de seguridad adecuado para sus propósitos.

Es importante entender que los estilos de seguridad no determinan qué tipos de clientes pueden o no pueden tener acceso a los datos. Los estilos de seguridad sólo determinan el tipo de permisos que ONTAP utiliza para controlar el acceso a los datos y qué tipo de cliente puede modificar estos permisos.

Por ejemplo, si un volumen utiliza el estilo de seguridad UNIX, los clientes SMB todavía pueden acceder a los datos (siempre y cuando estos se autenticuen y autoricen correctamente) debido a la naturaleza multiprotocolo de ONTAP. Sin embargo, ONTAP utiliza permisos UNIX que sólo los clientes UNIX pueden modificar mediante herramientas nativas.

| Estilo de seguridad | Clientes que pueden modificar permisos | Permisos que pueden utilizar los clientes | El estilo de seguridad efectivo resultante | Clientes que pueden acceder a los ficheros |
|--|--|---|--|--|
| UNIX | NFS | Bits del modo NFSv3 | UNIX | NFS y SMB |
| | | NFSv4.x ACL | | |
| NTFS | SMB | ACL de NTFS | NTFS | |
| Mixto | NFS o SMB | Bits del modo NFSv3 | UNIX | |
| | | NFSv4.ACL | | |
| | | ACL de NTFS | NTFS | |
| Unificado (Solo para Infinite Volume, en ONTAP 9,4 y versiones anteriores). | NFS o SMB | Bits del modo NFSv3 | UNIX | |
| | | ACL de NFSv4.1 | | |
| | | ACL de NTFS | NTFS | |

Los volúmenes de FlexVol son compatibles con UNIX, NTFS y estilos de seguridad mixtos. Cuando el estilo de seguridad es mixto o unificado, los permisos efectivos dependen del tipo de cliente que modificó por última vez los permisos porque los usuarios establecen el estilo de seguridad de forma individual. Si el último cliente que modificó permisos era un cliente NFSv3, los permisos son bits del modo NFSv3 de UNIX. Si el último cliente era un cliente NFSv4, los permisos son ACL de NFSv4. Si el último cliente era un cliente SMB, los permisos son ACL de Windows NTFS.

El estilo de seguridad unificado solo está disponible en Infinite Volume, que ya no son compatibles con ONTAP 9.5 y versiones posteriores. Para obtener más información, consulte [Información general de gestión de volúmenes de FlexGroup](#).

A partir de ONTAP 9,2, el `show-effective-permissions` parámetro de la `vserver security file-directory` El comando le permite mostrar permisos efectivos otorgados a un usuario de Windows o UNIX en la ruta de archivo o carpeta especificada. Además, el parámetro opcional `-share-name` permite mostrar el permiso de uso compartido efectivo.



ONTAP establece inicialmente algunos permisos de archivo predeterminados. De forma predeterminada, el estilo de seguridad efectivo de todos los datos de los volúmenes de estilo de seguridad mixto y unificado es UNIX y el tipo de permisos efectivos es bits de modo UNIX (0755 a menos que se especifique lo contrario) hasta que un cliente lo configure como permite el estilo de seguridad predeterminado. De forma predeterminada, el estilo de seguridad efectivo en todos los datos de los volúmenes de estilo de seguridad NTFS es NTFS y tiene una ACL que permite un control total para todos.

Dónde y cuándo establecer estilos de seguridad

Los estilos de seguridad se pueden establecer en volúmenes de FlexVol (tanto volúmenes raíz como de datos) y qtrees. Los estilos de seguridad se pueden configurar manualmente en el momento de la creación, heredados automáticamente o modificados posteriormente.

Decida qué estilo de seguridad se utilizará en las SVM

Para ayudar a decidir qué estilo de seguridad se debe usar en un volumen, se deben tener en cuenta dos factores. El factor principal es el tipo de administrador que administra el sistema de archivos. El factor secundario es el tipo de usuario o servicio que tiene acceso a los datos del volumen.

Al configurar el estilo de seguridad en un volumen, debe tener en cuenta las necesidades del entorno para garantizar que selecciona el mejor estilo de seguridad y evitar problemas con la gestión de permisos. Las siguientes consideraciones pueden ayudarle a decidir:

| Estilo de seguridad | Elija si... |
|---------------------|--|
| UNIX | <ul style="list-style-type: none">• Un administrador de UNIX gestiona el sistema de ficheros.• La mayoría de los usuarios son clientes NFS.• Una aplicación que accede a los datos utiliza un usuario UNIX como cuenta de servicio. |
| NTFS | <ul style="list-style-type: none">• Un administrador de Windows gestiona el sistema de archivos.• La mayoría de los usuarios son clientes SMB.• Una aplicación que accede a los datos utiliza un usuario de Windows como cuenta de servicio. |
| Mixto | <ul style="list-style-type: none">• El sistema de archivos lo gestionan administradores de UNIX y Windows, y los usuarios están formados por clientes NFS y SMB. |

Cómo funciona la herencia de estilos de seguridad

Si no especifica el estilo de seguridad al crear un nuevo volumen de FlexVol o un qtree, hereda su estilo de seguridad de formas diferentes.

Los estilos de seguridad se heredan de la siguiente manera:

- Un volumen FlexVol hereda el estilo de seguridad del volumen raíz de su SVM que contiene.
- Un qtree hereda el estilo de seguridad del volumen FlexVol que contiene.
- Un archivo o un directorio hereda el estilo de seguridad de su volumen o qtree de FlexVol.

Cómo ONTAP conserva los permisos de UNIX

Cuando las aplicaciones Windows editan y guardan archivos de un volumen FlexVol que actualmente tienen permisos UNIX, ONTAP puede preservar los permisos UNIX.

Cuando las aplicaciones de clientes de Windows editan y guardan archivos, leen las propiedades de seguridad del archivo, crean un nuevo archivo temporal, aplican esas propiedades al archivo temporal y, a continuación, asignan al archivo temporal el nombre de archivo original.

Cuando los clientes de Windows realizan una consulta para las propiedades de seguridad, reciben una ACL construida que representa exactamente los permisos de UNIX. El único propósito de esta ACL construida es preservar los permisos UNIX del archivo a medida que las aplicaciones de Windows actualizan los archivos.

para garantizar que los archivos resultantes tengan los mismos permisos UNIX. ONTAP no establece ninguna ACL de NTFS usando la ACL construida.

Administre los permisos de UNIX mediante la ficha Seguridad de Windows

Si desea manipular los permisos de UNIX de archivos o carpetas en volúmenes o qtrees de estilo de seguridad mixtos en las SVM, puede utilizar la pestaña Seguridad en clientes de Windows. También puede utilizar aplicaciones que puedan consultar y establecer ACL de Windows.

- Modificación de permisos de UNIX

Puede usar la pestaña Seguridad de Windows para ver y cambiar los permisos de UNIX para un volumen o un qtree de estilo de seguridad mixto. Si utiliza la ficha Seguridad de Windows principal para cambiar los permisos de UNIX, primero debe quitar la ACE existente que desea editar (esto establece los bits de modo en 0) antes de realizar los cambios. De forma alternativa, puede utilizar el editor avanzado para cambiar los permisos.

Si se utilizan permisos de modo, puede cambiar directamente los permisos de modo para el UID, GID y otros (todos los demás con una cuenta en el equipo) de la lista. Por ejemplo, si el UID mostrado tiene permisos r-x, puede cambiar los permisos de UID a rwx.

- Cambiar los permisos de UNIX a los permisos NTFS

Puede usar la pestaña Seguridad de Windows para reemplazar objetos de seguridad UNIX por objetos de seguridad de Windows en un volumen o qtree de estilo de seguridad mixto donde los archivos y carpetas tienen un estilo de seguridad efectivo de UNIX.

Primero debe quitar todas las entradas de permisos de UNIX enumeradas antes de que pueda reemplazarlas con los objetos de usuario y grupo de Windows deseados. A continuación, puede configurar ACL basados en NTFS en los objetos Usuario y Grupo de Windows. Si quita todos los objetos de seguridad de UNIX y agrega sólo usuarios y grupos de Windows a un archivo o carpeta de un volumen o qtree de estilo de seguridad mixto, cambie el estilo de seguridad efectivo del archivo o carpeta de UNIX a NTFS.

Al cambiar los permisos de una carpeta, el comportamiento predeterminado de Windows es propagar estos cambios a todas las subcarpetas y archivos. Por lo tanto, debe cambiar la opción de propagación a la configuración deseada si no desea propagar un cambio en el estilo de seguridad a todas las carpetas secundarias, subcarpetas y archivos.

Configurar estilos de seguridad en volúmenes raíz de SVM

El estilo de seguridad del volumen raíz de la máquina virtual de almacenamiento (SVM) se configura para determinar el tipo de permisos utilizados para los datos en el volumen raíz de la SVM.

Pasos

1. Utilice la `vserver create` con el `-rootvolume-security-style` parámetro para definir el estilo de seguridad.

Las opciones posibles para el estilo de seguridad del volumen raíz son `unix`, `ntfs`, o `mixed`.

2. Mostrar y verificar la configuración, incluido el estilo de seguridad del volumen raíz de la SVM que creó:

```
vserver show -vserver vserver_name
```

Configurar estilos de seguridad en volúmenes FlexVol

El estilo de seguridad del volumen FlexVol se configura para determinar el tipo de permisos utilizados para los datos en volúmenes FlexVol de la máquina virtual de almacenamiento (SVM).

Pasos

1. Ejecute una de las siguientes acciones:

| Si el volumen de FlexVol... | Usar el comando... |
|-----------------------------|---|
| Aún no existe | <code>volume create</code> e incluya la <code>-security-style</code> parámetro para especificar el estilo de seguridad. |
| Ya existe | <code>volume modify</code> e incluya la <code>-security-style</code> parámetro para especificar el estilo de seguridad. |

Las posibles opciones para el estilo de seguridad del volumen FlexVol son `unix`, `ntfs`, o `mixed`.

Si no se especifica un estilo de seguridad al crear un volumen FlexVol, el volumen hereda el estilo de seguridad del volumen raíz.

Para obtener más información acerca de `volume create` o `volume modify` comandos, consulte ["Gestión de almacenamiento lógico"](#).

2. Para ver la configuración, incluido el estilo de seguridad del volumen FlexVol que se creó, escriba el siguiente comando:

```
volume show -volume volume_name -instance
```

Configurar estilos de seguridad en qtrees

El estilo de seguridad del volumen de qtrees se configura para determinar el tipo de permisos utilizados para los datos en qtrees.

Pasos

1. Ejecute una de las siguientes acciones:

| Si el qtree... | Usar el comando... |
|----------------|---|
| Aún no existe | <code>volume qtree create</code> e incluya la <code>-security-style</code> parámetro para especificar el estilo de seguridad. |
| Ya existe | <code>volume qtree modify</code> e incluya la <code>-security-style</code> parámetro para especificar el estilo de seguridad. |

Las posibles opciones para el estilo de seguridad para qtrees son `unix`, `ntfs`, o `mixed`.

Si no se especifica un estilo de seguridad al crear un qtree, el estilo de seguridad predeterminado es `mixed`.

Para obtener más información acerca de `volume qtree create` o `volume qtree modify` comandos, consulte "[Gestión de almacenamiento lógico](#)".

2. Para ver la configuración, incluido el estilo de seguridad del qtree que ha creado, escriba el siguiente comando: `volume qtree show -qtree qtree_name -instance`

Configurar el acceso a archivos mediante NFS

Configurar el acceso a archivos con la información general de NFS

Debe completar una serie de pasos para permitir que los clientes accedan a archivos de máquinas virtuales de almacenamiento (SVM) mediante NFS. Existen algunos pasos adicionales que son opcionales en función de la configuración actual de su entorno.

Para que los clientes puedan acceder a los archivos de las SVM mediante NFS, debe realizar las siguientes tareas:

1. Habilite el protocolo NFS en la SVM.

Debe configurar la SVM para permitir el acceso a los datos desde clientes a través de NFS.

2. Cree un servidor NFS en la SVM.

Un servidor NFS es una entidad lógica en la SVM que permite que la SVM sirva archivos a través de NFS. Debe crear el servidor NFS y especificar las versiones de protocolo NFS que desea permitir.

3. Configure las políticas de exportación en la SVM.

Es necesario configurar las políticas de exportación para que los volúmenes y qtrees estén disponibles para los clientes.

4. Configuración del servidor NFS con la seguridad y otras opciones adecuadas en función de la red y el entorno de almacenamiento.

Este paso puede incluir la configuración de Kerberos, LDAP, NIS, asignaciones de nombres y usuarios locales.

Acceso NFS seguro mediante políticas de exportación

Cómo las políticas de exportación controlan el acceso de los clientes a volúmenes o qtrees

Las políticas de exportación contienen una o varias *reglas de exportación* que procesan cada solicitud de acceso de cliente. El resultado del proceso determina si se deniega o se concede acceso al cliente y qué nivel de acceso. Para que los clientes accedan a los datos, debe haber una política de exportación con reglas de exportación en la máquina virtual de almacenamiento (SVM).

Se asocia exactamente una política de exportación a cada volumen o qtree para configurar el acceso de los clientes al volumen o qtree. La SVM puede contener varias políticas de exportación. Esto le permite hacer lo siguiente para las SVM con varios volúmenes o qtrees:

- Asigne diferentes políticas de exportación a cada volumen o qtree de la SVM para controlar el acceso de cliente individual a cada volumen o qtree de la SVM.
- Asigne la misma política de exportación a varios volúmenes o qtrees de la SVM para un control de acceso del cliente idéntico sin que tenga que crear una nueva política de exportación para cada volumen o qtree.

Si un cliente realiza una solicitud de acceso que no está permitida por la política de exportación aplicable, la solicitud falla con un mensaje de permiso denegado. Si un cliente no coincide con ninguna regla de la política de exportación, se deniega el acceso. Si una política de exportación está vacía, se deniegan implícitamente todos los accesos.

Puede modificar dinámicamente una política de exportación en un sistema que ejecuta ONTAP.

Política de exportación predeterminada para las SVM

Cada SVM tiene una política de exportación predeterminada que no contiene reglas. Para que los clientes puedan acceder a los datos en la SVM, debe haber una política de exportación con reglas. Cada volumen FlexVol que contiene la SVM debe estar asociado a una política de exportación.

Cuando se crea una SVM, el sistema de almacenamiento crea automáticamente una política de exportación predeterminada llamada `default` Para el volumen raíz de la SVM. Debe crear una o varias reglas para la política de exportación predeterminada para que los clientes puedan acceder a los datos de la SVM. También puede crear una política de exportación personalizada con reglas. Puede modificar y cambiar el nombre de la política de exportación predeterminada, pero no puede eliminar la política de exportación predeterminada.

Cuando se crea un volumen FlexVol en la SVM que contiene, el sistema de almacenamiento crea el volumen y asocia el volumen con la política de exportación predeterminada para el volumen raíz de la SVM. De manera predeterminada, cada volumen creado en la SVM está asociado con la política de exportación predeterminada para el volumen raíz. Puede usar la política de exportación predeterminada para todos los volúmenes contenidos en la SVM, o bien puede crear una política de exportación única para cada volumen. Es posible asociar varios volúmenes con la misma política de exportación.

Cómo funcionan las reglas de exportación

Las reglas de exportación son los elementos funcionales de una política de exportación. Las reglas de exportación coinciden con las solicitudes de acceso de los clientes a un volumen con los parámetros específicos que se configuran para determinar cómo se manejan las solicitudes de acceso de los clientes.

La política de exportación debe contener al menos una regla de exportación para permitir el acceso a los clientes. Si una política de exportación contiene más de una regla, se procesan las reglas en el orden en que aparecen en la política de exportación. El orden de las reglas viene determinado por el número de índice de reglas. Si una regla coincide con un cliente, se utilizan los permisos de esa regla y no se procesan otras reglas. Si no hay reglas que coincidan, se deniega el acceso al cliente.

Puede configurar reglas de exportación para determinar los permisos de acceso de clientes con los siguientes criterios:

- El protocolo de acceso a archivos que utiliza el cliente para enviar la solicitud, por ejemplo, NFSv4 o SMB.

- Un identificador de cliente, por ejemplo, un nombre de host o una dirección IP.

El tamaño máximo de `-clientmatch` el campo tiene 4096 caracteres.

- Tipo de seguridad utilizado por el cliente para autenticar, por ejemplo, Kerberos v5, NTLM o AUTH_SYS.

Si una regla especifica varios criterios, el cliente debe coincidir con todos ellos para que se aplique la regla.



A partir de ONTAP 9.3, puede habilitar la comprobación de la configuración de la política de exportación como un trabajo en segundo plano que registra cualquier infracción de reglas en una lista de reglas de error. La `vserver export-policy config-checker` los comandos invocan al comprobador y muestran los resultados, que se pueden utilizar para verificar la configuración y eliminar reglas erróneas de la directiva.

Los comandos solo validan la configuración de exportación para los nombres de host, grupos de red y usuarios anónimos.

Ejemplo

La política de exportación contiene una regla de exportación con los siguientes parámetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

La solicitud de acceso del cliente se envía mediante el protocolo NFSv3 y el cliente tiene la dirección IP 10.1.17.37.

Aunque el protocolo de acceso del cliente coincida, la dirección IP del cliente se encuentra en una subred diferente de la especificada en la regla de exportación. Por lo tanto, la coincidencia de cliente falla y esta regla no se aplica a este cliente.

Ejemplo

La política de exportación contiene una regla de exportación con los siguientes parámetros:

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

La solicitud de acceso del cliente se envía con el protocolo NFSv4 y el cliente tiene la dirección IP 10.1.16.54.

El protocolo de acceso del cliente coincide y la dirección IP del cliente se encuentra en la subred especificada. Por lo tanto, la coincidencia de cliente es correcta y esta regla se aplica a este cliente. El cliente obtiene acceso de lectura y escritura independientemente de su tipo de seguridad.

Ejemplo

La política de exportación contiene una regla de exportación con los siguientes parámetros:

- `-protocol nfs3`

- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`

El cliente n.º 1 tiene la dirección IP 10.1.16.207, envía una solicitud de acceso con el protocolo NFSv3 y se autentica con Kerberos v5.

El cliente #2 tiene la dirección IP 10.1.16.211, envía una solicitud de acceso con el protocolo NFSv3 y se autentica con AUTH_SYS.

El protocolo de acceso del cliente y la dirección IP coinciden con los dos clientes. El parámetro de solo lectura permite un acceso de solo lectura a todos los clientes independientemente del tipo de seguridad con el que se autenticuen. Por lo tanto, ambos clientes obtienen acceso de solo lectura. Sin embargo, sólo el cliente #1 obtiene acceso de lectura y escritura porque utilizó el tipo de seguridad aprobado Kerberos v5 para autenticar. El cliente n.º 2 no obtiene acceso de lectura/escritura.

Administrar clientes con un tipo de seguridad sin lista

Cuando un cliente se presenta a sí mismo con un tipo de seguridad que no aparece en un parámetro de acceso de una regla de exportación, tiene la opción de denegar el acceso al cliente o asignarlo al ID de usuario anónimo en su lugar mediante la opción `none` en el parámetro `access`.

Es posible que un cliente se presente a sí mismo con un tipo de seguridad que no aparece en un parámetro de acceso porque se autentica con un tipo de seguridad diferente o que no se haya autenticado en absoluto (tipo de seguridad AUTH_NONE). De forma predeterminada, al cliente se le deniega automáticamente el acceso a ese nivel. Sin embargo, puede agregar la opción `none` al parámetro `access`. Como resultado, los clientes con un estilo de seguridad no enumerado se asignan al ID de usuario anónimo en su lugar. La `-anon` Parámetro determina qué ID de usuario se asigna a esos clientes. El ID de usuario especificado para `-anon` el parámetro debe ser un usuario válido configurado con los permisos que considere apropiados para el usuario anónimo.

Valores válidos para `-anon` intervalo de parámetros desde 0 para 65535.

| ID de usuario asignado a. <code>-anon</code> | Tratamiento resultante de las solicitudes de acceso de los clientes |
|--|--|
| 0 - 65533 | La solicitud de acceso de cliente se asigna al ID de usuario anónimo y obtiene acceso en función de los permisos configurados para este usuario. |
| 65534 | La solicitud de acceso de cliente no se asigna al usuario y obtiene acceso en función de los permisos configurados para este usuario. Este es el valor predeterminado. |

| ID de usuario asignado a. -anon | Tratamiento resultante de las solicitudes de acceso de los clientes |
|---------------------------------|---|
| 65535 | La solicitud de acceso de cualquier cliente se deniega cuando se asigna a este ID y el cliente se presenta con el tipo de seguridad AUTH_NONE. La solicitud de acceso de los clientes con ID de usuario 0 se deniega cuando se asigna a este ID y el cliente se presenta a sí mismo con cualquier otro tipo de seguridad. |

Al utilizar la opción `none`, es importante recordar que el parámetro de sólo lectura se procesa primero. Tenga en cuenta las siguientes directrices al configurar reglas de exportación para clientes con tipos de seguridad no listados:

| Incluye solo lectura <code>none</code> | Incluye lectura y escritura <code>none</code> | Acceso resultante para clientes con tipos de seguridad no listados |
|--|---|--|
| No | No | Denegada |
| No | Sí | Denegado porque sólo lectura se procesa primero |
| Sí | No | Sólo lectura como anónimo |
| Sí | Sí | Lectura y escritura como anónimo |

Ejemplo

La política de exportación contiene una regla de exportación con los siguientes parámetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule any`
- `-anon 70`

El cliente n.º 1 tiene la dirección IP 10.1.16.207, envía una solicitud de acceso con el protocolo NFSv3 y se autentica con Kerberos v5.

El cliente #2 tiene la dirección IP 10.1.16.211, envía una solicitud de acceso con el protocolo NFSv3 y se autentica con AUTH_SYS.

El cliente #3 tiene la dirección IP 10.1.16.234, envía una solicitud de acceso con el protocolo NFSv3 y no se autentica (es decir, el tipo de seguridad AUTH_NONE).

El protocolo de acceso del cliente y la dirección IP coinciden con los tres clientes. El parámetro de sólo lectura permite el acceso de sólo lectura a clientes con su propio ID de usuario que se autentica con AUTH_SYS. El parámetro de sólo lectura permite el acceso de sólo lectura como usuario anónimo con ID de usuario 70 a

clientes autenticados mediante cualquier otro tipo de seguridad. El parámetro de lectura y escritura permite acceso de lectura y escritura a cualquier tipo de seguridad, pero en este caso solo se aplica a los clientes ya filtrados por la regla de solo lectura.

Por lo tanto, los clientes #1 y #3 obtienen acceso de lectura y escritura sólo como el usuario anónimo con ID de usuario 70. El cliente #2 obtiene acceso de lectura y escritura con su propio ID de usuario.

Ejemplo

La política de exportación contiene una regla de exportación con los siguientes parámetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule none`
- `-anon 70`

El cliente n.º 1 tiene la dirección IP 10.1.16.207, envía una solicitud de acceso con el protocolo NFSv3 y se autentica con Kerberos v5.

El cliente #2 tiene la dirección IP 10.1.16.211, envía una solicitud de acceso con el protocolo NFSv3 y se autentica con AUTH_SYS.

El cliente #3 tiene la dirección IP 10.1.16.234, envía una solicitud de acceso con el protocolo NFSv3 y no se autentica (es decir, el tipo de seguridad AUTH_NONE).

El protocolo de acceso del cliente y la dirección IP coinciden con los tres clientes. El parámetro de sólo lectura permite el acceso de sólo lectura a clientes con su propio ID de usuario que se autentica con AUTH_SYS. El parámetro de sólo lectura permite el acceso de sólo lectura como usuario anónimo con ID de usuario 70 a clientes autenticados mediante cualquier otro tipo de seguridad. El parámetro de lectura y escritura permite el acceso de lectura y escritura sólo como el usuario anónimo.

Por lo tanto, el cliente #1 y el cliente #3 obtienen acceso de lectura y escritura sólo como el usuario anónimo con el ID de usuario 70. El cliente #2 obtiene acceso de sólo lectura con su propio ID de usuario pero se le deniega el acceso de lectura y escritura.

Cómo los tipos de seguridad determinan los niveles de acceso de los clientes

El tipo de seguridad con el que el cliente autenticado desempeña un rol especial en las reglas de exportación. Debe entender la manera en que el tipo de seguridad determina los niveles de acceso que el cliente obtiene a un volumen o un qtree.

Los tres niveles de acceso posibles son los siguientes:

1. Solo lectura
2. Lectura-escritura
3. Superusuario (para clientes con ID de usuario 0)

Dado que el nivel de acceso por tipo de seguridad se evalúa en este orden, debe observar las siguientes reglas al construir parámetros de nivel de acceso en las reglas de exportación:

| Para que un cliente obtenga el nivel de acceso... | Estos parámetros de acceso deben coincidir con el tipo de seguridad del cliente... |
|---|---|
| Usuario normal de solo lectura | Solo lectura (<code>-rorule</code>) |
| Lectura y escritura normal del usuario | Solo lectura (<code>-rorule</code>) y lectura y escritura (<code>-rwrule</code>) |
| Sólo lectura de superusuario | Solo lectura (<code>-rorule</code>) y. <code>-superuser</code> |
| Lectura y escritura de superusuario | Solo lectura (<code>-rorule</code>) y lectura y escritura (<code>-rwrule</code>) y. <code>-superuser</code> |

A continuación, se muestran tipos de seguridad válidos para cada uno de estos tres parámetros de acceso:

- `any`
- `none`
- `never`

Este tipo de seguridad no es válido para su uso con `-superuser` parámetro.

- `krb5`
- `krb5i`
- `krb5p`
- `ntlm`
- `sys`

Al hacer coincidir el tipo de seguridad de un cliente con cada uno de los tres parámetros de acceso, hay tres resultados posibles:

| Si el tipo de seguridad del cliente... | A continuación, el cliente... |
|--|--|
| Coincide con el especificado en el parámetro <code>access</code> . | Obtiene acceso para ese nivel con su propio ID de usuario. |
| No coincide con el especificado, pero el parámetro <code>access</code> incluye la opción <code>none</code> . | Obtiene acceso para ese nivel pero como usuario anónimo con el ID de usuario especificado por <code>-anon</code> parámetro. |
| No coincide con el especificado y el parámetro <code>access</code> no incluye la opción <code>none</code> . | No obtiene acceso para ese nivel. Esto no se aplica a <code>-superuser</code> parámetro porque siempre incluye <code>none</code> incluso cuando no se especifique. |

Ejemplo

La política de exportación contiene una regla de exportación con los siguientes parámetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule sys,krb5`
- `-superuser krb5`

El cliente #1 tiene la dirección IP 10.1.16.207, tiene el ID de usuario 0, envía una solicitud de acceso con el protocolo NFSv3 y se autentica con Kerberos v5.

El cliente #2 tiene la dirección IP 10.1.16.211, tiene el ID de usuario 0, envía una solicitud de acceso con el protocolo NFSv3 y se autentica con AUTH_SYS.

El cliente #3 tiene la dirección IP 10.1.16.234, tiene el ID de usuario 0, envía una solicitud de acceso con el protocolo NFSv3 y no se autentica (AUTH_NONE).

El protocolo de acceso del cliente y la dirección IP coinciden con los tres clientes. El parámetro de solo lectura permite el acceso de solo lectura a todos los clientes independientemente del tipo de seguridad. El parámetro de lectura y escritura permite acceder de lectura y escritura a clientes con su propio ID de usuario que se autentica con AUTH_SYS o Kerberos v5. El parámetro superusuario permite el acceso de superusuario a clientes con ID de usuario 0 que se autentiquen con Kerberos v5.

Por lo tanto, el cliente #1 obtiene acceso de lectura y escritura de superusuario porque coincide con los tres parámetros de acceso. El cliente #2 obtiene acceso de lectura y escritura, pero no acceso de superusuario. El cliente #3 obtiene acceso de sólo lectura pero no acceso de superusuario.

Administrar solicitudes de acceso de superusuario

Cuando configura políticas de exportación, debe tener en cuenta lo que desea que suceda si el sistema de almacenamiento recibe una solicitud de acceso de cliente con ID de usuario 0, lo que significa como superusuario y configure las reglas de exportación según corresponda.

En el mundo UNIX, un usuario con el ID de usuario 0 se conoce como superusuario, normalmente llamado root, que tiene derechos de acceso ilimitados en un sistema. El uso de privilegios de superusuario puede ser peligroso por varias razones, como la violación de la seguridad del sistema y de los datos.

De forma predeterminada, ONTAP asigna los clientes que presentan el ID de usuario 0 al usuario anónimo. Sin embargo, puede especificar el `-superuser` Parámetro en reglas de exportación para determinar cómo gestionar los clientes que presentan el ID de usuario 0 en función de su tipo de seguridad. A continuación, se muestran opciones válidas para el `-superuser` parámetro:

- `any`
- `none`

Esta es la configuración predeterminada si no se especifica el `-superuser` parámetro.

- `krb5`
- `ntlm`
- `sys`

Hay dos maneras diferentes de manejar los clientes que presentan con ID de usuario 0, dependiendo de la `-superuser` configuración de parámetros:

| Si la <code>-superuser</code> parámetro y tipo de seguridad del cliente... | A continuación, el cliente... |
|--|--|
| Coincidencia | Obtiene acceso de superusuario con ID de usuario 0. |
| No coinciden | Obtiene acceso como usuario anónimo con el ID de usuario especificado por <code>-anon</code> parámetro y sus permisos asignados. Esto es independientemente de si el parámetro de solo lectura o de lectura y escritura especifica la opción <code>none</code> . |

Si un cliente presenta con el ID de usuario 0 para acceder a un volumen con estilo de seguridad NTFS y el `-superuser` el parámetro se establece en `none`, ONTAP utiliza la asignación de nombres del usuario anónimo para obtener las credenciales adecuadas.

Ejemplo

La política de exportación contiene una regla de exportación con los siguientes parámetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-anon 127`

El cliente #1 tiene la dirección IP 10.1.16.207, tiene el ID de usuario 746, envía una solicitud de acceso mediante el protocolo NFSv3 y se autentica con Kerberos v5.

El cliente #2 tiene la dirección IP 10.1.16.211, tiene el ID de usuario 0, envía una solicitud de acceso con el protocolo NFSv3 y se autentica con AUTH_SYS.

El protocolo de acceso del cliente y la dirección IP coinciden con los dos clientes. El parámetro de solo lectura permite un acceso de solo lectura a todos los clientes independientemente del tipo de seguridad con el que se autenticuen. Sin embargo, sólo el cliente #1 obtiene acceso de lectura y escritura porque utilizó el tipo de seguridad aprobado Kerberos v5 para autenticar.

El cliente #2 no obtiene acceso de superusuario. En su lugar, se asigna a anónimo porque el `-superuser` no se ha especificado el parámetro. Esto significa que de forma predeterminada es `none` Y asigna automáticamente el ID de usuario 0 al anónimo. El cliente #2 sólo obtiene acceso de sólo lectura porque su tipo de seguridad no coincide con el parámetro de lectura y escritura.

Ejemplo

La política de exportación contiene una regla de exportación con los siguientes parámetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`

- `-rwrule krb5,ntlm`
- `-superuser krb5`
- `-anon 0`

El cliente #1 tiene la dirección IP 10.1.16.207, tiene el ID de usuario 0, envía una solicitud de acceso con el protocolo NFSv3 y se autentica con Kerberos v5.

El cliente #2 tiene la dirección IP 10.1.16.211, tiene el ID de usuario 0, envía una solicitud de acceso con el protocolo NFSv3 y se autentica con AUTH_SYS.

El protocolo de acceso del cliente y la dirección IP coinciden con los dos clientes. El parámetro de solo lectura permite un acceso de solo lectura a todos los clientes independientemente del tipo de seguridad con el que se autenticuen. Sin embargo, sólo el cliente #1 obtiene acceso de lectura y escritura porque utilizó el tipo de seguridad aprobado Kerberos v5 para autenticar. El cliente n.o 2 no obtiene acceso de lectura/escritura.

La regla de exportación permite el acceso de superusuario para clientes con ID de usuario 0. El cliente #1 obtiene acceso de superusuario porque coincide con el ID de usuario y el tipo de seguridad para los de sólo lectura y. `-superuser` parámetros. El cliente #2 no obtiene acceso de lectura-escritura o superusuario porque su tipo de seguridad no coincide con el parámetro de lectura-escritura o el `-superuser` parámetro. En su lugar, el cliente #2 está asignado al usuario anónimo, que en este caso tiene el ID de usuario 0.

Cómo utiliza ONTAP las cachés de la política de exportación

Para mejorar el rendimiento del sistema, ONTAP utiliza cachés locales para almacenar información como nombres de host y grupos de redes. De este modo, ONTAP puede procesar reglas de política de exportación más rápidamente que recuperar la información de fuentes externas. Comprender qué son las cachés y qué hacen puede ayudarlo a solucionar los problemas de acceso de los clientes.

Puede configurar políticas de exportación para controlar el acceso de los clientes a las exportaciones de NFS. Cada política de exportación contiene reglas y cada regla contiene parámetros que coincidan con los de los clientes que soliciten acceso. Algunos de estos parámetros requieren que ONTAP se ponga en contacto con un origen externo, como los servidores DNS o NIS, para resolver objetos como nombres de dominio, nombres de host o grupos de red.

Estas comunicaciones con fuentes externas tardan una pequeña cantidad de tiempo. Para aumentar el rendimiento, ONTAP reduce la cantidad de tiempo que se necesita para resolver los objetos de reglas de políticas de exportación almacenando la información localmente en cada nodo en varias cachés.

| Nombre de caché | Tipo de información almacenada |
|-----------------|---|
| Acceso | Asignaciones de clientes a las correspondientes políticas de exportación |
| Nombre | Se asignan los nombres de usuario UNIX a los correspondientes ID de usuario UNIX |
| ID | Mapeos de ID de usuario de UNIX a ID de usuario de UNIX correspondientes e ID de grupo de UNIX ampliado |

| Nombre de caché | Tipo de información almacenada |
|-----------------|---|
| Host | Asignación de los nombres de host a las direcciones IP correspondientes |
| Grupo de red | Asignaciones de grupos de red a las direcciones IP correspondientes de los miembros |
| Showmount | Lista de directorios exportados desde el espacio de nombres de SVM |

Si cambia información de los servidores de nombres externos de su entorno después de que ONTAP haya recuperado y almacenado localmente, es posible que las cachés contengan información obsoleta. Aunque las actualizaciones de ONTAP se actualizan automáticamente en caché tras ciertos periodos de tiempo, diferentes cachés tienen tiempos y algoritmos de caducidad y actualización diferentes.

Otra posible razón para que las cachés contengan información obsoleta es cuando ONTAP intenta actualizar la información almacenada en caché pero encuentra un error al intentar comunicarse con servidores de nombres. Si esto sucede, ONTAP sigue usando la información actualmente almacenada en la caché local para evitar que se produzca una interrupción del cliente.

Como resultado, las solicitudes de acceso a clientes que se supone que tienen éxito pueden fallar y las solicitudes de acceso de clientes que se supone que fallan se pueden realizar correctamente. Puede ver y purgar manualmente algunas de las cachés de políticas de exportación al solucionar los problemas de acceso de los clientes.

Cómo funciona la caché de acceso

ONTAP usa una caché de acceso para almacenar los resultados de la evaluación de las reglas de política de exportación para las operaciones de acceso de los clientes a un volumen o un qtree. Esto genera mejoras en el rendimiento porque la información se puede recuperar mucho más rápido de la caché de acceso que pasar por el proceso de evaluación de las reglas de la política de exportación cada vez que un cliente envía una solicitud de I/O.

Siempre que un cliente NFS envía una solicitud de I/o para acceder a los datos de un volumen o un qtree, ONTAP debe evaluar cada solicitud de I/o para determinar si desea conceder o denegar la solicitud de I/O. Esta evaluación implica la comprobación de cada regla de política de exportación de la política de exportación asociada con el volumen o el qtree. Si la ruta al volumen o qtree implica cruzar uno o más puntos de unión, puede ser necesario realizar esta comprobación en busca de varias políticas de exportación por la ruta.

Tenga en cuenta que esta evaluación se produce para cada solicitud de I/o que se envía desde un cliente NFS, como operaciones de lectura, escritura, lista, copia y otras, y no solo para solicitudes de montaje iniciales.

Una vez que ONTAP ha identificado las reglas de política de exportación aplicables y ha decidido si permitir o denegar la solicitud, ONTAP creará una entrada en la caché de acceso para almacenar dicha información.

Cuando un cliente NFS envía una solicitud de I/o, ONTAP señala la dirección IP del cliente, el ID de la SVM y la política de exportación asociada con el volumen o qtree de destino, y, primero, comprueba la caché de acceso para ver si existe una entrada correspondiente. Si existe una entrada coincidente en la caché de acceso, ONTAP utiliza la información almacenada para permitir o denegar la solicitud de E/S. Si no existe una

entrada coincidente, ONTAP pasa por el proceso normal de evaluación de todas las reglas de política aplicables como se ha explicado anteriormente.

Las entradas de la caché de acceso que no se utilizan activamente no se actualizan. Esto reduce la comunicación innecesaria y innecesaria con servicios de nombres externos.

La recuperación de la información de la caché de acceso es mucho más rápida que pasar por todo el proceso de evaluación de las reglas de política de exportación para cada solicitud de I/O. Por lo tanto, el uso de la caché de acceso mejora considerablemente el rendimiento, ya que reduce la sobrecarga de las comprobaciones del acceso de los clientes.

Cómo funciona el acceso a los parámetros de caché

Varios parámetros controlan los períodos de actualización de las entradas de la caché de acceso. Comprender cómo funcionan estos parámetros le permite modificarlos para ajustar la caché de acceso y equilibrar el rendimiento con lo reciente que es la información almacenada.

La caché de acceso almacena entradas que constan de una o varias reglas de exportación que se aplican a los clientes que intentan acceder a volúmenes o qtrees. Estas entradas se almacenan durante cierto tiempo antes de que se actualicen. El tiempo de actualización viene determinado por los parámetros de la caché de acceso y depende del tipo de entrada de la caché de acceso.

Puede especificar parámetros de caché de acceso para SVM individuales. Esto permite que los parámetros difieren de acuerdo con los requisitos de acceso de la SVM. Las entradas de la caché de acceso que no se utilizan activamente no se actualizan, lo que reduce la comunicación innecesaria y innecesaria con servicios de nombres externos.

| Tipo de entrada de la caché de acceso | Descripción | Actualice el periodo en segundos |
|---------------------------------------|---|---|
| Entradas positivas | Acceso a las entradas de caché que no han dado lugar a una denegación de acceso a los clientes. | Mínimo: 300 Máximo: 86,400 El valor predeterminado es 3,600 |
| Entradas negativas | Las entradas de caché de acceso que han dado lugar a una denegación de acceso a los clientes. | Mínimo: 60 Máximo: 86,400 El valor predeterminado es 3,600 |

Ejemplo

Un cliente NFS intenta acceder a un volumen de un clúster de. ONTAP coincide con el cliente con una regla de política de exportación y determina que el cliente obtiene acceso en función de la configuración de la regla de la política de exportación. ONTAP almacena la regla de política de exportación en la caché de acceso como una entrada positiva. De forma predeterminada, ONTAP mantiene la entrada positiva de la caché de acceso durante una hora (3,600 segundos) y, a continuación, actualiza automáticamente la entrada para mantener la información actualizada.

Para evitar que la caché de acceso se llene innecesariamente, hay un parámetro adicional para borrar las entradas existentes de la caché de acceso que no se han utilizado durante un determinado período de tiempo para decidir el acceso de cliente. Este `-harvest-timeout` el parámetro tiene un intervalo permitido de 60 a 2,592,000 segundos y un ajuste predeterminado de 86,400 segundos.

Quitar una política de exportación de un qtree

Si decide que ya no desea asignar una política de exportación específica a un qtree, puede eliminar la política de exportación modificando el qtree para que herede la política de exportación del volumen que lo contiene. Para ello, utilice `volume qtree modify` con el `-export-policy` parámetro y cadena de nombre vacía (`""`).

Pasos

- 1. Para quitar una política de exportación de un qtree, introduzca el siguiente comando:

```
volume qtree modify -vserver vservice_name -qtree-path
/vol/volume_name/qtree_name -export-policy ""
```

- 2. Compruebe que el qtree se ha modificado en consecuencia:

```
volume qtree show -qtree qtree_name -fields export-policy
```

Validar los ID de Qtree para operaciones de archivos de qtree

ONTAP puede realizar una validación adicional opcional de identificadores de qtree. Esta validación garantiza que las solicitudes de operaciones de archivos cliente utilicen un identificador de qtree válido y que los clientes solo puedan mover archivos dentro del mismo qtree. Puede habilitar o deshabilitar esta validación modificando el `-validate-qtree-export` parámetro. Este parámetro está habilitado de forma predeterminada.

Acerca de esta tarea

Este parámetro solo es eficaz cuando se ha asignado una política de exportación directamente a uno o varios qtrees de la máquina virtual de almacenamiento (SVM).

Pasos

- 1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

- 2. Ejecute una de las siguientes acciones:

| Si desea que la validación de ID de qtree sea... | Introduzca el siguiente comando... |
|--|--|
| Activado | <pre>vserver nfs modify -vserver vserver_name -validate-qtree-export enabled</pre> |

| Si desea que la validación de ID de qtree sea... | Introduzca el siguiente comando... |
|--|---|
| Deshabilitado | <pre>vserver nfs modify -vserver vserver_name -validate-qtree-export disabled</pre> |

3. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

Restricciones de la directiva de exportación y uniones anidadas para volúmenes FlexVol

Si ha configurado políticas de exportación para establecer una política menos restrictiva en una unión anidada, pero una política más restrictiva en una unión de nivel superior, puede que no se pueda acceder a la unión de nivel inferior.

Debe asegurarse de que las uniones de nivel superior tienen políticas de exportación menos restrictivas que las uniones de nivel inferior.

Uso de Kerberos con NFS para una mayor seguridad

Compatibilidad de ONTAP para Kerberos

Kerberos proporciona una autenticación segura y segura para aplicaciones cliente/servidor. La autenticación permite verificar las identidades de usuario y proceso a un servidor. En el entorno de ONTAP, Kerberos proporciona autenticación entre máquinas virtuales de almacenamiento (SVM) y clientes NFS.

En ONTAP 9, se admiten las siguientes funcionalidades de Kerberos:

- Autenticación Kerberos 5 con comprobación de integridad (krb5i)

Krb5i utiliza sumas de comprobación para verificar la integridad de cada mensaje de NFS transferido entre el cliente y el servidor. Esto resulta útil por motivos de seguridad (por ejemplo, para garantizar que los datos no se han alterado) y por motivos de integridad de los datos (por ejemplo, para evitar que se dañen los datos cuando se utilizan NFS en redes no fiables).

- Autenticación Kerberos 5 con comprobación de privacidad (krb5p)

Krb5p utiliza sumas de comprobación para cifrar todo el tráfico entre cliente y servidor. Esto es más seguro y también implica más carga.

- Cifrado AES de 128 bits y 256 bits

El estándar de cifrado avanzado (AES) es un algoritmo de cifrado para proteger los datos electrónicos. ONTAP admite AES con claves de 128 bits (AES-128) y AES con cifrado de claves de 256 bits (AES-256) para Kerberos para mayor seguridad.

- Configuraciones en dominio de Kerberos a nivel de SVM

Los administradores de SVM ahora pueden crear configuraciones de dominio de Kerberos en el nivel de SVM. Esto significa que los administradores de SVM ya no tienen que depender del administrador de

clúster para la configuración de dominio de Kerberos y pueden crear configuraciones de dominio de Kerberos individuales en un entorno multi-tenancy.

Requisitos para configurar Kerberos con NFS

Antes de configurar Kerberos con NFS en el sistema, debe comprobar que determinados elementos de la red y el entorno de almacenamiento están configurados correctamente.



Los pasos para configurar su entorno dependen de qué versión y tipo del sistema operativo cliente, controlador de dominio, Kerberos, DNS, etc., que usted está usando. La documentación de todas estas variables está fuera del alcance de este documento. Para obtener más información, consulte la documentación correspondiente de cada componente.

Para obtener un ejemplo detallado de cómo configurar ONTAP y Kerberos 5 con NFSv3 y NFSv4 en un entorno mediante hosts de Windows Server 2008 R2 Active Directory y Linux, consulte el informe técnico 4073.

Primero deben configurarse los siguientes elementos:

Requisitos del entorno de red

- Kerberos

Debe tener una configuración Kerberos en funcionamiento con un centro de distribución de claves (KDC), como Kerberos basado en Windows Active Directory o MIT Kerberos.

Los servidores NFS deben utilizar `nfs` como el principal componente de su máquina principal.

- Servicio de directorio

Debe utilizar un servicio de directorio seguro en su entorno, como Active Directory u OpenLDAP, que esté configurado para usar LDAP sobre SSL/TLS.

- NTP

Debe tener un servidor de tiempo de trabajo que ejecute NTP. Esto es necesario para evitar errores de autenticación de Kerberos debido a una desviación de tiempo.

- Resolución de nombres de dominio (DNS)

Cada cliente UNIX y cada LIF de SVM deben tener un registro de servicio (SRV) adecuado registrado con el KDC en zonas de búsqueda inversa y de reenvío. Todos los participantes deben poder resolverse correctamente a través de DNS.

- Cuentas de usuario

Cada cliente debe tener una cuenta de usuario en el dominio Kerberos. Los servidores NFS deberán utilizar «`nfs`» como componente principal de su principal equipo.

Requisitos del cliente NFS

- NFS

Cada cliente debe estar configurado correctamente para comunicarse a través de la red mediante NFSv3 o NFSv4.

Los clientes deben admitir RFC1964 y RFC2203.

- Kerberos

Cada cliente debe estar configurado correctamente para utilizar la autenticación Kerberos, incluidos los siguientes detalles:

- El cifrado para la comunicación TGS está activado.

AES-256 para obtener la máxima seguridad.

- El tipo de cifrado más seguro para la comunicación TGT está activado.
- El dominio y el dominio de Kerberos están configurados correctamente.
- GSS está activado.

Al utilizar las credenciales de la máquina:

- No correr `gssd` con la `-n` parámetro.
- No correr `kinit` como usuario raíz.

- Cada cliente debe utilizar la versión más reciente y actualizada del sistema operativo.

Esto proporciona la mejor compatibilidad y fiabilidad para el cifrado AES con Kerberos.

- DNS

Cada cliente debe estar configurado correctamente para utilizar DNS con la resolución de nombres correcta.

- NTP

Cada cliente debe sincronizarse con el servidor NTP.

- Información sobre el host y el dominio

El de cada cliente `/etc/hosts` y `/etc/resolv.conf` Los archivos deben contener el nombre de host y la información de DNS correctos, respectivamente.

- Archivos keytab

Cada cliente debe tener un archivo keytab del KDC. El Reino debe estar en letras mayúsculas. El tipo de cifrado debe ser AES-256 para obtener una seguridad más potente.

- Opcional: Para obtener el mejor rendimiento, los clientes se benefician de tener al menos dos interfaces de red: Una para comunicarse con la red de área local y otra para comunicarse con la red de almacenamiento.

Requisitos del sistema de almacenamiento

- Licencia de NFS

El sistema de almacenamiento debe tener instalada una licencia NFS válida.

- Licencia CIFS

La licencia CIFS es opcional. Sólo es necesario comprobar las credenciales de Windows cuando se utiliza la asignación de nombres multiprotocolo. No es necesario en entornos estrictos sólo UNIX.

- SVM

Debe tener al menos una SVM configurada en el sistema.

- DNS en la SVM

Debe haber configurado DNS en cada SVM.

- Servidor NFS

Debe haber configurado NFS en la SVM.

- Cifrado AES

Para obtener la mayor seguridad, debe configurar el servidor NFS para permitir solo el cifrado AES-256 para Kerberos.

- Servidor SMB

Si ejecuta un entorno multiprotocolo, debe haber configurado SMB en la SVM. Se requiere el servidor SMB para la asignación de nombres multiprotocolo.

- Volúmenes

Debe tener un volumen raíz y, al menos, un volumen de datos configurado para que lo utilice la SVM.

- Volumen raíz

El volumen raíz de la SVM debe tener la siguiente configuración:

| Nombre | Ajuste |
|---------------------|-------------|
| Estilo de seguridad | UNIX |
| UID | Raíz o ID 0 |
| GID | Raíz o ID 0 |
| Permisos UNIX | 777 |

A diferencia del volumen raíz, los volúmenes de datos pueden tener cualquier estilo de seguridad.

- Grupos UNIX

La SVM debe tener configurados los siguientes grupos UNIX:

| Nombre del grupo | ID de grupo |
|------------------|--|
| daemon | 1 |
| raíz | 0 |
| pcuser | 65534 (creado automáticamente por ONTAP cuando se crea la SVM) |

- Usuarios de UNIX

La SVM debe tener configurados los siguientes usuarios de UNIX:

| Nombre de usuario | ID de usuario | ID del grupo principal | Comentar |
|-------------------|---------------|------------------------|---|
| nfs | 500 | 0 | Necesario para la fase de INICIO DE GSS El primer componente del SPN de usuario del cliente NFS se utiliza como usuario. |
| pcuser | 65534 | 65534 | Necesario para el uso multiprotocolo de NFS y CIFS ONTAP lo crea y añade automáticamente al grupo pcuser cuando crea la SVM. |
| raíz | 0 | 0 | Necesario para el montaje |

El usuario nfs no es necesario si existe una asignación de nombre Kerberos-UNIX para el SPN del usuario cliente NFS.

- Reglas y políticas de exportación

Debe haber configurado políticas de exportación con las reglas de exportación necesarias para los volúmenes raíz y de datos y qtrees. Si se accede a todos los volúmenes del SVM a través de Kerberos, puede configurar las opciones de regla de exportación `-rorule`, `-rwrule`, y `-superuser` para el volumen raíz a `krb5`, `krb5i`, o `krb5p`.

- Asignación de nombres Kerberos-UNIX

Si desea que el usuario identificado por el SPN de usuario del cliente NFS tenga permisos raíz, debe crear una asignación de nombre a root.

Información relacionada

"Informe técnico de NetApp 4073: Autenticación unificada segura"

"Herramienta de matriz de interoperabilidad de NetApp"

"Administración del sistema"

"Gestión de almacenamiento lógico"

Especifique el dominio de ID de usuario para NFSv4

Para especificar el dominio de ID de usuario, puede establecer el `-v4-id-domain` opción.

Acerca de esta tarea

De forma predeterminada, ONTAP utiliza el dominio NIS para la asignación del ID de usuario de NFSv4, si hay algún establecido. Si no se establece un dominio NIS, se utiliza el dominio DNS. Es posible que deba establecer el dominio de ID de usuario si, por ejemplo, tiene varios dominios de ID de usuario. El nombre de dominio debe coincidir con la configuración de dominio del controlador de dominio. No es necesaria para NFSv3.

Paso

- 1. Introduzca el siguiente comando:

```
vserver nfs modify -vserver vserver_name -v4-id-domain NIS_domain_name
```

Configure los servicios de nombres

Cómo funciona la configuración de switch de servicio de nombres ONTAP

ONTAP almacena información de configuración del servicio de nombres en una tabla que equivale a `/etc/nsswitch.conf` Fichero de sistemas UNIX. Debe comprender la función de la tabla y cómo la utiliza ONTAP para poder configurarla de forma adecuada para su entorno.

La tabla de conmutador de servicio de nombres ONTAP determina qué orígenes de servicio de nombres consulta ONTAP para recuperar información de un determinado tipo de información del servicio de nombres. ONTAP mantiene una tabla de switch de servicio de nombres independiente para cada SVM.

Tipos de base de datos

La tabla almacena una lista de servicios de nombres independiente para cada uno de los siguientes tipos de base de datos:

| Tipo de base de datos | Define orígenes de servicio de nombres para... | Los orígenes válidos son... |
|-----------------------|--|-----------------------------|
| hosts | Conversión de nombres de host a direcciones IP | archivos, dns |
| grupo | Búsqueda de información de grupo de usuarios | archivos, nis, ldap |

| Tipo de base de datos | Define orígenes de servicio de nombres para... | Los orígenes válidos son... |
|-----------------------|--|-----------------------------|
| passwd | Búsqueda de información de usuario | archivos, nis, ldap |
| grupo de red | Buscando información de netgroup | archivos, nis, ldap |
| mapa de nombres | Asignando los nombres de usuario | archivos, ldap |

Tipos de origen

Los orígenes especifican el nombre de origen de servicio que se utilizará para recuperar la información adecuada.

| Especificar tipo de origen... | Para buscar información en... | Administrado por las familias de comandos... |
|-------------------------------|--|---|
| archivos | Archivos de origen local | <pre>vserver services name- service unix-user vserver services name-service unix-group vserver services name- service netgroup vserver services name- service dns hosts</pre> |
| nis | Servidores NIS externos tal como se especifica en la configuración de dominio NIS de la SVM | <pre>vserver services name- service nis-domain</pre> |
| ldap | Servidores LDAP externos tal como se especifica en la configuración del cliente LDAP de la SVM | <pre>vserver services name- service ldap</pre> |
| dns | Servidores DNS externos como se especifica en la configuración de DNS de la SVM | <pre>vserver services name- service dns</pre> |

Aunque tenga pensado utilizar NIS o LDAP tanto para el acceso a datos como para la autenticación de administración de SVM, debería seguir incluyéndose `files` Y configure los usuarios locales como respaldo en caso de que falle la autenticación de NIS o LDAP.

Protocolos utilizados para acceder a fuentes externas

Para acceder a los servidores de fuentes externas, ONTAP utiliza los siguientes protocolos:

| Fuente externa del servicio de nombres | Protocolo utilizado para acceder |
|--|----------------------------------|
| NIS | UDP |
| DNS | UDP |
| LDAP | TCP |

Ejemplo

En el ejemplo siguiente se muestra el nombre de configuración del switch de servicio para la SVM svm svm_1:

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
```

| Vserver | Database | Source | Order |
|---------|----------|--------|-------|
| svm_1 | hosts | files, | dns |
| svm_1 | group | files | |
| svm_1 | passwd | files | |
| svm_1 | netgroup | nis, | files |

Para buscar direcciones IP para hosts, ONTAP consulta primero los archivos de origen local. Si la consulta no devuelve ningún resultado, los servidores DNS se comprueban a continuación.

Para buscar información de usuarios o grupos, ONTAP sólo consulta archivos de fuentes locales. Si la consulta no devuelve ningún resultado, la búsqueda fallará.

Para buscar información de grupos de red, ONTAP consulta primero los servidores NIS externos. Si la consulta no devuelve ningún resultado, el archivo de netgroup local se activa a continuación.

No hay entradas del servicio de nombres para la asignación de nombres en la tabla de la SVM svm svm_1. Por lo tanto, ONTAP sólo consulta archivos de origen local de forma predeterminada.

Información relacionada

["Informe técnico de NetApp 4668: Guía de prácticas recomendadas de servicios de nombres"](#)

Utilice LDAP

Descripción general de LDAP

Un servidor LDAP (protocolo ligero de acceso a directorios) le permite mantener la información de usuario de forma centralizada. Si almacena su base de datos de usuario en un servidor LDAP del entorno, puede configurar el sistema de almacenamiento para buscar información de usuario en su base de datos LDAP existente.

- Antes de configurar LDAP para ONTAP, debe verificar que la implementación del sitio cumple las prácticas recomendadas para la configuración del cliente y el servidor LDAP. En particular, deben cumplirse las

siguientes condiciones:

- El nombre de dominio del servidor LDAP debe coincidir con la entrada del cliente LDAP.
- Los tipos hash de contraseña de usuario LDAP compatibles con el servidor LDAP deben incluir los compatibles con ONTAP:
 - CRIPTA (todos los tipos) y SHA-1 (SHA, SSHA).
 - A partir de los valores hash de ONTAP 9.8, SHA-2 (SHA-256, SSH-384, SHA-512, SSHA-256, También se admiten SSHA-384 y SSHA-512).
- Si el servidor LDAP requiere medidas de seguridad de la sesión, debe configurarlas en el cliente LDAP.

Están disponibles las siguientes opciones de seguridad de la sesión:

- La firma LDAP (proporciona comprobación de la integridad de los datos) y la firma y el sellado LDAP (proporciona cifrado y comprobación de la integridad de los datos).
- INICIE TLS
- LDAPS (LDAP sobre TLS o SSL)
- Para habilitar consultas LDAP firmadas y selladas, se deben configurar los siguientes servicios:
 - Los servidores LDAP deben ser compatibles con el mecanismo SASL GSSAPI (Kerberos).
 - Los servidores LDAP deben tener registros DNS A/AAAA, así como registros PTR configurados en el servidor DNS.
 - Los servidores Kerberos deben tener registros SRV presentes en el servidor DNS.
- Para habilitar el INICIO de TLS o LDAPS, se deben tener en cuenta los siguientes puntos.
 - Se trata de una práctica recomendada de NetApp para usar Start TLS en lugar de LDAPS.
 - Si se usa LDAPS, el servidor LDAP debe habilitar para TLS o SSL en ONTAP 9.5 y versiones posteriores. SSL no es compatible con ONTAP 9.0-9.4.
 - Ya debe configurarse un servidor de certificados en el dominio.
- Para habilitar la búsqueda de referencias LDAP (en ONTAP 9.5 y posterior), se deben cumplir las siguientes condiciones:
 - Ambos dominios deben configurarse con una de las siguientes relaciones de confianza:
 - Bidireccional
 - Unidireccional, donde la primaria confía en el dominio de referencia
 - Padre-hijo
 - El DNS debe configurarse de modo que resuelva todos los nombres de servidor a los que se hace referencia.
 - Las contraseñas de dominio deben ser las mismas para autenticar cuándo `--bind-as-cifs-server` establezca en true.

Las siguientes configuraciones no son compatibles con la búsqueda de referencias LDAP.



- Para todas las versiones de ONTAP:
- Clientes LDAP en una SVM de administrador
- Para ONTAP 9.8 y versiones anteriores (se admiten en la versión 9.9.1 y posteriores):
- Firma y sellado LDAP (la `-session-security` opción)
- Conexiones TLS cifradas (la `-use-start-tls` opción)
- Comunicaciones por puerto LDAPS 636 (el `-use-ldaps-for-ad-ldap` opción)

- A partir de ONTAP 9.11.1, se puede utilizar ["Enlace rápido LDAP para la autenticación nsswitch."](#)
- Debe introducir un esquema de LDAP al configurar el cliente LDAP en la SVM.

En la mayoría de los casos, uno de los esquemas ONTAP predeterminados será apropiado. Sin embargo, si el esquema LDAP del entorno difiere de éste, debe crear un nuevo esquema de cliente LDAP para ONTAP antes de crear el cliente LDAP. Consulte a su administrador LDAP sobre los requisitos de su entorno.

- No se admite el uso de LDAP para la resolución de nombres de host.

Para obtener más información, consulte ["Informe técnico de NetApp 4835: Cómo configurar LDAP en ONTAP"](#).

Conceptos de firma y sellado LDAP

A partir de ONTAP 9, puede configurar la firma y el sellado para habilitar la seguridad de la sesión LDAP en consultas a un servidor de Active Directory (AD). Debe configurar los ajustes de seguridad del servidor NFS en la máquina virtual de almacenamiento (SVM) para corresponder a los del servidor LDAP.

La firma comprueba la integridad de la carga de datos LDAP mediante una tecnología de clave secreta. El sellado cifra la carga de datos LDAP para impedir la transmisión de información confidencial en texto sin cifrar. Una opción *LDAP Security Level* indica si es necesario firmar, firmar y sellar el tráfico LDAP o no. El valor predeterminado es `none`. prueba

La firma LDAP y el sellado en el tráfico SMB se habilitan en la SVM con el `-session-security-for-ad-ldap` de la `vserver cifs security modify` comando.

Conceptos LDAPS

Debe comprender ciertos términos y conceptos sobre cómo ONTAP protege la comunicación LDAP. ONTAP puede usar START TLS o LDAPS para configurar sesiones autenticadas entre servidores LDAP integrados de Active Directory o servidores LDAP basados en UNIX.

Terminología

Existen ciertos términos que se deben entender de qué manera ONTAP utiliza LDAPS para proteger la comunicación de LDAP.

- **LDAP**

(Protocolo ligero de acceso a directorios) Protocolo para acceder y administrar directorios de información. LDAP se utiliza como directorio de información para almacenar objetos como usuarios, grupos y netgroups. LDAP también proporciona servicios de directorio que administran estos objetos y satisfacen las solicitudes LDAP de los clientes LDAP.

- **SSL**

(Capa de sockets seguros) Protocolo desarrollado para enviar información de forma segura a través de Internet. SSL es compatible con ONTAP 9 y posterior, pero ha sido anticuado a favor de TLS.

- **TLS**

(Transport Layer Security) Protocolo de seguimiento de estándares IETF basado en las especificaciones anteriores de SSL. Es el sucesor de SSL. TLS es compatible con ONTAP 9,5 y versiones posteriores.

- **LDAPS (LDAP sobre SSL o TLS)**

Protocolo que utiliza TLS o SSL para proteger la comunicación entre clientes LDAP y servidores LDAP. Los términos *ldap sobre SSL* y *ldap sobre TLS* a veces se utilizan indistintamente. ONTAP 9,5 y versiones posteriores es compatible con LDAPS.

- En ONTAP 9.5-9.8, LDAPS solo puede habilitar LDAPS en el puerto 636. Para ello, utilice `-use -ldaps-for-ad-ldap` con el `vserver cifs security modify` comando.
- A partir de ONTAP 9.9.1, LDAPS puede habilitar LDAPS en cualquier puerto, aunque el puerto 636 sigue siendo el predeterminado. Para ello, ajuste la `-ldaps-enabled` parámetro a `true` y especifique lo que desee `-port` parámetro. Para obtener más información, consulte `vserver services name-service ldap client create` página de manual



Se trata de una práctica recomendada de NetApp para usar Start TLS en lugar de LDAPS.

- **Iniciar TLS**

(También conocido como *start_tls*, *STARTTLS* y *StartTLS*) un mecanismo para proporcionar una comunicación segura mediante el uso de los protocolos TLS.

ONTAP utiliza STARTTLS para garantizar la comunicación LDAP y utiliza el puerto LDAP predeterminado (389) para comunicarse con el servidor LDAP. El servidor LDAP debe configurarse para permitir conexiones a través del puerto LDAP 389; de lo contrario, se producirá un error en las conexiones LDAP TLS desde la SVM al servidor LDAP.

Cómo utiliza ONTAP LDAPS

ONTAP admite la autenticación del servidor TLS, lo que permite que el cliente LDAP de SVM confirme la identidad del servidor LDAP durante la operación de enlace. Los clientes LDAP habilitados para TLS pueden utilizar técnicas estándar de criptografía de clave pública para comprobar que el certificado y el ID público de un servidor son válidos y que han sido emitidos por una entidad emisora de certificados (CA) que aparece en la lista de entidades emisoras de certificados de confianza del cliente.

LDAP admite STARTTLS para cifrar las comunicaciones mediante TLS. STARTTLS comienza como una conexión de texto sin formato a través del puerto LDAP estándar (389), y esa conexión se actualiza a TLS.

ONTAP admite lo siguiente:

- LDAPS para tráfico relacionado con SMB entre los servidores LDAP integrados de Active Directory y la SVM
- LDAPS para el tráfico LDAP para la asignación de nombres y otra información de UNIX

Los servidores LDAP integrados en Active Directory o los servidores LDAP basados en UNIX se pueden utilizar para almacenar información para la asignación de nombres LDAP y otra información UNIX, como usuarios, grupos y netgroups.

- Certificados de CA raíz autofirmados

Cuando se utiliza un LDAP integrado de Active Directory, el certificado raíz autofirmado se genera cuando el servicio de certificados de Windows Server está instalado en el dominio. Cuando se utiliza un servidor LDAP basado en UNIX para asignar nombres LDAP, se genera el certificado raíz autofirmado y se guarda mediante medios adecuados para esa aplicación LDAP.

De manera predeterminada, LDAPS.

Active la compatibilidad con LDAP RFC2307bis

Si desea utilizar LDAP y necesita la capacidad adicional para utilizar pertenencias a grupos anidados, puede configurar ONTAP para habilitar la compatibilidad con RFC2307bis LDAP.

Lo que necesitará

Debe haber creado una copia de uno de los esquemas de cliente LDAP predeterminados que desea utilizar.

Acerca de esta tarea

En los esquemas de cliente LDAP, los objetos de grupo utilizan el atributo `memberUid`. Este atributo puede contener varios valores y enumera los nombres de los usuarios que pertenecen a ese grupo. En los esquemas de cliente LDAP habilitados para RFC2307bis, los objetos de grupo utilizan el atributo `uniqueMember`. Este atributo puede contener el nombre completo (DN) de otro objeto del directorio LDAP. Esto le permite utilizar grupos anidados porque los grupos pueden tener otros grupos como miembros.

El usuario no debe ser miembro de más de 256 grupos, incluidos los grupos anidados. ONTAP ignora los grupos por encima del límite de 256 grupos.

De forma predeterminada, la compatibilidad con RFC2307bis está desactivada.



La compatibilidad con RFC2307bis se habilita automáticamente en ONTAP cuando se crea un cliente LDAP con el esquema MS-AD-BIS.

Para obtener más información, consulte ["Informe técnico de NetApp 4835: Cómo configurar LDAP en ONTAP"](#).

Pasos

1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Modifique el esquema de cliente LDAP RFC2307 copiado para habilitar la compatibilidad con RFC2307bis:

```
vserver services name-service ldap client schema modify -vserver vserver_name
```

```
-schema schema-name -enable-rfc2307bis true
```

3. Modifique el esquema para que coincida con la clase de objeto admitida en el servidor LDAP:

```
vserver services name-service ldap client schema modify -vserver vserver-name  
-schema schema_name -group-of-unique-names-object-class object_class
```

4. Modifique el esquema para que coincida con el nombre de atributo admitido en el servidor LDAP:

```
vserver services name-service ldap client schema modify -vserver vserver-name  
-schema schema_name -unique-member-attribute attribute_name
```

5. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

Opciones de configuración para las búsquedas de directorios LDAP

Puede optimizar las búsquedas de directorios LDAP, incluida la información de usuario, grupo y grupo de red, configurando el cliente LDAP de ONTAP para que se conecte a servidores LDAP de la forma más adecuada para su entorno. Es necesario entender cuándo son suficientes los valores predeterminados de la base LDAP y de la búsqueda de ámbito y qué parámetros especificar cuando los valores personalizados son más apropiados.

Las opciones de búsqueda de clientes LDAP para información de usuarios, grupos y netgroup pueden ayudar a evitar consultas LDAP que han fallado y, por lo tanto, permitir que el cliente acceda a los sistemas de almacenamiento con errores. También ayudan a garantizar que las búsquedas sean lo más eficientes posible para evitar problemas de rendimiento de los clientes.

Valores de búsqueda base y ámbito predeterminados

La base LDAP es el DN base predeterminado que utiliza el cliente LDAP para realizar consultas LDAP. Todas las búsquedas, incluidas las búsquedas de usuario, grupo y netgroup, se realizan utilizando el DN base. Esta opción es apropiada cuando el directorio LDAP es relativamente pequeño y todas las entradas relevantes se encuentran en el mismo DN.

Si no especifica un DN base personalizado, el valor predeterminado es `root`. Esto significa que cada consulta busca en todo el directorio. A pesar de que esto maximiza las posibilidades de éxito de la consulta LDAP, puede resultar ineficiente y producir una reducción significativa del rendimiento con grandes directorios LDAP.

El ámbito de base LDAP es el ámbito de búsqueda predeterminado que utiliza el cliente LDAP para realizar consultas LDAP. Todas las búsquedas, incluidas las de usuario, grupo y netgroup, se realizan utilizando el ámbito base. Determina si la consulta LDAP busca sólo la entrada con nombre, las entradas de un nivel por debajo del DN o el subárbol entero por debajo del DN.

Si no especifica un ámbito base personalizado, el valor predeterminado es `subtree`. Esto significa que cada consulta busca todo el subárbol que se encuentra debajo del DN. A pesar de que esto maximiza las posibilidades de éxito de la consulta LDAP, puede resultar ineficiente y producir una reducción significativa del rendimiento con grandes directorios LDAP.

Valores de búsqueda de base y ámbito personalizados

Opcionalmente, puede especificar valores de base y ámbito independientes para búsquedas de usuarios, grupos y grupos de red. Limitar la base de búsqueda y el ámbito de las consultas de esta manera puede mejorar significativamente el rendimiento porque limita la búsqueda a una subsección más pequeña del directorio LDAP.

Si se especifican valores de base y ámbito personalizados, se reemplazan la base de búsqueda y el ámbito predeterminados generales para las búsquedas de usuarios, grupos y grupos de red. Los parámetros para especificar valores de base y ámbito personalizados están disponibles en el nivel de privilegio avanzado.

| Parámetro de cliente LDAP... | Especifica el valor personalizado... |
|------------------------------|---|
| -base-dn | DN base de todas las búsquedas de LDAP se pueden introducir varios valores si es necesario (por ejemplo, si la búsqueda de referencias de LDAP está habilitada en ONTAP 9.5 y versiones posteriores). |
| -base-scope | Ámbito base para todas las búsquedas LDAP |
| -user-dn | DNS base para todas las búsquedas de usuarios LDAP.este parámetro también se aplica a las búsquedas de asignación de nombres de usuario. |
| -user-scope | Ámbito base para todas las búsquedas de usuarios LDAP este parámetro también se aplica a las búsquedas de asignación de nombres de usuario. |
| -group-dn | DNS base para todas las búsquedas de grupos LDAP |
| -group-scope | Ámbito base para todas las búsquedas de grupos LDAP |
| -netgroup-dn | DNS base para todas las búsquedas de grupos de red LDAP |
| -netgroup-scope | Alcance base para todas las búsquedas de grupos de red LDAP |

Varios valores DN base personalizados

Si su estructura de directorios LDAP es más compleja, puede ser necesario especificar varios DNS base para buscar varias partes del directorio LDAP para cierta información. Puede especificar varios DNS para los parámetros de DN de usuario, grupo y grupo de red separándolos con punto y coma (;) y encerrando toda la lista de búsqueda de DN con comillas dobles ("). Si un DN contiene un punto y coma, debe agregar un carácter de escape (\) inmediatamente antes del punto y coma en el DN.

Tenga en cuenta que el ámbito se aplica a toda la lista de DNS especificada para el parámetro correspondiente. Por ejemplo, si especifica una lista de tres DNS de usuario y subárbol diferentes para el ámbito de usuario, el usuario LDAP buscará en todo el subárbol para cada uno de los tres DNS especificados.

A partir de ONTAP 9.5, también puede especificar LDAP *referenciación persiguiendo*, lo que permite al cliente LDAP de ONTAP remitir solicitudes de búsqueda a otros servidores LDAP si el servidor LDAP principal no devuelve una respuesta de referencia LDAP. El cliente utiliza esos datos de referencia para recuperar el objeto

de destino del servidor descrito en los datos de referencia. Para buscar objetos presentes en los servidores LDAP a los que se hace referencia, se puede agregar la base-dn de los objetos a los que se hace referencia a base-dn como parte de la configuración del cliente LDAP. Sin embargo, los objetos a los que se hace referencia sólo se buscan cuando se activa la búsqueda de referencias (mediante la `-referral-enabled true` Opción) durante la creación o modificación de un cliente LDAP.

Mejorar el rendimiento de las búsquedas de red de directorio LDAP-por-host

Si el entorno LDAP está configurado para permitir búsquedas de `netgroup-by-host`, puede configurar ONTAP para aprovechar esta característica y realizar búsquedas de `netgroup-by-host`. Esto puede acelerar significativamente las búsquedas de `netgroup` y reducir posibles problemas de acceso de clientes NFS debido a la latencia durante las búsquedas de `netgroup`.

Lo que necesitará

Su directorio LDAP debe contener un `netgroup.byhost` mapa.

Los servidores DNS deben contener registros de búsqueda de reenvío (A) e inverso (PTR) para clientes NFS.

Al especificar direcciones IPv6 en grupos de red, siempre debe acortar y comprimir cada dirección como se especifica en RFC 5952.

Acerca de esta tarea

Los servidores NIS almacenan información sobre el grupo de red en tres mapas independientes denominados `netgroup`, `netgroup.byuser`, y `netgroup.byhost`. El propósito de la `netgroup.byuser` y `netgroup.byhost` mapas es acelerar las búsquedas de `netgroup`. ONTAP puede realizar búsquedas de `netgroup-by-host` en servidores NIS para mejorar los tiempos de respuesta de montaje.

De forma predeterminada, los directorios LDAP no tienen tal `netgroup.byhost` Asignar como servidores NIS. Sin embargo, con la ayuda de herramientas de terceros es posible importar un NIS `netgroup.byhost` Asignar a directorios LDAP para permitir búsquedas rápidas de `netgroup-by-host`. Si ha configurado el entorno LDAP para permitir búsquedas de `netgroup-by-host`, puede configurar el cliente LDAP de ONTAP con el `netgroup.byhost` Asignar el nombre, el DN y el alcance de búsqueda para realizar búsquedas más rápidas de `netgroup-by-host`.

Al recibir los resultados de las búsquedas de `netgroup-by-host` con mayor rapidez, ONTAP procesa las reglas de exportación con mayor rapidez cuando los clientes NFS solicitan acceso a las exportaciones. Esto reduce la posibilidad de retrasos en el acceso debido a problemas de latencia de búsqueda en `netgroup`.

Pasos

1. Obtenga el nombre completo exacto del NIS `netgroup.byhost` Asignar importado a su directorio LDAP.

El DN de mapa puede variar en función de la herramienta de terceros que haya utilizado para la importación. Para obtener el mejor rendimiento, debe especificar el DN exacto del mapa.

2. Configure el nivel de privilegio en Advanced: `set -privilege advanced`
3. Habilite las búsquedas de `netgroup-by-host` en la configuración de cliente LDAP de la máquina virtual de almacenamiento (SVM): `vserver services name-service ldap client modify -vserver vserver_name -client-config config_name -is-netgroup-byhost-enabled true -netgroup-byhost-dn netgroup-by-host_map_distinguished_name -netgroup-byhost -scope netgroup-by-host_search_scope`

`-is-netgroup-byhost-enabled {true false}` Activa o desactiva la búsqueda `netgroup-by-host` para directorios LDAP. El valor predeterminado es `false`.

`-netgroup-byhost-dn netgroup-by-host_map_distinguished_name` especifica el nombre distintivo de `netgroup.byhost`. Asignar en el directorio LDAP. Reemplaza el DN base para las búsquedas de `netgroup-by-host`. Si no se especifica este parámetro, ONTAP utiliza el DN base.

`-netgroup-byhost-scope {base|onelevel subtree}` especifica el ámbito de búsqueda para las búsquedas de `netgroup-by-host`. Si no se especifica este parámetro, el valor predeterminado es `subtree`.

Si todavía no existe la configuración de cliente LDAP, puede habilitar las búsquedas de `netgroup-by-host` especificando estos parámetros al crear una nueva configuración de cliente LDAP mediante la `vserver services name-service ldap client create` comando.



A partir de ONTAP 9.2, el campo `-ldap-servers` reemplaza el campo `-servers`. Este nuevo campo puede tomar un nombre de host o una dirección IP para el servidor LDAP.

4. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

Ejemplo

El siguiente comando modifica la configuración de cliente LDAP existente denominada `"ldap_corp"` para permitir búsquedas de `netgroup-by-host` mediante el `netgroup.byhost` Mapa denominado `"nisMapName=netgroup.byhost",dc=corp,dc=example,dc=com"` y el ámbito de búsqueda predeterminado `subtree`:

```
cluster1::*> vserver services name-service ldap client modify -vserver vs1
-client-config ldap_corp -is-netgroup-byhost-enabled true -netgroup-byhost
-dn nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com
```

Después de terminar

La `netgroup.byhost` y `netgroup` los mapas del directorio deben mantenerse sincronizados en todo momento para evitar problemas de acceso de los clientes.

Información relacionada

["RFC de IETF 5952: Recomendación para la representación de texto de direcciones IPv6"](#)

Utilice el enlace rápido LDAP para la autenticación nsswitch

A partir de ONTAP 9.11.1, puede aprovechar la funcionalidad LDAP *fast bind* (también conocida como *concurrente bind*) para obtener solicitudes de autenticación de clientes más rápidas y sencillas. Para utilizar esta funcionalidad, el servidor LDAP debe admitir la funcionalidad de enlace rápido.

Acerca de esta tarea

Sin enlace rápido, ONTAP utiliza la vinculación simple de LDAP para autenticar usuarios administradores con el servidor LDAP. Con este método de autenticación, ONTAP envía un nombre de usuario o de grupo al servidor LDAP, recibe la contraseña hash almacenada y compara el código hash del servidor con la contraseña hash generada localmente desde la contraseña de usuario. Si son idénticas, ONTAP otorga permiso de inicio de sesión.

Con la funcionalidad de enlace rápido, ONTAP sólo envía credenciales de usuario (nombre de usuario y contraseña) al servidor LDAP a través de una conexión segura. A continuación, el servidor LDAP valida estas credenciales y le indica a ONTAP que conceda permisos de inicio de sesión.

Una ventaja de enlace rápido es que no es necesario que ONTAP admita todos los nuevos algoritmos de hash compatibles con los servidores LDAP, ya que el servidor LDAP realiza hash de contraseñas.

["Aprenda sobre el uso de FAST BIND."](#)

Puede utilizar las configuraciones de cliente LDAP existentes para enlace rápido LDAP. Sin embargo, se recomienda encarecidamente que el cliente LDAP esté configurado para TLS o LDAPS; de lo contrario, la contraseña se envía por el cable en texto sin formato.

Para habilitar el enlace rápido de LDAP en un entorno ONTAP, debe cumplir con estos requisitos:

- Los usuarios del administrador de ONTAP deben estar configurados en un servidor LDAP que admita el enlace rápido.
- La SVM de ONTAP debe configurarse para LDAP en la base de datos de switches de servicios de nombres (nsswitch).
- Las cuentas de usuario y de grupo admin de ONTAP deben configurarse para la autenticación nsswitch mediante fast bind.

Pasos

1. Confirme con el administrador LDAP que el enlace rápido LDAP es compatible con el servidor LDAP.
2. Asegúrese de que las credenciales de usuario administrador de ONTAP estén configuradas en el servidor LDAP.
3. Confirmar que el administrador o la SVM de datos están configurados correctamente para el enlace LDAP rápido.

- a. Para confirmar que el servidor de enlace rápido LDAP aparece en la configuración de cliente LDAP, introduzca:

```
vserver services name-service ldap client show
```

["Obtenga información acerca de la configuración del cliente LDAP."](#)

- b. Para confirmarlo ldap es una de las fuentes configuradas para nsswitch passwd database, introduzca:

```
vserver services name-service ns-switch show
```

["Más información sobre la configuración de nsswitch."](#)

4. Asegúrese de que los usuarios de administrador se autenticen con nsswitch y de que la autenticación de enlace rápido LDAP esté habilitada en sus cuentas.
 - Para los usuarios existentes, introduzca `security login modify` y verifique los siguientes ajustes de parámetros:

```
-authentication-method nsswitch
```

```
-is-ldap-fastbind true
```

- Para los nuevos usuarios administradores, consulte ["Habilite el acceso a cuenta de LDAP o NIS."](#)

Mostrar estadísticas de LDAP

A partir de ONTAP 9.2, puede mostrar estadísticas de LDAP de las máquinas virtuales de almacenamiento (SVM) en un sistema de almacenamiento para supervisar el rendimiento y diagnosticar problemas.

Lo que necesitará

- Debe haber configurado un cliente LDAP en la SVM.
- Debe haber identificado los objetos LDAP desde los cuales se pueden ver datos.

Paso

1. Vea los datos de rendimiento para los objetos de contador:

```
statistics show
```

Ejemplos

El siguiente ejemplo muestra los datos de rendimiento de un objeto `secd_external_service_op`:

```
cluster::*> statistics show -vserver vserverName -object
secd_external_service_op -instance "vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1"
```

```
Object: secd_external_service_op
Instance: vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1
Start-time: 4/13/2016 22:15:38
End-time: 4/13/2016 22:15:38
Scope: vserverName
```

| Counter | Value |
|--------------------------|---|
| instance_name | vserverName:LDAP (NIS & Name Mapping):GetUserInfoFromName:1.1.1.1 |
| last_modified_time | 1460610787 |
| node_name | nodeName |
| num_not_found_responses | 1 |
| num_request_failures | 1 |
| num_requests_sent | 1 |
| num_responses_received | 1 |
| num_successful_responses | 0 |
| num_timeouts | 0 |
| operation | GetUserInfoFromName |
| process_name | secd |
| request_latency | 52131us |

Configurar las asignaciones de nombres

Configure la información general de asignaciones de nombres

ONTAP utiliza la asignación de nombres para asignar identidades SMB a identidades UNIX, identidades Kerberos a identidades UNIX e identidades UNIX a identidades SMB. Necesita esta información para obtener credenciales de usuario y proporcionar un acceso adecuado a los archivos independientemente de si se están conectando desde un cliente NFS o un cliente SMB.

Existen dos excepciones en las que no es necesario utilizar la asignación de nombres:

- Configura un entorno UNIX puro y no planea usar el acceso SMB o el estilo de seguridad NTFS en los volúmenes.
- En su lugar, puede configurar el usuario predeterminado que se utilizará.

En este escenario, no es necesario asignar nombres porque en lugar de asignar cada credencial de cliente individual todas las credenciales de cliente se asignan al mismo usuario predeterminado.

Tenga en cuenta que sólo puede utilizar la asignación de nombres para usuarios, no para grupos.

Sin embargo, puede asignar un grupo de usuarios individuales a un usuario específico. Por ejemplo, puede asignar todos los usuarios de AD que comiencen o terminen con la palabra SALES a un usuario UNIX específico y al UID del usuario.

Cómo funciona la asignación de nombres

Cuando ONTAP tiene que asignar credenciales para un usuario, primero comprueba la base de datos de asignación de nombres local y el servidor LDAP para buscar una asignación existente. Si comprueba uno o ambos y en qué orden se determina mediante la configuración del servicio de nombres de la SVM.

- Para la asignación de Windows a UNIX

Si no se encuentra ninguna asignación, ONTAP comprueba si el nombre de usuario de Windows en minúsculas es un nombre de usuario válido en el dominio UNIX. Si esto no funciona, utiliza el usuario UNIX predeterminado siempre que esté configurado. Si el usuario UNIX predeterminado no está configurado y ONTAP no puede obtener una asignación de esta manera, se produce un error en la asignación y se devuelve un error.

- De asignación de UNIX a Windows

Si no se encuentra ninguna asignación, ONTAP intenta encontrar una cuenta de Windows que coincida con el nombre UNIX en el dominio SMB. Si esto no funciona, utiliza el usuario SMB predeterminado, siempre que esté configurado. Si el usuario SMB predeterminado no está configurado y ONTAP no puede obtener una asignación de esta manera, se produce un error en la asignación y se devuelve un error.

Las cuentas de equipo se asignan al usuario UNIX predeterminado especificado de forma predeterminada. Si no se especifica ningún usuario UNIX predeterminado, las asignaciones de cuentas de equipo fallan.

- A partir de ONTAP 9.5, puede asignar cuentas de equipo a usuarios distintos del usuario UNIX predeterminado.

- En ONTAP 9.4 y versiones anteriores, no es posible asignar cuentas de equipo a otros usuarios.

Incluso si se definen las asignaciones de nombre para las cuentas de equipo, las asignaciones se omiten.

Busca usuarios de UNIX a través de multidominio para mapeos de nombres de usuario de Windows

ONTAP admite las búsquedas multidominio al asignar usuarios de UNIX a usuarios de Windows. Se buscan todos los dominios de confianza detectados para que coincidan con el patrón de reemplazo hasta que se devuelva un resultado coincidente. También puede configurar una lista de dominios de confianza preferidos, que se utiliza en lugar de la lista de dominios de confianza detectados y se busca en orden hasta que se devuelve un resultado coincidente.

Cómo afectan las confianzas de dominio a las búsquedas de asignación de nombres de usuario de UNIX a Windows

Para comprender cómo funciona la asignación de nombres de usuario multidominio, debe comprender cómo funcionan las relaciones de confianza de dominios con ONTAP. Las relaciones de confianza de Active Directory con el dominio raíz del servidor SMB pueden ser una confianza bidireccional o pueden ser uno de los dos tipos de confianzas unidireccionales, ya sea una confianza entrante o una confianza saliente. El dominio inicial es el dominio al que pertenece el servidor SMB en la SVM.

- *Confianza bidireccional*

Con confianzas bidireccionales, ambos dominios confían entre sí. Si el dominio principal del servidor SMB tiene una confianza bidireccional con otro dominio, el dominio principal puede autenticar y autorizar a un usuario que pertenece al dominio de confianza y viceversa.

Las búsquedas de asignación de nombres de usuario de UNIX a usuario de Windows sólo se pueden realizar en dominios con relaciones de confianza bidireccionales entre el dominio principal y el otro dominio.

- *Confianza saliente*

Con una confianza saliente, el dominio principal confía en el otro dominio. En este caso, el dominio principal puede autenticar y autorizar a un usuario que pertenezca al dominio de confianza saliente.

Se realiza una búsqueda en un dominio con una confianza saliente con el dominio principal al realizar búsquedas de asignación de nombres de usuario de UNIX a usuario de Windows.

- *Confianza entrante*

Con una confianza entrante, el otro dominio confía en el dominio raíz del servidor SMB. En este caso, el dominio principal no puede autenticar ni autorizar a un usuario que pertenezca al dominio de confianza entrante.

Se busca un dominio con una confianza entrante con el dominio principal cuando se realizan búsquedas de asignación de nombres de usuario de UNIX a nombre de usuario de Windows.

Cómo se utilizan los comodines (*) para configurar las búsquedas multidominio para la asignación de nombres

Las búsquedas de asignación de nombres multidominio se facilitan mediante el uso de caracteres comodín en

la sección de dominio del nombre de usuario de Windows. En la siguiente tabla se muestra cómo utilizar comodines en la parte de dominio de una entrada de asignación de nombres para habilitar las búsquedas multidominio:

| Patrón | Sustitución | Resultado |
|--------|--|--|
| raíz | {asterisco}{barra diagonal inversa}{barra invertida}administrador | El usuario UNIX «'root'» está asignado al usuario denominado «'Administrator'». Todos los dominios de confianza se buscan en orden hasta que se encuentre el primer usuario coincidente denominado «'Administrator'». |
| * | {asterisco}{barra diagonal inversa}{barra diagonal inversa}{asterisco} | <div> <div>Los usuarios UNIX válidos se asignan a los usuarios de Windows correspondientes. Todos los dominios de confianza se buscan en orden hasta que se encuentre el primer usuario que coincida con ese nombre.</div> <div> <div> <div></div> <div>El patrón {asterisco}{barra diagonal inversa}{barra diagonal inversa}{asterisco} sólo es válido para la asignación de nombres de UNIX a Windows, no al revés.</div> </div> </div> </div> |

Cómo se realizan las búsquedas de nombres multidominio

Puede elegir uno de los dos métodos para determinar la lista de dominios de confianza utilizados para las búsquedas de nombres multidominio:

- Utilice la lista de confianza bidireccional detectada automáticamente compilada por ONTAP
- Utilice la lista de dominios de confianza preferida que compila

Si un usuario de UNIX se asigna a un usuario de Windows con un comodín utilizado para la sección de dominio del nombre de usuario, se busca al usuario de Windows en todos los dominios de confianza de la siguiente manera:

- Si se configura una lista de dominio de confianza preferido, el usuario de Windows asignado se busca sólo en esta lista de búsqueda, en orden.
- Si no se configura una lista preferida de dominios de confianza, se busca al usuario de Windows en todos los dominios de confianza bidireccionales del dominio principal.
- Si no hay dominios de confianza bidireccional para el dominio principal, se busca al usuario en el dominio

principal.

Si un usuario de UNIX está asignado a un usuario de Windows sin una sección de dominio en el nombre de usuario, se busca al usuario de Windows en el dominio principal.

Reglas de conversión de asignación de nombres

Un sistema ONTAP mantiene un conjunto de reglas de conversión para cada SVM. Cada regla consta de dos piezas: Un *pattern* y un *substitut*. Las conversiones comienzan al principio de la lista apropiada y realizan una sustitución basada en la primera regla de coincidencia. El patrón es una expresión regular de estilo UNIX. El reemplazo es una cadena que contiene secuencias de escape que representan subexpresiones del patrón, como en UNIX `sed` programa.

Cree una asignación de nombres

Puede utilizar el `vserver name-mapping create` comando para crear una asignación de nombres. Se usan asignaciones de nombres para habilitar a los usuarios de Windows a fin de acceder a los volúmenes de estilo de seguridad de UNIX y al revés.

Acerca de esta tarea

Con cada SVM, ONTAP admite hasta 12,500 asignaciones de nombres para cada dirección.

Paso

1. Crear una asignación de nombres:

```
vserver name-mapping create -vserver vserver_name -direction {krb-unix|win-unix|unix-win} -position integer -pattern text -replacement text
```



La `-pattern` y `-replacement` las declaraciones se pueden formular como expresiones regulares. También puede utilizar el `-replacement` instrucción para denegar explícitamente una asignación al usuario mediante la cadena de reemplazo nula " " (el carácter de espacio). Consulte `vserver name-mapping create` manual para más detalles.

Cuando se crean las asignaciones de Windows a UNIX, todos los clientes de SMB que tengan conexiones abiertas al sistema ONTAP en el momento en el que se creen las nuevas asignaciones deben cerrar e iniciar sesión para ver las nuevas asignaciones.

Ejemplos

El siguiente comando crea un mapa de nombre en la SVM llamada vs1. La asignación es una asignación de UNIX a Windows en la posición 1 de la lista de prioridades. La asignación asigna el usuario UNIX johnd al usuario de Windows ENG\JohnDoe.

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win  
-position 1 -pattern johnd  
-replacement "ENG\\JohnDoe"
```

El siguiente comando crea otra asignación de nombre en la SVM llamada vs1. La asignación es una

asignación de Windows a UNIX en la posición 1 de la lista de prioridades. Aquí el patrón y reemplazo incluyen expresiones regulares. La asignación asigna cada usuario CIFS del dominio ENG a los usuarios del dominio LDAP asociado con la SVM.

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\\1"
```

El siguiente comando crea otra asignación de nombre en la SVM llamada vs1. Aquí el patrón incluye "\$" como elemento del nombre de usuario de Windows que debe escaparse. La asignación asigna al usuario de Windows ENG\john\$OPS al usuario UNIX john_OPS.

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john$ops
-replacement john_ops
```

Configure el usuario predeterminado

Puede configurar un usuario predeterminado para que lo utilice si todos los demás intentos de asignación fallan para un usuario o si no desea asignar usuarios individuales entre UNIX y Windows. Si desea que la autenticación de usuarios no asignados falle, no debe configurar un usuario predeterminado.

Acerca de esta tarea

Para la autenticación CIFS, si no desea asignar cada usuario de Windows a un usuario individual de UNIX, puede especificar un usuario predeterminado de UNIX.

Para la autenticación NFS, si no desea asignar cada usuario UNIX a un usuario individual de Windows, puede especificar un usuario predeterminado de Windows.

Paso

- 1. Ejecute una de las siguientes acciones:

| Si desea... | Introduzca el siguiente comando... |
|--|---|
| Configure el usuario UNIX predeterminado | <code>vserver cifs options modify -default-unix-user user_name</code> |
| Configure el usuario predeterminado de Windows | <code>vserver nfs modify -default-win-user user_name</code> |

Comandos para gestionar las asignaciones de nombres

Hay comandos de la ONTAP específicos para gestionar las asignaciones de nombres.

| Si desea... | Se usa este comando... |
|-------------|------------------------|
|-------------|------------------------|

| | |
|--|---|
| Cree una asignación de nombres | <code>vserver name-mapping create</code> |
| Inserte una asignación de nombres en una posición específica | <code>vserver name-mapping insert</code> |
| Mostrar asignaciones de nombres | <code>vserver name-mapping show</code> |
| Cambie la posición de dos asignaciones de nombre NOTA: No se permite un intercambio cuando la asignación de nombres está configurada con una entrada de cualificador de ip. | <code>vserver name-mapping swap</code> |
| Modificar una asignación de nombres | <code>vserver name-mapping modify</code> |
| Eliminar una asignación de nombres | <code>vserver name-mapping delete</code> |
| Validar la asignación de nombre correcta | <code>vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1</code> |

Consulte la página de manual de cada comando para obtener más información.

Permita el acceso a clientes NFS de Windows

ONTAP admite el acceso a archivos desde clientes de Windows NFSv3. Esto significa que los clientes que ejecutan sistemas operativos Windows con compatibilidad NFSv3 pueden acceder a archivos de las exportaciones NFSv3 del clúster. Para utilizar correctamente esta funcionalidad, debe configurar correctamente la máquina virtual de almacenamiento (SVM) y tener en cuenta ciertos requisitos y limitaciones.

Acerca de esta tarea

De manera predeterminada, la compatibilidad con el cliente de Windows NFSv3 está deshabilitada.

Antes de empezar

Debe estar habilitado NFSv3 en la SVM.

Pasos

1. Habilitar la compatibilidad con clientes de Windows NFSv3:

```
vserver nfs modify -vserver svm_name -v3-ms-dos-client enabled -mount-rootonly disabled
```

2. En todas las SVM que admiten clientes Windows NFSv3, deshabilite el `-enable-ejokebox` y.. `-v3 -connection-drop` parámetros:

```
vserver nfs modify -vserver vserver_name -enable-ejokebox false -v3-connection
-drop disabled
```

Los clientes de Windows NFSv3 ahora pueden montar las exportaciones en el sistema de almacenamiento.

3. Asegúrese de que cada cliente Windows NFSv3 utilice montajes hard especificando el `-o mtype=hard` opción.

Esto es necesario para garantizar montajes fiables.

```
mount -o mtype=hard \\10.53.33.10\vol\vol1 z:\
```

Habilite la visualización de exportaciones NFS en clientes NFS

Los clientes NFS pueden utilizar la `showmount -e` Comando para ver una lista de exportaciones disponibles en un servidor NFS de ONTAP. Esto puede ayudar a los usuarios a identificar el sistema de archivos que desean montar.

A partir de ONTAP 9.2, ONTAP permite que los clientes NFS vean la lista de exportaciones de manera predeterminada. En versiones anteriores, el `showmount` opción de `vserver nfs modify` el comando debe habilitarse explícitamente. Para ver la lista de exportación, debe habilitarse NFSv3 en la SVM.

Ejemplo

El siguiente comando muestra la función `showmount` en la SVM denominada `vs1`:

```
cluster1 : : > vserver nfs show -vserver vs1 -fields showmount
vserver showmount
-----
vs1      enabled
```

El siguiente comando ejecutado en un cliente NFS muestra la lista de exportaciones en un servidor NFS con la dirección IP 10.63.21.9:

```
showmount -e 10.63.21.9
Export list for 10.63.21.9:
/unix      (everyone)
/unix/unix1 (everyone)
/unix/unix2 (everyone)
/          (everyone)
```

Gestione el acceso a archivos mediante NFS

Habilite o deshabilite NFSv3

Puede habilitar o deshabilitar NFSv3 modificando el `-v3` opción. De este modo, los clientes pueden acceder a archivos mediante el protocolo NFSv3. De forma

predeterminada, NFSv3 está habilitado.

Paso

1. Ejecute una de las siguientes acciones:

| Si desea... | Introduzca el comando... |
|-----------------|--|
| Habilite NFSv3 | <code>vserver nfs modify -vserver vserver_name -v3 enabled</code> |
| Desactive NFSv3 | <code>vserver nfs modify -vserver vserver_name -v3 disabled</code> |

Activar o desactivar NFSv4.0

Puede activar o desactivar NFSv4.0 modificando el `-v4.0` opción. De este modo, los clientes pueden acceder a los archivos mediante el protocolo NFSv4.0. En ONTAP 9.9.1, NFSv4.0 está habilitado de forma predeterminada; en versiones anteriores, está deshabilitado de forma predeterminada.

Paso

1. Ejecute una de las siguientes acciones:

| Si desea... | Introduzca el siguiente comando... |
|---------------------|--|
| Habilitar NFSv4,0 | <code>vserver nfs modify -vserver vserver_name -v4.0 enabled</code> |
| Deshabilite NFSv4.0 | <code>vserver nfs modify -vserver vserver_name -v4.0 disabled</code> |

Habilitar o deshabilitar NFSv4.1

Puede activar o desactivar NFSv4,1 modificando el `-v4.1` opción. De este modo, los clientes pueden acceder a los archivos que utilizan el protocolo NFSv4,1. En ONTAP 9.9.1, NFSv4.1 está habilitado de forma predeterminada; en las versiones anteriores, está deshabilitado de forma predeterminada.

Paso

1. Ejecute una de las siguientes acciones:

| Si desea... | Introduzca el siguiente comando... |
|--------------------|--|
| Habilitar NFSv4,1 | <code>vserver nfs modify -vserver vserver_name -v4.1 enabled</code> |
| Desactivar NFSv4,1 | <code>vserver nfs modify -vserver vserver_name -v4.1 disabled</code> |

Gestione los límites de los grupos de almacenamiento de NFSv4

A partir de ONTAP 9.13, los administradores pueden permitir que sus servidores NFSv4 denieguen recursos a NFSv4 clientes cuando hayan alcanzado los límites de recursos por cada pool de clientes. Cuando los clientes consumen demasiados recursos de la agrupación de almacenamiento NFSv4, esto puede provocar que otros clientes NFSv4 se bloqueen debido a la falta de disponibilidad de los recursos de la agrupación de almacenamiento NFSv4.

La activación de esta función también permite a los clientes ver el consumo de recursos del grupo de almacenamiento activo por cada cliente. Esto facilita la identificación de clientes que agotan los recursos del sistema y permite imponer límites de recursos por cliente.

Ver los recursos del almacén consumidos

La `vserver nfs storepool show` comando muestra el número de recursos de la agrupación de almacenamiento consumidos. Una tienda es un conjunto de recursos utilizados por los clientes de NFSv4.

Paso

1. Como administrador, ejecute el `vserver nfs storepool show` Comando para mostrar la información de la agrupación de almacenes de clientes NFSv4.

Ejemplo

Este ejemplo muestra la información de la agrupación de almacenamiento de clientes NFSv4.

```
cluster1::*> vserver nfs storepool show

Node: node1

Vserver: vs1

Data-IP: 10.0.1.1

Client-IP Protocol IsTrunked OwnerCount OpenCount DelegCount LockCount
-----
-----
10.0.2.1      nfs4.1      true      2 1 0 4
10.0.2.2      nfs4.2      true      2 1 0 4

2 entries were displayed.
```

Activar o desactivar los controles de límite de grupo de almacenamiento

Los administradores pueden utilizar los siguientes comandos para activar o desactivar los controles de límite de storepool.

Paso

1. Como administrador, realice una de las siguientes acciones:

| Si desea... | Introduzca el siguiente comando... |
|--|--|
| Active los controles de límite de grupo de almacenamiento | <code>vserver nfs storepool config modify -limit-enforce enabled</code> |
| Desactive los controles de límite de la agrupación de almacenamiento | <code>vserver nfs storepool config modify -limit-enforce disabled</code> |

Ver una lista de clientes bloqueados

Si el límite de grupo de almacenamiento está activado, los administradores pueden ver qué clientes se han bloqueado al alcanzar el umbral de recursos por cliente. Los administradores pueden usar el siguiente comando para ver qué clientes se han marcado como clientes bloqueados.

Pasos

1. Utilice la `vserver nfs storepool blocked-client show` Comando para mostrar la lista de clientes bloqueados NFSv4.

Eliminar un cliente de la lista de clientes bloqueados

Los clientes que alcancen su umbral por cliente se desconectarán y añadirán a la caché del cliente de bloques. Los administradores pueden usar el siguiente comando para eliminar el cliente de la caché del cliente de bloques. Esto permitirá que el cliente se conecte al servidor ONTAP NFSv4.

Pasos

1. Utilice la `vserver nfs storepool blocked-client flush -client-ip <ip address>` comando para vaciar la caché de cliente bloqueada de storepool.
2. Utilice la `vserver nfs storepool blocked-client show` comando para verificar que el cliente se ha eliminado de la caché del cliente de bloques.

Ejemplo

En este ejemplo, se muestra un cliente bloqueado con la dirección IP «10.2.1.1» vaciada en todos los nodos.

```
cluster1::*>vserver nfs storepool blocked-client flush -client-ip 10.2.1.1

cluster1::*>vserver nfs storepool blocked-client show

Node: node1

Client IP
-----
10.1.1.1

1 entries were displayed.
```

Habilite o deshabilite pNFS

PNFs mejora el rendimiento al permitir que los clientes NFS realicen operaciones de lectura/escritura en dispositivos de almacenamiento directamente y en paralelo, evitando así el servidor NFS como un posible cuello de botella. Para habilitar o deshabilitar pNFS (NFS paralelo), puede modificar el `-v4.1-pnfs` opción.

| Si la versión de ONTAP es... | El valor predeterminado de pNFS es... |
|------------------------------|---------------------------------------|
| 9,8 o posterior | deshabilitado |
| 9,7 o anterior | activado |

Lo que necesitará

Se requiere compatibilidad con NFSv4.1 para poder utilizar pNFS.

Si desea habilitar pNFS, primero debe deshabilitar las referencias NFS. No se pueden habilitar ambos a la vez.

Si utiliza pNFS con Kerberos en SVM, debe habilitar Kerberos en cada LIF de la SVM.

Paso

1. Ejecute una de las siguientes acciones:

| Si desea... | Introduzca el comando... |
|------------------|---|
| Habilite pNFS | <pre>vserver nfs modify -vserver vserver_name -v4.1-pnfs enabled</pre> |
| Deshabilite pNFS | <pre>vserver nfs modify -vserver vserver_name -v4.1-pnfs disabled</pre> |

Información relacionada

- [Descripción general de trunking NFS](#)

Control del acceso NFS a través de TCP y UDP

Puede habilitar o deshabilitar el acceso de NFS a máquinas virtuales de almacenamiento (SVM) a través de TCP y UDP modificando el `-tcp` y.. `-udp` parámetros, respectivamente. De este modo, puede controlar si los clientes NFS pueden acceder a los datos a través de TCP o UDP de su entorno.

Acerca de esta tarea

Estos parámetros solo se aplican a NFS. No afectan a los protocolos auxiliares. Por ejemplo, si NFS over TCP está deshabilitado, las operaciones de montaje mediante TCP siguen teniendo éxito. Para bloquear completamente el tráfico TCP o UDP, puede utilizar reglas de política de exportación.



Debe desactivar SnapDiff RPC Server antes de deshabilitar TCP para NFS para evitar un error de comando. Puede deshabilitar TCP con el comando `vserver snapdiff-rpc-server off -vserver vserver name`.

Paso

1. Ejecute una de las siguientes acciones:

| Si desea que el acceso NFS sea... | Introduzca el comando... |
|-----------------------------------|---|
| Habilitado a través de TCP | <code>vserver nfs modify -vserver vserver_name -tcp enabled</code> |
| Deshabilitado a través de TCP | <code>vserver nfs modify -vserver vserver_name -tcp disabled</code> |
| Activado a través de UDP | <code>vserver nfs modify -vserver vserver_name -udp enabled</code> |
| Desactivado en UDP | <code>vserver nfs modify -vserver vserver_name -udp disabled</code> |

Controle las solicitudes NFS de puertos no reservados

Puede rechazar las solicitudes de montaje de NFS de puertos no reservados habilitando el `-mount-rootonly` opción. Para rechazar todas las solicitudes NFS de puertos no reservados, puede habilitar el `-nfs-rootonly` opción.

Acerca de esta tarea

De forma predeterminada, la opción `-mount-rootonly` es `enabled`.

De forma predeterminada, la opción `-nfs-rootonly` es `disabled`.

Estas opciones no se aplican al procedimiento `NULL`.

Paso

1. Ejecute una de las siguientes acciones:

| Si desea... | Introduzca el comando... |
|---|--|
| Permita las solicitudes de montaje NFS de puertos no reservados | <code>vserver nfs modify -vserver vserver_name -mount-rootonly disabled</code> |
| Rechace las solicitudes de montaje NFS de puertos no reservados | <code>vserver nfs modify -vserver vserver_name -mount-rootonly enabled</code> |
| Permita todas las solicitudes NFS de puertos no reservados | <code>vserver nfs modify -vserver vserver_name -nfs-rootonly disabled</code> |

| | |
|--|--|
| Rechace todas las solicitudes NFS de puertos no reservados | <code>vserver nfs modify -vserver vserver_name -nfs -rootonly enabled</code> |
|--|--|

Gestione el acceso NFS a volúmenes NTFS o qtrees para usuarios UNIX desconocidos

Si ONTAP no puede identificar a los usuarios de UNIX que intentan conectarse a volúmenes o qtrees con un estilo de seguridad NTFS, no puede asignar explícitamente el usuario a un usuario de Windows. Puede configurar ONTAP para denegar el acceso a dichos usuarios para una seguridad más estricta o para asignarlos a un usuario de Windows predeterminado para garantizar un nivel mínimo de acceso a todos los usuarios.

Lo que necesitará

Si desea habilitar esta opción, se debe configurar un usuario de Windows predeterminado.

Acerca de esta tarea

Si un usuario de UNIX intenta acceder a volúmenes o qtrees con estilo de seguridad NTFS, el usuario de UNIX primero debe asignarse a un usuario de Windows para que ONTAP pueda evaluar correctamente los permisos NTFS. Sin embargo, si ONTAP no puede buscar el nombre del usuario UNIX en los orígenes del servicio de nombres de información de usuario configurados, no puede asignar explícitamente el usuario UNIX a un usuario específico de Windows. Puede decidir cómo manejar estos usuarios de UNIX desconocidos de las siguientes formas:

- Denegar el acceso a usuarios UNIX desconocidos.

Esto aplica una seguridad más estricta al requerir una asignación explícita para que todos los usuarios de UNIX obtengan acceso a volúmenes o qtrees NTFS.
- Asignar usuarios UNIX desconocidos a un usuario predeterminado de Windows.

Esto proporciona menos seguridad pero más comodidad al garantizar que todos los usuarios obtienen un nivel mínimo de acceso a volúmenes o qtrees NTFS a través de un usuario de Windows predeterminado.

Pasos

1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Ejecute una de las siguientes acciones:

| | |
|--|---|
| Si desea el usuario predeterminado de Windows para usuarios UNIX desconocidos... | Introduzca el comando... |
| Activado | <code>vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user enabled</code> |

| | |
|---------------|--|
| Deshabilitado | <code>vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user disabled</code> |
|---------------|--|

3. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

Consideraciones sobre los clientes que montan exportaciones NFS mediante un puerto no reservado

La `-mount-rootonly` La opción debe deshabilitarse en un sistema de almacenamiento que debe admitir clientes que montan exportaciones NFS mediante un puerto no reservado incluso cuando el usuario inicia sesión como raíz. Entre estos clientes se encuentran los clientes Hummingbird y los clientes Solaris NFS/IPv6.

Si la `-mount-rootonly` La opción está habilitada, ONTAP no permite que los clientes NFS que utilizan puertos no reservados, lo cual significa que los puertos con números superiores a 1,023, no puedan montar exportaciones NFS.

Realice una comprobación de acceso más estricta para los grupos de red mediante la verificación de dominios

De forma predeterminada, ONTAP realiza una verificación adicional al evaluar el acceso de cliente para un grupo de red. La comprobación adicional garantiza que el dominio del cliente coincida con la configuración de dominio de la máquina virtual de almacenamiento (SVM). De lo contrario, ONTAP niega el acceso del cliente.

Acerca de esta tarea

Cuando ONTAP evalúa las reglas de política de exportación para el acceso de cliente y una regla de política de exportación contiene un grupo de red, ONTAP debe determinar si la dirección IP de un cliente pertenece al grupo de redes. Con este fin, ONTAP convierte la dirección IP del cliente en un nombre de host mediante DNS y obtiene un nombre de dominio completo (FQDN).

Si el archivo `netgroup` sólo enumera un nombre corto para el host y el nombre corto para el host existe en varios dominios, es posible que un cliente de un dominio diferente obtenga acceso sin esta comprobación.

Para evitar esto, ONTAP compara el dominio que ha devuelto el DNS del host con la lista de nombres de dominio DNS configurados para la SVM. Si coincide, se permite el acceso. Si no coincide, se deniega el acceso.

Esta verificación está habilitada de forma predeterminada. Puede gestionarlo modificando el `-netgroup-dns -domain-search` parámetro, que está disponible en el nivel de privilegios avanzado.

Pasos

1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Realice la acción deseada:

| Si desea que la verificación del dominio para los grupos de red sea... | Introduzca... |
|--|---|
| Activado | <code>vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search enabled</code> |
| Deshabilitado | <code>vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search disabled</code> |

3. Configure el nivel de privilegio en admin:

```
set -privilege admin
```

Modifique los puertos que se utilizan para los servicios NFSv3

El servidor NFS del sistema de almacenamiento usa servicios como el demonio de montaje y Network Lock Manager para comunicarse con los clientes NFS a través de puertos de red predeterminados específicos. En la mayoría de los entornos NFS, los puertos predeterminados funcionan correctamente y no requieren modificación, pero si desea utilizar puertos de red NFS diferentes en su entorno NFSv3, puede hacerlo.

Lo que necesitará

Cambiar los puertos NFS del sistema de almacenamiento requiere que todos los clientes NFS se vuelvan a conectar al sistema, por lo que debe comunicar esta información a los usuarios antes de realizar el cambio.

Acerca de esta tarea

Puede establecer los puertos utilizados por los servicios de daemon de montaje NFS, Network Lock Manager, Network Status Monitor y NFS quota para cada máquina virtual de almacenamiento (SVM). El cambio de número de puerto afecta a los clientes NFS que acceden a los datos a través de TCP y UDP.

Los puertos de NFSv4 y NFSv4.1 no se pueden cambiar.

Pasos

1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Desactivar el acceso a NFS:

```
vserver nfs modify -vserver vserver_name -access false
```

3. Establezca el puerto NFS para el servicio NFS específico:

```
vserver nfs modify -vserver vserver_name nfs_port_parameter port_number
```

| Parámetro de puerto NFS | Descripción | Puerto predeterminado |
|-------------------------|---------------------------------|-----------------------|
| -mountd-port | Daemon de montaje NFS | 635 |
| -nlm-port | Administrador de bloqueo de red | 4045 |
| -nsm-port | Monitor de estado de red | 4046 |
| -rquotad-port | Daemon de cuota NFS | 4049 |

Además del puerto predeterminado, el intervalo permitido de números de puerto es de 1024 a 65535. Cada servicio NFS debe utilizar un puerto único.

4. Habilitar el acceso a NFS:

```
vserver nfs modify -vserver vserver_name -access true
```

5. Utilice la `network connections listening show` comando para verificar los cambios en el número de puerto.

6. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

Ejemplo

Los siguientes comandos establecen el puerto del daemon de montaje NFS en 1113 en la SVM llamada vs1:

```

vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
        them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -access false

vs1::*> vserver nfs modify -vserver vs1 -mountd-port 1113

vs1::*> vserver nfs modify -vserver vs1 -access true


vs1::*> network connections listening show
Vserver Name      Interface Name:Local Port      Protocol/Service
-----
Node: cluster1-01
Cluster           cluster1-01_clus_1:7700        TCP/ctlopcp
vs1                data1:4046                    TCP/sm
vs1                data1:4046                    UDP/sm
vs1                data1:4045                    TCP/nlm-v4
vs1                data1:4045                    UDP/nlm-v4
vs1                data1:1113                    TCP/mount
vs1                data1:1113                    UDP/mount
...
vs1::*> set -privilege admin

```

Comandos para gestionar servidores NFS

Hay comandos ONTAP específicos para gestionar los servidores NFS.

| Si desea... | Se usa este comando... |
|----------------------------|---------------------------------|
| Cree un servidor NFS | <code>vserver nfs create</code> |
| Muestre los servidores NFS | <code>vserver nfs show</code> |
| Modifique un servidor NFS | <code>vserver nfs modify</code> |
| Eliminar un servidor NFS | <code>vserver nfs delete</code> |

| | |
|--|---|
| Oculte el <code>.snapshot</code> Lista de directorios en puntos de montaje NFSv3 | <code>vserver nfs</code> comandos con el <code>-v3-hide-snapshot</code> opción habilitada |
|  <p>Acceso explícito a la <code>.snapshot</code> se seguirá permitiendo el directorio aunque la opción esté activada.</p> | |

Consulte la página de manual de cada comando para obtener más información.

Solucionar problemas del servicio de nombres

Cuando los clientes experimentan errores de acceso debido a problemas del servicio de nombres, puede utilizar el `vserver services name-service getxxbyyy` familia de comandos para realizar manualmente varias búsquedas del servicio de nombres y examinar los detalles y los resultados de la búsqueda para ayudar con la solución de problemas.

Acerca de esta tarea

- Para cada comando, puede especificar lo siguiente:
 - Nombre del nodo o de la máquina virtual de almacenamiento (SVM) en la que se realiza la búsqueda.

Esto le permite probar las búsquedas del servicio de nombres para un nodo o SVM específicos a fin de limitar la búsqueda de un posible problema de configuración del servicio de nombres.
 - Si se muestra el origen utilizado para la búsqueda.

Esto le permite comprobar si se ha utilizado la fuente correcta.
- ONTAP selecciona el servicio para realizar la búsqueda de acuerdo con el orden del switch de servicio de nombres configurado.
- Estos comandos están disponibles en el nivel de privilegio avanzado.

Pasos

1. Ejecute una de las siguientes acciones:

| Para recuperar... | Usar el comando... |
|--------------------------------------|---|
| Dirección IP de un nombre de host | <code>vserver services name-service getxxbyyy getaddrinfo</code> <code>vserver services name-service getxxbyyy gethostbyname</code> (Solo direcciones IPv4) |
| Miembros de un grupo por ID de grupo | <code>vserver services name-service getxxbyyy getgrbygid</code> |

| | |
|--|---|
| Miembros de un grupo por nombre de grupo | <code>vserver services name-service getxxbyyy getgrbyname</code> |
| Lista de grupos a los que pertenece un usuario | <code>vserver services name-service getxxbyyy getgrlist</code> |
| Nombre de host de una dirección IP | <code>vserver services name-service getxxbyyy getnameinfo vserver services name-service getxxbyyy gethostbyaddr</code> (Solo direcciones IPv4) |
| Información de usuario por nombre de usuario | <code>vserver services name-service getxxbyyy getpwbyname</code> Puede probar la resolución de nombres de los usuarios de RBAC especificando el <code>-use-rbac</code> parámetro como <code>true</code> . |
| Información de usuario por ID de usuario | <code>vserver services name-service getxxbyyy getpwbyuid</code> Puede probar la resolución de nombres de los usuarios de RBAC especificando el <code>-use-rbac</code> parámetro como <code>true</code> . |
| Pertenencia a netgroup de un cliente | <code>vserver services name-service getxxbyyy netgrp</code> |
| Pertenencia a netgroup de un cliente mediante la búsqueda netgroup-by-host | <code>vserver services name-service getxxbyyy netgrpbyhost</code> |

En el siguiente ejemplo, se muestra una prueba de búsqueda DNS para la SVM vs1 intentando obtener la dirección IP del host `acast1.eng.example.com`:

```
cluster1::*> vserver services name-service getxxbyyy getaddrinfo -vserver
vs1 -hostname acast1.eng.example.com -address-family all -show-source true
Source used for lookup: DNS
Host name: acast1.eng.example.com
Canonical Name: acast1.eng.example.com
IPv4: 10.72.8.29
```

En el siguiente ejemplo, se muestra una prueba de búsqueda de NIS para el SVM vs1 intentando recuperar la información de usuario de un usuario con el UID 501768:

```
cluster1::*> vserver services name-service getxxbyyy getpwbyuid -vserver
vs1 -userID 501768 -show-source true
Source used for lookup: NIS
pw_name: jsmith
pw_passwd: $1$y8rA4XX7$/DDOXAvC2PC/IsNFozfIN0
pw_uid: 501768
pw_gid: 501768
pw_gecos:
pw_dir: /home/jsmith
pw_shell: /bin/bash
```

En el siguiente ejemplo, se muestra una prueba de búsqueda LDAP para la SVM vs1 intentando recuperar la información de usuario de un usuario con el nombre ldap1:

```
cluster1::*> vserver services name-service getxxbyyy getpwbyname -vserver
vs1 -username ldap1 -use-rbac false -show-source true
Source used for lookup: LDAP
pw_name: ldap1
pw_passwd: {crypt}JSPM6yc/ilIX6
pw_uid: 10001
pw_gid: 3333
pw_gecos: ldap1 user
pw_dir: /u/ldap1
pw_shell: /bin/csh
```

En el siguiente ejemplo se muestra una prueba de búsqueda de netgroup para la SVM vs1 intentando averiguar si el cliente dnshost0 es miembro del netgroup lnetgroup136:

```
cluster1::*> vserver services name-service getxxbyyy netgrp -vserver vs1
-netgroup lnetgroup136 -client dnshost0 -show-source true
Source used for lookup: LDAP
dnshost0 is a member of lnetgroup136
```

1. Analice los resultados de la prueba realizada y tome las medidas necesarias.

| Si... | Compruebe... |
|---|--|
| Error en la búsqueda del nombre de host o de la dirección IP o se obtuvieron resultados incorrectos | Configuración de DNS |
| La búsqueda se ha consultado con un origen incorrecto | Asigne un nombre a la configuración del switch de servicio |

| Si... | Compruebe... |
|---|--|
| Error de búsqueda de usuarios o grupos o resultados incorrectos | <ul style="list-style-type: none"> • Asigne un nombre a la configuración del switch de servicio • Configuración de origen (archivos locales, dominio NIS, cliente LDAP) • Configuración de red (por ejemplo, LIF y rutas) |
| Se ha producido un error en la búsqueda del nombre de host o se ha agotado el tiempo de espera y el servidor DNS no resuelve los nombres cortos de DNS (por ejemplo, host1) | Configuración de DNS para consultas de dominio de nivel superior (TLD). Puede desactivar las consultas TLD mediante el <code>-is-tld-query-enabled false</code> de la <code>vserver services name-service dns modify</code> comando. |

Información relacionada

["Informe técnico de NetApp 4668: Guía de prácticas recomendadas de servicios de nombres"](#)

Verifique las conexiones del servicio de nombres

A partir de ONTAP 9.2, puede comprobar los servidores de nombres DNS y LDAP para verificar que están conectados a ONTAP. Estos comandos están disponibles en el nivel de privilegios de administrador.

Acerca de esta tarea

Puede comprobar que la configuración del servicio de nombres DNS o LDAP sea válida según sea necesario mediante el comprobador de configuración del servicio de nombres. Esta comprobación de validación puede iniciarse en la línea de comandos o en System Manager.

Para las configuraciones DNS, todos los servidores se han probado y deben funcionar para que la configuración se considere válida. Para las configuraciones LDAP, siempre que un servidor esté activo, la configuración es válida. Los comandos del servicio de nombres aplican el comprobador de configuración a menos que el `skip-config-validation` el campo es verdadero (el valor predeterminado es falso).

Paso

1. Utilice el comando apropiado para comprobar la configuración de un servicio de nombres. La interfaz de usuario muestra el estado de los servidores configurados.

| Para comprobar... | Se usa este comando... |
|---------------------------------|---|
| Estado de configuración de DNS | <code>vserver services name-service dns check</code> |
| Estado de configuración de LDAP | <code>vserver services name-service ldap check</code> |

```
cluster1::> vserver services name-service dns check -vserver vs0
```

| Vserver | Name Server | Status | Status Details |
|---------|-------------|--------|--------------------------|
| vs0 | 10.11.12.13 | up | Response time (msec): 55 |
| vs0 | 10.11.12.14 | up | Response time (msec): 70 |
| vs0 | 10.11.12.15 | down | Connection refused. |

```
cluster1::> vserver services name-service ldap check -vserver vs0
```

```
| Vserver: vs0 |
| Client Configuration Name: c1 |
| LDAP Status: up |
| LDAP Status Details: Successfully connected to LDAP server |
"10.11.12.13". |
```

La validación de la configuración se realiza correctamente si se puede acceder al menos uno de los servidores configurados (servidores/servidores ldap) y se proporciona el servicio. Se muestra una advertencia si algunos de los servidores no son accesibles.

Comandos para administrar las entradas del conmutador de servicio de nombres

Puede administrar las entradas del conmutador de servicios de nombres creando, visualizando, modificando y eliminando.

| Si desea... | Se usa este comando... |
|--|---|
| Crear una entrada de conmutador de servicio de nombres | <code>vserver services name-service ns-switch create</code> |
| Mostrar las entradas del conmutador de servicio de nombres | <code>vserver services name-service ns-switch show</code> |
| Modificar una entrada de cambio de servicio de nombres | <code>vserver services name-service ns-switch modify</code> |
| Eliminar una entrada de cambio de servicio de nombres | <code>vserver services name-service ns-switch delete</code> |

Consulte la página de manual de cada comando para obtener más información.

Información relacionada

["Informe técnico de NetApp 4668: Guía de prácticas recomendadas de servicios de nombres"](#)

Comandos para gestionar la caché de servicio de nombres

Puede gestionar la caché del servicio de nombres modificando el valor de tiempo de vida (TTL). El valor TTL determina el tiempo que la información del servicio de nombre es persistente en la caché.

| Si desea modificar el valor TTL para... | Se usa este comando... |
|---|--|
| Usuarios de UNIX | <code>vserver services name-service cache unix-user settings</code> |
| Grupos UNIX | <code>vserver services name-service cache unix-group settings</code> |
| Grupos de redes UNIX | <code>vserver services name-service cache netgroups settings</code> |
| Hosts | <code>vserver services name-service cache hosts settings</code> |
| Pertenencia a grupos | <code>vserver services name-service cache group-membership settings</code> |

Información relacionada

["Comandos de ONTAP 9"](#)

Comandos para gestionar las asignaciones de nombres

Hay comandos de la ONTAP específicos para gestionar las asignaciones de nombres.

| Si desea... | Se usa este comando... |
|--|--|
| Cree una asignación de nombres | <code>vserver name-mapping create</code> |
| Inserte una asignación de nombres en una posición específica | <code>vserver name-mapping insert</code> |
| Mostrar asignaciones de nombres | <code>vserver name-mapping show</code> |
| Cambie la posición de dos asignaciones de nombre NOTA: No se permite un intercambio cuando la asignación de nombres está configurada con una entrada de cualificador de ip. | <code>vserver name-mapping swap</code> |

| | |
|--|---|
| Modificar una asignación de nombres | <code>vserver name-mapping modify</code> |
| Eliminar una asignación de nombres | <code>vserver name-mapping delete</code> |
| Validar la asignación de nombre correcta | <code>vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1</code> |

Consulte la página de manual de cada comando para obtener más información.

Comandos para gestionar usuarios UNIX locales

Hay comandos específicos de la ONTAP para administrar los usuarios locales de UNIX.

| Si desea... | Se usa este comando... |
|---|--|
| Cree un usuario UNIX local | <code>vserver services name-service unix-user create</code> |
| Cargar usuarios UNIX locales desde un URI | <code>vserver services name-service unix-user load-from-uri</code> |
| Mostrar usuarios UNIX locales | <code>vserver services name-service unix-user show</code> |
| Modificar un usuario UNIX local | <code>vserver services name-service unix-user modify</code> |
| Elimine un usuario UNIX local | <code>vserver services name-service unix-user delete</code> |

Consulte la página de manual de cada comando para obtener más información.

Comandos para administrar grupos UNIX locales

Hay comandos específicos de la ONTAP para administrar los grupos UNIX locales.

| Si desea... | Se usa este comando... |
|--|---|
| Cree un grupo UNIX local | <code>vserver services name-service unix-group create</code> |
| Agregar un usuario a un grupo UNIX local | <code>vserver services name-service unix-group adduser</code> |
| Cargar grupos UNIX locales desde un URI | <code>vserver services name-service unix-group load-from-uri</code> |
| Mostrar grupos UNIX locales | <code>vserver services name-service unix-group show</code> |

| | |
|--|---|
| Modificar un grupo UNIX local | <code>vserver services name-service unix-group modify</code> |
| Eliminar un usuario de un grupo UNIX local | <code>vserver services name-service unix-group deluser</code> |
| Elimine un grupo UNIX local | <code>vserver services name-service unix-group delete</code> |

Consulte la página de manual de cada comando para obtener más información.

Límites para usuarios, grupos y miembros de grupo de UNIX locales

ONTAP ha introducido límites para el número máximo de usuarios y grupos de UNIX en el clúster, así como comandos para gestionar estos límites. Estos límites pueden ayudar a evitar problemas de rendimiento, ya que impiden que los administradores creen demasiados usuarios y grupos locales de UNIX en el clúster.

Hay un límite para el número combinado de grupos de usuarios UNIX locales y miembros de grupo. Hay un límite independiente para los usuarios locales de UNIX. Los límites se limitan a todo el clúster. Cada uno de estos nuevos límites se establece en un valor predeterminado que se puede modificar hasta un límite rígido preasignado.

| Base de datos | Límite predeterminado | Limitación estricta |
|--|-----------------------|---------------------|
| Usuarios UNIX locales | 32.768 | 65.536 |
| Grupos UNIX locales y miembros del grupo | 32.768 | 65.536 |

Administrar límites para usuarios y grupos de UNIX locales

Hay comandos específicos de ONTAP para administrar límites para usuarios y grupos de UNIX locales. Los administradores de clústeres pueden utilizar estos comandos para solucionar problemas de rendimiento en el clúster que se creen que están relacionados con un número excesivo de usuarios y grupos UNIX locales.

Acerca de esta tarea

Estos comandos están disponibles para el administrador del clúster en el nivel de privilegio avanzado.

Paso

1. Ejecute una de las siguientes acciones:

| Si desea... | Usar el comando... |
|--|--|
| Mostrar información acerca de los límites de usuario local de UNIX | <code>vserver services unix-user max-limit show</code> |

| Si desea... | Usar el comando... |
|--|---|
| Muestra información acerca de los límites de grupos UNIX locales | <code>vserver services unix-group max-limit show</code> |
| Modificar los límites de usuarios UNIX locales | <code>vserver services unix-user max-limit modify</code> |
| Modificar los límites de grupos UNIX locales | <code>vserver services unix-group max-limit modify</code> |

Consulte la página de manual de cada comando para obtener más información.

Comandos para administrar grupos de red locales

Puede administrar los grupos de red locales cargándolos desde un URI, verificando su estado entre los nodos, mostrándolos y borrándolos.

| Si desea... | Usar el comando... |
|---|---|
| Cargar grupos de red desde un URI | <code>vserver services name-service netgroup load</code> |
| Compruebe el estado de los grupos de red en los nodos | <code>vserver services name-service netgroup status</code> Disponible a nivel de privilegio avanzado y superior. |
| Mostrar grupos de redes locales | <code>vserver services name-service netgroup file show</code> |
| Elimine un netgroup local | <code>vserver services name-service netgroup file delete</code> |

Consulte la página de manual de cada comando para obtener más información.

Comandos para administrar configuraciones de dominio NIS

Hay comandos específicos de ONTAP para administrar configuraciones de dominio NIS.

| Si desea... | Se usa este comando... |
|---|--|
| Cree una configuración de dominio NIS | <code>vserver services name-service nis-domain create</code> |
| Mostrar configuraciones de dominio NIS | <code>vserver services name-service nis-domain show</code> |
| Mostrar el estado de enlace de una configuración de dominio NIS | <code>vserver services name-service nis-domain show-bound</code> |

| | |
|--|---|
| Mostrar estadísticas NIS | <code>vserver services name-service nis-domain show-statistics</code> Disponible a nivel de privilegio avanzado y superior. |
| Borrar estadísticas de NIS | <code>vserver services name-service nis-domain clear-statistics</code> Disponible a nivel de privilegio avanzado y superior. |
| Modifique una configuración de dominio NIS | <code>vserver services name-service nis-domain modify</code> |
| Elimine una configuración de dominio NIS | <code>vserver services name-service nis-domain delete</code> |
| Habilite el almacenamiento en caché para búsquedas de netgroup-by-host | <code>vserver services name-service nis-domain netgroup-database config modify</code> Disponible a nivel de privilegio avanzado y superior. |

Consulte la página de manual de cada comando para obtener más información.

Comandos para gestionar las configuraciones del cliente LDAP

Hay comandos ONTAP específicos para gestionar las configuraciones de cliente LDAP.



Los administradores de SVM no pueden modificar ni eliminar las configuraciones de cliente LDAP que crearon los administradores del clúster.

| Si desea... | Se usa este comando... |
|--|---|
| Cree una configuración de cliente LDAP | <code>vserver services name-service ldap client create</code> |
| Mostrar las configuraciones del cliente LDAP | <code>vserver services name-service ldap client show</code> |
| Modifique una configuración de cliente LDAP | <code>vserver services name-service ldap client modify</code> |
| Cambie la contraseña de ENLACE de cliente LDAP | <code>vserver services name-service ldap client modify-bind-password</code> |
| Eliminar una configuración de cliente LDAP | <code>vserver services name-service ldap client delete</code> |

Consulte la página de manual de cada comando para obtener más información.

Comandos para gestionar las configuraciones LDAP

Hay comandos de la ONTAP específicos para gestionar las configuraciones LDAP.

| Si desea... | Se usa este comando... |
|------------------------------------|--|
| Cree una configuración LDAP | <code>vserver services name-service ldap create</code> |
| Mostrar configuraciones LDAP | <code>vserver services name-service ldap show</code> |
| Modificar una configuración LDAP | <code>vserver services name-service ldap modify</code> |
| Eliminar una configuración de LDAP | <code>vserver services name-service ldap delete</code> |

Consulte la página de manual de cada comando para obtener más información.

Comandos para administrar plantillas de esquema de cliente LDAP

Hay comandos ONTAP específicos para administrar plantillas de esquema de cliente LDAP.



Los administradores de SVM no pueden modificar ni eliminar esquemas de cliente LDAP que crearon los administradores de clúster.

| Si desea... | Se usa este comando... |
|---|--|
| Copie una plantilla de esquema LDAP existente | <code>vserver services name-service ldap client schema copy</code> Disponible a nivel de privilegio avanzado y superior. |
| Mostrar plantillas de esquema LDAP | <code>vserver services name-service ldap client schema show</code> |
| Modificar una plantilla de esquema LDAP | <code>vserver services name-service ldap client schema modify</code> Disponible a nivel de privilegio avanzado y superior. |
| Eliminar una plantilla de esquema LDAP | <code>vserver services name-service ldap client schema delete</code> Disponible a nivel de privilegio avanzado y superior. |

Consulte la página de manual de cada comando para obtener más información.

Comandos para gestionar las configuraciones de la interfaz de Kerberos de NFS

Hay comandos de ONTAP específicos para gestionar las configuraciones de la interfaz de Kerberos de NFS.

| Si desea... | Se usa este comando... |
|----------------------------------|--|
| Habilite NFS Kerberos en una LIF | <code>vserver nfs kerberos interface enable</code> |

| | |
|--|---|
| Mostrar las configuraciones de la interfaz Kerberos para NFS | <code>vserver nfs kerberos interface show</code> |
| Modifique la configuración de una interfaz NFS Kerberos | <code>vserver nfs kerberos interface modify</code> |
| Desactive NFS Kerberos en una LIF | <code>vserver nfs kerberos interface disable</code> |

Consulte la página de manual de cada comando para obtener más información.

Comandos para gestionar configuraciones de dominio de Kerberos de NFS

Hay comandos específicos de ONTAP para gestionar configuraciones de dominio de Kerberos de NFS.

| Si desea... | Se usa este comando... |
|---|--|
| Cree una configuración de dominio de Kerberos para NFS | <code>vserver nfs kerberos realm create</code> |
| Mostrar configuraciones de dominio de Kerberos para NFS | <code>vserver nfs kerberos realm show</code> |
| Modificar una configuración de dominio de Kerberos para NFS | <code>vserver nfs kerberos realm modify</code> |
| Elimine una configuración de dominio de Kerberos para NFS | <code>vserver nfs kerberos realm delete</code> |

Consulte la página de manual de cada comando para obtener más información.

Comandos para gestionar políticas de exportación

Hay comandos de ONTAP específicos para gestionar las políticas de exportación.

| Si desea... | Se usa este comando... |
|--|---|
| Mostrar información acerca de las políticas de exportación | <code>vserver export-policy show</code> |
| Cambiar el nombre de una política de exportación | <code>vserver export-policy rename</code> |
| Copiar una política de exportación | <code>vserver export-policy copy</code> |
| Eliminar una política de exportación | <code>vserver export-policy delete</code> |

Consulte la página de manual de cada comando para obtener más información.

Comandos para gestionar las reglas de exportación

Hay comandos ONTAP específicos para gestionar las reglas de exportación.

| Si desea... | Se usa este comando... |
|---|--|
| Cree una regla de exportación | <code>vserver export-policy rule create</code> |
| Muestra información acerca de las reglas de exportación | <code>vserver export-policy rule show</code> |
| Modificar una regla de exportación | <code>vserver export-policy rule modify</code> |
| Eliminar una regla de exportación | <code>vserver export-policy rule delete</code> |



Si ha configurado varias reglas de exportación idénticas que coinciden con distintos clientes, asegúrese de mantenerlas sincronizadas al gestionar las reglas de exportación.

Consulte la página de manual de cada comando para obtener más información.

Configure la caché de credenciales NFS

Motivos para modificar el tiempo de funcionamiento de la caché de credenciales NFS

ONTAP utiliza la memoria caché de credenciales para almacenar la información necesaria para la autenticación de usuarios para acceder a la exportación de NFS con el fin de proporcionar un acceso más rápido y mejorar el rendimiento. Puede configurar el tiempo que se almacena la información en la caché de credenciales para personalizarla en su entorno.

Hay varios escenarios cuando se modifica el tiempo de vida de la caché de credenciales de NFS (TTL) puede ayudar a resolver los problemas. Usted debe entender cuáles son estos escenarios así como las consecuencias de hacer estas modificaciones.

Razones

Considere cambiar el TTL predeterminado en las siguientes circunstancias:

| Problema | Acción correctiva |
|---|--|
| Los servidores de nombres de su entorno están experimentando una degradación del rendimiento debido a una gran carga de solicitudes de ONTAP. | Aumente el TTL para las credenciales positivas y negativas en la caché para reducir el número de solicitudes de ONTAP a los servidores de nombres. |

| Problema | Acción correctiva |
|---|---|
| El administrador del servidor de nombres realizó cambios para permitir el acceso a usuarios NFS que se denegaron anteriormente. | Disminuya el TTL para las credenciales negativas en la caché a fin de reducir el tiempo que los usuarios NFS tienen que esperar a que ONTAP solicite credenciales nuevas de los servidores de nombres externos para que puedan acceder. |
| El administrador del servidor de nombres realizó cambios para denegar el acceso a usuarios NFS que se habían permitido previamente. | Reduzca el TTL para las credenciales positivas en caché para reducir el tiempo antes de que ONTAP solicite credenciales nuevas de los servidores de nombres externos, de modo que los usuarios de NFS no tengan acceso. |

Consecuencias

Puede modificar el período de tiempo individualmente para almacenar en caché las credenciales positivas y negativas. Sin embargo, usted debe ser consciente de las ventajas y desventajas de hacerlo.

| Si... | La ventaja es... | La desventaja es... |
|---|--|---|
| Aumente el tiempo positivo de la caché de credenciales | ONTAP envía solicitudes de credenciales a servidores de nombres con menos frecuencia, lo que reduce la carga en los servidores de nombres. | La denegación del acceso a los usuarios de NFS tarda más tiempo, pero ya no es así. |
| Reduzca el tiempo positivo de la caché de credenciales | Tarda menos tiempo en denegar el acceso a los usuarios de NFS a los que antes no se había permitido, pero ya no lo están. | ONTAP envía solicitudes de credenciales a los servidores de nombres con mayor frecuencia, lo que aumenta la carga en los servidores de nombres. |
| Aumente el tiempo de la caché de credenciales negativas | ONTAP envía solicitudes de credenciales a servidores de nombres con menos frecuencia, lo que reduce la carga en los servidores de nombres. | Lleva más tiempo conceder acceso a los usuarios de NFS que antes no estaban permitidos pero que ahora lo son. |
| Reduzca el tiempo de la caché de credenciales negativas | Tarda menos tiempo en conceder acceso a los usuarios de NFS que antes no estaban permitidos pero que ahora lo son. | ONTAP envía solicitudes de credenciales a los servidores de nombres con mayor frecuencia, lo que aumenta la carga en los servidores de nombres. |

Configure el tiempo de espera para las credenciales de usuario NFS almacenadas en caché

Puede configurar el lapso en que ONTAP almacena credenciales para los usuarios NFS en su caché interna (tiempo de actividad o TTL) mediante la modificación del servidor NFS de la máquina virtual de almacenamiento (SVM). De este modo, puede solucionar

algunos problemas relacionados con la alta carga de los servidores de nombres o con los cambios de las credenciales que afectan al acceso del usuario NFS.

Acerca de esta tarea

Estos parámetros están disponibles en el nivel de privilegios avanzado.

Pasos

- 1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

- 2. Realice la acción deseada:

| | |
|--|--|
| Si desea modificar el TTL para el almacenamiento en caché... | Usar el comando... |
| Credenciales positivas | <div>vserver nfs modify -vserver vserver_name -cached -cred-positive-ttl time_to_live</div> <div>El TTL se mide en milisegundos. A partir de ONTAP 9.10.1 y versiones posteriores, el valor predeterminado es de 1 hora (3.600.000 milisegundos). En ONTAP 9.9.1 y las versiones anteriores, el valor predeterminado es de 24 horas (86.400.000 milisegundos). El intervalo permitido para este valor es de 1 minuto (60000 milisegundos) a 7 días (604,800,000 milisegundos).</div> |
| Credenciales negativas | <div>vserver nfs modify -vserver vserver_name -cached -cred-negative-ttl time_to_live</div> <div>El TTL se mide en milisegundos. El valor predeterminado es 2 horas (7.200.000 milisegundos). El intervalo permitido para este valor es de 1 minuto (60000 milisegundos) a 7 días (604,800,000 milisegundos).</div> |

- 3. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

Gestione las cachés de la política de exportación

Volcar cachés de políticas de exportación

ONTAP usa varios cachés de políticas de exportación para almacenar información relacionada con las políticas de exportación para agilizar el acceso. Vaciado manual de las cachés de directivas de exportación (`vserver export-policy cache flush`) Quita información potencialmente obsoleta y fuerza a ONTAP a recuperar información actual de los recursos externos apropiados. Esto puede ayudar a resolver diversos problemas relacionados con el acceso de clientes a exportaciones NFS.

Acerca de esta tarea

La información de la caché de la directiva de exportación puede quedar obsoleta por los siguientes motivos:

- Un cambio reciente en las reglas de política de exportación
- Un cambio reciente en los registros de nombres de host en servidores de nombres
- Un cambio reciente en las entradas de netgroup en los servidores de nombres
- Recuperación de una interrupción de la red que impidió que los grupos de red se cargaran por completo

Pasos

1. Si no se cuenta con la caché de servicio de nombres habilitada, realice una de las siguientes acciones en el modo de privilegio avanzado:

| Si quieres tirar la cadena... | Introduzca el comando... |
|---|--|
| Todas las cachés de directivas de exportación (excepto showmount) | <pre>vserver export-policy cache flush -vserver vserver_name</pre> |
| La política de exportación rige la caché de acceso | <pre>vserver export-policy cache flush -vserver vserver_name -cache access</pre> <p>Puede incluir la opción <code>-node</code> parámetro para especificar el nodo en el que se desea vaciar la caché de acceso.</p> |
| La caché de nombres del host | <pre>vserver export-policy cache flush -vserver vserver_name -cache host</pre> |
| La caché de netgroup | <pre>vserver export-policy cache flush -vserver vserver_name -cache netgroup</pre> <p>El procesamiento de netgroups requiere muchos recursos. Solo debe vaciar la caché de netgroup si intenta resolver un problema de acceso de cliente causado por un grupo de red obsoleto.</p> |
| La caché showmount | <pre>vserver export-policy cache flush -vserver vserver_name -cache showmount</pre> |

2. Si la caché del servicio de nombres está habilitada, realice una de las siguientes acciones:

| Si quieres tirar la cadena... | Introduzca el comando... |
|--|---|
| La política de exportación rige la caché de acceso | <pre>vserver export-policy cache flush -vserver vserver_name -cache access</pre> <p>Puede incluir la opción <code>-node</code> parámetro para especificar el nodo en el que se desea vaciar la caché de acceso.</p> |
| La caché de nombres del host | <pre>vserver services name-service cache hosts forward-lookup delete-all</pre> |

| Si quieres tirar la cadena... | Introduzca el comando... |
|-------------------------------|--|
| La caché de netgroup | <code>vserver services name-service cache netgroups ip-to-netgroup delete-all</code> <code>vserver services name-service cache netgroups members delete-all</code> El procesamiento de netgroups requiere muchos recursos. Solo debe vaciar la caché de netgroup si intenta resolver un problema de acceso de cliente causado por un grupo de red obsoleto. |
| La caché showmount | <code>vserver export-policy cache flush</code> <code>-vserver vserver_name -cache showmount</code> |

Mostrar la cola y la caché del grupo de red de directivas de exportación

ONTAP utiliza la cola de netgroup al importar y resolver grupos de red y utiliza la caché de netgroup para almacenar la información resultante. Al solucionar problemas relacionados con el grupo de directivas de exportación, puede utilizar la `vserver export-policy netgroup queue show` y `vserver export-policy netgroup cache show` comandos para mostrar el estado de la cola de netgroup y el contenido de la caché de netgroup.

Paso

1. Ejecute una de las siguientes acciones:

| | |
|--|--|
| Para mostrar el grupo de red de la directiva de exportación... | Introduzca el comando... |
| Cola | <code>vserver export-policy netgroup queue show</code> |
| Almacenamiento en caché | <code>vserver export-policy netgroup cache show -vserver vserver_name</code> |

Consulte la página de manual de cada comando para obtener más información.

Compruebe si una dirección IP de cliente es miembro de un grupo de red

Al solucionar problemas de acceso de cliente NFS relacionados con los grupos de red, puede utilizar `vserver export-policy netgroup check-membership` Comando para ayudar a determinar si una IP de cliente es miembro de un determinado netgroup.

Acerca de esta tarea

Al comprobar la pertenencia a un grupo de red, puede determinar si ONTAP sabe que un cliente es o no miembro de un grupo de red. También le permite saber si la caché del netgroup de ONTAP está en un estado transitorio mientras actualiza la información del netgroup. Esta información puede ayudarle a entender por qué

se puede conceder o denegar el acceso a un cliente de forma inesperada.

Paso

1. Compruebe la pertenencia al grupo de redes a una dirección IP de cliente: `vserver export-policy netgroup check-membership -vserver vserver_name -netgroup netgroup_name -client-ip client_ip`

El comando puede mostrar los siguientes resultados:

- El cliente es un miembro del netgroup.

Esto se ha confirmado mediante una búsqueda inversa o una búsqueda de netgroup-by-host.

- El cliente es un miembro del netgroup.

Se encontró en la caché de netgroup de ONTAP.

- El cliente no es miembro del netgroup.
- La pertenencia al cliente aún no se puede determinar porque ONTAP está actualizando la caché de netgroup.

Hasta que esto se haga, la membresía no puede ser explícitamente dentro o fuera. Utilice la `vserver export-policy netgroup queue show` comando para supervisar la carga del netgroup y volver a intentar la comprobación después de que haya finalizado.

Ejemplo

En el siguiente ejemplo, se comprueba si un cliente con la dirección IP 172.17.16.72 es miembro del netgroup Mercury en la SVM vs1:

```
cluster1::> vserver export-policy netgroup check-membership -vserver vs1  
-netgroup mercury -client-ip 172.17.16.72
```

Optimice el rendimiento de la caché de acceso

Puede configurar varios parámetros para optimizar la caché de acceso y encontrar el equilibrio perfecto entre el rendimiento y la corriente de la información almacenada en la caché de acceso.

Acerca de esta tarea

Cuando configure los periodos de actualización de la caché de acceso, tenga en cuenta lo siguiente:

- Valores más altos significa que las entradas permanecen más tiempo en la caché de acceso.

La ventaja es que ofrece un mejor rendimiento, ya que ONTAP gasta menos recursos en actualizar las entradas de la caché de acceso. La desventaja es que si las reglas de la política de exportación cambian y las entradas de la caché de acceso se quedan obsoletas como resultado, se necesita más tiempo para actualizarlas. Como resultado, los clientes que deberían obtener acceso podrían ser denegados, y los clientes que deberían ser denegados podrían obtener acceso.

- Los valores más bajos significan ONTAP que las entradas de la caché de acceso se actualizan con más frecuencia.

La ventaja es que las entradas son más actuales y es más probable que los clientes se les conceda o deniegue el acceso correctamente. La desventaja es una reducción del rendimiento, ya que ONTAP gasta más recursos en actualizar las entradas de la caché de acceso.

Pasos

- 1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

- 2. Realice la acción deseada:

| Para modificar... | Introduzca... |
|--|--|
| Período de actualización para entradas positivas | <code>vserver export-policy access-cache config modify-all-vservers -refresh -period-positive timeout_value</code> |
| Actualizar período para entradas negativas | <code>vserver export-policy access-cache config modify-all-vservers -refresh -period-negative timeout_value</code> |
| Tiempo de espera para entradas antiguas | <code>vserver export-policy access-cache config modify-all-vservers -harvest -timeout timeout_value</code> |

- 3. Compruebe la nueva configuración de parámetros:

```
vserver export-policy access-cache config show-all-vservers
```

- 4. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

Administrar bloqueos de archivos

Acerca del bloqueo de archivos entre protocolos

El bloqueo de archivos es un método que utilizan las aplicaciones cliente para evitar que un usuario acceda a un archivo abierto previamente por otro usuario. La forma en que ONTAP bloquea los archivos depende del protocolo del cliente.

Si el cliente es NFS, los bloqueos son consultivos; si el cliente es un cliente SMB, los bloqueos son obligatorios.

Debido a las diferencias entre los bloqueos de archivos NFS y SMB, es posible que un cliente NFS no pueda acceder a un archivo que abrió previamente una aplicación SMB.

Lo siguiente se produce cuando un cliente NFS intenta acceder a un archivo bloqueado por una aplicación SMB:

- En volúmenes mixtos o NTFS, operaciones de manipulación de archivos como `rm`, `rmdir`, y `mv` Puede provocar un fallo en la aplicación NFS.
- Las operaciones de lectura y escritura de NFS se deniegan en los modos abiertos Deny-Read y Deny-write de SMB, respectivamente.
- Error en las operaciones de escritura de NFS cuando el rango escrito del archivo está bloqueado por un bytelock exclusivo de SMB.

En los volúmenes de estilo de seguridad de UNIX, las operaciones de desenlace y cambio de nombre de NFS ignoran el estado de bloqueo de SMB y permiten el acceso al archivo. Todas las demás operaciones de NFS en volúmenes de estilo de seguridad de UNIX honran el estado de bloqueo de SMB.

Cómo trata ONTAP bits de sólo lectura

El bit de sólo lectura se establece en base a archivo para reflejar si un archivo es grabable (deshabilitado) o de sólo lectura (habilitado).

Los clientes SMB que usan Windows pueden establecer un bit de solo lectura por archivo. Los clientes NFS no establecen un bit de solo lectura por archivo, ya que los clientes NFS no tienen ninguna operación de protocolo que utilice un bit de solo lectura por archivo.

ONTAP puede establecer un bit de solo lectura en un archivo cuando un cliente SMB que utiliza Windows crea ese archivo. ONTAP también puede establecer un bit de solo lectura cuando se comparte un archivo entre los clientes NFS y los clientes SMB. Parte del software, cuando lo utilizan los clientes NFS y clientes SMB, requiere que se habilite el bit de solo lectura.

Para que ONTAP mantenga los permisos de lectura y escritura adecuados en un archivo compartido entre clientes NFS y clientes SMB, trata el bit de solo lectura de acuerdo con las siguientes reglas:

- NFS trata cualquier archivo con el bit de solo lectura habilitado como si no tiene bits de permiso de escritura habilitados.
- Si un cliente NFS deshabilita todos los bits de permiso de escritura y al menos uno de esos bits se había habilitado anteriormente, ONTAP habilita el bit de solo lectura para ese archivo.
- Si un cliente NFS habilita algún bit de permiso de escritura, ONTAP deshabilita el bit de solo lectura para ese archivo.
- Si se habilita el bit de solo lectura de un archivo y un cliente NFS intenta detectar permisos para el archivo, los bits de permiso del archivo no se envían al cliente NFS; en su lugar, ONTAP envía los bits de permiso al cliente NFS con los bits de permiso de escritura enmascarados.
- Si se habilita el bit de solo lectura de un archivo y un cliente SMB deshabilita el bit de solo lectura, ONTAP habilita el bit de permiso de escritura del propietario para el archivo.
- Los archivos con el bit de sólo lectura activado sólo son grabables por raíz.



Los cambios en los permisos de archivo se aplican inmediatamente en los clientes SMB, pero es posible que no se apliquen de inmediato en los clientes NFS si el cliente NFS habilita el almacenamiento de atributos en caché.

Diferencias entre ONTAP y Windows al administrar bloqueos en los componentes de ruta de acceso compartida

A diferencia de Windows, ONTAP no bloquea cada componente de la ruta de acceso a un archivo abierto mientras el archivo está abierto. Este comportamiento también afecta a las rutas de recursos compartidos de SMB.

Como ONTAP no bloquea cada componente de la ruta, es posible cambiar el nombre de un componente de ruta por encima del archivo o el recurso compartido abierto, lo que puede provocar problemas en determinadas aplicaciones o hacer que la ruta del recurso compartido en la configuración del SMB no sea válida. Esto puede hacer que el recurso compartido sea inaccesible.

Para evitar problemas causados por el cambio de nombre de los componentes de la ruta de acceso, puede aplicar la configuración de seguridad Lista de control de acceso (ACL) de Windows que impide que los usuarios o aplicaciones cambien el nombre de los directorios críticos.

Más información acerca de ["Cómo evitar que se cambie el nombre de los directorios mientras los clientes acceden a ellos"](#).

Mostrar información sobre bloqueos

Puede mostrar información acerca de los bloqueos de archivos actuales, incluidos los tipos de bloqueos que se conservan y el estado de bloqueo, detalles sobre bloqueos de rango de bytes, modos sharelock, bloqueos de delegación y bloqueos oportunistas, y si se abren bloqueos con identificadores duraderos o persistentes.

Acerca de esta tarea

No se puede mostrar la dirección IP del cliente para los bloqueos establecidos a través de NFSv4 o NFSv4.1.

De forma predeterminada, el comando muestra información sobre todos los bloqueos. Puede usar los parámetros del comando para mostrar información sobre los bloqueos de una máquina virtual de almacenamiento (SVM) específica o para filtrar el resultado del comando según otros criterios.

La `vserver locks show` el comando muestra información sobre cuatro tipos de bloqueos:

- Bloqueos de rango de bytes, que bloquean sólo una parte de un archivo.
- Bloqueos de uso compartido, que bloquean los archivos abiertos.
- Bloqueos oportunistas, que controlan el almacenamiento en caché en el cliente a través de SMB.
- Delegaciones, que controlan el almacenamiento en caché en el cliente a través de NFSv4.x.

Al especificar parámetros opcionales, puede determinar información importante sobre cada tipo de bloqueo. Consulte la página de manual del comando para obtener más información.

Paso

1. Muestra información sobre los bloqueos mediante `vserver locks show` comando.

Ejemplos

En el siguiente ejemplo, se muestra información de resumen para un bloqueo de NFSv4 en un archivo con la ruta `/vol1/file1`. El modo de acceso sharelock es `write-deny_none`, y el bloqueo se concedió mediante la delegación de escritura:

```
cluster1::> vserver locks show
```

```
Vserver: vs0
```

| Volume | Object Path | LIF | Protocol | Lock Type | Client |
|--------|---------------------------------|-------|----------|-------------|--------|
| ----- | ----- | ----- | ----- | ----- | |
| ---- | | | | | |
| vol1 | /vol1/file1 | lif1 | nfsv4 | share-level | - |
| | Sharelock Mode: write-deny_none | | | | |
| | | | | delegation | - |
| | Delegation Type: write | | | | |

En el siguiente ejemplo se muestra información detallada sobre oplock y sharelock acerca del bloqueo SMB en un archivo con la ruta de acceso /data2/data2_2/intro.pptx. Se concede un identificador duradero en el archivo con un modo de acceso de bloqueo compartido de Write-Deny_none a un cliente con una dirección IP de 10.3.1.3. Un plock de arrendamiento se concede con un nivel de plock por lotes:

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx
```

```

    Vserver: vs1
      Volume: data2_2
    Logical Interface: lif2
      Object Path: /data2/data2_2/intro.pptx
      Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
      Lock Protocol: cifs
      Lock Type: share-level
    Node Holding Lock State: node3
      Lock State: granted
    Bytelock Starting Offset: -
      Number of Bytes Locked: -
      Bytelock is Mandatory: -
      Bytelock is Exclusive: -
      Bytelock is Superlock: -
      Bytelock is Soft: -
      Oplock Level: -
    Shared Lock Access Mode: write-deny_none
      Shared Lock is Soft: false
      Delegation Type: -
      Client Address: 10.3.1.3
      SMB Open Type: durable
      SMB Connect State: connected
    SMB Expiration Time (Secs): -
      SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

    Vserver: vs1
```

```
Volume: data2_2
Logical Interface: lif2
Object Path: /data2/data2_2/test.pptx
Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
Lock Protocol: cifs
Lock Type: op-lock
Node Holding Lock State: node3
Lock State: granted
Bytelock Starting Offset: -
Number of Bytes Locked: -
Bytelock is Mandatory: -
Bytelock is Exclusive: -
Bytelock is Superlock: -
Bytelock is Soft: -
Oplock Level: batch
Shared Lock Access Mode: -
Shared Lock is Soft: -
Delegation Type: -
Client Address: 10.3.1.3
SMB Open Type: -
SMB Connect State: connected
SMB Expiration Time (Secs): -
SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

Bloqueos de ruptura

Cuando los bloqueos de archivos impiden que los clientes accedan a los archivos, puede mostrar información sobre los bloqueos retenidos actualmente y romperán bloqueos específicos. Entre los ejemplos de escenarios en los que es posible que necesite romper los bloqueos se incluyen las aplicaciones de depuración.

Acerca de esta tarea

La `vserver locks break` el comando solo está disponible en el nivel de privilegios avanzado y superior. La página man del comando contiene información detallada.

Pasos

1. Para encontrar la información que necesita para romper un bloqueo, utilice `vserver locks show` comando.

La página man del comando contiene información detallada.

2. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

3. Ejecute una de las siguientes acciones:

| | |
|--|--|
| Si desea romper un bloqueo especificando... | Introduzca el comando... |
| El nombre de SVM, el nombre del volumen, el nombre de LIF y la ruta de archivo | <code>vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif</code> |
| El ID del bloqueo | <code>vserver locks break -lockid UUID</code> |

4. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

Cómo funcionan los filtros de primera lectura y primera escritura de FPolicy con NFS

Los clientes NFS experimentan un tiempo de respuesta elevado durante el tráfico elevado de solicitudes de lectura/escritura cuando se habilita FPolicy mediante un servidor FPolicy externo con operaciones de lectura/escritura como eventos supervisados. Para los clientes NFS, el uso de filtros de primera lectura y primera escritura en FPolicy reduce el número de notificaciones de FPolicy y mejora el rendimiento.

En NFS, el cliente realiza operaciones de I/O en un archivo mediante la recuperación de su gestor. Este identificador puede seguir siendo válido durante todos los reinicios del servidor y el cliente. Por lo tanto, el cliente puede almacenar en caché el identificador y enviar solicitudes al mismo sin recuperar los controladores de nuevo. En una sesión normal, se envían muchas solicitudes de lectura/escritura al servidor de archivos. Si se generan notificaciones para todas estas solicitudes, se podrían producir los siguientes problemas:

- Mayor carga gracias al procesamiento de notificaciones adicional y al mayor tiempo de respuesta.
- Un gran número de notificaciones que se envían al servidor de FPolicy aunque el servidor no se vea afectado por todas las notificaciones.

Después de recibir la primera solicitud de lectura/escritura de un cliente para un archivo concreto, se crea una entrada de caché y se aumenta el número de lectura/escritura. Esta solicitud se marca como la primera operación de lectura/escritura y se genera un evento FPolicy. Antes de planificar y crear los filtros FPolicy para un cliente NFS, debe comprender los conceptos básicos de cómo funcionan los filtros FPolicy.

- Primera lectura: Filtra las solicitudes de lectura del cliente para la primera lectura.

Cuando este filtro se utiliza para eventos NFS, el `-file-session-io-grouping-count` y `-file-session-io-grouping-duration` Los ajustes determinan la solicitud de primera lectura para la que se procesa FPolicy.

- Primera escritura: Filtra las solicitudes de escritura del cliente para la primera escritura.

Cuando este filtro se utiliza para eventos NFS, el `-file-session-io-grouping-count` y `-file-session-io-grouping-duration` Los ajustes determinan la solicitud de primera escritura para la que se procesó FPolicy.

Las siguientes opciones se agregan a la base de datos de servidores NFS.

```
file-session-io-grouping-count: Number of I/O Ops on a File to Be Clubbed
and Considered as One Session
for Event Generation
file-session-io-grouping-duration: Duration for Which I/O Ops on a File to
Be Clubbed and Considered as
One Session for Event Generation
```

Modifique el ID de implementación del servidor NFSv4.1

El protocolo NFSv4.1 incluye un ID de implementación del servidor que documenta el dominio, el nombre y la fecha del servidor. Puede modificar los valores predeterminados del ID de implementación del servidor. Cambiar los valores predeterminados puede ser útil, por ejemplo, al recopilar estadísticas de uso o solucionar problemas de interoperabilidad. Para obtener más información, consulte RFC 5661.

Acerca de esta tarea

Los valores predeterminados de las tres opciones son los siguientes:

| Opción | Nombre de la opción | Valor predeterminado |
|--|--|----------------------------------|
| Dominio de ID de implementación de NFSv4.1 | <code>-v4.1-implementation-domain</code> | netapp.com |
| Nombre de ID de implementación de NFSv4.1 | <code>-v4.1-implementation-name</code> | Nombre de la versión del clúster |
| Fecha del ID de implementación de NFSv4.1 | <code>-v4.1-implementation-date</code> | Fecha de versión del clúster |

Pasos

1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Ejecute una de las siguientes acciones:

| Si desea modificar el ID de implementación de NFSv4.1... | Introduzca el comando... |
|--|---|
| Dominio | <code>vserver nfs modify -v4.1 -implementation-domain domain</code> |
| Nombre | <code>vserver nfs modify -v4.1 -implementation-name name</code> |

| Si desea modificar el ID de implementación de NFSv4.1... | Introduzca el comando... |
|--|---|
| Fecha | <code>vserver nfs modify -v4.1 -implementation-date date</code> |

3. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

Gestione las ACL de NFSv4

Ventajas de habilitar las ACL de NFSv4

Existen muchas ventajas a la hora de habilitar las ACL de NFSv4.

Entre las ventajas de habilitar las ACL de NFSv4 se incluyen las siguientes:

- Control más detallado del acceso de los usuarios a archivos y directorios
- Mejor seguridad NFS
- Interoperabilidad mejorada con CIFS
- Eliminación de la limitación de NFS de 16 grupos por usuario

Funcionamiento de las ACL de NFSv4

Un cliente que utilice las ACL de NFSv4 puede establecer y ver las ACL en archivos y directorios del sistema. Cuando se crea un nuevo archivo o subdirectorio en un directorio que tiene una ACL, el nuevo archivo o subdirectorio hereda todas las entradas de ACL (ACE) de la ACL que se han etiquetado con los indicadores de herencia correspondientes.

Cuando se crea un archivo o un directorio como resultado de una solicitud de NFSv4, la ACL del archivo o directorio resultante depende de si la solicitud de creación de archivos incluye una ACL o solo permisos de acceso estándar a archivos UNIX y si el directorio principal tiene una ACL:

- Si la solicitud incluye una ACL, se utiliza esa ACL.
- Si la solicitud incluye sólo permisos de acceso estándar a archivos UNIX pero el directorio principal tiene una ACL, el archivo o directorio nuevos heredan los ACE de la ACL del directorio principal siempre que se hayan etiquetado los ACE con los indicadores de herencia correspondientes.



Una ACL primaria se hereda aunque `-v4.0-acl` se establece en `off`.

- Si la solicitud incluye sólo permisos de acceso estándar a archivos UNIX y el directorio principal no tiene una ACL, el modo de archivo de cliente se utiliza para establecer permisos de acceso estándar a archivos UNIX.
- Si la solicitud incluye sólo permisos de acceso estándar a archivos UNIX y el directorio primario tiene una ACL no heredable, el nuevo objeto se crea sólo con bits de modo.



Si la `-chown-mode` el parámetro se ha establecido en `restricted` con comandos en la `vserver nfs 0.vserver export-policy rule` Las familias, la propiedad de los archivos solo puede cambiarla el superusuario, incluso si los permisos de disco establecidos con ACL de NFSv4 permiten que un usuario no raíz cambie la propiedad del archivo. Para obtener más información, consulte las páginas de manual correspondientes.

Habilite o deshabilite la modificación de ACL de NFSv4

Cuando ONTAP recibe un `chmod` Comando para un archivo o directorio con una ACL, de forma predeterminada se conserva y se modifica la ACL para reflejar el cambio de bits de modo. Puede deshabilitar el `-v4-acl-preserve` Parámetro para cambiar el comportamiento si desea que se corte la ACL en su lugar.

Acerca de esta tarea

Cuando se utiliza un estilo de seguridad unificado, este parámetro también especifica si los permisos de archivo NTFS se conservan o se borran cuando un cliente envía un comando `chmod`, `chgroup` o `chown` para un archivo o directorio.

El valor predeterminado de este parámetro es `Enabled`.

Pasos

1. Configure el nivel de privilegio en `Advanced`:

```
set -privilege advanced
```

2. Ejecute una de las siguientes acciones:

| Si desea... | Introduzca el siguiente comando... |
|---|--|
| Habilitación de la retención y modificación de las ACL de NFSv4 existentes (predeterminado) | <pre>vserver nfs modify -vserver vserver_name -v4-acl -preserve enabled</pre> |
| Deshabilite la retención y borre las ACL de NFSv4 cuando cambie los bits de modo | <pre>vserver nfs modify -vserver vserver_name -v4-acl -preserve disabled</pre> |

3. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

Cómo utiliza ONTAP las ACL de NFSv4 para determinar si pueden eliminar un archivo

Para determinar si puede eliminar un archivo, ONTAP utiliza una combinación del bit `DE ELIMINACIÓN` del archivo y el bit `DELETE_CHILD` del directorio que lo contiene. Para obtener más información, consulte `NFS 4.1 RFC 5661`.

Habilite o deshabilite las ACL de NFSv4

Para habilitar o deshabilitar las ACL de NFSv4, puede modificar las `-v4.0-acl` y..

`-v4.1-acl` opciones. Estas opciones están desactivadas de forma predeterminada.

Acerca de esta tarea

La `-v4.0-acl` o. `-v4.1-acl` La opción controla la configuración y la visualización de ACL de NFSv4; no controla la aplicación de estas ACL para la comprobación de acceso.

Paso

1. Ejecute una de las siguientes acciones:

| Si desea... | Realice lo siguiente... |
|---------------------------------|--|
| Habilitar ACL de NFSv4.0 | Introduzca el siguiente comando: <pre>vserver nfs modify -vserver vserver_name -v4.0-acl enabled</pre> |
| Desactive las ACL de NFSv4.0 | Introduzca el siguiente comando: <pre>vserver nfs modify -vserver vserver_name -v4.0-acl disabled</pre> |
| Habilite las ACL de NFSv4.1 | Introduzca el siguiente comando: <pre>vserver nfs modify -vserver vserver_name -v4.1-acl enabled</pre> |
| Deshabilitar las ACL de NFSv4.1 | Introduzca el siguiente comando: <pre>vserver nfs modify -vserver vserver_name -v4.1-acl disabled</pre> |

Modifique el límite máximo de ACE para ACL de NFSv4

Puede modificar el número máximo de ACE permitidos para cada ACL de NFSv4 mediante la modificación del parámetro `-v4-acl-max-aces`. De forma predeterminada, el límite se establece en 400 ACE para cada ACL. El aumento de este límite puede ayudar a garantizar una correcta migración de datos con ACL que contengan más de 400 ACE en sistemas de almacenamiento que ejecuten ONTAP.

Acerca de esta tarea

Si aumenta este límite, el rendimiento de los clientes que acceden a archivos con ACL de NFSv4.

Pasos

1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Modifique el límite máximo de ACE para ACL de NFSv4:

```
vserver nfs modify -v4-acl-max-aces max_ace_limit
```

El rango válido de

max_ace_limit es 192 para 1024.

3. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

Gestione las delegaciones de archivos NFSv4

Habilite o deshabilite las delegaciones de archivos de lectura de NFSv4

Para habilitar o deshabilitar las delegaciones de archivos de lectura de NFSv4, puede modificar la `-v4.0-read-delegation` opción. Al activar las delegaciones de archivos de lectura, puede eliminar gran parte de la sobrecarga de mensajes asociada con la apertura y el cierre de archivos.

Acerca de esta tarea

De forma predeterminada, las delegaciones de archivos de lectura están deshabilitadas.

La desventaja de habilitar las delegaciones de archivos de lectura es que el servidor y sus clientes deben recuperar las delegaciones una vez que se reinicia o reinicia el servidor, se reinicia o reinicia un cliente o se produce una partición de red.

Paso

1. Ejecute una de las siguientes acciones:

| Si desea... | Realice lo siguiente... |
|--|---|
| Habilite las delegaciones de archivos de lectura de NFSv4 | Introduzca el siguiente comando: <pre>vserver nfs modify -vserver vserver_name -v4.0 -read-delegation enabled</pre> |
| Habilitar las delegaciones de archivos de lectura de NFSv4.1 | Introduzca el siguiente comando: + <pre>vserver nfs modify -vserver vserver_name -v4.1 -read-delegation enabled</pre> |
| Deshabilite las delegaciones de archivos de lectura de NFSv4 | Introduzca el siguiente comando: <pre>vserver nfs modify -vserver vserver_name -v4.0 -read-delegation disabled</pre> |

| | |
|---|---|
| Deshabilitar las delegaciones de archivos de lectura de NFSv4.1 | <p>Introduzca el siguiente comando:</p> <pre>vserver nfs modify -vserver vserver_name -v4.1 -read-delegation disabled</pre> |
|---|---|

Resultado

Las opciones de delegación de archivos surten efecto tan pronto como se cambien. No es necesario reiniciar o reiniciar NFS.

Habilite o deshabilite las delegaciones de archivos de escritura de NFSv4

Para habilitar o deshabilitar las delegaciones de archivos de escritura, puede modificar la `-v4.0-write-delegation` opción. Al habilitar las delegaciones de archivos de escritura, puede eliminar gran parte de la sobrecarga de mensajes asociada con el bloqueo de archivos y registros, además de abrir y cerrar archivos.

Acerca de esta tarea

De forma predeterminada, las delegaciones de archivos de escritura están deshabilitadas.

La desventaja de habilitar las delegaciones de archivos de escritura es que el servidor y sus clientes deben realizar tareas adicionales para recuperar delegaciones una vez que se reinicia o reinicia el servidor, un cliente se reinicia o reinicia, o se produce una partición de red.

Paso

1. Ejecute una de las siguientes acciones:

| Si desea... | Realice lo siguiente... |
|---|---|
| Habilite las delegaciones de archivos de escritura de NFSv4 | Introduzca el siguiente comando: <pre>vserver nfs modify -vserver vserver_name -v4.0 -write-delegation enabled</pre> |
| Habilite las delegaciones de archivos de escritura de NFSv4.1 | Introduzca el siguiente comando: <pre>vserver nfs modify -vserver vserver_name -v4.1 -write-delegation enabled</pre> |
| Deshabilite las delegaciones de archivos de escritura de NFSv4 | Introduzca el siguiente comando: <pre>vserver nfs modify -vserver vserver_name -v4.0 -write-delegation disabled</pre> |
| Deshabilitar las delegaciones de archivos de escritura de NFSv4.1 | Introduzca el siguiente comando: <pre>vserver nfs modify -vserver vserver_name -v4.1 -write-delegation disabled</pre> |

Resultado

Las opciones de delegación de archivos surten efecto tan pronto como se cambien. No es necesario reiniciar o reiniciar NFS.

Configure el bloqueo de archivos y registros de NFSv4

Acerca del bloqueo de archivos y registros de NFSv4

En el caso de los clientes NFSv4, ONTAP admite el mecanismo de bloqueo de archivos NFSv4 y mantiene el estado de todos los bloqueos de archivos bajo un modelo basado en arrendamiento.

["Informe técnico de NetApp 3580: Guía de mejoras y prácticas recomendadas de NFSv4: Implementación de Data ONTAP"](#)

Especifique el período de concesión de bloqueo de NFSv4

Para especificar el período de concesión del bloqueo de NFSv4 (es decir, el período de tiempo en el que ONTAP concede irrevocablemente un bloqueo a un cliente), puede modificar el `-v4-lease-seconds` opción. Los periodos de concesión más breves aceleran la recuperación del servidor, a la vez que los periodos de concesión más largos son beneficiosos para los servidores que gestionan una gran cantidad de clientes.

Acerca de esta tarea

De forma predeterminada, esta opción se establece en 30. El valor mínimo para esta opción es 10. El valor máximo para esta opción es el período de gracia de bloqueo, que se puede establecer con `locking.lease_seconds` opción.

Pasos

1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Introduzca el siguiente comando:

```
vserver nfs modify -vserver vserver_name -v4-lease-seconds number_of_seconds
```

3. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

Especifique el período de gracia de bloqueo de NFSv4

Para especificar el período de gracia de bloqueo de NFSv4 (es decir, el período de tiempo en el que los clientes intentan reclamar su estado de bloqueo de ONTAP durante la recuperación del servidor), puede modificar el `-v4-grace-seconds` opción.

Acerca de esta tarea

De forma predeterminada, esta opción se establece en 45.

Pasos

1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Introduzca el siguiente comando:

```
vserver nfs modify -vserver vserver_name -v4-grace-seconds number_of_seconds
```

3. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

Cómo funcionan las referencias de NFSv4

Al activar las referencias de NFSv4, ONTAP proporciona referencias «intra-SVM» a los clientes de NFSv4. La referencia dentro de SVM se produce cuando un nodo de clúster que recibe la solicitud NFSv4 hace referencia al cliente NFSv4 a otra interfaz lógica (LIF) de la máquina virtual de almacenamiento (SVM).

El cliente NFSv4 debe acceder a la ruta que ha recibido la referencia en la LIF de destino desde ese punto. El nodo de clúster original proporciona una referencia de este tipo cuando determina que hay una LIF en la SVM que reside en el nodo de clúster en el que reside el volumen de datos, lo cual permite que los clientes accedan más rápido a los datos y eviten una comunicación adicional del clúster.

Habilite o deshabilite las referencias de NFSv4

Puede habilitar las referencias de NFSv4 en máquinas virtuales de almacenamiento (SVM) mediante las opciones `-v4-fsid-change` y.. `-v4.0-referrals`so.. La habilitación de las referencias A NFSV4 puede resultar en un acceso más rápido a los datos para los clientes de NFSv4 que admiten esta función.

Lo que necesitará

Si desea habilitar las referencias NFS, primero debe deshabilitar NFS paralelo. No puede habilitar ambos a la vez.

Pasos

1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Ejecute una de las siguientes acciones:

| Si desea... | Introduzca el comando... |
|-----------------------------------|---|
| Habilite las referencias de NFSv4 | <pre>vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.0-referrals enabled</pre> |
| Desactive las referencias a NFSv4 | <pre>vserver nfs modify -vserver vserver_name -v4.0 -referrals disabled</pre> |

| | |
|---|---|
| Activar NFSv4,1 referencias | <code>vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.1-referrals enabled</code> |
| Deshabilitar las referencias de NFSv4.1 | <code>vserver nfs modify -vserver vserver_name -v4.1 -referrals disabled</code> |

3. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

Muestra las estadísticas de NFS

Puede mostrar estadísticas de NFS de las máquinas virtuales de almacenamiento (SVM) en el sistema de almacenamiento para supervisar el rendimiento y diagnosticar problemas.

Pasos

1. Utilice la `statistics catalog object show` Comando para identificar los objetos NFS desde los que se pueden ver datos.

```
statistics catalog object show -object nfs*
```

2. Utilice la `statistics start` y opcional `statistics stop` comandos para recoger un ejemplo de datos de uno o más objetos.
3. Utilice la `statistics show` para ver los datos de ejemplo.

Ejemplo: Supervisión del rendimiento de NFSv3

El siguiente ejemplo muestra datos de rendimiento para el protocolo NFSv3.

El siguiente comando inicia la recogida de datos de una nueva muestra:

```
vs1::> statistics start -object nfsv3 -sample-id nfs_sample
```

El siguiente comando muestra datos de la muestra especificando contadores que muestran el número de solicitudes de lectura y escritura correctas, en comparación con el número total de solicitudes de lectura y escritura:

```
vs1::> statistics show -sample-id nfs_sample -counter  
read_total|write_total|read_success|write_success
```

```
Object: nfsv3  
Instance: vs1  
Start-time: 2/11/2013 15:38:29  
End-time: 2/11/2013 15:38:41  
Cluster: cluster1
```

| Counter | Value |
|---------------|---------|
| read_success | 40042 |
| read_total | 40042 |
| write_success | 1492052 |
| write_total | 1492052 |

Información relacionada

["Configuración de supervisión del rendimiento"](#)

Mostrar las estadísticas de DNS

Puede mostrar estadísticas de DNS para las máquinas virtuales de almacenamiento (SVM) en el sistema de almacenamiento para supervisar el rendimiento y diagnosticar problemas.

Pasos

1. Utilice la `statistics catalog object show` Comando para identificar los objetos DNS desde los que puede ver datos.

```
statistics catalog object show -object external_service_op*
```

2. Utilice la `statistics start` y `statistics stop` comandos para recoger un ejemplo de datos de uno o más objetos.
3. Utilice la `statistics show` para ver los datos de ejemplo.

Supervisar las estadísticas de DNS

Los siguientes ejemplos muestran datos de rendimiento para las consultas DNS. Los siguientes comandos inician la recopilación de datos de una nueva muestra:

```
vs1::*> statistics start -object external_service_op -sample-id  
dns_sample1  
vs1::*> statistics start -object external_service_op_error -sample-id  
dns_sample2
```

El siguiente comando muestra datos de la muestra especificando contadores que muestran el número de

consultas DNS enviadas en comparación con el número de consultas DNS recibidas, con errores o con tiempo de espera agotado:

```
vs1::*> statistics show -sample-id dns_sample1 -counter
num_requests_sent|num_responses_received|num_successful_responses|num_time
outs|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:DNS:Query:10.72.219.109
Start-time: 3/8/2016 11:15:21
End-time: 3/8/2016 11:16:52
Elapsed-time: 91s
Scope: vs1
```

| Counter | Value |
|--------------------------|-------|
| num_not_found_responses | 0 |
| num_request_failures | 0 |
| num_requests_sent | 1 |
| num_responses_received | 1 |
| num_successful_responses | 1 |
| num_timeouts | 0 |

6 entries were displayed.

El siguiente comando muestra los datos de la muestra especificando contadores que muestran el número de veces que se recibió un error específico para una consulta DNS en el servidor concreto:

```
vs1::*> statistics show -sample-id dns_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:DNS:Query:NXDOMAIN:10.72.219.109
Start-time: 3/8/2016 11:23:21
End-time: 3/8/2016 11:24:25
Elapsed-time: 64s
Scope: vs1
```

| Counter | Value |
|-------------------|---------------|
| count | 1 |
| error_string | NXDOMAIN |
| server_ip_address | 10.72.219.109 |

3 entries were displayed.

Información relacionada

Mostrar estadísticas NIS

Puede mostrar estadísticas de NIS para las máquinas virtuales de almacenamiento (SVM) en el sistema de almacenamiento para supervisar el rendimiento y diagnosticar problemas.

Pasos

1. Utilice la `statistics catalog object show` Comando para identificar los objetos NIS desde los que puede ver datos.

```
statistics catalog object show -object external_service_op*
```

2. Utilice la `statistics start` y `statistics stop` comandos para recoger un ejemplo de datos de uno o más objetos.
3. Utilice la `statistics show` para ver los datos de ejemplo.

Seguimiento de las estadísticas de NIS

Los siguientes ejemplos muestran datos de rendimiento para consultas NIS. Los siguientes comandos inician la recopilación de datos de una nueva muestra:

```
vs1::*> statistics start -object external_service_op -sample-id  
nis_sample1  
vs1::*> statistics start -object external_service_op_error -sample-id  
nis_sample2
```

El siguiente comando muestra los datos de la muestra especificando contadores que muestran el número de consultas NIS enviadas en comparación con el número de consultas NIS recibidas, fallidas o con el tiempo de espera agotado:

```
vs1::*> statistics show -sample-id nis_sample1 -counter
instance|num_requests_sent|num_responses_received|num_successful_responses
|num_timeouts|num_request_failures|num_not_found_responses
```

```
Object: external_service_op
Instance: vs1:NIS:Query:10.227.13.221
Start-time: 3/8/2016 11:27:39
End-time: 3/8/2016 11:27:56
Elapsed-time: 17s
Scope: vs1
```

| Counter | Value |
|--------------------------|-------|
| num_not_found_responses | 0 |
| num_request_failures | 1 |
| num_requests_sent | 2 |
| num_responses_received | 1 |
| num_successful_responses | 1 |
| num_timeouts | 0 |

6 entries were displayed.

El siguiente comando muestra los datos de la muestra especificando contadores que muestran el número de veces que se recibió un error específico para una consulta NIS en el servidor concreto:

```
vs1::*> statistics show -sample-id nis_sample2 -counter
server_ip_address|error_string|count
```

```
Object: external_service_op_error
Instance: vs1:NIS:Query:YP_NOTFOUND:10.227.13.221
Start-time: 3/8/2016 11:33:05
End-time: 3/8/2016 11:33:10
Elapsed-time: 5s
Scope: vs1
```

| Counter | Value |
|-------------------|---------------|
| count | 1 |
| error_string | YP_NOTFOUND |
| server_ip_address | 10.227.13.221 |

3 entries were displayed.

Información relacionada

["Configuración de supervisión del rendimiento"](#)

Compatibilidad con VMware vStorage sobre NFS

ONTAP admite ciertas funciones de VMware vStorage APIs for Array Integration (VAAI) en un entorno NFS.

Funciones admitidas

Se admiten las siguientes funciones:

- Descarga de copias

Permite que un host ESXi copie máquinas virtuales o discos de máquinas virtuales (VMDK) directamente entre la ubicación de almacén de datos de origen y destino sin implicar al host. Esto ahorra ciclos de CPU del host ESXi y ancho de banda de red. La descarga de copia preserva la eficiencia del espacio si el volumen de origen es escaso.

- Reserva de espacio

Garantiza espacio de almacenamiento para un archivo VMDK reservando espacio para él.

Limitaciones

VMware vStorage over NFS tiene las siguientes limitaciones:

- Las operaciones de descarga de copia pueden fallar en las siguientes situaciones:
 - Mientras se ejecuta waiflron en el volumen de origen o de destino porque desconecta temporalmente el volumen
 - Al mover el volumen de origen o el de destino
 - Al mover las LIF de origen o de destino
 - Al realizar operaciones de toma de control o devolución del retorno al nodo primario
 - Al mismo tiempo que realiza operaciones de conmutación de sitios o conmutación de estado
- La copia del servidor puede fallar debido a diferencias de formato de gestión de archivos en el siguiente escenario:

Se intentan copiar datos de las SVM que tienen actualmente o habían exportado qtrees anteriormente a las SVM que nunca han exportado qtrees. Para solucionar esta limitación, puede exportar al menos un qtree en la SVM de destino.

Información relacionada

["¿Qué operaciones de VAAI descargados son compatibles con Data ONTAP?"](#)

Activar o desactivar VMware vStorage over NFS

Puede habilitar o deshabilitar la compatibilidad de VMware vStorage sobre NFS en máquinas virtuales de almacenamiento (SVM) mediante el `vserver nfs modify` comando.

Acerca de esta tarea

De forma predeterminada, la compatibilidad con VMware vStorage over NFS está deshabilitada.

Pasos

1. Mostrar el estado actual de soporte de vStorage para las SVM:

```
vserver nfs show -vserver vserver_name -instance
```

2. Ejecute una de las siguientes acciones:

| Si desea... | Introduzca el siguiente comando... |
|--|--|
| Activar la compatibilidad con VMware vStorage | <pre>vserver nfs modify -vserver vserver_name -vstorage enabled</pre> |
| Desactivar la compatibilidad con VMware vStorage | <pre>vserver nfs modify -vserver vserver_name -vstorage disabled</pre> |

Después de terminar

Para poder utilizar esta funcionalidad, es necesario instalar el plugin de NFS para VMware VAAI. Para obtener más información, consulte *Installing the NetApp NFS Plug-in for VMware VAAI*.

Información relacionada

["Documentación de NetApp: Plugin de NetApp NFS para VMware VAAI"](#)

Activa o desactiva la compatibilidad con rquota

ONTAP admite la versión 1 del protocolo de cuota remota (rcupo v1). El protocolo rquota permite a los clientes NFS obtener información de cuotas para los usuarios desde una máquina remota. Puede habilitar rquota en máquinas virtuales de almacenamiento (SVM) mediante el `vserver nfs modify` comando.

Acerca de esta tarea

De forma predeterminada, rquota está desactivado.

Paso

1. Ejecute una de las siguientes acciones:

| Si desea... | Introduzca el siguiente comando... |
|---|---|
| Habilite la compatibilidad de rquota para SVM | <pre>vserver nfs modify -vserver vserver_name -rquota enable</pre> |
| Deshabilite el soporte rquota para SVM | <pre>vserver nfs modify -vserver vserver_name -rquota disable</pre> |

Para obtener más información acerca de las cuotas, consulte ["Gestión de almacenamiento lógico"](#).

Mejora del rendimiento de NFSv3 y NFSv4 mediante la modificación del tamaño de transferencia de TCP

Puede mejorar el rendimiento de los clientes NFSv3 y NFSv4 que se conectan a los sistemas de almacenamiento a través de una red de alta latencia al modificar el tamaño máximo de transferencia de TCP.

Cuando los clientes acceden a los sistemas de almacenamiento a través de una red de alta latencia, como una red de área extensa (WAN) o una red de área metropolitana (MAN) con una latencia superior a 10 milisegundos, es posible que pueda mejorar el rendimiento de la conexión modificando el tamaño máximo de transferencia de TCP. Los clientes que acceden a sistemas de almacenamiento en una red de baja latencia, como una red de área local (LAN), pueden esperar muy poco o ningún beneficio de la modificación de estos parámetros. Si la mejora del rendimiento no supera el impacto en la latencia, no debe usar estos parámetros.

Para determinar si su entorno de almacenamiento se beneficiaría de la modificación de estos parámetros, primero debe realizar una evaluación completa del rendimiento de un cliente NFS de bajo rendimiento. Revise si el bajo rendimiento se debe a una latencia excesiva de ida y vuelta y una solicitud pequeña en el cliente. En estas condiciones, el cliente y el servidor no pueden utilizar por completo el ancho de banda disponible porque gastan la mayoría de sus ciclos de servicio esperando a que pequeñas solicitudes y respuestas se transmitan a través de la conexión.

Al aumentar el tamaño de las solicitudes de NFSv3 y NFSv4, el cliente y el servidor pueden utilizar el ancho de banda disponible de forma más eficaz para mover más datos por unidad y, de este modo, aumentar la eficiencia general de la conexión.

Tenga en cuenta que la configuración entre el sistema de almacenamiento y el cliente puede variar. El sistema de almacenamiento y el cliente admiten un tamaño máximo de 1 MB para las operaciones de transferencia. Sin embargo, si configura el sistema de almacenamiento para que admita un tamaño de transferencia máximo de 1 MB pero el cliente solo admita 64 KB, el tamaño de transferencia de montaje estará limitado a 64 KB o menos.

Antes de modificar estos parámetros, debe tener en cuenta que genera un consumo adicional de memoria en el sistema de almacenamiento durante el período de tiempo necesario para ensamblar y transmitir una gran respuesta. Cuanto más conexiones de alta latencia tenga con el sistema de almacenamiento, mayor será el consumo de memoria adicional. Los sistemas de almacenamiento con una gran capacidad de memoria pueden experimentar un efecto muy reducido a partir de este cambio. Los sistemas de almacenamiento con baja capacidad de memoria pueden experimentar una degradación considerable del rendimiento.

El uso correcto de este parámetro depende de la capacidad de recuperar datos de varios nodos de un clúster. La latencia inherente de la red de clúster podría aumentar la latencia general de la respuesta. La latencia general tiende a aumentar cuando se usa estos parámetros. Como resultado, las cargas de trabajo sensibles a la latencia pueden mostrar un impacto negativo.

Modifique el tamaño de transferencia máximo de TCP de NFSv3 y NFSv4

Puede modificar el `-tcp-max-xfer-size` Opción de configurar los tamaños máximos de transferencia para todas las conexiones TCP mediante los protocolos NFSv3 y NFSv4.x.

Acerca de esta tarea

Puede modificar estas opciones de forma individual para cada máquina virtual de almacenamiento (SVM).

A partir de ONTAP 9, el `v3-tcp-max-read-size` y `v3-tcp-max-write-size` las opciones son

obsoletas. Debe utilizar el `-tcp-max-xfer-size` en su lugar.

Pasos

- 1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

- 2. Ejecute una de las siguientes acciones:

| Si desea... | Introduzca el comando... |
|---|--|
| Modifique el tamaño de transferencia máximo de TCP de NFSv3 o NFSv4 | <pre>vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer_max_xfer_size</pre> |

| Opción | Rango | Predeterminado |
|---------------------------------|-------------------------|----------------|
| <code>-tcp-max-xfer-size</code> | de 8192 a 1048576 bytes | 65536 bytes |



El tamaño de transferencia máximo introducido debe ser un múltiplo de 4 KB (4096 bytes). Las solicitudes que no están alineadas correctamente afectan negativamente al rendimiento.

- 3. Utilice la `vserver nfs show -fields tcp-max-xfer-size` comando para verificar los cambios.
- 4. Si alguno de los clientes utiliza montajes estáticos, desmonte y vuelva a montar para que el nuevo tamaño de parámetro entre en vigor.

Ejemplo

El siguiente comando establece el tamaño de transferencia máximo de TCP de NFSv3 y NFSv4.x en 1048576 bytes de la SVM llamada vs1:

```
vs1::> vserver nfs modify -vserver vs1 -tcp-max-xfer-size 1048576
```

Configure el número de ID de grupo permitidos para los usuarios NFS

De forma predeterminada, ONTAP admite hasta 32 identificadores de grupo al gestionar credenciales de usuario de NFS mediante la autenticación Kerberos (RPCSEC_GSS). Cuando se utiliza la autenticación AUTH_SYS, el número máximo predeterminado de ID de grupo es 16, tal como se define en RFC 5531. Puede aumentar el máximo hasta 1,024 si tiene usuarios que son miembros de más del número predeterminado de grupos.

Acerca de esta tarea

Si un usuario tiene más de la cantidad predeterminada de identificadores de grupo en sus credenciales, los ID de grupo restantes se truncan y el usuario podría recibir errores al intentar acceder a los archivos desde el sistema de almacenamiento. Debe establecer el número máximo de grupos, por SVM, en un número que represente los grupos máximos en su entorno.

En la siguiente tabla se muestran los dos parámetros del `vserver nfs modify` Comando que determina el número máximo de ID de grupo en tres configuraciones de ejemplo:

| Parámetros | Configuración | Límite de ID de grupo resultante |
|---------------------------|--|----------------------------------|
| -extended-groups-limit | 32 | RPCSEC_GSS: 32 |
| -auth-sys-extended-groups | disabled | AUTH_SYS: 16 |
| | Esta es la configuración predeterminada. | |
| -extended-groups-limit | 256 | RPCSEC_GSS: 256 |
| -auth-sys-extended-groups | disabled | AUTH_SYS: 16 |
| -extended-groups-limit | 512 | RPCSEC_GSS: 512 |
| -auth-sys-extended-groups | enabled | AUTH_SYS: 512 |

Pasos

1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Realice la acción deseada:

| | |
|---|---|
| Si desea establecer el número máximo de grupos auxiliares permitidos... | Introduzca el comando... |
| Sólo para RPCSEC_GSS y deje AUTH_SYS establecido en el valor predeterminado de 16 | <code>vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups disabled</code> |
| Para RPCSEC_GSS y AUTH_SYS | <code>vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups enabled</code> |

3. Compruebe el `-extended-groups-limit` Value y verifique si AUTH_SYS utiliza grupos extendidos:

```
vserver nfs show -vserver vserver_name -fields auth-sys-extended-groups,extended-groups-limit
```

4. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

Ejemplo

En el ejemplo siguiente se habilitan grupos extendidos para la autenticación AUTH_SYS y se establece el número máximo de grupos extendidos en 512 para la autenticación AUTH_SYS y RPCSEC_GSS. Estos cambios se realizan solo para los clientes que acceden al SVM denominado vs1:

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
        them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -auth-sys-extended-groups enabled
        -extended-groups-limit 512

vs1::*> vserver nfs show -vserver vs1 -fields auth-sys-extended-
        groups,extended-groups-limit
vserver auth-sys-extended-groups extended-groups-limit
-----
vs1      enabled                  512

vs1::*> set -privilege admin
```

Controlar el acceso de usuario raíz a datos de estilo de seguridad NTFS

Puede configurar ONTAP para permitir que los clientes NFS accedan a datos de estilo de seguridad NTFS y a clientes NTFS para acceder a los datos de estilo de seguridad NFS. Cuando se utiliza un estilo de seguridad NTFS en un almacén de datos NFS, se debe decidir cómo tratar el acceso por parte del usuario raíz y configurar la máquina virtual de almacenamiento (SVM) según corresponda.

Acerca de esta tarea

Cuando un usuario raíz accede a datos de estilo de seguridad NTFS, tiene dos opciones:

- Asignar el usuario raíz a un usuario de Windows como cualquier otro usuario NFS y gestionar el acceso según ACL de NTFS.
- Ignorar las ACL de NTFS y proporcionar acceso completo a la raíz.

Pasos

1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Realice la acción deseada:

| | |
|--|--|
| Si desea que el usuario raíz... | Introduzca el comando... |
| Estar asignado a un usuario de Windows | vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root disabled |

| | |
|-------------------------------------|---|
| Omitir la comprobación de ACL de NT | <code>vserver nfs modify -vserver vserver_name -ignore-nt-acl-for-root enabled</code> |
|-------------------------------------|---|

De manera predeterminada, este parámetro está deshabilitado.

Si este parámetro está habilitado pero no hay ninguna asignación de nombres para el usuario raíz, ONTAP utiliza una credencial de administrador de SMB predeterminada para la auditoría.

3. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

Admiten versiones y clientes NFS

Información general sobre las versiones y los clientes de NFS admitidos

Antes de poder utilizar NFS en la red, debe saber qué versiones de NFS y clientes admite ONTAP.

Esta tabla indica si las versiones de protocolo NFS principales y secundarias son compatibles de forma predeterminada con ONTAP. La compatibilidad de forma predeterminada no indica que esta es la versión más antigua de ONTAP compatible con ese protocolo NFS.

| Versión | Activado de forma predeterminada |
|---------|----------------------------------|
| NFSv3 | Sí |
| NFSv4,0 | Sí, a partir de ONTAP 9.9.1 |
| NFSv4,1 | Sí, a partir de ONTAP 9.9.1 |
| NFSv4,2 | Sí, a partir de ONTAP 9.9.1 |
| PNFs | No |

Para obtener la información más reciente sobre la compatibilidad con ONTAP para clientes NFS, consulte la matriz de interoperabilidad.

["Herramienta de matriz de interoperabilidad de NetApp"](#)

Funcionalidad NFSv4.0 compatible con ONTAP

ONTAP admite todas las funciones obligatorias de NFSv4.0 excepto los mecanismos de seguridad SPKM3 y LIPKEY.

Se admiten las siguientes funciones DE NFSV4:

- **COMPUESTO**

Permite a un cliente solicitar varias operaciones de archivo en una única solicitud de llamada a procedimiento remoto (RPC).

- **Delegación de archivos**

Permite al servidor delegar el control de archivos en algunos tipos de clientes para el acceso de lectura y escritura.

- **Pseudofs**

Los servidores NFSv4 los utilizan para determinar los puntos de montaje del sistema de almacenamiento. No existe ningún protocolo de montaje en NFSv4.

- **Bloqueo**

Basado en arrendamiento. No hay protocolos NLM (Network Lock Manager) o NSM (Network Status Monitor) separados en NFSv4.

Para obtener más información acerca del protocolo NFSv4.0, consulte RFC 3530.

Limitaciones del soporte de ONTAP para NFSv4

Debe conocer varias limitaciones del soporte de ONTAP para NFSv4.

- La función de delegación no es compatible con todos los tipos de cliente.
- En ONTAP 9.4 y versiones anteriores, el sistema de almacenamiento rechaza los nombres con caracteres no ASCII en volúmenes distintos a UTF8.

En ONTAP 9.5 y versiones posteriores, los volúmenes creados con la configuración de idioma utf8mb4 y montados con NFS v4 ya no están sujetos a esta restricción.

- Todos los identificadores de archivos son persistentes; el servidor no proporciona identificadores de archivos volátiles.
- No se admiten la migración ni la replicación.
- Los clientes NFSv4 no son compatibles con los reflejos de uso compartido de carga de solo lectura.

ONTAP enruta los clientes NFSv4 al origen de la duplicación de uso compartido de la carga para obtener acceso directo de lectura y escritura.

- No se admiten los atributos con nombre.
- Se admiten todos los atributos recomendados, excepto los siguientes:

- `archive`
- `hidden`
- `homogeneous`
- `mimetype`
- `quota_avail_hard`
- `quota_avail_soft`
- `quota_used`

- ° `system`
- ° `time_backup`



Aunque no es compatible con `quota*` Atributos, ONTAP admite cuotas de usuario y grupo a través del protocolo de banda lateral RQUOTA.

Compatibilidad de ONTAP con NFSv4.1

A partir de ONTAP 9.8, la funcionalidad `nconnect` está disponible de forma predeterminada con NFSv4.1 habilitado.

En las implementaciones anteriores de clientes NFS solo se utiliza una única conexión TCP con un montaje. En ONTAP, una única conexión TCP puede convertirse en un cuello de botella que aumenta las IOPS. Sin embargo, un cliente habilitado para `nconnect` puede tener varias conexiones TCP (hasta 16) asociadas a un único montaje NFS. Este cliente NFS multiplicará las operaciones de ficheros en varias conexiones TCP por turno rotatorio y obtendrá así un mayor rendimiento del ancho de banda de red disponible. NConnect solo se recomienda para montajes NFSv3 y NFSv4.1.

Consulte su documentación de cliente NFS para confirmar si `nconnect` es compatible con su versión de cliente.

NFSv4.1 está habilitado de forma predeterminada en ONTAP 9.9.1 y versiones posteriores. En las versiones anteriores, puede habilitarla mediante el uso de `-v4.1` y establecerla en `enabled` Al crear un servidor NFS en la máquina virtual de almacenamiento (SVM).

ONTAP no es compatible con las delegaciones a nivel de archivo y directorio de NFSv4.1.

Compatibilidad con ONTAP para NFSv4.2

A partir de ONTAP 9.8, ONTAP admite el protocolo NFSv4,2 para permitir acceso a clientes habilitados para NFSv4,2.

NFSv4.2 está habilitado de forma predeterminada en ONTAP 9.9.1 y posteriores. En ONTAP 9.8, debe habilitar manualmente `v4,2` especificando el `-v4.1` y establecerla en `enabled` Al crear un servidor NFS en la máquina virtual de almacenamiento (SVM). Al habilitar NFSv4.1, los clientes también pueden utilizar las funciones de NFSv4.1 mientras están montados como `v4.2`.

Las versiones sucesivas de ONTAP amplían la compatibilidad de NFSv4,2 funciones opcionales.

| Empezando por... | NFSv4,2 características opcionales incluyen... |
|------------------|---|
| ONTAP 9.12.1 | <ul style="list-style-type: none"> • Atributos NFS extendidos • Archivos dispersos • Reservas de espacio |
| ONTAP 9.9.1 | El control de acceso obligatorio (MAC) tiene la etiqueta NFS |

Etiquetas de seguridad de NFS v4,2

A partir de ONTAP 9.9.1, se pueden habilitar las etiquetas de seguridad NFS. Están desactivadas de forma predeterminada.

Con etiquetas de seguridad NFS v4.2, los servidores NFS de ONTAP tienen en cuenta el control de acceso obligatorio (MAC), al almacenar y recuperar atributos `sec_label` enviados por los clientes.

Para obtener más información, consulte ["RFC 7240"](#).

A partir de ONTAP 9.12.1, las etiquetas de seguridad v4.2 de NFS son compatibles con las operaciones de volcado NDMP. Si las etiquetas de seguridad se encuentran en archivos o directorios en versiones anteriores, el volcado falla.

Pasos

1. Cambie la configuración del privilegio a avanzado:

```
set -privilege advanced
```

2. Habilitar etiquetas de seguridad:

```
vserver nfs modify -vserver _svm_name_ -v4.2-seclabel enabled
```

Atributos NFS extendidos

A partir de ONTAP 9.12.1, los atributos extendidos de NFS (xattrs) están habilitados de forma predeterminada.

Los atributos extendidos son los atributos NFS estándar definidos por ["RFC 8276"](#) Y se habilita en los clientes NFS actuales. Se pueden utilizar para adjuntar metadatos definidos por el usuario a objetos del sistema de archivos, y son de interés en implementaciones de seguridad avanzadas.

Los atributos extendidos de NFS no se admiten actualmente para las operaciones de volcado de NDMP. Si se encuentran atributos extendidos en archivos o directorios, el volcado se realiza pero no realiza una copia de seguridad de los atributos extendidos en esos archivos o directorios.

Si necesita desactivar atributos extendidos, utilice `vserver nfs modify -v4.2-xattrs disabled` comando.

Compatibilidad con ONTAP para NFS paralelo

ONTAP es compatible con NFS paralelo (pNFS). El protocolo pNFS ofrece mejoras en el rendimiento al proporcionar a los clientes acceso directo a los datos de un conjunto de archivos distribuidos por varios nodos de un clúster. Ayuda a los clientes a localizar la ruta óptima para un volumen.

Uso de soportes duros

Al solucionar los problemas de montaje, debe asegurarse de utilizar el tipo de montaje correcto. NFS admite dos tipos de montaje: Montajes soft y montajes hard. Solo debe

utilizar montajes hard por motivos de fiabilidad.

No debería utilizar montajes soft, especialmente cuando hay una posibilidad de tiempos de espera de NFS frecuentes. Las condiciones de carrera pueden producirse como resultado de estos tiempos de espera, que pueden provocar daños en los datos.

Dependencias de nomenclatura de archivos y directorios NFS y SMB

Información general sobre las dependencias de nomenclatura de archivos y directorios de NFS y SMB

Las convenciones de nomenclatura de archivos y directorios dependen tanto de los sistemas operativos de los clientes de red como de los protocolos de uso compartido de archivos, además de la configuración de idioma del clúster ONTAP y de los clientes.

El sistema operativo y los protocolos de uso compartido de archivos determinan lo siguiente:

- Caracteres que puede utilizar un nombre de archivo
- Distinción entre mayúsculas y minúsculas de un nombre de archivo

ONTAP admite caracteres de varios bytes en nombres de archivos, directorios y qtrees, según la versión de ONTAP.

Caracteres que puede utilizar un nombre de archivo o directorio

Si accede a un archivo o directorio desde clientes con sistemas operativos diferentes, debe utilizar caracteres válidos en ambos sistemas operativos.

Por ejemplo, si utiliza UNIX para crear un archivo o directorio, no utilice dos puntos (:) en el nombre porque no se permiten dos puntos en los nombres de archivos o directorios de MS-dos. Debido a que las restricciones de caracteres válidos varían de un sistema operativo a otro, consulte la documentación del sistema operativo cliente para obtener más información acerca de los caracteres prohibidos.

Distinción entre mayúsculas y minúsculas de nombres de archivos y directorios en un entorno multiprotocolo

Los nombres de archivo y directorio distinguen mayúsculas y minúsculas para los clientes NFS y no distinguen entre mayúsculas y minúsculas, pero sí lo hacen para los clientes SMB. Debe comprender las implicaciones que tiene en un entorno multiprotocolo y las acciones que podría tener que tomar al especificar la ruta al crear recursos compartidos de SMB y al acceder a datos dentro de los recursos compartidos.

Si un cliente SMB crea un directorio llamado `testdir`, Tanto los clientes SMB como NFS muestran el nombre de archivo como `testdir`. Sin embargo, si un usuario SMB posteriormente intenta crear un nombre de directorio `TESTDIR`, El nombre no está permitido porque, para el cliente SMB, ese nombre existe actualmente. Si un usuario NFS crea más adelante un directorio llamado `TESTDIR`, Los clientes NFS y SMB muestran el nombre del directorio de forma diferente, de la siguiente manera:

- En los clientes NFS, se ven los dos nombres de directorio tal como se crearon, por ejemplo `testdir` y `TESTDIR`, porque los nombres de directorio distinguen entre mayúsculas y minúsculas.
- Los clientes SMB utilizan los nombres 8.3 para distinguir entre los dos directorios. Un directorio tiene el nombre del archivo base. A directorios adicionales se les asigna un nombre de archivo 8.3.

- En los clientes SMB, consulte `testdir` y.. `TESTDI~1`.
- ONTAP creará el `TESTDI~1` nombre de directorio para diferenciar los dos directorios.

En este caso, debe usar el nombre 8.3 al especificar una ruta de recurso compartido mientras crea o modifica un recurso compartido en una máquina virtual de almacenamiento (SVM).

Del mismo modo para los archivos, si un cliente SMB crea `test.txt`, Tanto los clientes SMB como NFS muestran el nombre de archivo como `test.txt`. Sin embargo, si un usuario SMB posteriormente intenta crear `Test.txt`, El nombre no está permitido porque, para el cliente SMB, ese nombre existe actualmente. Si más adelante un usuario NFS crea un archivo llamado `Test.txt`, Los clientes NFS y SMB muestran el nombre del archivo de forma diferente, de la siguiente manera:

- En los clientes NFS, se ven los dos nombres de archivo tal como se crearon, `test.txt` y.. `Test.txt`, porque los nombres de archivo distinguen entre mayúsculas y minúsculas.
- Los clientes SMB utilizan los nombres 8.3 para distinguir entre los dos archivos. Un archivo tiene el nombre del archivo base. Se asigna un nombre de archivo 8.3 a archivos adicionales.
 - En los clientes SMB, consulte `test.txt` y.. `TEST~1.TXT`.
 - ONTAP creará el `TEST~1.TXT` nombre de archivo para diferenciar los dos archivos.



Si se ha creado una asignación de caracteres con los comandos de asignación de caracteres CIFS de Vserver, una búsqueda de Windows que normalmente no distingue entre mayúsculas y minúsculas puede distinguir entre mayúsculas y minúsculas. Esto significa que las búsquedas de nombre de archivo solo serán sensibles a mayúsculas/minúsculas si se ha creado la asignación de caracteres y el nombre de archivo está utilizando esa asignación de caracteres.

Cómo crea ONTAP nombres de archivos y directorios

ONTAP crea y mantiene dos nombres para archivos o directorios en cualquier directorio que tenga acceso desde un cliente SMB: El nombre largo original y un nombre en formato 8.3.

Para los nombres de archivos o directorios que excedan el nombre de ocho caracteres o el límite de extensión de tres caracteres (para archivos), ONTAP genera un nombre de formato de 8.3 de la siguiente manera:

- Trunca el nombre del archivo o directorio original a seis caracteres, si el nombre supera los seis.
- Agrega una tilde (~) y un número, de uno a cinco, a los nombres de archivo o directorio que ya no son únicos después de truncarse.

Si se queda sin números porque hay más de cinco nombres similares, crea un nombre único que no tiene relación con el nombre original.

- En el caso de los archivos, trunca la extensión del nombre de archivo a tres caracteres.

Por ejemplo, si un cliente NFS crea un archivo llamado `specifications.html`, El nombre de archivo de formato 8.3 creado por ONTAP es `specif~1.htm`. Si este nombre ya existe, ONTAP utiliza un número diferente al final del nombre de archivo. Por ejemplo, si un cliente NFS crea otro archivo llamado `specifications_new.html`, el formato 8.3 de `specifications_new.html` es `specif~2.htm`.

Cómo maneja ONTAP los nombres de archivos, directorios y qtrees de varios bytes

A partir de ONTAP 9.5, la compatibilidad con nombres codificados UTF-8 de 4 bytes permite la creación y visualización de nombres de archivos, directorios y árboles que incluyen caracteres complementarios Unicode fuera del plano multilingüe básico (BMP). En las versiones anteriores, estos caracteres complementarios no se mostraba correctamente en entornos multiprotocolo.

Para habilitar la compatibilidad con nombres codificados UTF-8 de 4 bytes, hay disponible un nuevo código de idioma *utf8mb4* para *vserver* y.. *volume* familias de comando.

- Debe crear un nuevo volumen de una de las siguientes maneras:
- Configuración del volumen `-language` opción explícitamente:

```
volume create -language utf8mb4 {...}
```

- Heredar el volumen `-language` Opción de una SVM que se ha creado con la opción o que se ha modificado para ella:

```
vserver [create|modify] -language utf8mb4 {...}``volume create {...}
```

- Si utiliza ONTAP 9,6 y versiones anteriores, no podrá modificar los volúmenes existentes para admitir *utf8mb4*; debe crear un nuevo volumen listo para *utf8mb4* y después migrar los datos con las herramientas de copia basadas en cliente.

Si utiliza ONTAP 9.7P1 o una versión posterior, puede modificar los volúmenes existentes para *utf8mb4* con una solicitud de soporte. Para obtener más información, consulte "[¿Se puede cambiar el idioma del volumen después de crearlo en ONTAP?](#)".

Puede actualizar las SVM para que admitan *utf8mb4*, pero los volúmenes existentes conservan sus códigos de idioma originales.



Los nombres de las LUN con caracteres UTF-8 de 4 bytes no se admiten actualmente.

- Los datos de caracteres Unicode se suelen representar en aplicaciones de sistemas de archivos Windows que utilizan el formato de transformación Unicode de 16 bits (UTF-16) y en sistemas de archivos NFS que utilizan el formato de transformación Unicode de 8 bits (UTF-8).

En las versiones anteriores a ONTAP 9.5, los nombres incluidos los caracteres complementarios UTF-16 creados por los clientes de Windows se mostraban correctamente a otros clientes de Windows pero no se tradujeron correctamente a UTF-8 para los clientes NFS. Del mismo modo, los nombres con caracteres complementarios UTF-8 de los clientes NFS creados no se tradujeron correctamente a UTF-16 para los clientes Windows.

- Cuando se crean nombres de archivo en sistemas que ejecutan ONTAP 9.4 o una versión anterior que contienen caracteres complementarios válidos o no válidos, ONTAP rechaza el nombre de archivo y devuelve un error de nombre de archivo no válido.

Para evitar este problema, utilice sólo los caracteres BMP en los nombres de archivo y evite utilizar caracteres complementarios, o actualice a ONTAP 9.5 o posterior.

Se permiten caracteres Unicode en nombres de qtree.

- Puede utilizar cualquiera de los dos `volume qtree` Familia de comandos o System Manager para establecer o modificar los nombres de qtree.
- Los nombres de qtree pueden incluir caracteres de varios bytes en formato Unicode, como los caracteres japoneses y chinos.
- En versiones anteriores a ONTAP 9.5, sólo se admiten los caracteres BMP (es decir, los que podrían representarse en 3 bytes).



En las versiones anteriores a ONTAP 9.5, la ruta de unión del volumen principal del qtree puede contener nombres de qtree y directorio con caracteres Unicode. La `volume show` El comando muestra estos nombres correctamente cuando el volumen primario tiene una configuración de idioma UTF-8. Sin embargo, si el idioma del volumen principal no es uno de los valores de idioma UTF-8, algunas partes de la ruta de unión se muestran utilizando un nombre NFS alternativo numérico.

- En las versiones 9.5 y posteriores, se admiten caracteres de 4 bytes en nombres de qtree, siempre y cuando el qtree se encuentre en un volumen habilitado para utf8mb4.

Configurar la asignación de caracteres para la traducción de nombres de archivo SMB en volúmenes

Los clientes NFS pueden crear nombres de archivo que contengan caracteres que no son válidos para los clientes SMB y ciertas aplicaciones Windows. Puede configurar la asignación de caracteres para la traducción de nombres de archivo en volúmenes para permitir que los clientes SMB accedan a archivos con nombres NFS que, de lo contrario, no serían válidos.

Acerca de esta tarea

Cuando los clientes SMB acceden a los archivos creados por los clientes NFS, ONTAP observa el nombre del archivo. Si el nombre no es un nombre de archivo SMB válido (por ejemplo, si tiene un carácter ":" incrustado en dos puntos), ONTAP devuelve el nombre de archivo 8.3 que se mantiene para cada archivo. Sin embargo, esto causa problemas para las aplicaciones que codifican información importante en nombres de archivos largos.

Por lo tanto, si comparte un archivo entre clientes en diferentes sistemas operativos, debe utilizar caracteres en los nombres de archivo válidos en ambos sistemas operativos.

Sin embargo, si tiene clientes NFS que crean nombres de archivo que contienen caracteres que no son nombres de archivo válidos para clientes SMB, puede definir un mapa que convierte los caracteres NFS no válidos en caracteres Unicode que tanto SMB como determinadas aplicaciones Windows aceptan. Por ejemplo, esta funcionalidad admite las aplicaciones CATIA MCAD y Mathematica, así como otras aplicaciones que tienen este requisito.

Puede configurar la asignación de caracteres de volumen a volumen.

Debe tener en cuenta lo siguiente al configurar la asignación de caracteres en un volumen:

- La asignación de caracteres no se aplica a través de puntos de unión.

Debe configurar explícitamente la asignación de caracteres para cada volumen de unión.

- Debe asegurarse de que los caracteres Unicode que se utilizan para representar caracteres no válidos o ilegales son caracteres que normalmente no aparecen en los nombres de archivo; de lo contrario, se producen asignaciones no deseadas.

Por ejemplo, si intenta asignar dos puntos (:) a un guión (-) pero el guión (-) se utilizó correctamente en el nombre del archivo, un cliente de Windows que intente acceder a un archivo denominado «'a-b'» tendría su solicitud asignada al nombre NFS de «'a:b'» (no al resultado deseado).

- Después de aplicar la asignación de caracteres, si la asignación aún contiene un carácter de Windows no válido, ONTAP vuelve a los nombres de archivo de Windows 8.3.
- En las notificaciones de FPolicy, los registros de auditoría de NAS y los mensajes de seguimiento de seguridad, se muestran los nombres de archivos asignados.
- Cuando se crea una relación de SnapMirror del tipo DP, la asignación de caracteres del volumen de origen no se replica en el volumen de DP de destino.
- Distinción entre mayúsculas y minúsculas: Debido a que los nombres de Windows asignados se convierten en nombres NFS, la búsqueda de los nombres sigue a la semántica NFS. Esto incluye el hecho de que las búsquedas de NFS distinguen mayúsculas de minúsculas. Esto significa que las aplicaciones que acceden a recursos compartidos asignados no deben depender de un comportamiento que no distingue mayúsculas y minúsculas de Windows. Sin embargo, el nombre 8.3 está disponible y no distingue mayúsculas y minúsculas.
- Asignaciones parciales o no válidas: Tras asignar un nombre para devolver a los clientes que realizan enumeración de directorios ("dir"), se comprueba la validez de Windows en el nombre Unicode resultante. Si ese nombre sigue teniendo caracteres no válidos, o si no es válido para Windows (p. ej., finaliza en "" o en blanco) se devuelve el nombre 8.3 en lugar del nombre no válido.

Paso

1. Configurar asignación de caracteres:

```
vserver cifs character-mapping create -vserver vserver_name -volume  
volume_name -mapping mapping_text, ...
```

El mapeo consta de una lista de pares de caracteres fuente-objetivo separados por ":". Los caracteres son caracteres Unicode introducidos mediante dígitos hexadecimales. Por ejemplo: 3C:E03C.

El primer valor de cada uno `mapping_text` El par separado por dos puntos es el valor hexadecimal del carácter NFS que desea traducir y el segundo valor es el valor Unicode que utiliza SMB. Las parejas de asignación deben ser únicas (debe existir una asignación uno a uno).

- Asignación de origen

La siguiente tabla muestra el conjunto de caracteres Unicode permisible para la asignación de origen:

| Carácter Unicode | Carácter impreso | Descripción |
|------------------|------------------|--|
| 0x01-0x19 | No aplicable | Caracteres de control que no se imprimen |
| 0x5c | \ | Barra invertida |
| 0x3A | : | Dos puntos |
| 0x2A | * | Asterisco |
| 0x3f | ? | Signo de interrogación |

| | | |
|----------------|------|----------------|
| 0x22 | " | Entre comillas |
| 0x3C | < | Menor que |
| 0x3E | > | Mayor que |
| 0x7C | | |
| Línea vertical | 0xB1 | ± |

- Asignación de objetivos

Puede especificar caracteres de destino en el "Área de uso privado" de Unicode en el siguiente intervalo: U+E0000...U+F8FF.

Ejemplo

El siguiente comando crea una asignación de caracteres para un volumen denominado «data» en la máquina virtual de almacenamiento (SVM) vs1:

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show
```

| Vserver | Volume Name | Character Mapping |
|---------|-------------|---------------------------|
| ----- | ----- | ----- |
| vs1 | data | 3c:e17c, 3e:f17d, 2a:f745 |

Comandos para administrar las asignaciones de caracteres para la traducción de nombres de archivo SMB

Puede gestionar la asignación de caracteres creando, modificando, mostrando información o eliminando asignaciones de caracteres de archivo utilizadas para la traducción del nombre del archivo SMB en volúmenes FlexVol.

| Si desea... | Se usa este comando... |
|---|--|
| Cree nuevas asignaciones de caracteres de archivo | <code>vserver cifs character-mapping create</code> |
| Mostrar información acerca de las asignaciones de caracteres de archivo | <code>vserver cifs character-mapping show</code> |
| Modifique las asignaciones de caracteres de archivo existentes | <code>vserver cifs character-mapping modify</code> |

Eliminar asignaciones de caracteres de archivo

```
vserver cifs character-mapping delete
```

Para obtener más información, consulte la página de manual de cada comando.

Gestión de enlaces NFS

Descripción general de trunking NFS

A partir de ONTAP 9.14.1, los clientes NFSv4,1 pueden aprovechar la conexión de enlaces de sesión para abrir varias conexiones a diferentes LIF en el servidor NFS, lo que aumenta la velocidad de transferencia de datos y ofrece resiliencia a través de la multivía.

La conexión de enlaces proporciona ventajas para exportar volúmenes de FlexVol a clientes con capacidad de Trunking, en particular clientes VMware y Linux o para NFS a través de RDMA, TCP o pNFS.

En ONTAP 9.14.1, la conexión de enlaces se limita a las LIF en un único nodo; la conexión de enlaces no puede abarcar las LIF en varios nodos.

Los volúmenes FlexGroup se admiten para la conexión de enlaces. Aunque puede proporcionar un mejor rendimiento, el acceso multivía a un volumen FlexGroup solo puede configurarse en un único nodo.

En esta versión, solo se admite la conexión troncal de sesión para el acceso multivía.

Cómo utilizar trunking

Para aprovechar las ventajas de las rutas múltiples que ofrece la conexión de enlaces, necesita un conjunto de LIF, denominados *grupo de conexión troncal*, asociados a la SVM que contiene un servidor NFS habilitado para conexión de enlaces. Las LIF de un grupo de enlaces deben tener puertos iniciales en el mismo nodo del clúster y deben residir en esos puertos iniciales. Es recomendable que todas las LIF de un grupo de enlaces sean miembros del mismo grupo de recuperación tras fallos.

ONTAP admite hasta 16 conexiones troncalizadas por nodo desde un cliente determinado.

Cuando un cliente monta exportaciones desde un servidor habilitado para conexión de enlaces, especifica una serie de direcciones IP para las LIF en un grupo de conexiones. Una vez que el cliente se conecta a la primera LIF, los LIF adicionales solo se agregan a la sesión NFSv4,1 y se usan para la conexión de enlaces si cumplen los requisitos de grupo de Trunking. A continuación, el cliente distribuye las operaciones de NFS a través de las múltiples conexiones basadas en su propio algoritmo (como round-robin).

Para obtener el mejor rendimiento, se debe configurar el enlace de enlaces en una SVM que se dedique a proporcionar exportaciones multivía, no de rutas únicas. Es decir, solo debe habilitar la conexión troncal en un servidor NFS en una SVM cuyas exportaciones se proporcionan únicamente a clientes habilitados para la conexión troncal.

Clientes admitidos

El servidor ONTAP NFSv4,1 admite la conexión troncal con cualquier cliente capaz de realizar una conexión troncal de sesión NFSv4,1.

Los siguientes clientes han sido probados con ONTAP 9.14.1:

- VMware: ESXi 7.0U3F y versiones posteriores
- Linux: Red Hat Enterprise Linux (RHEL) 8,8 y 9,3



Al habilitar la conexión troncal en un servidor NFS, los usuarios que acceden a recursos compartidos exportados en clientes NFS que no admiten la conexión troncal pueden ver una caída de rendimiento. Esto se debe a que solo se utiliza una única conexión TCP para varios montajes en las LIF de datos de SVM.

Diferencia entre la conexión de enlaces NFS y nconnect

A partir de ONTAP 9.8, la funcionalidad `nconnect` está disponible de forma predeterminada con NFSv4.1 habilitado. En clientes que admiten `nconnect`, un solo montaje NFS puede tener varias conexiones TCP (hasta 16) a través de un único LIF.

Por el contrario, la función de enlace es la funcionalidad *multipathing*, que proporciona varias conexiones TCP a través de varias LIF. Si tiene la capacidad de emplear NIC adicionales en su entorno, la troncalización proporciona un mayor paralelismo y rendimiento más allá de la capacidad de `nconnect`.

Más información acerca de ["nconectar."](#)

Configurar un nuevo servidor NFS y exportar para trunking

Cree un servidor NFS habilitado para la conexión de enlaces

A partir de ONTAP 9.14.1, se puede habilitar la conexión troncal en servidores NFS. NFSv4,1 está habilitado de forma predeterminada cuando se crean servidores NFS.

Antes de empezar

La SVM debe ser:

- respaldado por suficiente almacenamiento para los requisitos de datos de cliente.
- Habilitado para NFS.
- Dedicado al trunking NFS. No se debe configurar ningún otro cliente en él.

Pasos

1. Si no existe una SVM adecuada, cree una:

```
vserver create -vserver svm_name -rootvolume root_volume_name -aggregate
aggregate_name -rootvolume-security-style unix -language C.UTF-8
```

2. Compruebe la configuración y el estado de la SVM recién creada:

```
vserver show -vserver svm_name
```

Más información acerca de ["Creación de una SVM."](#)

3. Cree el servidor NFS:

```
vserver nfs create -vserver svm_name -v3 disabled -v4.0 disabled -v4.1 enabled
-v4.1-trunking enabled -v4-id-domain my_domain.com
```

4. Compruebe que NFS está ejecutando:

```
vserver nfs status -vserver svm_name
```

5. Compruebe que NFS está configurado como se desea:

```
vserver nfs show -vserver svm_name
```

Más información acerca de ["Configuración del servidor NFS."](#)

Después de terminar

Configure los siguientes servicios según sea necesario:

- ["DNS"](#)
- ["LDAP"](#)
- ["Kerberos"](#)

Prepare la red para la conexión de enlaces

Para aprovechar la conexión de enlaces NFSv4,1, los LIF de un grupo de enlaces deben residir en el mismo nodo y tener puertos de inicio en el mismo nodo. Las LIF deben estar configuradas en un grupo de conmutación por error del mismo nodo.

Acerca de esta tarea

Una asignación uno a uno de LIF y NIC proporciona la mayor ganancia de rendimiento, pero no es necesaria para permitir la conexión de enlaces. Tener al menos dos NIC instaladas puede ofrecer un beneficio de rendimiento, pero no es necesario.

Puede tener varios grupos de conmutación por error, pero el grupo de conmutación por error para la conexión troncal debe incluir sólo esos LIFS en el grupo de troncalización.

Debe ajustar el grupo de conmutación por error de troncalización cada vez que agregue o elimine conexiones (y NIC subyacentes) de un grupo de conmutación por error.

Antes de empezar

- Debe conocer los nombres de puerto asociados a las NIC si desea crear un grupo de conmutación por error.
- Los puertos deben estar todos en el mismo nodo.

Pasos

1. Compruebe los nombres y el estado de los puertos de red que desea utilizar:

```
network port status
```

2. Cree el grupo de failover:

```
network interface failover-groups create -vserver svm_name -failover-group failover_group_name -targets ports_list
```



No es un requisito tener un grupo de recuperación tras fallos, pero es muy recomendable.

- `svm_name` Es el nombre de la SVM que contiene el servidor NFS.
- `ports_list` es la lista de puertos que se agregarán al grupo de conmutación por error.

Los puertos se agregan con el formato `node_name:port_number`, por ejemplo, `node1:e0c`.

El siguiente comando crea el grupo de conmutación al nodo de respaldo FG3 para SVM VS1 y añade tres puertos:

```
network interface failover-groups create -vserver vs1 -failover-group fg3
-targets cluster1-01:e0c,cluster1-01:e0d,cluster1-01:e0e
```

Más información acerca de ["grupos de conmutación por error."](#)

3. Si es necesario, cree LIF para los miembros del grupo de enlaces:

```
network interface create -vserver svm_name -lif lif_name -home-node node_name
-home-port port_name -address IP_address -netmask IP_address [-service-policy
policy] [-auto-revert {true|false}]
```

- `-home-node` - El nodo al que regresa la LIF cuando se ejecuta el comando `network interface revert` en la LIF.

También puede especificar si el LIF debería volver automáticamente al nodo raíz y al puerto raíz con el `-auto-revert` opción.

- `-home-port` Es el puerto físico o lógico al que devuelve la LIF cuando el comando de reversión de la interfaz de red se ejecuta en la LIF.
- Puede especificar una dirección IP con el `-address` y.. `-netmask` opciones, no con el `-subnet` opción.
- Al asignar direcciones IP, es posible que deba configurar una ruta predeterminada a una puerta de enlace si hay clientes o controladores de dominio en una subred IP diferente. La `network route create` La página man contiene información sobre la creación de una ruta estática dentro de una SVM.
- `-service-policy` - La política de servicio para la LIF. Si no se especifica ninguna política, se asignará automáticamente una política predeterminada. Utilice la `network interface service-policy show` comando para revisar las políticas de servicio disponibles.
- `-auto-revert` - Especificar si una LIF de datos se revierte automáticamente a su nodo de inicio en circunstancias como el inicio, cambios en el estado de la base de datos de administración, o cuando se realiza la conexión de red. La configuración predeterminada es `false`, pero puede establecerla en `true` en función de las políticas de gestión de red del entorno.

Repita este paso para cada LIF del grupo de enlaces.

Se crea el siguiente comando `lif-A` Para la SVM `vs1`, en el puerto `e0c` del nodo `cluster1_01`:

```
network interface create -vserver vs1 -lif lif-A -service-policy ??? -home
-node cluster1_01 -home-port e0c -address 192.0.2.0
```

Más información acerca de ["Creación de LIF."](#)

4. Comprobar que se han creado las LIF:

```
network interface show
```

5. Compruebe que se pueda acceder a la dirección IP configurada:

| Para verificar una... | Usar... |
|-----------------------|----------------------------|
| Dirección IPv4 | <code>network ping</code> |
| Dirección IPv6 | <code>network ping6</code> |

Exportar datos para el acceso del cliente

Para ofrecer al cliente acceso a recursos compartidos de datos, debe crear uno o varios volúmenes y el volumen debe tener políticas de exportación con al menos una regla.

Requisitos de exportación del cliente:

- Los clientes de Linux deben tener un montaje independiente y un punto de montaje independiente para cada conexión de Trunking (es decir, para cada LIF).
- Los clientes de VMware solo requieren un único punto de montaje para un volumen exportado, con varias LIF especificadas.

Los clientes de VMware requieren acceso raíz en la política de exportación.

Pasos

1. Cree una política de exportación:

```
vserver export-policy create -vserver svm_name -policyname policy_name
```

El nombre de la política puede tener hasta 256 caracteres.

2. Compruebe que se ha creado la política de exportación:

```
vserver export-policy show -policyname policy_name
```

Ejemplo

Los siguientes comandos crean y verifican la creación de una política de exportación llamada `exp1` en la SVM llamada `vs1`:

```
vs1::> vserver export-policy create -vserver vs1 -policyname exp1
```

3. Cree una regla de exportación y añádala a una política de exportación existente:

```
vserver export-policy rule create -vserver svm_name -policyname policy_name  
-ruleindex integer -protocol nfs4 -clientmatch { text | "text,text,..." }  
-rorule security_type -rwrule security_type -superuser security_type -anon  
user_ID
```

La `-clientmatch` Parámetro debe identificar los clientes Linux o VMware compatibles con la conexión troncal que montarán la exportación.

Más información acerca de ["creación de reglas de exportación."](#)

4. Cree el volumen con un punto de unión:

```
volume create -vserver svm_name -volume volume_name -aggregate aggregate_name  
-size {integer[KB|MB|GB|TB|PB]} -security-style unix -user user_name_or_number  
-group group_name_or_number -junction-path junction_path -policy  
export_policy_name
```

Descubra ["creando volúmenes."](#)

5. Compruebe que el volumen se ha creado con el punto de unión deseado:

```
volume show -vserver svm_name -volume volume_name -junction-path
```

Crear montajes de cliente

Los clientes de Linux y VMware compatibles con la conexión de enlaces pueden montar volúmenes o recursos compartidos de datos desde un servidor ONTAP NFSv4,1 que esté habilitado para la conexión de enlaces.

Al introducir los comandos de montaje en los clientes, debe introducir las direcciones IP para cada LIF del grupo de enlaces.

Descubra ["clientes admitidos"](#).

Requisitos del cliente Linux

Se necesita un punto de montaje independiente para cada conexión del grupo de troncalización.

Monte los volúmenes exportados con comandos similares a los siguientes:

```
mount lif1_ip:/vol-test /mnt/test1 -o vers=4.1,max_connect=16
```

```
mount lif2_ip:/vol-test /mnt/test2 -o vers=4.1,max_connect=16
```

La versión (`vers`) el valor debe ser 4.1 o posterior.

La `max_connect` el valor corresponde al número de conexiones del grupo de troncalización.

Requisitos del cliente de VMware

Se necesita una sentencia mount que incluya una dirección IP para cada conexión del grupo de enlaces.

Monte el almacén de datos exportado con un comando similar al siguiente:

```
#esxcli storage nfs41 -H lif1_ip, lif2_ip -s /mnt/sh are1 -v nfs41share
```

La `-H` los valores corresponden a las conexiones del grupo de troncalización.

Adapte las exportaciones NFS existentes para la conexión de enlaces

Visión general de la adaptación de exportaciones de una ruta de acceso única

Puede adaptar una exportación NFSv4,1 de ruta única existente (no troncalizada) para utilizar troncalización. Los clientes compatibles con trunking pueden aprovechar el rendimiento mejorado en cuanto se activa la troncalización en el servidor, siempre y cuando se cumplan los requisitos previos del servidor y del cliente.

La adaptación de una exportación de ruta única para la conexión de enlaces le permite mantener conjuntos de datos exportados en sus volúmenes y SVM existentes. Para ello, debe habilitar la conexión troncal en el servidor NFS, actualizar la configuración de redes y exportación y volver a montar el recurso compartido exportado en los clientes.

La activación de la conexión troncal tiene el efecto de reiniciar el servidor. Luego, los clientes de VMware deben volver a montar los almacenes de datos exportados; los clientes Linux deben volver a montar los volúmenes exportados con el `max_connect` opción.

Active la conexión troncal en el servidor NFS

La conexión troncal debe estar explícitamente habilitada en los servidores NFS. NFSv4,1 está habilitado de forma predeterminada cuando se crean servidores NFS.

Después de activar la conexión troncal, verifique que los siguientes servicios estén configurados según sea necesario.

- ["DNS"](#)
- ["LDAP"](#)
- ["Kerberos"](#)

Pasos

1. Active la conexión troncal y asegúrese de que NFSv4,1 está activado:

```
vserver nfs create -vserver svm_name -v4.1 enabled -v4.1-trunking enabled
```

2. Compruebe que NFS está ejecutando:

```
vserver nfs status -vserver svm_name
```

3. Compruebe que NFS está configurado como se desea:

```
vserver nfs show -vserver svm_name
```

Más información acerca de ["Configuración del servidor NFS."](#)

.. Si ofrece servicio a clientes de Windows desde esta SVM, mueva los recursos compartidos y elimine el servidor.

```
vserver cifs show -vserver svm_name
```

+

```
vserver cifs delete -vserver svm_name
```

Actualice la red para la conexión troncal

La conexión de enlaces NFSv4,1 requiere que las LIF de un grupo de enlaces residan en

el mismo nodo y tengan puertos iniciales en el mismo nodo. Todas las LIF deben configurarse en un grupo de conmutación al nodo de respaldo del mismo nodo.

Acerca de esta tarea

Una asignación uno a uno de LIF y NIC proporciona la mayor ganancia de rendimiento, pero no es necesaria para permitir la conexión de enlaces.

Puede tener varios grupos de conmutación por error, pero el grupo de conmutación por error para la conexión troncal debe incluir sólo esos LIFS en el grupo de troncalización.

Debe ajustar el grupo de conmutación por error de troncalización cada vez que agregue o elimine conexiones (y NIC subyacentes) de un grupo de conmutación por error.

Antes de empezar

- Debe conocer los nombres de puerto asociados a las NIC para crear un grupo de conmutación por error.
- Los puertos deben estar todos en el mismo nodo.

Pasos

1. Compruebe los nombres y el estado de los puertos de red que desea utilizar:

```
network port show
```

2. Cree un grupo de failover de trunking o modifique uno existente para trunking:

```
network interface failover-groups create -vserver svm_name -failover-group failover_group_name -targets ports_list
```

```
network interface failover-groups modify -vserver svm_name -failover-group failover_group_name -targets ports_list
```



No es un requisito tener un grupo de recuperación tras fallos, pero es muy recomendable.

° *svm_name* Es el nombre de la SVM que contiene el servidor NFS.

° *ports_list* es la lista de puertos que se agregarán al grupo de conmutación por error.

Los puertos se añaden en el formato *node_name:port_number*, por ejemplo, *node1:e0c*.

El siguiente comando crea un grupo de recuperación tras fallos *fg3* Para SVM *VS1* y añade tres puertos:

```
network interface failover-groups create -vserver vs1 -failover-group fg3 -targets cluster1-01:e0c,cluster1-01:e0d,cluster1-01:e0e
```

Más información acerca de ["grupos de conmutación por error."](#)

3. Cree LIF adicionales para los miembros del grupo de enlaces según sea necesario:

```
network interface create -vserver svm_name -lif lif_name -home-node node_name -home-port port_name -address IP_address -netmask IP_address [-service-policy policy] [-auto-revert {true|false}]
```

- `-home-node` - El nodo al que regresa la LIF cuando se ejecuta el comando `network interface revert` en la LIF.

Puede especificar si la LIF debe volver automáticamente al nodo de inicio y al puerto de inicio con el `-auto-revert` opción.

- `-home-port` Es el puerto físico o lógico al que devuelve la LIF cuando el comando de reversión de la interfaz de red se ejecuta en la LIF.
- Puede especificar una dirección IP con el `-address` y.. `-netmask` opciones.
- Cuando se asignan direcciones IP manualmente (sin utilizar una subred), es posible que deba configurar una ruta predeterminada a una puerta de enlace si existen clientes o controladores de dominio en una subred IP diferente. La página del comando `man create` de la ruta de red contiene información sobre la creación de una ruta estática dentro de una SVM.
- `-service-policy` - La política de servicio para la LIF. Si no se especifica ninguna política, se asignará automáticamente una política predeterminada. Utilice la `network interface service-policy show` comando para revisar las políticas de servicio disponibles.
- `-auto-revert` - Especificar si una LIF de datos se revierte automáticamente a su nodo de inicio en circunstancias como el inicio, cambios en el estado de la base de datos de administración, o cuando se realiza la conexión de red. **La configuración predeterminada es false**, pero puedes configurarla en `true` dependiendo de las políticas de administración de red de tu entorno.

Repita este paso con cada LIF adicional necesario en el grupo de enlaces.

El siguiente comando crea `lif-A` para la SVM `VS1`, en el puerto `e0c` del nodo `cluster1_01`:

```
network interface create -vserver vs1 -lif lif-A -service-policy default-
intercluster -home-node cluster1_01 -home-port e0c -address 192.0.2.0
```

Más información acerca de ["Creación de LIF."](#)

4. Compruebe que las LIF se han creado:

```
network interface show
```

5. Compruebe que se pueda acceder a la dirección IP configurada:

| Para verificar una... | Usar... |
|-----------------------|----------------------------|
| Dirección IPv4 | <code>network ping</code> |
| Dirección IPv6 | <code>network ping6</code> |

Modificar la exportación de datos para el acceso del cliente

Para que los clientes puedan aprovechar la conexión de enlaces para los recursos compartidos de datos existentes, es posible que deba modificar las políticas y reglas de exportación y los volúmenes a los que están asociados. Hay diversos requisitos de exportación para los clientes Linux y los almacenes de datos VMware.

Requisitos de exportación del cliente:

- Los clientes de Linux deben tener un montaje independiente y un punto de montaje independiente para cada conexión de Trunking (es decir, para cada LIF).

Si va a actualizar a ONTAP 9.14.1 y ya ha exportado un volumen, puede seguir usando ese volumen en un grupo de enlaces.

- Los clientes de VMware solo requieren un único punto de montaje para un volumen exportado, con varias LIF especificadas.

Los clientes de VMware requieren acceso raíz en la política de exportación.

Pasos

1. Compruebe que haya vigente una política de exportación existente:

```
vserver export-policy show
```

2. Compruebe que las reglas de política de exportación existentes son adecuadas para la configuración de trunking:

```
vserver export-policy rule show -policyname policy_name
```

En particular, compruebe que el `-clientmatch` El parámetro identifica correctamente los clientes Linux o VMware compatibles con la conexión troncal que montarán la exportación.

Si es necesario realizar ajustes, modifique la regla mediante `vserver export-policy rule modify` comando o crear una nueva regla:

```
vserver export-policy rule create -vserver svm_name -policyname policy_name
-ruleindex integer -protocol nfs4 -clientmatch { text | "text,text,..." }
-rorule security_type -rwrule security_type -superuser security_type -anon
user_ID
```

Más información acerca de ["creación de reglas de exportación."](#)

3. Verifique que los volúmenes exportados existentes estén en línea:

```
volume show -vserver svm_name
```

Restablecer montajes de cliente

Para convertir conexiones de cliente no troncalizadas en conexiones troncales, los montajes existentes en clientes Linux y VMware deben desmontarse y volver a montarse utilizando la información acerca de las LIF.

Al introducir los comandos de montaje en los clientes, debe introducir las direcciones IP para cada LIF del grupo de enlaces.

Descubra ["clientes admitidos"](#).



El desmontaje de los clientes de VMware provoca interrupciones en las máquinas virtuales del almacén de datos. Una alternativa sería crear un nuevo almacén de datos habilitado para trunking, y usar **storage vmotion** para mover sus VM del antiguo almacén de datos al nuevo. Consulte la documentación de VMware para más detalles.

Requisitos del cliente Linux

Se necesita un punto de montaje independiente para cada conexión del grupo de troncalización.

Monte los volúmenes exportados con comandos similares a los siguientes:

```
mount lif1_ip:/vol-test /mnt/test1 -o vers=4.1,max_connect=2
```

```
mount lif2_ip:/vol-test /mnt/test2 -o vers=4.1,max_connect=2
```

La `vers` el valor debe ser 4.1 o posterior.

La `max_connect` el valor debe corresponder al número de conexiones del grupo de troncalización.

Requisitos del cliente de VMware

Se necesita una sentencia mount que incluya una dirección IP para cada conexión del grupo de enlaces.

Monte el almacén de datos exportado con un comando similar al siguiente:

```
#esxcli storage nfs41 -H lif1_ip, lif2_ip -s /mnt/sh are1 -v nfs41share
```

La `-H` los valores deben corresponder a las conexiones del grupo de troncalización.

Gestione NFS a través de RDMA

NFS sobre RDMA

NFS a través de RDMA utiliza adaptadores RDMA, que permiten que los datos se copien directamente entre la memoria del sistema de almacenamiento y la memoria del sistema host, lo que elude las interrupciones y la sobrecarga de la CPU.

Las configuraciones de NFS sobre RDMA están diseñadas para clientes con cargas de trabajo sensibles a la latencia o de gran ancho de banda, como el aprendizaje automático y el análisis. NVIDIA ha ampliado NFS a través de RDMA para habilitar GPU Direct Storage (GDS). GDS acelera aún más las cargas de trabajo habilitadas para GPU al omitir completamente la CPU y la memoria principal, mediante RDMA, que transfiere datos entre el sistema de almacenamiento y la memoria de la GPU directamente.

A partir de ONTAP 9.14.1, se admiten las configuraciones de NFS over RDMA con el protocolo NFSv4.1.

A partir de ONTAP 9.10.1, las configuraciones de NFS over RDMA se admiten para el protocolo NFSv4.0 cuando se utiliza con el adaptador Mellanox CX-5 o CX-6, que ofrece compatibilidad para RDMA con la versión 2 del protocolo RoCE. GDS solo es compatible con el uso de GPU de la familia NVIDIA Tesla y Ampere con tarjetas NIC Mellanox y software MOFED.

La compatibilidad con NFS a través de RDMA se limita únicamente al tráfico local del nodo. FlexVols o FlexGroups estándares, en los que todos los componentes están en el mismo nodo son compatibles y deben


accederse a ellos desde un LIF en el mismo nodo. Los tamaños de montaje de NFS superiores a 64 000 dan como resultado un rendimiento inestable con NFS en configuraciones RDMA.

Requisitos

- Los sistemas de almacenamiento deben ejecutar ONTAP 9.10.1 o una versión posterior
 - Es posible configurar NFS a través de RDMA con System Manager que empieza con ONTAP 9.12.1. En ONTAP 9.10.1 y 9.11.1, tiene que utilizar la CLI para configurar NFS sobre RDMA.
- Los dos nodos de la pareja de alta disponibilidad deben tener la misma versión.
- Las controladoras de los sistemas de almacenamiento deben ser compatibles con RDMA

| Comenzando en ONTAP... | Las siguientes controladoras admiten RDMA... |
|--------------------------------------|--|
| 9.10.1 y posterior | <ul style="list-style-type: none">• A400• A700• A800 |
| ONTAP 9.14.1 y versiones posteriores | <ul style="list-style-type: none">• AFF C-Series• A900 |

- Dispositivo de almacenamiento configurado con hardware compatible con RDMA (p. ej., Mellanox CX-5 o CX-6).
- Deben configurarse los LIF de datos para que sean compatibles con RDMA.
- Los clientes Mellanox deben utilizar tarjetas NIC compatibles con RDMA y el software de red Mellanox OFED (MOFED).



Los grupos de interfaces no son compatibles con NFS sobre RDMA.

El futuro

- [Configure las NIC para NFS a través de RDMA](#)
- [Configure LIF para NFS a través de RDMA](#)
- [Configuración de NFS para NFS sobre RDMA](#)

Información relacionada

- ["RDMA"](#)
- [Descripción general de trunking NFS](#)
- ["RFC 7530: Protocolo NFS versión 4"](#)
- ["RFC 8166: Transporte de acceso directo a memoria remota para llamada de procedimiento remoto versión 1"](#)
- ["RFC 8167: Llamada de procedimiento remoto bidireccional en transpuertos RPC a través de RDMA"](#)
- ["RFC 8267: Enlace de capa superior de NFS a RPC-over-RDMA versión 1"](#)

Configure las NIC para NFS a través de RDMA

NFS a través de RDMA requiere la configuración de NIC tanto para el sistema cliente como para la plataforma de almacenamiento.

Configuración de la plataforma de almacenamiento

Es necesario instalar un adaptador RDMA X1148 en el servidor. Si se utiliza una configuración ha, debe tener el adaptador X1148 correspondiente en el partner de conmutación por error para que el servicio RDMA pueda continuar durante la conmutación por error. La NIC debe ser compatible con roce.

A partir de ONTAP 9.10.1, es posible ver una lista de protocolos de descarga RDMA con el comando:

```
network port show -rdma-protocols roce
```

Configuración del sistema cliente

Los clientes Mellanox deben utilizar tarjetas NIC compatibles con RDMA (p. ej. X1148) y software de red Mellanox OFED. Consulte la documentación de Mellanox para conocer modelos y versiones compatibles. Aunque el cliente y el servidor pueden conectarse directamente, se recomienda el uso de switches debido a un rendimiento mejorado de la conmutación por error con un switch.

El cliente, el servidor y todos los switches, así como todos los puertos de los switches, deben configurarse mediante tramas gigantes. Asegúrese también de que el control de flujo de prioridad está en vigor en cualquier conmutador.

Una vez confirmada esta configuración, puede montar el NFS.

System Manager

Debe utilizar ONTAP 9.12.1 o una versión posterior para configurar interfaces de red con NFS a través de RDMA mediante System Manager.

Pasos

1. Compruebe si es compatible con RDMA. Vaya a **Red > puertos Ethernet** y seleccione el nodo apropiado en la vista de grupo. Cuando expanda el nodo, mire el campo **protocolos RDMA** para un puerto dado: El valor **roce** indica que es compatible con RDMA; un guión (-) indica que no es compatible.
2. Para agregar una VLAN, seleccione **+ VLAN**. Seleccione el nodo que corresponda. En el menú desplegable **Puerto**, los puertos disponibles mostrarán el texto **roce Enabled** si admiten RDMA; no se mostrará ningún texto si no son compatibles con RDMA.
3. Siga el flujo de trabajo en [Almacenamiento NAS para servidores Linux mediante NFS](#) Para configurar un nuevo servidor NFS.

Al agregar interfaces de red, tendrá la opción de seleccionar **utilizar puertos roce**. Seleccione esta opción para las interfaces de red que desee utilizar NFS a través de RDMA.

CLI

1. Compruebe si el acceso RDMA está habilitado en el servidor NFS con el comando:

```
vserver nfs show-vserver SVM_name
```

De forma predeterminada, `-rdma` debe estar activado. Si no lo está, habilite el acceso RDMA en el servidor NFS:

```
vserver nfs modify -vserver SVM_name -rdma enabled
```

2. Monte el cliente a través de NFSv4.0 por RDMA:
 - a. La entrada del parámetro `proto` depende de la versión del protocolo IP del servidor. Si es IPv4, utilice `proto=rdma`. Si es IPv6, utilice `proto=rdma6`.
 - b. Especifique el puerto de destino NFS como `port=20049` en lugar del puerto estándar 2049:

```
mount -o vers=4,minorversion=0,proto=rdma,port=20049 Server_IP_address  
:/volume_path mount_point
```

3. **OPCIONAL:** Si necesita desmontar el cliente, ejecute el comando `umount mount_path`

Más información

- [Cree un servidor NFS](#)
- [Almacenamiento NAS para servidores Linux mediante NFS](#)

Configure LIF para NFS a través de RDMA

Para utilizar NFS a través de RDMA, debe configurar sus LIF (interfaz de red) para que sean compatibles con RDMA. Tanto el LIF como su pareja de conmutación por error deben ser compatibles con RDMA.

Cree una nueva LIF

System Manager

Debe estar ejecutando ONTAP 9.12.1 o posterior para crear una interfaz de red para NFS a través de RDMA con System Manager.

Pasos

1. Seleccione **Red > Descripción general > interfaces de red**.
2. Seleccione **+ Add**.
3. Al seleccionar **NFS,SMB/CIFS,S3**, tendrá la opción de **utilizar puertos roce**. Seleccione la casilla de verificación **usar puertos roce**.
4. Seleccione la máquina virtual de almacenamiento y el nodo principal. Asigne un nombre. Introduzca la dirección IP y la máscara de subred.
5. Una vez que se introducen la dirección IP y la máscara de subred, System Manager filtrará la lista de dominios de retransmisión a los que tengan puertos compatibles con roce. Seleccione un dominio de retransmisión. Opcionalmente, puede añadir una puerta de enlace.
6. Seleccione **Guardar**.

CLI

Pasos

1. Cree una LIF:

```
network interface create -vserver SVM_name -lif lif_name -service-policy  
service_policy_name -home-node node_name -home-port port_name {-address  
IP_address -netmask netmask_value | -subnet-name subnet_name} -firewall  
-policy policy_name -auto-revert {true|false} -rdma-protocols roce
```


- La política de servicio debe ser los archivos de datos predeterminados o una política personalizada que incluya el servicio de interfaz de red data-nfs.
- La `-rdma-protocols` el parámetro acepta una lista, que está vacía de forma predeterminada. Cuando `roce` Se añade como valor, el LIF solo puede configurarse en puertos que admitan la descarga de roce, lo que afecta a la migración LIF bot y la conmutación por error.

Modificar una LIF

System Manager

Debe estar ejecutando ONTAP 9.12.1 o posterior para crear una interfaz de red para NFS a través de RDMA con System Manager.

Pasos

1. Seleccione **Red > Descripción general > interfaces de red**.
2. Seleccione  > **Editar** junto a la interfaz de red que desea cambiar.
3. Seleccione **usar puertos roce** para activar NFS sobre RDMA o anule la selección de la casilla para desactivarla. Si la interfaz de red se encuentra en un puerto con capacidad para roce, aparecerá una casilla de verificación junto a **usar puertos roce**.
4. Modifique los demás ajustes según sea necesario.
5. Seleccione **Guardar** para confirmar los cambios.

CLI

1. Puede comprobar el estado de sus LIF con el `network interface show` comando. La política de servicio debe incluir el servicio de interfaz de red `data-nfs`. La `-rdma-protocols` la lista debe incluir `roce`. Si alguna de estas condiciones no es verdadera, modifique la LIF.
2. Para modificar la LIF, ejecute:

```
network interface modify vserver SVM_name -lif lif_name -service-policy
service_policy_name -home-node node_name -home-port port_name {-address
IP_address -netmask netmask_value | -subnet-name subnet_name} -firewall
-policy policy_name -auto-revert {true|false} -rdma-protocols roce
```



Modificar una LIF para requerir un protocolo de descarga determinado cuando la LIF no está asignada actualmente a un puerto que admita ese protocolo producirá un error.

Migre una LIF

ONTAP también le permite migrar interfaces de red (LIF) para utilizar NFS a través de RDMA. Cuando realice esta migración, debe asegurarse de que el puerto de destino sea compatible con roce. A partir de ONTAP 9.12.1, puede completar este procedimiento en System Manager. Al seleccionar un puerto de destino para la interfaz de red, System Manager designará si los puertos son compatibles con roce.

Solo puede migrar un LIF a una configuración de NFS sobre RDMA si:

- Es una interfaz de red (LIF) RDMA de NFS alojada en un puerto compatible con roce.
- Es una interfaz de red TCP (LIF) NFS alojada en un puerto compatible con roce.
- Es una interfaz de red TCP (LIF) de NFS alojada en un puerto no compatible con roce.

Para obtener más información sobre la migración de una interfaz de red, consulte [Migre una LIF](#).

Más información

- [Cree una LIF](#)
- [Cree una LIF](#)
- [Modificar una LIF](#)

- [Migre una LIF](#)

Modifique la configuración NFS

En la mayoría de los casos, no es necesario modificar la configuración de una máquina virtual de almacenamiento con NFS habilitado para NFS sobre RDMA.

Sin embargo, si tiene que enfrentarse a problemas relacionados con chips Mellanox y la migración de LIF, debe aumentar el período de gracia de bloqueo de NFSv4. De forma predeterminada, el período de gracia se establece en 45 segundos. A partir de ONTAP 9.10.1, el período de gracia tiene un valor máximo de 180 (segundos).

Pasos

1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Introduzca el siguiente comando:

```
vserver nfs modify -vserver SVM_name -v4-grace-seconds number_of_seconds
```

Para obtener más información acerca de esta tarea, consulte [Especificar el período de gracia de bloqueo de NFSv4](#).

Configure SMB con la interfaz de línea de comandos

Información general de configuración de SMB con la CLI

Es posible usar comandos de la CLI de ONTAP 9 para configurar el acceso del cliente SMB a los archivos ubicados en un volumen o un qtree nuevos de una SVM nueva o existente.



SMB (bloque de mensajes del servidor) hace referencia a los dialectos modernos del protocolo del sistema común de archivos de Internet (CIFS). Seguirá viendo *CIFS* en la interfaz de línea de comandos (CLI) de ONTAP y en las herramientas de gestión de OnCommand.

Use estos procedimientos si desea configurar el acceso de SMB a un volumen o qtree de la siguiente forma:

- Desea utilizar SMB versión 2 o posterior.
- Desea ofrecer servicio únicamente a clientes SMB, no a clientes NFS (no a configuración multiprotocolo).
- Se utilizarán permisos de archivo NTFS para proteger el nuevo volumen.
- Tiene privilegios de administrador de clúster, no de administrador de SVM.

Se necesitan privilegios de administrador de clúster para crear SVM y LIF. Los privilegios de administrador de SVM son suficientes para otras tareas de configuración de SMB.

- Desea utilizar la CLI, no System Manager ni una herramienta de secuencias de comandos automatizadas.

Para usar System Manager para configurar el acceso multiprotocolo NAS, consulte ["Aprovisione almacenamiento NAS para Windows y Linux usando NFS y SMB"](#).

- Quiere utilizar las prácticas recomendadas, no explorar todas las opciones disponibles.

Puede obtener más detalles acerca de la sintaxis de los comandos en la ayuda de la CLI y en las páginas de manual de ONTAP.

Si desea obtener detalles acerca del rango de funcionalidades del protocolo SMB de ONTAP, consulte la ["Información general sobre la referencia de SMB"](#).

Otras maneras de hacerlo en ONTAP

| Para ejecutar estas tareas con... | Consulte... |
|--|---|
| System Manager rediseñado (disponible con ONTAP 9.7 y versiones posteriores) | "Aprovisionar almacenamiento NAS para servidores de Windows mediante SMB" |
| System Manager Classic (disponible con ONTAP 9.7 y versiones anteriores) | "Información general de la configuración de SMB" |

Flujo de trabajo de configuración de SMB

La configuración de SMB implica evaluar los requisitos de almacenamiento físico y de red y, a continuación, elegir un flujo de trabajo específico del objetivo; configurar el acceso de SMB a una SVM nueva o existente; o añadir un volumen o qtree a una SVM existente que ya esté completamente configurada para el acceso del bloque de mensajes del servidor.

Preparación

Evaluar los requisitos de almacenamiento físico

Antes de aprovisionar almacenamiento de SMB para clientes, debe asegurarse de que haya espacio suficiente en un agregado existente para el nuevo volumen. Si no lo hay, puede añadir discos a un agregado existente o crear uno nuevo con el tipo deseado.

Pasos

1. Mostrar el espacio disponible en los agregados existentes: `storage aggregate show`

Si hay un agregado con suficiente espacio, registre su nombre en la hoja de cálculo.

```
cluster::> storage aggregate show
```

| Aggregate | Size | Available | Used% | State | #Vols | Nodes | RAID | Status |
|-----------|---------|-----------|-------|--------|-------|-------|----------|--------|
| aggr_0 | 239.0GB | 11.13GB | 95% | online | 1 | node1 | raid_dp, | normal |
| aggr_1 | 239.0GB | 11.13GB | 95% | online | 1 | node1 | raid_dp, | normal |
| aggr_2 | 239.0GB | 11.13GB | 95% | online | 1 | node2 | raid_dp, | normal |
| aggr_3 | 239.0GB | 11.13GB | 95% | online | 1 | node2 | raid_dp, | normal |
| aggr_4 | 239.0GB | 238.9GB | 95% | online | 5 | node3 | raid_dp, | normal |
| aggr_5 | 239.0GB | 239.0GB | 95% | online | 4 | node4 | raid_dp, | normal |

6 entries were displayed.

- Si no hay agregados con espacio suficiente, añada discos a un agregado existente mediante el `storage aggregate add-disks` o cree un nuevo agregado con el `storage aggregate create` comando.

Evaluar los requisitos de red

Antes de proporcionar almacenamiento SMB a los clientes, debe comprobar que las redes se han configurado correctamente para cumplir los requisitos de aprovisionamiento de SMB.

Antes de empezar

Deben configurarse los siguientes objetos de red de clúster:

- Puertos físicos y lógicos
- Dominios de retransmisión
- Subredes (si es necesario)
- Espacios IP (según se requiera, además del espacio IP predeterminado)
- Grupos de conmutación por error (según sea necesario, además del grupo de conmutación por error predeterminado para cada dominio de retransmisión).
- Firewalls externos

Pasos

- Mostrar los puertos físicos y virtuales disponibles: `network port show`
 - Cuando sea posible, debe utilizar el puerto con la velocidad más alta para la red de datos.
 - Todos los componentes de la red de datos deben tener la misma configuración de MTU para obtener el mejor rendimiento.
- Si tiene pensado utilizar un nombre de subred para asignar la dirección IP y el valor de máscara de red para una LIF, compruebe que la subred existe y que tenga suficientes direcciones disponibles: `network subnet show`

Las subredes contienen un grupo de direcciones IP que pertenecen a la misma subred de capa 3. Las subredes se crean mediante la `network subnet create` comando.

3. Mostrar espacios IP disponibles: `network ipspace show`

Puede usar el espacio IP predeterminado o un espacio IP personalizado.

4. Si desea usar direcciones IPv6, compruebe que IPv6 esté habilitado en el clúster: `network options ipv6 show`

Si es necesario, puede habilitar IPv6 con el `network options ipv6 modify` comando.

Decidir dónde aprovisionar la nueva capacidad de almacenamiento para las pymes

Antes de crear un volumen o qtree de SMB nuevo, debe decidir si colocarlo en una SVM nueva o existente y cuánta configuración requiere la SVM. Esta decisión determina su flujo de trabajo.

Opciones

- Si desea aprovisionar un volumen o qtree en una SVM nueva o en una SVM existente con SMB habilitado pero sin configurar, complete los pasos de «"Configuración del acceso de SMB a una SVM" y «"adición de capacidad de almacenamiento a una SVM habilitada para SMB"».

[Configurar el acceso de SMB a una SVM](#)

[Configurar el acceso de clientes SMB a almacenamiento compartido](#)

Puede optar por crear una nueva SVM si se cumple alguna de las siguientes condiciones:

- Debe habilitar SMB en un clúster por primera vez.
- Tiene SVM existentes en un clúster en el cual no desea habilitar la compatibilidad con SMB.
- Tiene una o varias SVM habilitadas para SMB en un clúster y desea una de las siguientes conexiones:
 - A un bosque o grupo de trabajo de Active Directory diferente.
 - A un servidor SMB en un espacio de nombres aislado (escenario de multi-tenancy).
También debe elegir esta opción para aprovisionar almacenamiento en una SVM existente con SMB habilitado pero sin configurar. Este puede ser el caso si se creó la SVM para el acceso SAN o si no se habilitó ningún protocolo cuando se creó la SVM.

Después de habilitar SMB en la SVM, continúe aprovisionando un volumen o un qtree.

- Si desea aprovisionar un volumen o qtree en una SVM existente que esté completamente configurada para el acceso SMB, complete los pasos del apartado «"adición de capacidad de almacenamiento a una SVM habilitada para SMB"».

[Configurar el acceso de clientes SMB a almacenamiento compartido](#)

Hoja de trabajo para recopilar información de configuración de SMB

La hoja de datos de configuración de SMB permite recopilar la información necesaria para configurar el acceso SMB para clientes.

Debe rellenar una o ambas secciones de la hoja de datos, en función de la decisión que haya tomado sobre dónde aprovisionar almacenamiento:

- Si va a configurar el acceso SMB a una SVM, debe completar ambas secciones.

[Configurar el acceso de SMB a una SVM](#)

[Configurar el acceso de clientes SMB a almacenamiento compartido](#)

- Si va a añadir capacidad de almacenamiento a una SVM habilitada para SMB, solo debe completar la segunda sección.

[Configurar el acceso de clientes SMB a almacenamiento compartido](#)

Las páginas manuales de comandos contienen detalles sobre los parámetros.

Configurar el acceso de SMB a una SVM

Parámetros para crear una SVM

Proporcione estos valores con `vserver create` Si va a crear una SVM nueva.

| Campo | Descripción | Su valor |
|---|--|----------------------|
| <code>-vserver</code> | Un nombre que se proporciona para la SVM nueva que es un nombre de dominio completo (FQDN) o sigue otra convención que aplica nombres de SVM únicos en un clúster. | |
| <code>-aggregate</code> | El nombre de un agregado en el clúster con espacio suficiente para la nueva capacidad de almacenamiento de SMB. | |
| <code>-rootvolume</code> | Un nombre único que se proporciona para el volumen raíz de SVM. | |
| <code>-rootvolume-security-style</code> | Utilice el estilo de seguridad NTFS para la SVM. | <code>ntfs</code> |
| <code>-language</code> | Utilice la configuración de idioma predeterminada en este flujo de trabajo. | <code>C.UTF-8</code> |
| <code>ipspace</code> | Opcional: Los espacios IP son espacios de direcciones IP distintos en los que residen las SVM. | |

Parámetros para crear una LIF

Proporcione estos valores con `network interface create` Comando cuando crea las LIF.

| Campo | Descripción | Su valor |
|-------------------------------|---|-------------------|
| <code>-lif</code> | Nombre que se proporciona para la nueva LIF. | |
| <code>-role</code> | Utilice el rol de LIF de datos en este flujo de trabajo. | <code>data</code> |
| <code>-data-protocol</code> | Utilice solo el protocolo SMB en este flujo de trabajo. | <code>cifs</code> |
| <code>-home-node</code> | El nodo al que devuelve el LIF cuando el <code>network interface revert</code> El comando se ejecuta en la LIF. | |
| <code>-home-port</code> | El puerto o el grupo de interfaces al que devuelve la LIF cuando el <code>network interface revert</code> El comando se ejecuta en la LIF. | |
| <code>-address</code> | La dirección IPv4 o IPv6 del clúster que se usará para el acceso a los datos mediante la nueva LIF. | |
| <code>-netmask</code> | La máscara de red y la puerta de enlace para la LIF. | |
| <code>-subnet</code> | Un conjunto de direcciones IP. En lugar de <code>-address</code> y <code>-netmask</code> para asignar direcciones y máscaras de red automáticamente. | |
| <code>-firewall-policy</code> | Utilice la política de firewall de datos predeterminada en este flujo de trabajo. | <code>data</code> |
| <code>-auto-revert</code> | Opcional: Especifica si un LIF de datos se revierte automáticamente a su nodo principal en el inicio o bajo otras circunstancias. El valor predeterminado es <code>false</code> . | |

Parámetros para la resolución del nombre de host DNS

Proporcione estos valores con `vserver services name-service dns create` Comando cuando está

configurando DNS.

| Campo | Descripción | Su valor |
|----------------------------|--|----------|
| <code>-domains</code> | Hasta cinco nombres de dominio DNS. | |
| <code>-name-servers</code> | Hasta tres direcciones IP para cada servidor de nombres DNS. | |

Configuración de un servidor SMB en un dominio de Active Directory

Parámetros para la configuración del servicio de tiempo

Proporcione estos valores con `cluster time-service ntp server create` comando al configurar los servicios de hora.

| Campo | Descripción | Su valor |
|----------------------|---|----------|
| <code>-server</code> | El nombre de host o la dirección IP del servidor NTP para el dominio de Active Directory. | |

Parámetros para crear un servidor SMB en un dominio de Active Directory

Proporcione estos valores con `vserver cifs create` Cuando se crea un nuevo servidor SMB y se especifica la información del dominio.

| Campo | Descripción | Su valor |
|---------------------------|---|----------|
| <code>-vserver</code> | Nombre de la SVM en la que se creará el servidor SMB. | |
| <code>-cifs-server</code> | El nombre del servidor SMB (hasta 15 caracteres). | |
| <code>-domain</code> | El nombre de dominio completo (FQDN) del dominio de Active Directory para asociarlo con el servidor SMB. | |
| <code>-ou</code> | Opcional: La unidad organizativa del dominio de Active Directory que se asocia con el servidor SMB. De forma predeterminada, este parámetro se establece en CN=Computers. | |

| Campo | Descripción | Su valor |
|-------------------------------|--|----------|
| <code>-netbios-aliases</code> | Opcional: Lista de alias NetBIOS, que son nombres alternativos al nombre del servidor SMB. | |
| <code>-comment</code> | Opcional: Comentario de texto para el servidor. Los clientes de Windows pueden ver esta descripción del servidor SMB al explorar servidores en la red. | |

Configuración de un servidor SMB en un grupo de trabajo

Parámetros para crear un servidor SMB en un grupo de trabajo

Proporcione estos valores con `vserver cifs create` Comando cuando crea un nuevo servidor SMB y especifica las versiones de SMB admitidas.

| Campo | Descripción | Su valor |
|---------------------------|--|----------|
| <code>-vserver</code> | Nombre de la SVM en la que se creará el servidor SMB. | |
| <code>-cifs-server</code> | El nombre del servidor SMB (hasta 15 caracteres). | |
| <code>-workgroup</code> | El nombre del grupo de trabajo (hasta 15 caracteres). | |
| <code>-comment</code> | Opcional: Comentario de texto para el servidor. Los clientes de Windows pueden ver esta descripción del servidor SMB al explorar servidores en la red. | |

Parámetros para crear usuarios locales

Estos valores se proporcionan cuando se crean usuarios locales mediante el `vserver cifs users-and-groups local-user create` comando. Son necesarios para los servidores SMB en grupos de trabajo y opcionales en dominios AD.

| Campo | Descripción | Su valor |
|-------------------------|---|----------|
| <code>-vserver</code> | El nombre de la SVM en la que se creará el usuario local. | |
| <code>-user-name</code> | El nombre del usuario local (hasta 20 caracteres). | |

| Campo | Descripción | Su valor |
|----------------------|--|----------|
| -full-name | Optional: Nombre completo del usuario. Si el nombre completo contiene un espacio, escriba el nombre completo entre comillas dobles. | |
| -description | Optional: Una descripción para el usuario local. Si la descripción contiene un espacio, el parámetro debe escribirse entre comillas. | |
| -is-account-disabled | Opcional: Especifica si la cuenta de usuario está habilitada o deshabilitada. Si no se especifica este parámetro, el valor predeterminado es habilitar la cuenta de usuario. | |

Parámetros para crear grupos locales

Estos valores se proporcionan cuando se crean grupos locales mediante el `vserver cifs users-and-groups local-group create` comando. Son opcionales para servidores SMB en dominios AD y grupos de trabajo.

| Campo | Descripción | Su valor |
|--------------|--|----------|
| -vserver | Nombre de la SVM en la que se creará el grupo local. | |
| -group-name | El nombre del grupo local (hasta 256 caracteres). | |
| -description | Opcional: Descripción del grupo local. Si la descripción contiene un espacio, el parámetro debe escribirse entre comillas. | |

Se añade capacidad de almacenamiento a una SVM habilitada para SMB

Parámetros para crear un volumen

Proporcione estos valores con `volume create` comando si crea un volumen en lugar de un qtrees.

| Campo | Descripción | Su valor |
|----------|--|----------|
| -vserver | El nombre de una SVM nueva o existente que alojará el nuevo volumen. | |

| Campo | Descripción | Su valor |
|-----------------|--|----------|
| -volume | Se suministra un nombre descriptivo único para el volumen nuevo. | |
| -aggregate | El nombre de un agregado en el clúster de con espacio suficiente para el nuevo volumen de SMB. | |
| -size | Se proporciona un entero para el tamaño del nuevo volumen. | |
| -security-style | Utilice el estilo de seguridad NTFS para este flujo de trabajo. | ntfs |
| -junction-path | Ubicación bajo la raíz (/) donde se va a montar el nuevo volumen. | |

Parámetros para crear un qtree

Proporcione estos valores con `volume qtree create` comando si va a crear un qtree en lugar de un volumen.

| Campo | Descripción | Su valor |
|-------------|--|----------|
| -vserver | El nombre de la SVM en la que reside el volumen que contiene el qtree. | |
| -volume | El nombre del volumen que contendrá el nuevo qtree. | |
| -qtree | Nombre descriptivo único que se proporciona para el nuevo qtree, con 64 caracteres o menos. | |
| -qtree-path | El argumento de ruta de qtree en el formato /vol/volume_name/qtree_name\> se puede especificar en lugar de especificar el volumen y qtree como argumentos independientes. | |

Parámetros para crear recursos compartidos SMB

Proporcione estos valores con `vserver cifs share create` comando.

| Campo | Descripción | Su valor |
|--------------------------------|---|----------|
| <code>-vserver</code> | Nombre de la SVM en la que se creará el recurso compartido de SMB. | |
| <code>-share-name</code> | El nombre del recurso compartido de SMB que se desea crear (hasta 256 caracteres). | |
| <code>-path</code> | El nombre de la ruta al recurso compartido de SMB (hasta 256 caracteres). Esta ruta debe existir en un volumen antes de crear el recurso compartido. | |
| <code>-share-properties</code> | Opcional: Una lista de propiedades de recursos compartidos. La configuración predeterminada es <code>oplocks, browsable, changenotify, y. show-previous-versions</code> . | |
| <code>-comment</code> | Optional: Comentario de texto para el servidor (hasta 256 caracteres). Los clientes de Windows pueden ver esta descripción del recurso compartido de SMB al navegar por la red. | |

Parámetros para crear listas de control de acceso de recursos compartidos SMB (ACL)

Proporcione estos valores con `vserver cifs share access-control create` comando.

| Campo | Descripción | Su valor |
|-------------------------------|--|----------------------|
| <code>-vserver</code> | Nombre de la SVM en la que se creará la ACL de SMB. | |
| <code>-share</code> | Nombre del recurso compartido de SMB en el que se va a crear. | |
| <code>-user-group-type</code> | El tipo del usuario o grupo que se añadirá a la ACL del recurso compartido. El tipo predeterminado es <code>windows</code> | <code>windows</code> |

| Campo | Descripción | Su valor |
|----------------|--|-----------------|
| -user-or-group | El usuario o grupo que se añadirá a la ACL del recurso compartido. Si especifica el nombre de usuario, debe incluir el dominio del usuario con el formato "dain\username". | |
| -permission | Especifica los permisos para el usuario o grupo. | `[No_access |
| Read | Change | Full_Control]` |

Configure el acceso de SMB a una SVM

Configure el acceso de SMB a una SVM

Si todavía no tiene una SVM configurada para el acceso de cliente de SMB, debe crear y configurar una SVM nueva o configurar una SVM existente. La configuración de SMB implica abrir el acceso a volumen raíz de SVM, crear un servidor SMB, crear una LIF, habilitar la resolución de nombres de host, configurar servicios de nombres y, si lo desea, Habilitar la seguridad Kerberos.

Cree una SVM

Si no tiene al menos una SVM en un clúster para proporcionar acceso a los datos a los clientes de SMB, debe crear una.

Antes de empezar

- A partir de ONTAP 9.13.1, puede establecer una capacidad máxima para una máquina virtual de almacenamiento. También puede configurar alertas cuando la SVM se acerca a un nivel de umbral de capacidad. Para obtener más información, consulte [Gestionar la capacidad de SVM](#).

Pasos

1. Cree una SVM: `vserver create -vserver svm_name -rootvolume root_volume_name -aggregate aggregate_name -rootvolume-security-style ntfs -language C.UTF-8 -ipSPACE ipSPACE_name`
 - Utilice el valor NTFS para `-rootvolume-security-style` opción.
 - Utilice el C.UTF-8 predeterminado `-language` opción.
 - La `ipSPACE` el ajuste es opcional.
2. Compruebe la configuración y el estado de la SVM recién creada: `vserver show -vserver vserver_name`

La Allowed Protocols El campo debe incluir CIFS. Puede editar esta lista más tarde.

La Vserver Operational State el campo debe mostrar la `running` estado. Si muestra la `initializing` estado, significa que hubo un error en algunas operaciones intermedias, como la creación del volumen raíz, y que debe eliminarse la SVM y volver a crearla.

Ejemplos

El siguiente comando crea una SVM para el acceso de los datos en el espacio IP `ipspaceA`:

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style ntfs -language C.UTF-8 -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

El siguiente comando muestra que se creó una SVM con un volumen raíz de 1 GB, y se inició automáticamente y está en `running` estado. El volumen raíz tiene una política de exportación predeterminada que no incluye reglas, por lo que el volumen raíz no se exporta tras la creación.

```
cluster1::> vserver show -vserver vs1.example.com
                                Vserver: vs1.example.com
                                Vserver Type: data
                                Vserver Subtype: default
                                Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_vs1
                                Aggregate: aggr1
                                NIS Domain: -
                                Root Volume Security Style: ntfs
                                LDAP Client: -
                                Default Volume Language Code: C.UTF-8
                                Snapshot Policy: default
                                Comment:
                                Quota Policy: default
                                List of Aggregates Assigned: -
Limit on Maximum Number of Volumes allowed: unlimited
                                Vserver Admin State: running
                                Vserver Operational State: running
                                Vserver Operational State Stopped Reason: -
                                Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
                                Disallowed Protocols: -
                                QoS Policy Group: -
                                Config Lock: false
                                IPspace Name: ipspaceA
```



A partir de ONTAP 9.13.1, puede establecer una plantilla de grupo de políticas de calidad de servicio adaptativa, aplicando un límite máximo y mínimo de rendimiento a los volúmenes en la SVM. Solo puede aplicar esta política después de crear la SVM. Para obtener más información sobre este proceso, consulte [Defina una plantilla de grupo de políticas adaptativas](#).

Compruebe que el protocolo SMB esté habilitado en la SVM

Antes de poder configurar y utilizar SMB en las SVM, debe comprobar que el protocolo esté habilitado.

Acerca de esta tarea

Esto suele hacerse durante la configuración de la SVM, pero si no ha habilitar el protocolo durante la configuración, puede habilitarla más adelante mediante el `vserver add-protocols` comando.



Una vez creado, no puede agregar ni quitar un protocolo de una LIF.

También puede deshabilitar protocolos en las SVM mediante el `vserver remove-protocols` comando.

Pasos

1. Compruebe qué protocolos están habilitados y deshabilitados actualmente para la SVM: `vserver show -vserver vserver_name -protocols`

También puede utilizar el `vserver show-protocols` Comando para ver los protocolos habilitados actualmente en todas las SVM del clúster.

2. Si es necesario, habilite o deshabilite un protocolo:

- Para habilitar el protocolo SMB: `vserver add-protocols -vserver vserver_name -protocols cifs`
- Para desactivar un protocolo: `vserver remove-protocols -vserver vserver_name -protocols protocol_name[,protocol_name,...]`

3. Confirme que los protocolos activados y deshabilitados se han actualizado correctamente: `vserver show -vserver vserver_name -protocols`

Ejemplo

El siguiente comando muestra qué protocolos están habilitados y deshabilitados actualmente (permitidos y deshabilitados) en la SVM llamada vs1:

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver          Allowed Protocols          Disallowed Protocols
-----          -
vs1.example.com  cifs                        nfs, fcp, iscsi, ndmp
```

El siguiente comando permite acceder a través de SMB añadiendo `cifs` A la lista de protocolos habilitados en la SVM llamada vs1:

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols cifs
```

Abra la política de exportación del volumen raíz de la SVM

La política de exportación predeterminada del volumen raíz de la SVM debe incluir una regla para permitir que todos los clientes tengan acceso abierto a través de SMB. Sin

esta regla, se deniega el acceso a la SVM y a sus volúmenes a todos los clientes SMB.

Acerca de esta tarea

Cuando se crea una SVM nueva, se crea automáticamente una política de exportación predeterminada (denominada predeterminada) para el volumen raíz de la SVM. Debe crear una o varias reglas para la política de exportación predeterminada para que los clientes puedan acceder a los datos de la SVM.

Debe verificar que todo el acceso a SMB esté abierto en la política de exportación predeterminada y, más adelante, restringir el acceso a volúmenes individuales mediante la creación de políticas de exportación personalizadas para volúmenes o qtrees individuales.

Pasos

1. Si va a utilizar una SVM existente, compruebe la política de exportación de volumen raíz predeterminada:
`vserver export-policy rule show`

El resultado del comando debe ser similar a lo siguiente:

```
cluster::> vserver export-policy rule show -vserver vs1.example.com
-policyname default -instance

                                Vserver: vs1.example.com
                                Policy Name: default
                                Rule Index: 1
                                Access Protocol: cifs
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                                RO Access Rule: any
                                RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
                                Superuser Security Types: any
                                Honor SetUID Bits in SETATTR: true
                                Allow Creation of Devices: true
```

Si existe una regla de este tipo que permite el acceso abierto, esta tarea se completa. De lo contrario, continúe con el siguiente paso.

2. Cree una regla de exportación para el volumen raíz de la SVM: `vserver export-policy rule create -vserver vserver_name -policyname default -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule any -rwrule any -superuser any`
3. Compruebe la creación de reglas mediante `vserver export-policy rule show` comando.

Resultados

Ahora, cualquier cliente de SMB puede acceder a cualquier volumen o qtree creado en la SVM.

Cree una LIF

Una LIF es una dirección IP asociada con un puerto físico o lógico. Si hay un fallo de un componente, un LIF puede conmutar al respaldo o migrarse a un puerto físico diferente, lo que continúa comunicándose con la red.

Antes de empezar

- El puerto de red físico o lógico subyacente debe haber sido configurado para el administrador up estado.
- Si tiene pensado utilizar un nombre de subred para asignar la dirección IP y el valor de máscara de red para una LIF, la subred ya debe existir.

Las subredes contienen un grupo de direcciones IP que pertenecen a la misma subred de capa 3. Se crean mediante la `network subnet create` comando.

- El mecanismo para especificar el tipo de tráfico que maneja una LIF ha cambiado. Para ONTAP 9.5 y versiones anteriores, LIF usaba funciones para especificar el tipo de tráfico que gestionaría. A partir de ONTAP 9.6, los LIF utilizan políticas de servicio para especificar el tipo de tráfico que manejaría.

Acerca de esta tarea

- Puede crear tanto LIF IPv4 como IPv6 en el mismo puerto de red.
- Si tiene un gran número de LIF en su clúster, puede verificar la capacidad de LIF admitida en el clúster mediante el `network interface capacity show` Comando y la capacidad de LIF admitida en cada nodo mediante el `network interface capacity details show` (en el nivel de privilegio avanzado).
- A partir de ONTAP 9.7, si ya existen otras LIF para la SVM en la misma subred, no es necesario especificar el puerto de inicio de la LIF. ONTAP elige automáticamente un puerto aleatorio en el nodo raíz especificado en el mismo dominio de retransmisión que las otras LIF ya configuradas en la misma subred.

Pasos

1. Cree una LIF:

```
network interface create -vserver vservice_name -lif lif_name -role data -data
-protocol cifs -home-node node_name -home-port port_name {-address IP_address
-netmask IP_address | -subnet-name subnet_name} -firewall-policy data -auto
-revert {true|false}
```

| ONTAP 9.5 y anteriores |
|---|
| <code>`network interface create -vserver vservice_name -lif lif_name -role data -data-protocol cifs -home-node node_name -home-port port_name {-address IP_address -netmask IP_address</code> |
| <code>-subnet-name subnet_name} -firewall-policy data -auto-revert {true</code> |
| <code>false}`</code> |

| ONTAP 9.6 y posterior |
|---|
| <code>`network interface create -vserver vservice_name -lif lif_name -service-policy service_policy_name -home -node node_name -home-port port_name {-address IP_address -netmask IP_address</code> |
| <code>-subnet-name subnet_name} -firewall-policy data -auto-revert {true</code> |
| <code>false}`</code> |

- La `-role` No se requiere el parámetro al crear una LIF con una política de servicio (a partir de ONTAP 9.6).
- La `-data-protocol` No se requiere el parámetro al crear una LIF con una política de servicio (a partir de ONTAP 9.6). Cuando se utiliza ONTAP 9,5 y versiones anteriores, el `-data-protocol` Debe

especificarse el parámetro cuando se crea el LIF y no se puede modificar más adelante sin destruir ni volver a crear la LIF de datos.

- `-home-node` Es el nodo al que devuelve el LIF cuando el `network interface revert` El comando se ejecuta en la LIF.

También puede especificar si el LIF debería volver automáticamente al nodo raíz y al puerto raíz con el `-auto-revert` opción.

- `-home-port` Es el puerto físico o lógico al que devuelve la LIF cuando el `network interface revert` El comando se ejecuta en la LIF.
- Puede especificar una dirección IP con el `-address` y.. `-netmask` o puede habilitar la asignación desde una subred con `-subnet_name` opción.
- Al usar una subred para suministrar la dirección IP y la máscara de red, si la subred se definió con una puerta de enlace, se añadirá automáticamente a la SVM una ruta predeterminada a esa puerta de enlace cuando se cree una LIF con dicha subred.
- Si asigna direcciones IP manualmente (sin una subred), es posible que deba configurar una ruta predeterminada para una puerta de enlace si hay clientes o controladores de dominio en una subred IP diferente. La `network route create` La página man contiene información sobre la creación de una ruta estática dentro de una SVM.
- Para la `-firewall-policy` opción, utilice el mismo valor predeterminado `data` Como el rol de LIF.

Si lo desea, puede crear y agregar una política de firewall personalizada más adelante.



A partir de ONTAP 9.10.1, las políticas de firewall están obsoletas y sustituidas por completo por políticas de servicios LIF. Para obtener más información, consulte ["Configurar políticas de firewall para LIF"](#).

- `-auto-revert` Permite especificar si un LIF de datos se revierte automáticamente a su nodo principal en circunstancias como el inicio, los cambios en el estado de la base de datos de gestión o el momento en que se realiza la conexión de red. El valor predeterminado es `false`, pero puede establecerlo en `false` según las políticas de administración de red del entorno.

2. Compruebe que la LIF se ha creado correctamente:

```
network interface show
```

3. Compruebe que se pueda acceder a la dirección IP configurada:

| Para verificar una... | Usar... |
|-----------------------|----------------------------|
| Dirección IPv4 | <code>network ping</code> |
| Dirección IPv6 | <code>network ping6</code> |

Ejemplos

El siguiente comando crea una LIF y especifica la dirección IP y los valores de máscara de red mediante el `-address` y.. `-netmask` parámetros:

```
network interface create -vserver vs1.example.com -lif datalif1 -role data  
-data-protocol cifs -home-node node-4 -home-port elc -address 192.0.2.145  
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

El siguiente comando crea una LIF y asigna valores de dirección IP y máscara de red a partir de la subred especificada (denominada cliente1_sub):

```
network interface create -vserver vs3.example.com -lif datalif3 -role data  
-data-protocol cifs -home-node node-3 -home-port elc -subnet-name  
client1_sub -firewall-policy data -auto-revert true
```

El siguiente comando muestra todas las LIF del clúster-1. Data LIF datalif1 y datalif3 están configurados con direcciones IPv4, y datalif4 está configurado con una dirección IPv6:

```
network interface show
```

| Vserver | Logical Interface | Status Admin/Oper | Network Address/Mask | Current Node | Current Port | Is |
|-----------------|-------------------|-------------------|----------------------|--------------|--------------|-------|
| Home | | | | | | |
| ----- | ----- | ----- | ----- | ----- | ----- | ----- |
| cluster-1 | | | | | | |
| cluster_mgmt | up/up | 192.0.2.3/24 | node-1 | e1a | | |
| true | | | | | | |
| node-1 | | | | | | |
| clus1 | up/up | 192.0.2.12/24 | node-1 | e0a | | |
| true | | | | | | |
| clus2 | up/up | 192.0.2.13/24 | node-1 | e0b | | |
| true | | | | | | |
| mgmt1 | up/up | 192.0.2.68/24 | node-1 | e1a | | |
| true | | | | | | |
| node-2 | | | | | | |
| clus1 | up/up | 192.0.2.14/24 | node-2 | e0a | | |
| true | | | | | | |
| clus2 | up/up | 192.0.2.15/24 | node-2 | e0b | | |
| true | | | | | | |
| mgmt1 | up/up | 192.0.2.69/24 | node-2 | e1a | | |
| true | | | | | | |
| vs1.example.com | | | | | | |
| datalif1 | up/down | 192.0.2.145/30 | node-1 | e1c | | |
| true | | | | | | |
| vs3.example.com | | | | | | |
| datalif3 | up/up | 192.0.2.146/30 | node-2 | e0c | | |
| true | | | | | | |
| datalif4 | up/up | 2001::2/64 | node-2 | e0c | | |
| true | | | | | | |

5 entries were displayed.

El siguiente comando muestra cómo crear una LIF de datos NAS asignada con default-data-files política de servicio:

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport e0d -service-policy default-data-files -subnet-name ipspace1
```

Habilite DNS para la resolución de nombres de host

Puede utilizar el `vserver services name-service dns` Comando para habilitar DNS en una SVM y configurarlo para usar DNS en la resolución de nombres de host. Los

nombres de host se resuelven mediante servidores DNS externos.

Antes de empezar

Un servidor DNS para todo el sitio debe estar disponible para las búsquedas de nombre de host.

Debe configurar más de un servidor DNS para evitar un único punto de error. La `vserver services name-service dns create` El comando emite una advertencia si introduce solo un nombre de servidor DNS.

Acerca de esta tarea

La *Network Management Guide* contiene información acerca de la configuración de DNS dinámico en la SVM.

Pasos

- 1. Habilite DNS en la SVM: `vserver services name-service dns create -vserver vserver_name -domains domain_name -name-servers ip_addresses -state enabled`

El siguiente comando habilita los servidores DNS externos en la SVM vs1:

```
vserver services name-service dns create -vserver vs1.example.com
-domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
enabled
```



A partir de ONTAP 9.2, el `vserver services name-service dns create` El comando realiza una validación automática de la configuración e informa de un mensaje de error si ONTAP no puede ponerse en contacto con el servidor de nombres.

- 2. Muestre las configuraciones del dominio DNS mediante `vserver services name-service dns show` comando. "

El siguiente comando muestra las configuraciones de DNS de todas las SVM del clúster:

```
vserver services name-service dns show
```

| Vserver | State | Domains | Name Servers |
|-----------------|---------|-------------|-----------------------------|
| cluster1 | enabled | example.com | 192.0.2.201, 192.0.2.202 |
| vs1.example.com | enabled | example.com | 192.0.2.201, 192.0.2.202 |

El siguiente comando muestra información detallada de la configuración de DNS para SVM vs1:

```
vserver services name-service dns show -vserver vs1.example.com
Vserver: vs1.example.com
Domains: example.com
Name Servers: 192.0.2.201, 192.0.2.202
Enable/Disable DNS: enabled
Timeout (secs): 2
Maximum Attempts: 1
```

3. Valide el estado de los servidores de nombres utilizando `vserver services name-service dns check` comando.

La `vserver services name-service dns check` El comando está disponible a partir de ONTAP 9.2.

```
vserver services name-service dns check -vserver vs1.example.com
```

| Vserver | Name Server | Status | Status Details |
|-----------------|-------------|--------|-------------------------|
| ----- | ----- | ----- | |
| vs1.example.com | 10.0.0.50 | up | Response time (msec): 2 |
| vs1.example.com | 10.0.0.51 | up | Response time (msec): 2 |

Configurar un servidor SMB en un dominio de Active Directory

Configurar los servicios de tiempo

Antes de crear un servidor SMB en una controladora de Active Domain, debe asegurarse de que la hora y la hora del clúster de los controladores de dominio al que pertenecerá el servidor SMB coincidan con en un plazo de cinco minutos.

Acerca de esta tarea

Debe configurar los servicios NTP del clúster para que usen los mismos servidores NTP para la sincronización horaria que utiliza el dominio de Active Directory.

A partir de ONTAP 9.5, puede configurar el servidor NTP con autenticación simétrica.

Pasos

1. Configure los servicios de hora mediante el `cluster time-service ntp server create` comando.
 - Para configurar los servicios de hora sin autenticación simétrica, introduzca el siguiente comando:
`cluster time-service ntp server create -server server_ip_address`
 - Para configurar los servicios de hora con autenticación simétrica, introduzca el siguiente comando:
`cluster time-service ntp server create -server server_ip_address -key-id key_id`
`cluster time-service ntp server create -server 10.10.10.1 cluster time-`
`service ntp server create -server 10.10.10.2`


2. Compruebe que los servicios de hora se han configurado correctamente mediante el `cluster time-service ntp server show` comando.


```
cluster time-service ntp server show
```

| Server | Version |
|------------|---------|
| ----- | ----- |
| 10.10.10.1 | auto |
| 10.10.10.2 | auto |

Comandos para gestionar la autenticación simétrica en servidores NTP

A partir de ONTAP 9.5, se admite la versión 3 del protocolo de tiempo de redes (NTP). NTPv3 incluye autenticación simétrica mediante claves SHA-1 que aumenta la seguridad de la red.

| Para hacer esto... | Se usa este comando... |
|---|---|
| Configure un servidor NTP sin autenticación simétrica | <code>cluster time-service ntp server create -server server_name</code> |
| Configure un servidor NTP con autenticación simétrica | <code>cluster time-service ntp server create -server server_ip_address -key-id key_id</code> |
| Habilitar autenticación simétrica para un servidor NTP existente se puede modificar el servidor NTP existente para habilitar la autenticación agregando el Id. De clave requerido | <code>cluster time-service ntp server modify -server server_name -key-id key_id</code> |
| Configure una clave NTP compartida | <code>cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value</code> <div>  <p>Las claves compartidas se refieren a un ID. El ID, su tipo y el valor deben ser idénticos tanto en el nodo como en el servidor NTP</p> </div> |
| Configure un servidor NTP con un ID de clave desconocido | <code>cluster time-service ntp server create -server server_name -key-id key_id</code> |

| Para hacer esto... | Se usa este comando... |
|---|---|
| Configure un servidor con un ID de clave no configurado en el servidor NTP. | <pre>cluster time-service ntp server create -server server_name -key-id key_id</pre> <div>  <p>El ID de clave, el tipo y el valor deben ser idénticos al ID de clave, el tipo y el valor configurados en el servidor NTP.</p> </div> |
| Deshabilitar la autenticación simétrica | <pre>cluster time-service ntp server modify -server server_name -authentication disabled</pre> |

Cree un servidor SMB en un dominio de Active Directory

Puede utilizar el `vserver cifs create` Para crear un servidor SMB en la SVM y especificar el dominio de Active Directory (AD) al que pertenece.

Antes de empezar

Las SVM y los LIF que utiliza para servir datos deben haberse configurado para permitir el protocolo SMB. Las LIF deben poder conectarse a los servidores DNS configurados en la SVM y a un controlador de dominio AD del dominio al que desea unirse al servidor SMB.

Cualquier usuario con autorización para crear cuentas de máquina en el dominio de AD al que se va a unir el servidor SMB puede crear el servidor SMB en la SVM. Esto puede incluir usuarios de otros dominios.

A partir de ONTAP 9.7, el administrador de AD puede proporcionarle un URI a un archivo keytab como alternativa a proporcionarle un nombre y una contraseña a una cuenta de Windows con privilegios. Cuando reciba el URI, inclúyalo en el `-keytab-uri` con el `vserver cifs` comandos.

Acerca de esta tarea

Al crear un servidor SMB en un dominio de directorio de actividades:

- Debe usar el nombre de dominio completo (FQDN) al especificar el dominio.
- La configuración predeterminada es agregar la cuenta de máquina del servidor SMB al objeto CN=Computer de Active Directory.
- Puede optar por agregar el servidor SMB a una unidad organizativa (OU) diferente mediante el `-ou` opción.
- Opcionalmente, puede elegir agregar una lista delimitada por comas de uno o más alias NetBIOS (hasta 200) para el servidor SMB.

La configuración de alias NetBIOS para un servidor SMB puede ser útil cuando está consolidando datos de otros servidores de archivos en el servidor SMB y desea que el servidor SMB responda a los nombres de los servidores originales.

La `vserver cifs` las páginas de manual contienen parámetros opcionales y requisitos de nomenclatura adicionales.



A partir de ONTAP 9.1, puede habilitar SMB versión 2.0 para conectarse a un controlador de dominio (DC). Hacerlo es necesario si ha deshabilitado SMB 1.0 en controladores de dominio. A partir de ONTAP 9.2, SMB 2.0 está habilitado de forma predeterminada.

A partir de ONTAP 9.8, puede especificar que se cifren las conexiones a los controladores de dominio. ONTAP requiere cifrado para las comunicaciones del controlador de dominio cuando el `-encryption-required -for-dc-connection` opción establecida en `true`; el valor predeterminado es `false`. Cuando se establece la opción, solo se utilizará el protocolo SMB3 para las conexiones ONTAP-DC, ya que el cifrado solo es compatible con SMB3. .

"[Gestión de SMB](#)" Contiene más información acerca de las opciones de configuración del servidor SMB.

Pasos

1. Compruebe que SMB tiene licencia en el clúster: `system license show -package cifs`

La licencia SMB se incluye con "ONTAP One". Si no tiene ONTAP One y la licencia no está instalada, póngase en contacto con su representante de ventas.

No se requiere una licencia de CIFS si el servidor SMB se usará solo para autenticación.

2. Cree el servidor SMB en un dominio de AD: `vserver cifs create -vserver vserver_name -cifs-server smb_server_name -domain FQDN [-ou organizational_unit] [-netbios-aliases NetBIOS_name, ...] [-keytab-uri {(ftp|http)://hostname|IP_address}] [-comment text]`

Al unirse a un dominio, este comando puede tardar varios minutos en completarse.

El siguiente comando crea el servidor SMB «s' mb_server01» en el dominio "example.com":

```
cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
smb_server01 -domain example.com
```

El siguiente comando crea el servidor SMB «smemoria_servidor 2» en el dominio «mydomain.com» y autentica al administrador ONTAP con un archivo keytab:

```
cluster1::> vserver cifs create -vserver vs1.mydomain.com -cifs-server
smb_server02 -domain mydomain.com -keytab-uri
http://admin.mydomain.com/ontap1.keytab
```

3. Compruebe la configuración del servidor SMB mediante el `vserver cifs show` comando.

En este ejemplo, el resultado del comando muestra que se creó en SVM vs1.example.com un servidor SMB denominado "MB_SERVER01", que se unió al dominio "example.com".

```
cluster1::> vserver cifs show -vserver vs1

Vserver: vs1.example.com
CIFS Server NetBIOS Name: SMB_SERVER01
NetBIOS Domain/Workgroup Name: EXAMPLE
Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
Authentication Style: domain
CIFS Server Administrative Status: up
CIFS Server Description: -
List of NetBIOS Aliases: -
```

4. Si lo desea, habilite la comunicación cifrada con el controlador de dominio (ONTAP 9.8 y posterior):
- ```
vserver cifs security modify -vserver svm_name -encryption-required-for-dc
-connection true
```

### Ejemplos

El siguiente comando crea un servidor SMB denominado «mb\_server02» en la SVM vs2.example.com en el dominio «'example.com'». La cuenta de equipo se crea en el contenedor "OU=eng,OU=corp,DC=example,DC=com". Al servidor SMB se le asigna un alias NetBIOS.

```
cluster1::> vserver cifs create -vserver vs2.example.com -cifs-server
smb_server02 -domain example.com -ou OU=eng,OU=corp -netbios-aliases
old_cifs_server01

cluster1::> vserver cifs show -vserver vs1

Vserver: vs2.example.com
CIFS Server NetBIOS Name: SMB_SERVER02
NetBIOS Domain/Workgroup Name: EXAMPLE
Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
Authentication Style: domain
CIFS Server Administrative Status: up
CIFS Server Description: -
List of NetBIOS Aliases: OLD_CIFS_SERVER01
```

El siguiente comando permite a un usuario de un dominio diferente, en este caso un administrador de un dominio de confianza, crear un servidor SMB denominado «smemoria\_servidor03» en la SVM vs3.example.com. La `-domain` La opción especifica el nombre del dominio principal (especificado en la configuración DNS) en el que desea crear el servidor SMB. La `username` la opción especifica el administrador del dominio de confianza.

- Dominio principal: example.com
- Dominio de confianza: trust.lab.com
- Nombre de usuario del dominio de confianza: Administrador1

```
cluster1::> vserver cifs create -vserver vs3.example.com -cifs-server
smb_server03 -domain example.com
```

```
Username: Administrator1@trust.lab.com
```

```
Password: . . .
```

### Crear archivos keytab para autenticación SMB

A partir de ONTAP 9.7, ONTAP admite la autenticación de SVM con servidores Active Directory (AD) mediante archivos keytab. Los administradores DE AD generan un archivo keytab y lo ponen a disposición de los administradores de ONTAP como un identificador uniforme de recursos (URI), que se proporciona cuando `vserver cifs`. Los comandos requieren autenticación Kerberos con el dominio AD.

Los administradores DE AD pueden crear los archivos keytab utilizando el servidor estándar de Windows `ktpass` comando. El comando debe ejecutarse en el dominio principal donde la autenticación es necesaria. La `ktpass` el comando se puede utilizar para generar archivos keytab sólo para usuarios de dominio principal; las claves generadas con usuarios de dominio de confianza no son compatibles.

Los archivos keytab se generan para usuarios específicos de administrador de ONTAP. Siempre que la contraseña del usuario administrador no cambie, las claves generadas para el tipo de cifrado específico y el dominio no cambiarán. Por lo tanto, se requiere un nuevo archivo keytab cada vez que se cambia la contraseña del usuario admin.

Se admiten los siguientes tipos de cifrado:

- AES256-SHA1
- DES-CBC-MD5



ONTAP no admite el tipo de cifrado DES-CBC-CRC.

- RC4-HMAC

AES256 es el tipo de cifrado más alto y se debe utilizar si está activado en el sistema ONTAP.

Los archivos keytab se pueden generar especificando la contraseña de administrador o mediante una contraseña generada aleatoriamente. Sin embargo, en cualquier momento sólo se puede utilizar una opción de contraseña, ya que en el servidor AD se necesita una clave privada específica para el usuario administrador para descifrar las claves del archivo keytab. Cualquier cambio en la clave privada de un administrador específico anulará el archivo keytab.

### Configurar un servidor SMB en un grupo de trabajo

#### Configure un servidor SMB en una descripción general de grupo de trabajo

La configuración de un servidor SMB como miembro de un grupo de trabajo consiste en crear el servidor SMB y, a continuación, crear usuarios y grupos locales.

Puede configurar un servidor SMB en un grupo de trabajo cuando la infraestructura de dominio de Microsoft Active Directory no está disponible.

Un servidor SMB en modo de grupo de trabajo sólo admite autenticación NTLM y no admite autenticación Kerberos.

### Cree un servidor SMB en un grupo de trabajo

Puede utilizar el `vserver cifs create` Comando para crear un servidor SMB en la SVM y especificar el grupo de trabajo al que pertenece.

#### Antes de empezar

Las SVM y los LIF que utiliza para servir datos deben haberse configurado para permitir el protocolo SMB. Los LIF deben poder conectarse con los servidores DNS que estén configurados en la SVM.

#### Acerca de esta tarea

Los servidores SMB en modo de grupo de trabajo no admiten las siguientes funciones de SMB:

- Protocolo de testimonio de SMB3
- Recursos compartidos de CA de SMB3
- SQL sobre SMB
- Redirección de carpetas
- Perfiles de roaming
- Objeto de directiva de grupo (GPO)
- Servicio Snapshot de volumen (VSS)

La `vserver cifs` las páginas de manual contienen parámetros de configuración y requisitos de nomenclatura opcionales adicionales.

#### Pasos

1. Compruebe que SMB tiene licencia en el clúster: `system license show -package cifs`

La licencia SMB se incluye con "ONTAP One". Si no tiene ONTAP One y la licencia no está instalada, póngase en contacto con su representante de ventas.

No se requiere una licencia de CIFS si el servidor SMB se usará solo para autenticación.

2. Cree el servidor SMB en un grupo de trabajo: `vserver cifs create -vserver vserver_name -cifs-server cifs_server_name -workgroup workgroup_name [-comment text]`

El siguiente comando crea el servidor SMB «s' mb\_server01» en el grupo de trabajo «'workgroup01'»:

```
cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
SMB_SERVER01 -workgroup workgroup01
```

3. Compruebe la configuración del servidor SMB mediante el `vserver cifs show` comando.

En el ejemplo siguiente, el resultado del comando muestra que se creó un servidor SMB denominado «MB\_server01» en SVM vs1.example.com en el grupo de trabajo «'workgroup01'»:

```
cluster1::> vserver cifs show -vserver vs0

Vserver: vs1.example.com
CIFS Server NetBIOS Name: SMB_SERVER01
NetBIOS Domain/Workgroup Name: workgroup01
Fully Qualified Domain Name: -
Organizational Unit: -
Default Site Used by LIFs Without Site Membership: -
Workgroup Name: workgroup01
Authentication Style: workgroup
CIFS Server Administrative Status: up
CIFS Server Description:
List of NetBIOS Aliases: -
```

### Después de terminar

Para un servidor CIFS en un grupo de trabajo, debe crear usuarios locales y, opcionalmente, grupos locales en la SVM.

### Información relacionada

["Gestión de SMB"](#)

### Crear cuentas de usuario locales

Se puede crear una cuenta de usuario local que se pueda utilizar para autorizar el acceso a los datos contenidos en la SVM a través de una conexión de SMB. También es posible usar cuentas de usuario locales para la autenticación al crear una sesión SMB.

### Acerca de esta tarea

La funcionalidad de usuario local se habilita de forma predeterminada cuando se crea la SVM.

Al crear una cuenta de usuario local, debe especificar un nombre de usuario y debe especificar la SVM con la que desea asociar la cuenta.

La `vserver cifs users-and-groups local-user` las páginas de manual contienen detalles sobre parámetros opcionales y requisitos de nomenclatura.

### Pasos

1. Cree el usuario local: `vserver cifs users-and-groups local-user create -vserver vserver_name -user-name user_name optional_parameters`

Los siguientes parámetros opcionales pueden ser útiles:

- `-full-name`

Nombre completo del usuario.

- `-description`

Una descripción para el usuario local.

◦ `-is-account-disabled {true|false}`

Especifica si la cuenta de usuario está habilitada o deshabilitada. Si no se especifica este parámetro, el valor predeterminado es habilitar la cuenta de usuario.

El comando solicita la contraseña del usuario local.

2. Introduzca una contraseña para el usuario local y confirme la contraseña.
3. Compruebe que el usuario se ha creado correctamente: `vserver cifs users-and-groups local-user show -vserver vserver_name`

### Ejemplo

En el siguiente ejemplo se crea un usuario local «MMB\_SERVER01\sue», con el nombre completo «Sue Chang», asociado a SVM vs1.example.com:

```
cluster1::> vserver cifs users-and-groups local-user create -vserver
vs1.example.com -user-name SMB_SERVER01\sue -full-name "Sue Chang"

Enter the password:
Confirm the password:

cluster1::> vserver cifs users-and-groups local-user show
Vserver User Name Full Name Description
----- -
vs1 SMB_SERVER01\Administrator Built-in administrator
account
vs1 SMB_SERVER01\sue Sue Chang
```

### Crear grupos locales

Es posible crear grupos locales que se puedan utilizar para autorizar el acceso a los datos asociados con la SVM a través de una conexión de SMB. También puede asignar privilegios que definen los derechos de usuario o las capacidades que tiene un miembro del grupo.

### Acerca de esta tarea

La funcionalidad de grupo local se habilita de forma predeterminada cuando se crea la SVM.

Cuando se crea un grupo local, debe especificar un nombre para el grupo y debe especificar la SVM con la que desea asociar el grupo. Puede especificar un nombre de grupo con o sin el nombre de dominio local y, opcionalmente, puede especificar una descripción para el grupo local. No puede agregar un grupo local a otro grupo local.

La `vserver cifs users-and-groups local-group` las páginas de manual contienen detalles sobre parámetros opcionales y requisitos de nomenclatura.

### Pasos

1. Cree el grupo local: `vserver cifs users-and-groups local-group create -vserver vserver_name -group-name group_name`

El siguiente parámetro opcional puede ser útil:

- `-description`

Una descripción para el grupo local.

2. Compruebe que el grupo se ha creado correctamente: `vserver cifs users-and-groups local-group show -vserver vserver_name`

### Ejemplo

En el siguiente ejemplo se crea un grupo local "MB\_SERVER01\engineering" asociado con SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group create -vserver
vs1.example.com -group-name SMB_SERVER01\engineering
```

```
cluster1::> vserver cifs users-and-groups local-group show -vserver
vs1.example.com
```

| Vserver         | Group Name               | Description               |
|-----------------|--------------------------|---------------------------|
| vs1.example.com | BUILTIN\Administrators   | Built-in Administrators   |
| vs1.example.com | BUILTIN\Backup Operators | Backup Operators group    |
| vs1.example.com | BUILTIN\Power Users      | Restricted administrative |
| vs1.example.com | BUILTIN\Users            | All users                 |
| vs1.example.com | SMB_SERVER01\engineering |                           |
| vs1.example.com | SMB_SERVER01\sales       |                           |

### Después de terminar

Debe agregar miembros al nuevo grupo.

### Administrar la pertenencia a grupos locales

Puede administrar la pertenencia a grupos locales agregando y eliminando usuarios locales o de dominio, o agregando y eliminando grupos de dominios. Esto resulta útil si desea controlar el acceso a los datos basándose en los controles de acceso colocados en el grupo o si desea que los usuarios tengan privilegios asociados a ese grupo.

### Acerca de esta tarea

Si ya no desea que un usuario local, un usuario de dominio o un grupo de dominio tenga derechos de acceso o privilegios basados en la pertenencia a un grupo, puede quitar el miembro del grupo.

Debe tener en cuenta lo siguiente al agregar miembros a un grupo local:

- No puede agregar usuarios al grupo especial *Everyone*.



- No puede agregar un grupo local a otro grupo local.
- Para agregar un usuario o grupo de dominio a un grupo local, ONTAP debe poder resolver el nombre a un SID.

Debe tener en cuenta lo siguiente al quitar miembros de un grupo local:

- No puede eliminar miembros del grupo especial *Everyone*.
- Para quitar un miembro de un grupo local, ONTAP debe poder resolver su nombre a un SID.

## Pasos

### 1. Agregar o quitar un miembro de un grupo.

- Añadir miembro: `vserver cifs users-and-groups local-group add-members -vserver vserver_name -group-name group_name -member-names name[,...]`

Puede especificar una lista delimitada por comas de usuarios locales, usuarios de dominio o grupos de dominio que desee agregar al grupo local especificado.

- Quitar un miembro: `vserver cifs users-and-groups local-group remove-members -vserver vserver_name -group-name group_name -member-names name[,...]`

Puede especificar una lista delimitada por comas de usuarios locales, usuarios de dominio o grupos de dominio que desee quitar del grupo local especificado.

## Ejemplos

En el siguiente ejemplo se agrega un usuario local "MB\_SERVER01\sue" al grupo local "MB\_SERVER01\engineering" en la SVM vs1.example.com:

```
cluster1::> vserver cifs users-and-groups local-group add-members -vserver
vs1.example.com -group-name SMB_SERVER01\engineering -member-names
SMB_SERVER01\sue
```

En el siguiente ejemplo se eliminan los usuarios locales "MB\_SERVER01\sue" y "MB\_SERVER01\james" del grupo local "MB\_SERVER01\engineering" en la SVM vs1.example.com:

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1.example.com -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

## Compruebe las versiones habilitadas de SMB

En la versión ONTAP 9, se determinan las versiones de SMB que se habilitan de forma predeterminada para las conexiones con clientes y controladoras de dominio. Debe verificar si el servidor SMB admite los clientes y la funcionalidad que requiere su entorno.

### Acerca de esta tarea

Para las conexiones con clientes y controladoras de dominio, debe habilitar SMB 2.0 y una versión posterior siempre que sea posible. Por motivos de seguridad, debe evitar el uso de SMB 1.0 y debe deshabilitarlo si ha

verificado que no es necesario en su entorno.

En ONTAP 9, las versiones 2.0 y posteriores de SMB se habilitan de forma predeterminada para conexiones cliente, pero la versión de SMB 1.0 habilitada de forma predeterminada depende de su versión de ONTAP.

- A partir de ONTAP 9.1 P8, SMB 1.0 se puede deshabilitar en las SVM.

La `-smb1-enabled` de la `vserver cifs options modify` El comando habilita o deshabilita SMB 1.0.

- A partir de ONTAP 9.3, está deshabilitado de forma predeterminada en las nuevas SVM.

Si el servidor SMB se encuentra en un dominio de Active Directory (AD), es posible habilitar SMB 2.0 para conectarse a un controlador de dominio (DC) empezando por ONTAP 9.1. Es necesario hacerlo si ha deshabilitado SMB 1.0 en los centros de datos. A partir de ONTAP 9.2, SMB 2.0 está habilitado de forma predeterminada para las conexiones de CC.



Si `-smb1-enabled-for-dc-connections` se establece en `false` aunque `-smb1-enabled` se establece en `true`, ONTAP deniega las conexiones SMB 1.0 como cliente, pero continúa aceptando conexiones SMB 1.0 entrantes como servidor.

**"Gestión de SMB"** Contiene detalles sobre las versiones y la funcionalidad SMB admitidas.

## Pasos

1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Compruebe qué versiones de SMB están habilitadas:

```
vserver cifs options show
```

Puede desplazarse hacia abajo por la lista para ver las versiones de SMB habilitadas para conexiones de clientes y si está configurando un servidor SMB en un dominio de AD para conexiones de dominio de AD.

3. Habilite o deshabilite el protocolo SMB para las conexiones de cliente según sea necesario:

- Para habilitar una versión de SMB:

```
vserver cifs options modify -vserver vserver_name smb_version true
```

- Para deshabilitar una versión de SMB:

```
vserver cifs options modify -vserver vserver_name smb_version false
```

Los valores posibles para `smb_version`:

- -smb1-enabled
- -smb2-enabled
- -smb3-enabled
- -smb31-enabled

El siguiente comando habilita SMB 3.1 en la SVM vs1.example.com:

```
cluster1::*> vserver cifs options modify -vserver vs1.example.com -smb31-enabled true
```

1. Si el servidor SMB se encuentra en un dominio de Active Directory, habilite o deshabilite el protocolo SMB para las conexiones DC según sea necesario:

- Para habilitar una versión de SMB:

```
vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc-connections true
```

- Para deshabilitar una versión de SMB:

```
vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc-connections false
```

2. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

## Asigne el servidor SMB en el servidor DNS

El servidor DNS del sitio debe tener una entrada que apunte el nombre del servidor SMB y cualquier alias NetBIOS a la dirección IP de la LIF de datos para que los usuarios de Windows puedan asignar una unidad al nombre del servidor SMB.

### Antes de empezar

Debe tener acceso administrativo al servidor DNS del sitio. Si no tiene acceso administrativo, debe solicitar al administrador DNS que realice esta tarea.

### Acerca de esta tarea

Si utiliza alias NetBIOS para el nombre del servidor SMB, es una práctica recomendada crear puntos de entrada del servidor DNS para cada alias.

### Pasos

1. Inicie sesión en el servidor DNS.

2. Cree entradas de búsqueda hacia delante (a - Registro de dirección) e inversa (PTR - Registro de puntero) para asignar el nombre del servidor SMB a la dirección IP de la LIF de datos.
3. Si utiliza alias NetBIOS, cree una entrada de búsqueda Alias nombre canónico (registro de recursos CNAME) para asignar cada alias a la dirección IP de la LIF de datos del servidor SMB.

## Resultados

Una vez que la asignación se propaga a través de la red, los usuarios de Windows pueden asignar una unidad al nombre del servidor SMB o sus alias NetBIOS.

## Configure el acceso de clientes SMB al almacenamiento compartido

### Configure el acceso de clientes SMB al almacenamiento compartido

Para proporcionar acceso al cliente SMB al almacenamiento compartido en una SVM, debe crear un volumen o qtree para proporcionar un contenedor de almacenamiento y, a continuación, crear o modificar un recurso compartido para ese contenedor. Luego, puede configurar los permisos de recursos compartidos y archivos, y probar el acceso desde sistemas cliente.

#### Antes de empezar

- El bloque de mensajes del servidor debe estar configurado por completo en la SVM.
- Se debe completar cualquier actualización de la configuración de los servicios de nombres.
- Cualquier adición o modificación a una configuración de dominio o grupo de trabajo de Active Directory debe estar completa.

### Cree un volumen o un contenedor de almacenamiento Qtree

#### Cree un volumen

Puede crear un volumen y especificar su punto de unión y otras propiedades mediante el `volume create` comando.

#### Acerca de esta tarea

Un volumen debe incluir una *ruta de unión* para que sus datos estén disponibles para los clientes. Puede especificar la ruta de unión cuando cree un nuevo volumen. Si crea un volumen sin especificar una ruta de unión, debe *Mount* el volumen en el espacio de nombres de la SVM mediante el `volume mount` comando.

#### Antes de empezar

- SMB debe estar configurado y en ejecución.
- El estilo de seguridad de la SVM debe ser NTFS.
- A partir de ONTAP 9.13.1, se pueden crear volúmenes con análisis de capacidad y seguimiento de actividades habilitados. Para activar la capacidad o el seguimiento de actividades, emita el `volume create` comando con `-analytics-state on` o `-activity-tracking-state establezca en on`.

Para obtener más información sobre el análisis de capacidad y el seguimiento de actividades, consulte [Active File System Analytics](#).

## Pasos

1. Cree el volumen con un punto de unión: `volume create -vserver svm_name -volume`

```
volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]}
-security-style ntfs -junction-path junction_path]
```

Las opciones para `-junction-path` son las siguientes:

- Directamente bajo la raíz, por ejemplo, `/new_vol`

Puede crear un nuevo volumen y especificar que se monte directamente en el volumen raíz de SVM.

- En un directorio existente, por ejemplo, `/existing_dir/new_vol`

Puede crear un nuevo volumen y especificar que se monte en un volumen existente (en una jerarquía existente), expresado como un directorio.

Si desea crear un volumen en un nuevo directorio (en una nueva jerarquía debajo de un nuevo volumen), por ejemplo, `/new_dir/new_vol`, Entonces debe crear primero un nuevo volumen principal que se junte al volumen raíz de la SVM. A continuación, creará el nuevo volumen secundario en la ruta de unión del nuevo volumen principal (nuevo directorio).

2. Compruebe que el volumen se ha creado con el punto de unión deseado: `volume show -vserver svm_name -volume volume_name -junction`

## Ejemplos

El siguiente comando crea un nuevo volumen denominado `user1` en la SVM `vs1.example.com` y el agregado `aggr1`. El nuevo volumen está disponible en `/users`. El tamaño del volumen es de 750 GB y su garantía de volumen es del tipo `volumen` (de forma predeterminada).

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1.example.com -volume users -junction
```

|                 |        | Junction |               | Junction    |
|-----------------|--------|----------|---------------|-------------|
| Vserver         | Volume | Active   | Junction Path | Path Source |
| vs1.example.com | users1 | true     | /users        | RW_volume   |

El siguiente comando crea un nuevo volumen denominado «'home4'» en la SVM «'vs1.example.com'» y el agregado «'aggr1'». El directorio `/eng/` Ya existe en el espacio de nombres para el SVM `vs1` y el nuevo volumen estará disponible en `/eng/home`, que se convierte en el directorio principal de `/eng/` espacio de nombres. El volumen tiene un tamaño de 750 GB y su garantía de volumen es de tipo `volume` (de forma predeterminada).

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
```

| Vserver         | Volume | Active | Junction Path | Junction Path Source |
|-----------------|--------|--------|---------------|----------------------|
| vs1.example.com | home4  | true   | /eng/home     | RW_volume            |

## Cree un qtree

Puede crear un qtree para que contenga datos y especificar sus propiedades mediante la `volume qtree create` comando.

## Antes de empezar

- La SVM y el volumen que contendrán el nuevo qtree ya deben existir.
- El estilo de seguridad de la SVM debe ser NTFS y el SMB debe configurarse y ejecutarse.

## Pasos

1. Cree el qtree: `volume qtree create -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path } -security-style ntfs`

Puede especificar el volumen y el qtree como argumentos independientes o especificar el argumento de la ruta de qtree en el formato `/vol/volume_name/_qtree_name`.

2. Compruebe que el qtree se ha creado con la ruta de unión que desee: `volume qtree show -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path }`

## Ejemplo

En el siguiente ejemplo se crea un qtree llamado qt01 ubicado en la SVM vs1.example.com que tiene una ruta de unión `/vol/data1`:

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path
/vol/data1/qt01 -security-style ntfs
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume qtree show -vserver vs1.example.com -qtree-path
/vol/data1/qt01
```

```

Vserver Name: vs1.example.com
Volume Name: data1
Qtree Name: qt01
Actual (Non-Junction) Qtree Path: /vol/data1/qt01
Security Style: ntfs
Oplock Mode: enable
Unix Permissions: ---rwxr-xr-x
Qtree Id: 2
Qtree Status: normal
Export Policy: default
Is Export Policy Inherited: true
```

## Requisitos y consideraciones para crear un recurso compartido de SMB

Antes de crear un recurso compartido SMB, debe comprender los requisitos para las rutas de acceso compartidas y las propiedades compartidas, especialmente para los directorios iniciales.

La creación de un recurso compartido SMB implica especificar una estructura de ruta de acceso de directorio (mediante el `-path` en la `vserver cifs share create`) a los que accederán los clientes. La ruta de directorio corresponde a la ruta de unión para un volumen o qtree que ha creado en el espacio de nombres de la SVM. Debe haber la ruta de directorio y la ruta de unión correspondiente antes de crear el recurso compartido.

Las rutas de recursos compartidos tienen los siguientes requisitos:

- Un nombre de ruta de acceso de directorio puede tener hasta 255 caracteres.
- Si hay un espacio en el nombre de la ruta de acceso, toda la cadena debe colocarse entre comillas (por ejemplo, `"/new volume/mount here"`).
- Si la ruta UNC (`\\servername\sharename\filepath`) Del recurso compartido contiene más de 256 caracteres (excluyendo el inicial `""` de la ruta UNC), y la ficha **Seguridad** del cuadro Propiedades de Windows no está disponible.

Se trata de un problema del cliente Windows y no de un problema de ONTAP. Para evitar este problema, no cree recursos compartidos con rutas UNC con más de 256 caracteres.

Se pueden cambiar los valores predeterminados de las propiedades compartidas:

- Las propiedades iniciales predeterminadas para todos los recursos compartidos son `oplocks`, `browsable`, `changenotify`, y `show-previous-versions`.

- Es opcional especificar propiedades de recurso compartido al crear un recurso compartido.

Sin embargo, si especifica propiedades de recurso compartido al crear el recurso compartido, no se utilizan los valores predeterminados. Si utiliza la `-share-properties` parámetro al crear un recurso compartido, debe especificar todas las propiedades de recurso compartido que desea aplicar al recurso compartido mediante una lista delimitada por comas.

- Para designar un recurso compartido de directorio principal, utilice `homedirectory` propiedad.

Esta función permite configurar un recurso compartido que se asigna a directorios diferentes en función del usuario que se conecta a él y un conjunto de variables. En lugar de tener que crear recursos compartidos independientes para cada usuario, puede configurar un solo recurso compartido con varios parámetros del directorio inicial para definir la relación de un usuario entre un punto de entrada (el recurso compartido) y su directorio inicial (un directorio en la SVM).



No puede agregar ni quitar esta propiedad después de crear el recurso compartido.

Los recursos compartidos del directorio inicial tienen los siguientes requisitos:

- Antes de crear directorios iniciales SMB, debe agregar al menos una ruta de búsqueda de directorio raíz mediante el `vserver cifs home-directory search-path add` comando.
- Los recursos compartidos del directorio inicial especificados por el valor de `homedirectory` en la `-share-properties` el parámetro debe incluir la `%w` Variable dinámica (nombre de usuario de Windows) en el nombre del recurso compartido.

El nombre del recurso compartido también puede contener el `%d` (nombre de dominio) variable dinámica (por ejemplo, `%d/%w`) o una parte estática en el nombre del recurso compartido (por ejemplo, `home1_%w`).

- Si los administradores o usuarios utilizan el recurso compartido para conectarse a los directorios de usuarios de otros usuarios (mediante las opciones de `vserver cifs home-directory modify` comando), el patrón de nombre de recurso compartido dinámico debe ir precedido de una tilde (`~`).

"[Gestión de SMB](#)" y.. `vserver cifs share` las páginas de manual tienen información adicional.

## Cree un recurso compartido de SMB

Debe crear un recurso compartido de SMB para poder compartir datos desde un servidor SMB con clientes SMB. Cuando se crea un recurso compartido, se pueden establecer propiedades de recurso compartido, como designar el recurso compartido como un directorio inicial. También puede personalizar el recurso compartido configurando ajustes opcionales.

### Antes de empezar

La ruta de directorio del volumen o `qtree` debe existir en el espacio de nombres de la SVM antes de crear el recurso compartido.

### Acerca de esta tarea

Al crear un recurso compartido, la ACL de recurso compartido predeterminada (permisos de uso compartido predeterminados) es `Everyone / Full Control`. Después de probar el acceso al recurso compartido, debe quitar la ACL de recurso compartido predeterminada y reemplazarla por una alternativa más segura.



**Pasos**

- 1. Si es necesario, cree la estructura de ruta de acceso de directorio para el recurso compartido.

La `vserver cifs share create` el comando comprueba la ruta especificada en el `-path` opcional durante la creación del recurso compartido. Si la ruta especificada no existe, el comando falla.

- 2. Cree un recurso compartido de SMB asociado con la SVM especificada: `vserver cifs share create -vserver vserver_name -share-name share_name -path path [-share-properties share_properties,...] [other_attributes] [-comment text]`
- 3. Compruebe que se ha creado el recurso compartido: `vserver cifs share show -share-name share_name`

**Ejemplos**

El siguiente comando crea un recurso compartido SMB denominado «SHARE1» en la SVM `vs1.example.com`. Su ruta de acceso de directorio es `/users`, y se crea con propiedades predeterminadas.

```
cluster1::> vserver cifs share create -vserver vs1.example.com -share-name
SHARE1 -path /users

cluster1::> vserver cifs share show -share-name SHARE1
```

| Vserver         | Share  | Path   | Properties             | Comment | ACL                     |
|-----------------|--------|--------|------------------------|---------|-------------------------|
| vs1.example.com | SHARE1 | /users | oplocks                | -       | Everyone / Full Control |
|                 |        |        | browsable              |         |                         |
|                 |        |        | changenotify           |         |                         |
|                 |        |        | show-previous-versions |         |                         |

**Comprobar el acceso de cliente de SMB**

Debe verificar si ha configurado SMB correctamente accediendo y escribiendo los datos en el recurso compartido. Debe probar el acceso utilizando el nombre del servidor SMB y todos los alias NetBIOS.

**Pasos**

- 1. Inicie sesión en un cliente Windows.
- 2. Probar el acceso mediante el nombre del servidor SMB:
  - a. En el Explorador de Windows, asigne una unidad al recurso compartido con el siguiente formato: `\\SMB_Server_Name\Share_Name`

Si la asignación no se realiza correctamente, es posible que la asignación DNS aún no se haya propagado por toda la red. Debe probar el acceso más adelante con el nombre del servidor SMB.

Si el servidor SMB se llama `vs1.example.com` y el recurso compartido se llama `SHARE1`, debe introducir lo siguiente: `\\vs0.example.com\SHARE1`

- b. En la unidad recién creada, cree un archivo de prueba y, a continuación, elimine el archivo.  
Verificó el acceso de escritura al recurso compartido mediante el nombre del servidor SMB.

3. Repita el paso 2 para cualquier alias NetBIOS.

### Cree listas de control de acceso a recursos compartidos de SMB

La configuración de permisos de uso compartido mediante la creación de listas de control de acceso (ACL) para recursos compartidos de SMB permite controlar el nivel de acceso a un recurso compartido para usuarios y grupos.

#### Antes de empezar

Debe haber decidido qué usuarios o grupos tendrán acceso al recurso compartido.

#### Acerca de esta tarea

Puede configurar ACL de nivel compartido utilizando nombres de usuarios o grupos locales o de Windows de dominio.

Antes de crear una ACL nueva, debe eliminar la ACL de recurso compartido predeterminada `Everyone / Full Control`, lo que supone un riesgo para la seguridad.

En modo de grupo de trabajo, el nombre de dominio local es el nombre del servidor SMB.

#### Pasos

1. Elimine la ACL de uso compartido predeterminada:  
`vserver cifs share access-control delete -vserver vserver_name -share share_name -user-or-group everyone`
2. Configure la nueva ACL:

| Si desea configurar las ACL utilizando... | Introduzca el comando...                                                                                                                                                                     |
|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Usuario de Windows                        | <code>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_domain_name\user_name -permission access_right</code> |
| Grupo Windows                             | <code>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_group_name -permission access_right</code>            |

3. Compruebe que la ACL aplicada al recurso compartido sea correcta mediante el `vserver cifs share access-control show` comando.

#### Ejemplo

El siguiente comando da Change Permisos al grupo de Windows «equipo de ventas» para la participación «números» en el «vs1.example.com"SVM:»

```
cluster1::> vsriver cifs share access-control create -vsriver
vs1.example.com -share sales -user-or-group "Sales Team" -permission
Change

cluster1::> vsriver cifs share access-control show
```

| Vsriver         | Share<br>Name | User/Group<br>Name     | User/Group<br>Type | Access<br>Permission |
|-----------------|---------------|------------------------|--------------------|----------------------|
| vs1.example.com | c\$           | BUILTIN\Administrators | windows            | Full_Control         |
| vs1.example.com | sales         | DOMAIN\ "Sales Team"   | windows            | Change               |

Los siguientes comandos dan Change Permiso para el grupo local de Windows llamado "Tiger Team" and Full\_Control Permiso para el usuario local de Windows denominado «Sue Chang» para la participación «daval5» en la «SVM»:

```
cluster1::> vsriver cifs share access-control create -vsriver vs1 -share
dataval5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vsriver cifs share access-control create -vsriver vs1 -share
dataval5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vsriver cifs share access-control show -vsriver vs1
```

| Vsriver | Share<br>Name | User/Group<br>Name     | User/Group<br>Type | Access<br>Permission |
|---------|---------------|------------------------|--------------------|----------------------|
| vs1     | c\$           | BUILTIN\Administrators | windows            | Full_Control         |
| vs1     | dataval5      | DOMAIN\ "Tiger Team"   | windows            | Change               |
| vs1     | dataval5      | DOMAIN\ "Sue Chang"    | windows            | Full_Control         |

## Configure los permisos de archivo NTFS en un recurso compartido

Para habilitar el acceso a archivos para los usuarios o grupos que tienen acceso a un recurso compartido, debe configurar permisos de archivos NTFS en archivos y directorios de ese recurso compartido desde un cliente de Windows.

### Antes de empezar

El administrador que realiza esta tarea debe tener suficientes permisos NTFS para cambiar los permisos en los objetos seleccionados.

### Acerca de esta tarea

"[Gestión de SMB](#)" Y la documentación de Windows contiene información sobre cómo establecer permisos NTFS estándar y avanzados.

### Pasos

1. Inicie sesión en un cliente Windows como administrador.
2. En el menú **Herramientas** del Explorador de Windows, seleccione **asignar unidad de red**.
3. Complete el cuadro **Unidad de red de mapas**:

- a. Seleccione una letra **Unidad**.
- b. En el cuadro **Folder**, escriba el nombre del servidor SMB que contiene el recurso compartido que contiene los datos a los que desea aplicar los permisos y el nombre del recurso compartido.

Si el nombre del servidor SMB es SMB\_SERVER01 y su recurso compartido se denomina «SHARE1», deberá introducir \\SMB\_SERVER01\SHARE1.



Puede especificar la dirección IP de la interfaz de datos para el servidor SMB en lugar del nombre del servidor SMB.

- c. Haga clic en **Finalizar**.

La unidad seleccionada está montada y lista con la ventana del Explorador de Windows que muestra archivos y carpetas contenidos en el recurso compartido.

4. Seleccione el archivo o directorio para el que desea establecer los permisos de archivo NTFS.
5. Haga clic con el botón secundario del ratón en el archivo o directorio y seleccione **Propiedades**.
6. Seleccione la ficha **Seguridad**.

La ficha Seguridad muestra la lista de usuarios y grupos para los que se ha establecido el permiso NTFS. El cuadro permisos para <Object> muestra una lista de los permisos permitir y denegar vigentes para el usuario o grupo seleccionado.

7. Haga clic en **Editar**.

Se abrirá el cuadro permisos para <Object>.

8. Realice las acciones deseadas:

| Si quieres                                                      | Haga lo siguiente...                                                                                                                                                                                                                                                                                                              |
|-----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Establezca permisos NTFS estándar para un nuevo usuario o grupo | <p>a. Haga clic en <b>Agregar</b>.</p> <p>Se abre la ventana Seleccionar usuario, equipos, cuentas de servicio o grupos.</p> <p>b. En el cuadro <b>Introduzca los nombres de objeto para seleccionar</b> , escriba el nombre del usuario o grupo en el que desea agregar permiso NTFS.</p> <p>c. Haga clic en <b>Aceptar</b>.</p> |
| Cambiar o quitar permisos NTFS estándar de un usuario o grupo   | En el cuadro <b>nombres de grupo o de usuario</b> , seleccione el usuario o grupo que desea cambiar o quitar.                                                                                                                                                                                                                     |

9. Realice las acciones deseadas:

| Si desea...                                                                 | Haga lo siguiente                                                                                                                                                                                        |
|-----------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Establezca permisos NTFS estándar para un usuario o grupo nuevo o existente | En el cuadro <b>permisos para &lt;Object&gt;</b> , seleccione los cuadros <b>permitir</b> o <b>Denegar</b> para el tipo de acceso que desea permitir o no permitir para el usuario o grupo seleccionado. |
| Quitar un usuario o un grupo                                                | Haga clic en <b>Quitar</b> .                                                                                                                                                                             |



Si algunos o todos los cuadros de permiso estándar no se pueden seleccionar, es porque los permisos se heredan del objeto primario. El cuadro **permisos especiales** no se puede seleccionar. Si está seleccionada, significa que se han establecido uno o más derechos avanzados granulares para el usuario o grupo seleccionado.

10. Después de terminar de agregar, quitar o editar permisos NTFS en ese objeto, haga clic en **Aceptar**.

### Comprobar el acceso del usuario

Debe probar que los usuarios configurados pueden acceder al recurso compartido de SMB y a los archivos que contiene.

#### Pasos

1. En un cliente Windows, inicie sesión como uno de los usuarios que ahora tiene acceso al recurso compartido.
2. En el menú **Herramientas** del Explorador de Windows, seleccione **asignar unidad de red**.
3. Complete el cuadro **Unidad de red de mapas**:
  - a. Seleccione una letra **Unidad**.
  - b. En el cuadro **carpeta**, escriba el nombre del recurso compartido que proporcionará a los usuarios.

Si el nombre del servidor SMB es SMB\_SERVER01 y su recurso compartido se denomina «SHARE1», deberá introducir \\SMB\_SERVER01\share1.

c. Haga clic en **Finalizar**.

La unidad seleccionada está montada y lista con la ventana del Explorador de Windows que muestra archivos y carpetas contenidos en el recurso compartido.

4. Cree un archivo de prueba, compruebe que existe, escriba texto y quite el archivo de prueba.

## Gestione SMB con la interfaz de línea de comandos

### Información general sobre la referencia de SMB

Las funciones de acceso a archivos ONTAP están disponibles para el protocolo SMB. Puede habilitar un servidor CIFS, crear recursos compartidos y habilitar servicios de Microsoft.



*SMB* (bloque de mensajes del servidor) hace referencia a los dialectos modernos del protocolo del sistema común de archivos de Internet (CIFS). Seguirá viendo *CIFS* en la interfaz de línea de comandos (CLI) de ONTAP y en las herramientas de gestión de OnCommand.

Debe utilizar estos procedimientos en las siguientes circunstancias:

- Quiere entender el rango de funcionalidades del protocolo SMB de ONTAP.
- Desea realizar tareas de configuración y mantenimiento menos comunes, no una configuración básica de SMB.
- Desea usar la interfaz de línea de comandos (CLI), no System Manager ni una herramienta de secuencias de comandos automatizadas.

### Compatibilidad con servidores SMB

#### Información general de soporte de SMB Server

Puede habilitar y configurar servidores SMB en máquinas virtuales de almacenamiento (SVM) para permitir que los clientes SMB accedan a los archivos del clúster.

- Cada SVM de datos del clúster puede vincularse a exactamente un dominio de Active Directory.
- No es necesario enlazar las SVM de datos con el mismo dominio.
- Pueden vincularse varias SVM al mismo dominio.

Debe configurar las SVM y las LIF que utiliza para proporcionar datos antes de poder crear un servidor SMB. Si la red de datos no es plano, también podría necesitar configurar espacios IP, dominios de retransmisión y subredes. La *Network Management Guide* contiene detalles.

#### Información relacionada

["Gestión de redes"](#)

[Modificar servidores SMB](#)

## Funcionalidades y versiones de SMB compatibles

Server Message Block (SMB) es un protocolo de uso compartido de archivos remoto que utilizan los servidores y clientes de Microsoft Windows. En ONTAP 9, se admiten todas las versiones de SMB; sin embargo, la compatibilidad predeterminada con SMB 1.0 depende de su versión de ONTAP. Debe verificar que el servidor SMB de ONTAP admite los clientes y la funcionalidad que se requieren en su entorno.

La información más reciente sobre los clientes SMB y los controladores de dominio compatibles con ONTAP está disponible en *Interoperability Matrix Tool*.

SMB 2.0 y las versiones posteriores están habilitadas de forma predeterminada para servidores SMB de ONTAP 9 y se pueden habilitar o deshabilitar, según sea necesario. En la siguiente tabla se muestran la compatibilidad con SMB 1.0 y la configuración predeterminada.

| Funcionalidad de SMB 1.0:               | En estas versiones de ONTAP 9: |                                  |     |                 |
|-----------------------------------------|--------------------------------|----------------------------------|-----|-----------------|
|                                         | 9,0                            | 9,1                              | 9,2 | 9,3 y posterior |
| Está habilitado de forma predeterminada | Sí                             | Sí                               | Sí  | No              |
| Se puede habilitar o deshabilitar       | No                             | Sí*9.1 P8 o posterior requerido. | Sí  | Sí              |



La configuración predeterminada de las conexiones SMB 1.0 y 2.0 con controladoras de dominio también depende de la versión ONTAP. Hay más información disponible en `vserver cifs security modify` página de manual. En el caso de entornos con servidores CIFS existentes que ejecuten SMB 1.0, debe migrar a una versión Lo antes posible. de SMB posterior con el fin de prepararse para las mejoras de seguridad y cumplimiento de normativas. Si quiere más información, póngase en contacto con su representante de NetApp.

La siguiente tabla muestra qué funciones de SMB son compatibles con cada versión de SMB. Algunas funciones de SMB se habilitan de forma predeterminada, por lo que algunas requieren más configuración.

| Esta funcionalidad :           | Requiere activación: | Es compatible con ONTAP 9 para estas versiones SMB: |     |     |     |       |
|--------------------------------|----------------------|-----------------------------------------------------|-----|-----|-----|-------|
|                                |                      | 1,0                                                 | 2,0 | 2,1 | 3,0 | 3.1.1 |
| Funcionalidad SMB 1.0 heredada |                      | X                                                   | X   | X   | X   | X     |

| Esta funcionalidad :                                                  | Requiere activación: | Es compatible con ONTAP 9 para estas versiones SMB: |   |   |   |   |
|-----------------------------------------------------------------------|----------------------|-----------------------------------------------------|---|---|---|---|
|                                                                       |                      |                                                     |   |   |   |   |
| Asas duraderas                                                        |                      |                                                     | X | X | X | X |
| Operaciones compuestas                                                |                      |                                                     | X | X | X | X |
| Operaciones asíncronas                                                |                      |                                                     | X | X | X | X |
| Se han aumentado los tamaños de búfer de lectura y escritura          |                      |                                                     | X | X | X | X |
| Mayor escalabilidad                                                   |                      |                                                     | X | X | X | X |
| Firma SMB                                                             | X                    | X                                                   | X | X | X | X |
| Formato de archivo de flujo de datos alternativo (ADS)                | X                    | X                                                   | X | X | X | X |
| MTU grande (habilitada de forma predeterminada a partir de ONTAP 9.7) | X                    |                                                     |   | X | X | X |
| Bloqueos oportunistas del arrendamiento                               |                      |                                                     |   | X | X | X |
| Recursos compartidos disponibles en todo momento                      | X                    |                                                     |   |   | X | X |



| Esta funcionalidad :                                               | Requiere activación: | Es compatible con ONTAP 9 para estas versiones SMB: |  |  |   |   |
|--------------------------------------------------------------------|----------------------|-----------------------------------------------------|--|--|---|---|
|                                                                    |                      |                                                     |  |  |   |   |
| Asas persistentes                                                  |                      |                                                     |  |  | X | X |
| Testigo                                                            |                      |                                                     |  |  | X | X |
| CIFRADO SMB: AES-128-CCM                                           | X                    |                                                     |  |  | X | X |
| Escalado horizontal (necesario por los recursos compartidos de CA) |                      |                                                     |  |  | X | X |
| Recuperación transparente tras fallas                              |                      |                                                     |  |  | X | X |
| Multicanal de SMB (a partir de ONTAP 9.4)                          | X                    |                                                     |  |  | X | X |
| Integridad de la preautenticación                                  |                      |                                                     |  |  |   | X |
| Recuperación tras fallos de cliente de clúster v.2 (CCFv2)         |                      |                                                     |  |  |   | X |
| Cifrado SMB: AES-128-GCM (empezando por ONTAP 9.1)                 | X                    |                                                     |  |  |   | X |

#### Información relacionada

[Utilizar la firma SMB para mejorar la seguridad de la red](#)

[Configurar el nivel de seguridad de autenticación mínimo del servidor SMB](#)

[Configurar el cifrado SMB necesario en servidores SMB para las transferencias de datos a través de SMB](#)

["Informe técnico de NetApp 4543: Prácticas recomendadas de los protocolos SMB"](#)

["Interoperabilidad de NetApp"](#)

## **Funciones de Windows no compatibles**

Antes de utilizar CIFS en la red, debe tener en cuenta determinadas funciones de Windows que ONTAP no admite.

ONTAP no admite las siguientes funciones de Windows:

- Sistema de archivos cifrados (EFS)
- Registro de eventos del sistema de archivos NT (NTFS) en el diario de cambios
- Servicio de replicación de archivos de Microsoft (FRS)
- Servicio de Index Server de Microsoft Windows
- Almacenamiento remoto a través de la gestión de almacenamiento jerárquico (HSM)
- Gestión de cuotas desde clientes Windows
- Semántica de cuotas de Windows
- El archivo LMHOSTS
- Compresión nativa de NTFS

## **Configure los servicios de nombres NIS o LDAP en la SVM**

Con el acceso SMB, se siempre se realiza la asignación de usuario a un usuario UNIX, incluso al acceder a los datos de un volumen de estilo de seguridad NTFS. Si asigna usuarios de Windows a los usuarios UNIX correspondientes cuya información se almacena en almacenes de directorios NIS o LDAP, o si utiliza LDAP para la asignación de nombres, deberá configurar estos servicios de nombres durante la instalación de SMB.

### **Antes de empezar**

Debe haber personalizado la configuración de la base de datos de servicios de nombres para que coincida con su infraestructura de servicios de nombres.

### **Acerca de esta tarea**

Las SVM utilizan las bases de datos ns-switch de servicios de nombres para determinar el orden en el que buscar los orígenes de una base de datos de servicios de nombres determinada. La fuente del conmutador NS puede ser cualquier combinación de "files", "nis" o "ldap". En la base de datos de grupos, ONTAP intenta obtener las pertenencias a grupos de todos los orígenes configurados y, a continuación, utiliza la información consolidada de pertenencia a grupos para las comprobaciones de acceso. Si uno de estos orígenes no está disponible en el momento de obtener información del grupo UNIX, ONTAP no puede obtener las credenciales de UNIX completas y las comprobaciones de acceso posteriores podrían fallar. Por lo tanto, siempre debe comprobar que todas las fuentes del conmutador ns están configuradas para la base de datos de grupo en la configuración del conmutador ns.

El valor predeterminado es que el servidor SMB asigne todos los usuarios de Windows al usuario UNIX predeterminado que se almacena en el local `passwd` base de datos. Si desea utilizar la configuración predeterminada, es opcional configurar los servicios de nombre de usuario y grupo de UNIX NIS o LDAP, o la asignación de usuario LDAP para el acceso a SMB.

**Pasos**

- 1. Si la información de usuario, grupo y `netgroup` de UNIX es administrada por servicios de nombres NIS, configure los servicios de nombres NIS:
  - a. Determine el pedido actual de servicios de nombres mediante el `vserver services name-service ns-switch show` comando.

En este ejemplo, las tres bases de datos (`group`, `passwd`, y `netgroup`) que puede utilizar `nis` como origen de servicio de nombre sólo está utilizando `files` como origen.

```
vserver services name-service ns-switch show -vserver vs1
```

| Vserver | Database | Enabled | Source Order  |
|---------|----------|---------|---------------|
| vs1     | hosts    | true    | dns,<br>files |
| vs1     | group    | true    | files         |
| vs1     | passwd   | true    | files         |
| vs1     | netgroup | true    | files         |
| vs1     | namemap  | true    | files         |

Debe añadir el `nis` fuente de la `group` y.. `passwd` y, opcionalmente, en la `netgroup` base de datos.

- b. Ajuste el orden de la base de datos del servicio de nombres `ns-switch` según lo desee mediante el `vserver services name-service ns-switch modify` comando.

Para obtener el mejor rendimiento, no debe agregar un servicio de nombres a una base de datos del servicio de nombres a menos que planifique configurar ese servicio de nombres en la SVM.

Si modifica la configuración de más de una base de datos de servicio de nombres, debe ejecutar el comando por separado para cada base de datos de servicio de nombres que desee modificar.

En este ejemplo: `nis` y.. `files` se configuran como orígenes para `group` y.. `passwd` bases de datos, en ese orden. El resto de las bases de datos de servicios de nombres no han cambiado.

```
vserver services name-service ns-switch modify -vserver vs1 -database group -sources nis,files
vserver services name-service ns-switch modify -vserver vs1 -database passwd -sources nis,files
```

- c. Compruebe que la solicitud de servicios de nombres es correcta mediante el `vserver services name-service ns-switch show` comando.

```
vserver services name-service ns-switch show -vserver vs1
```

| Vserver | Database | Enabled | Source Order  |
|---------|----------|---------|---------------|
| vs1     | hosts    | true    | dns,<br>files |
| vs1     | group    | true    | nis,<br>files |
| vs1     | passwd   | true    | nis,<br>files |
| vs1     | netgroup | true    | files         |
| vs1     | namemap  | true    | files         |

d. Cree la configuración del servicio de nombres NIS:

```
vserver services name-service nis-domain create -vserver vserver_name
-domain NIS_domain_name -servers NIS_server_IPaddress,... -active true+
```

```
vserver services name-service nis-domain create -vserver vs1 -domain
example.com -servers 10.0.0.60 -active true
```



A partir de ONTAP 9.2, el campo `-nis-servers` reemplaza el campo `-servers`. Este nuevo campo puede tomar un nombre de host o una dirección IP para el servidor NIS.

e. Compruebe que el servicio de nombres NIS está configurado correctamente y activo: `vserver services name-service nis-domain show vserver vserver_name`

```
vserver services name-service nis-domain show vserver vs1
```

| Vserver | Domain      | Active | Server    |
|---------|-------------|--------|-----------|
| vs1     | example.com | true   | 10.0.0.60 |

- Si la información de usuario, grupo y netgroup de UNIX o la asignación de nombres se gestiona mediante servicios de nombres LDAP, configure los servicios de nombres LDAP mediante la información ubicada ["Gestión de NFS"](#).

## Cómo funciona la configuración de switch de servicio de nombres ONTAP

ONTAP almacena información de configuración del servicio de nombres en una tabla que equivale a `/etc/nsswitch.conf` Fichero de sistemas UNIX. Debe comprender la función de la tabla y cómo la utiliza ONTAP para poder configurarla de forma adecuada para su entorno.

La tabla de conmutador de servicio de nombres ONTAP determina qué orígenes de servicio de nombres consulta ONTAP para recuperar información de un determinado tipo de información del servicio de nombres. ONTAP mantiene una tabla de switch de servicio de nombres independiente para cada SVM.

## Tipos de base de datos

La tabla almacena una lista de servicios de nombres independiente para cada uno de los siguientes tipos de base de datos:

| Tipo de base de datos | Define orígenes de servicio de nombres para... | Los orígenes válidos son... |
|-----------------------|------------------------------------------------|-----------------------------|
| hosts                 | Conversión de nombres de host a direcciones IP | archivos, dns               |
| grupo                 | Búsqueda de información de grupo de usuarios   | archivos, nis, ldap         |
| passwd                | Búsqueda de información de usuario             | archivos, nis, ldap         |
| grupo de red          | Buscando información de netgroup               | archivos, nis, ldap         |
| mapa de nombres       | Asignando los nombres de usuario               | archivos, ldap              |

## Tipos de origen

Los orígenes especifican el nombre de origen de servicio que se utilizará para recuperar la información adecuada.

| Especificar tipo de origen... | Para buscar información en...                                                                  | Administrado por las familias de comandos...                                                                                                                                                                         |
|-------------------------------|------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| archivos                      | Archivos de origen local                                                                       | <code>vserver services name-service unix-user vserver services name-service unix-group</code><br><br><code>vserver services name-service netgroup</code><br><br><code>vserver services name-service dns hosts</code> |
| nis                           | Servidores NIS externos tal como se especifica en la configuración de dominio NIS de la SVM    | <code>vserver services name-service nis-domain</code>                                                                                                                                                                |
| ldap                          | Servidores LDAP externos tal como se especifica en la configuración del cliente LDAP de la SVM | <code>vserver services name-service ldap</code>                                                                                                                                                                      |

| Especificar tipo de origen... | Para buscar información en...                                                   | Administrado por las familias de comandos...   |
|-------------------------------|---------------------------------------------------------------------------------|------------------------------------------------|
| dns                           | Servidores DNS externos como se especifica en la configuración de DNS de la SVM | <code>vserver services name-service dns</code> |

Aunque tenga pensado utilizar NIS o LDAP tanto para el acceso a datos como para la autenticación de administración de SVM, debería seguir incluyéndose `files` Y configure los usuarios locales como respaldo en caso de que falle la autenticación de NIS o LDAP.

### Protocolos utilizados para acceder a fuentes externas

Para acceder a los servidores de fuentes externas, ONTAP utiliza los siguientes protocolos:

| Fuente externa del servicio de nombres | Protocolo utilizado para acceder |
|----------------------------------------|----------------------------------|
| NIS                                    | UDP                              |
| DNS                                    | UDP                              |
| LDAP                                   | TCP                              |

### Ejemplo

En el ejemplo siguiente se muestra el nombre de configuración del switch de servicio para la SVM `svm_1`:

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
```

| Vserver | Database | Source        |
|---------|----------|---------------|
| -----   | -----    | -----         |
| svm_1   | hosts    | files,<br>dns |
| svm_1   | group    | files         |
| svm_1   | passwd   | files         |
| svm_1   | netgroup | nis,<br>files |

Para buscar información de usuarios o grupos, ONTAP sólo consulta archivos de fuentes locales. Si la consulta no devuelve ningún resultado, la búsqueda fallará.

Para buscar información de grupos de red, ONTAP consulta primero los servidores NIS externos. Si la consulta no devuelve ningún resultado, el archivo de netgroup local se activa a continuación.

No hay entradas del servicio de nombres para la asignación de nombres en la tabla de la SVM `svm_1`. Por lo tanto, ONTAP sólo consulta archivos de origen local de forma predeterminada.

## Gestione servidores SMB

## Modificar servidores SMB

Puede mover un servidor SMB de un grupo de trabajo a un dominio de Active Directory, de un grupo de trabajo a otro grupo de trabajo o de un dominio de Active Directory a un grupo de trabajo mediante el `vserver cifs modify` comando.

### Acerca de esta tarea

También puede modificar otros atributos del servidor SMB, como el nombre del servidor SMB y el estado administrativo. Consulte la página man para obtener más información.

### Opciones

- Mover el servidor SMB de un grupo de trabajo a un dominio de Active Directory:
  - a. Defina el estado administrativo del servidor SMB como down.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

- b. Mover el servidor SMB del grupo de trabajo a un dominio de Active Directory: `vserver cifs modify -vserver vserver_name -domain domain_name`

```
Cluster1::>vserver cifs modify -vserver vs1 -domain example.com
```

Para crear una cuenta de equipo de Active Directory para el servidor SMB, debe proporcionar el nombre y la contraseña de una cuenta de Windows con privilegios suficientes para agregar equipos al `ou=example` ou contenedor dentro de ``example`` dominio `.com`.

A partir de ONTAP 9.7, el administrador de AD puede proporcionarle un URI a un archivo keytab como alternativa a proporcionarle un nombre y una contraseña a una cuenta de Windows con privilegios. Cuando reciba el URI, inclúyalo en el `-keytab-uri` con el `vserver cifs` comandos.

- Mover el servidor SMB de un grupo de trabajo a otro grupo de trabajo:
  - a. Defina el estado administrativo del servidor SMB como down.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

- b. Modifique el grupo de trabajo para el servidor SMB: `vserver cifs modify -vserver vserver_name -workgroup new_workgroup_name`

```
Cluster1::>vserver cifs modify -vserver vs1 -workgroup workgroup2
```

- Mover el servidor SMB de un dominio de Active Directory a un grupo de trabajo:
  - a. Defina el estado administrativo del servidor SMB como down.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

- b. Mover el servidor SMB del dominio de Active Directory a un grupo de trabajo: `vserver cifs modify -vserver vserver_name -workgroup workgroup_name`

```
cluster1::> vserver cifs modify -vserver vs1 -workgroup workgroup1
```



Para entrar en el modo de grupo de trabajo, el sistema debe desactivar todas las características basadas en dominios y eliminar su configuración automáticamente, incluidos los recursos compartidos disponibles continuamente, las instantáneas y AES. Sin embargo, las ACL de uso compartido configuradas por el dominio como "EXAMPLE.COM\userName" no funcionarán correctamente, pero ONTAP no las podrá quitar. Quite estas ACL compartidas lo antes posible, utilizando herramientas externas una vez completado el comando. Si AES está activado, puede que se le solicite que proporcione el nombre y la contraseña de una cuenta de Windows con los privilegios suficientes para deshabilitarla en el dominio "example.com".

- Modifique otros atributos utilizando el parámetro apropiado del `vserver cifs modify` comando.

## Utilice opciones para personalizar los servidores SMB

### Opciones disponibles del servidor SMB

Resulta útil saber qué opciones hay disponibles cuando se piensa en cómo personalizar el servidor SMB. Aunque algunas opciones se utilizan para uso general en el servidor SMB, se utilizan varias para habilitar y configurar una funcionalidad SMB específica. Las opciones del servidor SMB se controlan con el `vserver cifs options modify` opción.

En la lista siguiente se especifican las opciones del servidor SMB que están disponibles en el nivel de privilegios de administrador:

- **Configuración del valor de tiempo de espera de la sesión SMB**

La configuración de esta opción permite especificar el número de segundos de tiempo de inactividad antes de desconectar una sesión SMB. Una sesión inactiva es una sesión en la que un usuario no tiene archivos o directorios abiertos en el cliente. El valor predeterminado es 900 segundos.

- **Configuración del usuario UNIX predeterminado**

La configuración de esta opción le permite especificar el usuario UNIX predeterminado que utiliza el servidor SMB. ONTAP crea automáticamente un usuario predeterminado denominado «'pcuser'» (con un UID de 65534), crea un grupo denominado «'pcuser'» (con un GID de 65534) y agrega el usuario predeterminado al grupo «'pcuser'». Cuando se crea un servidor SMB, ONTAP configura automáticamente «'pcuser'» como el usuario UNIX predeterminado.

- **Configuración del usuario UNIX invitado**



Al configurar esta opción, puede especificar el nombre de un usuario UNIX al que se asignan los usuarios que inician sesión desde dominios que no son de confianza, lo que permite a un usuario de un dominio que no es de confianza conectarse con el servidor SMB. De forma predeterminada, esta opción no está configurada (no hay ningún valor predeterminado); por lo tanto, el valor predeterminado es no permitir que los usuarios de dominios que no son de confianza se conecten con el servidor SMB.

- **Activación o desactivación de la ejecución de Read GRANT para bits de modo**

Habilitar o deshabilitar esta opción permite especificar si se permite a los clientes SMB ejecutar archivos ejecutables con bits de modo UNIX a los que tienen acceso de lectura, incluso cuando el bit ejecutable de UNIX no está establecido. Esta opción está deshabilitada de forma predeterminada.

- **Activación o desactivación de la capacidad de eliminar archivos de sólo lectura de clientes NFS**

Al habilitar o deshabilitar esta opción, se determina si se permite que los clientes NFS eliminen archivos o carpetas con el conjunto de atributos de sólo lectura. La semántica de eliminación NTFS no permite la eliminación de un archivo o carpeta cuando se establece el atributo de sólo lectura. La semántica de eliminación de UNIX ignora el bit de sólo lectura, utilizando los permisos de directorio principal en su lugar para determinar si un archivo o una carpeta se pueden eliminar. El valor predeterminado es `disabled`, que da como resultado la semántica de eliminación de NTFS.

- **Configuración de las direcciones del servidor del Servicio de nombres de Internet de Windows**

La configuración de esta opción le permite especificar una lista de direcciones de servidor del Servicio de nombres Internet de Windows (WINS) como una lista delimitada por comas. Debe especificar direcciones IPv4. Las direcciones IPv6 no son compatibles. No hay un valor predeterminado.

En la lista siguiente se especifican las opciones del servidor SMB que están disponibles en el nivel de privilegio avanzado:

- **Concesión de permisos de grupo UNIX a usuarios de CIFS**

La configuración de esta opción determina si el usuario CIFS entrante que no sea el propietario del archivo puede recibir el permiso de grupo. Si el usuario CIFS no es el propietario del archivo de estilo de seguridad de UNIX y este parámetro está configurado en `true`, a continuación, se concede el permiso de grupo para el archivo. Si el usuario CIFS no es el propietario del archivo de estilo de seguridad de UNIX y este parámetro está configurado en `false`, Las reglas UNIX normales se aplican para conceder el permiso de archivo. Este parámetro se aplica a archivos de estilo de seguridad UNIX que tienen permisos establecidos como `mode bits` Y no se aplica a archivos con el modo de seguridad NTFS o NFSv4. El valor predeterminado es `false`.

- **Activación o desactivación de SMB 1.0**

SMB 1.0 está deshabilitado de forma predeterminada en una SVM para la cual se crea un servidor SMB en ONTAP 9.3.



A partir de ONTAP 9.3, SMB 1.0 está deshabilitado de forma predeterminada para los nuevos servidores SMB creados en ONTAP 9.3. Debe migrar a una versión Lo antes posible. posterior de SMB para preparar las mejoras de seguridad y cumplimiento de normativas. Si quiere más información, póngase en contacto con su representante de NetApp.

- **Activación o desactivación de SMB 2.x**

SMB 2.0 es la versión mínima de SMB que admite la conmutación al nodo de respaldo de LIF. Si deshabilita SMB 2.x, ONTAP también deshabilita automáticamente SMB 3.X.

SMB 2.0 solo es compatible con SVM. La opción está habilitada de forma predeterminada en las SVM

- **Activación o desactivación de SMB 3,0**

SMB 3.0 es la versión mínima de SMB que admite recursos compartidos disponibles de forma continua. Windows Server 2012 y Windows 8 son las versiones mínimas de Windows que admiten SMB 3.0.

SMB 3,0 solo es compatible con las SVM. La opción está habilitada de forma predeterminada en las SVM

- **Activación o desactivación de SMB 3,1**

Windows 10 es la única versión de Windows que admite SMB 3.1.

SMB 3,1 solo es compatible con las SVM. La opción está habilitada de forma predeterminada en las SVM

- **Activación o desactivación de la descarga de copias ODX**

La descarga de copias ODX la utilizan automáticamente clientes de Windows que son compatibles con esta tecnología. Esta opción está habilitada de forma predeterminada.

- **Activación o desactivación del mecanismo de copia directa para la descarga de copias ODX**

El mecanismo de copia directa aumenta el rendimiento de la operación de descarga de copia cuando los clientes de Windows intentan abrir el archivo de origen de una copia en un modo que impide que se cambie el archivo mientras la copia está en curso. De forma predeterminada, el mecanismo de copia directa está habilitado.

- **Activación o desactivación de referencias automáticas a nodos**

Con las referencias automáticas a nodos, el servidor SMB hace referencia automáticamente a una LIF de datos local al nodo que aloja los datos a los que se accede a través del recurso compartido solicitado.

- **Activación o desactivación de políticas de exportación para SMB**

Esta opción está deshabilitada de forma predeterminada.

- **Activación o desactivación mediante puntos de unión como puntos de reanálisis**

Si esta opción está habilitada, el servidor SMB expone puntos de unión a clientes SMB como puntos de reanálisis. Esta opción solo es válida para conexiones SMB 2.x o SMB 3.0. Esta opción está habilitada de forma predeterminada.

Esta opción solo es compatible con las SVM. La opción está habilitada de forma predeterminada en las SVM

- **Configuración del número máximo de operaciones simultáneas por conexión TCP**

El valor predeterminado es 255.

- **Activación o desactivación de la funcionalidad de grupos y usuarios locales de Windows**

Esta opción está habilitada de forma predeterminada.

- **Activación o desactivación de la autenticación de usuarios locales de Windows**

Esta opción está habilitada de forma predeterminada.

- **Activación o desactivación de la función de copia de sombra VSS**

ONTAP utiliza la funcionalidad de copia de respaldo para realizar backups remotos de los datos almacenados mediante la solución Hyper-V mediante SMB.

Esta opción solo es compatible con las SVM y solo con configuraciones de Hyper-V en SMB. La opción está habilitada de forma predeterminada en las SVM

- **Configuración de la profundidad del directorio de instantáneas**

La configuración de esta opción permite definir la profundidad máxima de los directorios en los que crear instantáneas cuando se utiliza la función de copia oculta.

Esta opción solo es compatible con las SVM y solo con configuraciones de Hyper-V en SMB. La opción está habilitada de forma predeterminada en las SVM

- **Activación o desactivación de las capacidades de búsqueda multidominio para la asignación de nombres**

Si se habilita, cuando un usuario UNIX se asigna a un usuario de dominio de Windows mediante un comodín (\*) en la parte de dominio del nombre de usuario de Windows (por ejemplo, \*\joe), ONTAP busca el usuario especificado en todos los dominios con confianzas bidireccionales en el dominio principal. El dominio principal es el dominio que contiene la cuenta de equipo del servidor SMB.

Como alternativa a la búsqueda en todos los dominios de confianza bidireccional, puede configurar una lista de dominios de confianza preferidos. Si esta opción está activada y se ha configurado una lista preferida, la lista preferida se utiliza para realizar búsquedas de asignación de nombres multidominio.

La opción predeterminada es habilitar las búsquedas de asignación de nombres multidominio.

- **Configuración del tamaño del sector del sistema de archivos**

Esta opción le permite configurar el tamaño del sector del sistema de archivos en bytes que ONTAP informa a clientes SMB. Hay dos valores válidos para esta opción: 4096 y.. 512. El valor predeterminado es 4096. Es posible que tenga que configurar este valor en 512 Si la aplicación Windows sólo admite un tamaño de sector de 512 bytes.

- **Activación o desactivación del control de acceso dinámico**

Al habilitar esta opción, puede proteger objetos en el servidor SMB mediante el control de acceso dinámico (DAC), incluido el uso de auditorías para organizar políticas de acceso centrales y el uso de objetos de políticas de grupo para implementar políticas de acceso centrales. La opción está deshabilitada de forma predeterminada.

Esta opción solo es compatible con las SVM.

- **Establecer las restricciones de acceso para sesiones no autenticadas (restringir anónimo)**

Establecer esta opción determina cuáles son las restricciones de acceso para sesiones no autenticadas. Las restricciones se aplican a usuarios anónimos. De forma predeterminada, no hay restricciones de acceso para los usuarios anónimos.

- **Activación o desactivación de la presentación de ACL NTFS en volúmenes con seguridad efectiva UNIX (volúmenes de estilo de seguridad UNIX o volúmenes mixtos de estilo de seguridad con seguridad efectiva UNIX)**

Al habilitar o deshabilitar esta opción, se determina cómo se presenta la seguridad de archivos y carpetas con seguridad UNIX a los clientes SMB. Si está habilitada, ONTAP presenta archivos y carpetas en volúmenes con seguridad UNIX para clientes de SMB como si tuviera seguridad de archivos NTFS con ACL de NTFS. Si está deshabilitada, ONTAP presenta volúmenes con seguridad UNIX como volúmenes FAT, sin seguridad de archivos. De forma predeterminada, los volúmenes se presentan como con seguridad de archivos NTFS con ACL NTFS.

- **Activación o desactivación de la funcionalidad de apertura falsa SMB**

Al habilitar esta funcionalidad, se mejora el rendimiento de SMB 2.x y SMB 3.0, ya que se optimiza cómo ONTAP realiza solicitudes de apertura y cierre al consultar información sobre atributos de archivos y directorios. De manera predeterminada, la funcionalidad abierta falsa del SMB está habilitada. Esta opción solo es útil para las conexiones realizadas con SMB 2.x o posterior.

- **Activación o desactivación de las extensiones UNIX**

Al habilitar esta opción se habilitan las extensiones UNIX en un servidor SMB. Las extensiones UNIX permiten visualizar la seguridad de estilo POSIX/UNIX a través del protocolo SMB. De forma predeterminada, esta opción está deshabilitada.

Si tiene clientes SMB basados en UNIX, como clientes Mac OSX, en su entorno, debe habilitar extensiones UNIX. La habilitación de las extensiones UNIX permite al servidor SMB transmitir la información de seguridad de POSIX/UNIX a través de SMB al cliente basado en UNIX, lo que a continuación convierte la información de seguridad en la seguridad POSIX/UNIX.

- **Activación o desactivación de la compatibilidad para búsquedas cortas de nombres**

Al habilitar esta opción, el servidor SMB puede realizar búsquedas en nombres cortos. Una consulta de búsqueda con esta opción habilitada intenta coincidir con 8.3 nombres de archivo junto con nombres de archivo largos. El valor predeterminado de este parámetro es `false`.

- **Activación o desactivación del soporte para la publicidad automática de capacidades DFS**

Habilitar o deshabilitar esta opción determina si los servidores SMB anuncian automáticamente capacidades DFS a clientes SMB 2.x y SMB 3.0 que se conectan a recursos compartidos. ONTAP utiliza referencias DFS en la implementación de enlaces simbólicos para el acceso a SMB. Si está habilitada, el servidor SMB siempre anuncia las capacidades DFS independientemente de si el acceso al enlace simbólico está habilitado. Si está deshabilitado, el servidor SMB anuncia capacidades DFS solo cuando los clientes se conectan a recursos compartidos donde se habilita el acceso al enlace simbólico.

- **Configuración del número máximo de créditos SMB**

A partir de ONTAP 9.4, configure el `-max-credits` Opción le permite limitar el número de créditos que se concederán en una conexión SMB cuando los clientes y el servidor ejecuten SMB versión 2 o posterior. El valor predeterminado es 128.

- **Activación o desactivación de la compatibilidad con SMB multicanal**

Habilitar el `-is-multichannel-enabled` La opción en ONTAP 9.4 y versiones posteriores permite al servidor SMB establecer varias conexiones para una única sesión SMB cuando se implementan las NIC adecuadas en el clúster y sus clientes. Al hacerlo, se mejora el rendimiento y la tolerancia a fallos. El valor

predeterminado de este parámetro es `false`.

Cuando se habilita SMB MultiChannel, también es posible especificar los siguientes parámetros:

- El número máximo de conexiones permitidas por sesión multicanal. El valor predeterminado para este parámetro es 32.
- Número máximo de interfaces de red anunciadas por sesión multicanal. El valor predeterminado para este parámetro es 256.

### Configuración de las opciones del servidor SMB

Puede configurar las opciones del servidor SMB en cualquier momento después de crear un servidor SMB en una máquina virtual de almacenamiento (SVM).

#### Paso

1. Realice la acción deseada:

| Si desea configurar opciones del servidor SMB... | Introduzca el comando...                                                                                                                  |
|--------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| En el nivel de privilegios de administrador      | <pre>vserver cifs options modify -vserver<br/>vserver_name options</pre>                                                                  |
| En el nivel de privilegios avanzados             | <pre>a. set -privilege advanced<br/>b. vserver cifs options modify<br/>   -vserver vserver_name options<br/>c. set -privilege admin</pre> |

Para obtener más información acerca de la configuración de las opciones del servidor SMB, consulte la página man de `vserver cifs options modify` comando.

### Configure el permiso conceder grupo UNIX a los usuarios de SMB

Puede configurar esta opción para conceder permisos de grupo para tener acceso a archivos o directorios aunque el usuario SMB entrante no sea el propietario del archivo.

#### Pasos

1. Configure el nivel de privilegio en Advanced: `set -privilege advanced`
2. Configure el permiso conceder grupo UNIX según corresponda:

| Si desea                                                                                                                            | Introduzca el comando                                                              |
|-------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| Active el acceso a los archivos o directorios para obtener permisos de grupo incluso si el usuario no es el propietario del archivo | <pre>vserver cifs options modify -grant-<br/>unix-group-perms-to-others true</pre> |

| Si desea                                                                                                                               | Introduzca el comando                                                            |
|----------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| Desactive el acceso a los archivos o directorios para obtener permisos de grupo incluso si el usuario no es el propietario del archivo | <code>vserver cifs options modify -grant-unix-group-perms-to-others false</code> |

3. Compruebe que la opción está establecida en el valor deseado: `vserver cifs options show -fields grant-unix-group-perms-to-others`
4. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

#### Configurar restricciones de acceso para usuarios anónimos

De forma predeterminada, un usuario anónimo y sin autenticar (también conocido como *null user*) puede tener acceso a cierta información de la red. Puede usar una opción de servidor SMB para configurar restricciones de acceso para el usuario anónimo.

#### Acerca de esta tarea

La `-restrict-anonymous` La opción del servidor SMB se corresponde con la `RestrictAnonymous` Entrada de registro en Windows.

Los usuarios anónimos pueden enumerar o enumerar determinados tipos de información del sistema de los hosts de Windows de la red, incluidos los nombres y detalles de usuario, las directivas de cuenta y los nombres de recursos compartidos. Puede controlar el acceso para el usuario anónimo especificando uno de tres ajustes de restricción de acceso:

| Valor                                        | Descripción                                                                  |
|----------------------------------------------|------------------------------------------------------------------------------|
| <code>no-restriction</code> (predeterminado) | Especifica que no hay restricciones de acceso para los usuarios anónimos.    |
| <code>no-enumeration</code>                  | Especifica que sólo la enumeración está restringida a los usuarios anónimos. |
| <code>no-access</code>                       | Especifica que el acceso está restringido para usuarios anónimos.            |

#### Pasos

1. Configure el nivel de privilegio en Advanced: `set -privilege advanced`
2. Configure el valor Restrict Anonymous: `vserver cifs options modify -vserver vserver_name -restrict-anonymous {no-restriction|no-enumeration|no-access}`
3. Compruebe que la opción está establecida en el valor deseado: `vserver cifs options show -vserver vserver_name`
4. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

#### Información relacionada

[Opciones disponibles del servidor SMB](#)

## Gestione cómo se presenta la seguridad de archivos a los clientes SMB para una visión general de los datos de estilo de seguridad UNIX

Puede elegir cómo desea presentar la seguridad de archivos a los clientes de SMB para los datos de estilo de seguridad de UNIX habilitando o deshabilitando la presentación de ACL NTFS a clientes SMB. Existen ventajas en cada entorno, que debe entender para elegir el ajuste que mejor se ajuste a los requisitos de su negocio.

De forma predeterminada, ONTAP presenta los permisos de UNIX sobre volúmenes de estilo de seguridad de UNIX a clientes de SMB como ACL de NTFS. Hay escenarios en los que esto es deseable, incluyendo los siguientes:

- Desea ver y editar los permisos de UNIX mediante la ficha **Seguridad** del cuadro Propiedades de Windows.

No puede modificar los permisos de un cliente Windows si el sistema UNIX no permite la operación. Por ejemplo, no puede cambiar la propiedad de un archivo que no posee, ya que el sistema UNIX no permite esta operación. Esta restricción impide a los clientes SMB omitir los permisos de UNIX establecidos en los archivos y carpetas.

- Los usuarios están editando y guardando archivos en el volumen de estilo de seguridad de UNIX utilizando ciertas aplicaciones de Windows, por ejemplo, Microsoft Office, donde ONTAP debe conservar los permisos de UNIX durante las operaciones de guardado.
- Hay ciertas aplicaciones de Windows en su entorno que esperan leer ACL NTFS en los archivos que utilizan.

En determinadas circunstancias, es posible que desee deshabilitar la presentación de permisos UNIX como ACL NTFS. Si esta funcionalidad está deshabilitada, ONTAP presenta volúmenes de estilo de seguridad UNIX como volúmenes FAT a clientes SMB. Hay motivos específicos por los que puede que desee presentar volúmenes de estilo de seguridad de UNIX como volúmenes FAT a clientes SMB:

- Sólo se pueden cambiar los permisos de UNIX mediante montajes en clientes UNIX.

La pestaña Seguridad no está disponible cuando se asigna un volumen de estilo de seguridad UNIX en un cliente SMB. La unidad asignada parece formatearse con el sistema de archivos FAT, que no tiene permisos de archivo.

- Está utilizando aplicaciones a través de SMB que establecen ACL NTFS en archivos y carpetas a los que se tiene acceso, lo cual puede fallar si los datos residen en volúmenes de estilo de seguridad de UNIX.

Si ONTAP informa del volumen como FAT, la aplicación no intenta cambiar una ACL.

### Información relacionada

[Configuración de estilos de seguridad en volúmenes FlexVol](#)

[Configuración de estilos de seguridad en qtrees](#)

### Habilitar o deshabilitar la presentación de ACL NTFS para datos de estilo de seguridad de UNIX

Puede habilitar o deshabilitar la presentación de ACL NTFS a clientes SMB para datos de estilo de seguridad de UNIX (volúmenes de estilo de seguridad de UNIX y volúmenes

mixtos de estilo de seguridad con seguridad efectiva de UNIX).

### Acerca de esta tarea

Si habilita esta opción, ONTAP presenta archivos y carpetas en volúmenes con un estilo de seguridad UNIX efectivo para los clientes de SMB como si tuviera ACL NTFS. Si deshabilita esta opción, los volúmenes se presentan como volúmenes FAT a los clientes de SMB. El valor predeterminado es presentar ACL de NTFS a los clientes de SMB.

### Pasos

1. Configure el nivel de privilegio en Advanced: `set -privilege advanced`
2. Configure el valor de opción de ACL de UNIX NTFS: `vserver cifs options modify -vserver vserver_name -is-unix-nt-acl-enabled {true|false}`
3. Compruebe que la opción está establecida en el valor deseado: `vserver cifs options show -vserver vserver_name`
4. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

### Cómo ONTAP conserva los permisos de UNIX

Cuando las aplicaciones Windows editan y guardan archivos de un volumen FlexVol que actualmente tienen permisos UNIX, ONTAP puede preservar los permisos UNIX.

Cuando las aplicaciones de clientes de Windows editan y guardan archivos, leen las propiedades de seguridad del archivo, crean un nuevo archivo temporal, aplican esas propiedades al archivo temporal y, a continuación, asignan al archivo temporal el nombre de archivo original.

Cuando los clientes de Windows realizan una consulta para las propiedades de seguridad, reciben una ACL construida que representa exactamente los permisos de UNIX. El único propósito de esta ACL construida es preservar los permisos UNIX del archivo a medida que las aplicaciones de Windows actualizan los archivos para garantizar que los archivos resultantes tengan los mismos permisos UNIX. ONTAP no establece ninguna ACL de NTFS usando la ACL construida.

### Administre los permisos de UNIX mediante la ficha Seguridad de Windows

Si desea manipular los permisos de UNIX de archivos o carpetas en volúmenes o qtrees de estilo de seguridad mixtos en las SVM, puede utilizar la pestaña Seguridad en clientes de Windows. También puede utilizar aplicaciones que puedan consultar y establecer ACL de Windows.

- Modificación de permisos de UNIX

Puede usar la pestaña Seguridad de Windows para ver y cambiar los permisos de UNIX para un volumen o un qtree de estilo de seguridad mixto. Si utiliza la ficha Seguridad de Windows principal para cambiar los permisos de UNIX, primero debe quitar la ACE existente que desea editar (esto establece los bits de modo en 0) antes de realizar los cambios. De forma alternativa, puede utilizar el editor avanzado para cambiar los permisos.

Si se utilizan permisos de modo, puede cambiar directamente los permisos de modo para el UID, GID y otros (todos los demás con una cuenta en el equipo) de la lista. Por ejemplo, si el UID mostrado tiene permisos r-x, puede cambiar los permisos de UID a rwx.

- Cambiar los permisos de UNIX a los permisos NTFS



Puede usar la pestaña Seguridad de Windows para reemplazar objetos de seguridad UNIX por objetos de seguridad de Windows en un volumen o qtree de estilo de seguridad mixto donde los archivos y carpetas tienen un estilo de seguridad efectivo de UNIX.

Primero debe quitar todas las entradas de permisos de UNIX enumeradas antes de que pueda reemplazarlas con los objetos de usuario y grupo de Windows deseados. A continuación, puede configurar ACL basados en NTFS en los objetos Usuario y Grupo de Windows. Si quita todos los objetos de seguridad de UNIX y agrega sólo usuarios y grupos de Windows a un archivo o carpeta de un volumen o qtree de estilo de seguridad mixto, cambie el estilo de seguridad efectivo del archivo o carpeta de UNIX a NTFS.

Al cambiar los permisos de una carpeta, el comportamiento predeterminado de Windows es propagar estos cambios a todas las subcarpetas y archivos. Por lo tanto, debe cambiar la opción de propagación a la configuración deseada si no desea propagar un cambio en el estilo de seguridad a todas las carpetas secundarias, subcarpetas y archivos.

## **Gestione la configuración de seguridad del servidor SMB**

### **Cómo maneja ONTAP la autenticación de clientes SMB**

Antes de que los usuarios puedan crear conexiones SMB para acceder a los datos contenidos en la SVM, el dominio al que pertenece el servidor SMB debe autenticarse. El servidor SMB admite dos métodos de autenticación: Kerberos y NTLM (NTLMv1 o NTLMv2). Kerberos es el método predeterminado utilizado para autenticar usuarios de dominio.

### **Autenticación Kerberos**

ONTAP admite la autenticación Kerberos al crear sesiones SMB autenticadas.

Kerberos es el servicio de autenticación principal para Active Directory. El servidor Kerberos o el servicio de centro de distribución de claves Kerberos (KDC) almacena y recupera información acerca de los principios de seguridad en Active Directory. A diferencia del modelo NTLM, los clientes de Active Directory que deseen establecer una sesión con otro equipo, como el servidor SMB, póngase en contacto directamente con un KDC para obtener sus credenciales de sesión.

### **Autenticación NTLM**

La autenticación de clientes NTLM se realiza mediante un protocolo de respuesta a desafío basado en el conocimiento compartido de un secreto específico del usuario basado en una contraseña.

Si un usuario crea una conexión SMB con una cuenta de usuario local de Windows, el servidor SMB realiza la autenticación localmente con NTLMv2.

### **Directrices para la configuración de seguridad del servidor SMB en una configuración de recuperación ante desastres de SVM**

Antes de crear una SVM que se configura como un destino de recuperación de desastres donde no se conserva la identidad (la `-identity-preserve` opción establecida en `false` En la configuración de SnapMirror), debe saber cómo se gestionan las opciones de seguridad de servidores SMB en la SVM de destino.

- La configuración de seguridad del servidor SMB no predeterminada no se replica en el destino.

Cuando se crea un servidor SMB en la SVM de destino, todas las opciones de seguridad del servidor SMB se establecen en valores predeterminados. Cuando el destino de recuperación ante desastres de SVM se inicializa, se actualiza o se vuelve a sincronizar, la configuración de seguridad del servidor SMB en el origen no se replica en el destino.

- Debe configurar manualmente las opciones de seguridad del servidor SMB no predeterminadas.

Si tiene configuradas las opciones de seguridad del servidor SMB no predeterminadas en la SVM de origen, debe configurar manualmente estas mismas opciones en la SVM de destino después de que el destino pase a ser de lectura y escritura (después de que se rompa la relación de SnapMirror).

#### Mostrar información sobre la configuración de seguridad del servidor SMB

Puede ver información acerca de la configuración de seguridad del servidor SMB en las máquinas virtuales de almacenamiento (SVM). Puede utilizar esta información para comprobar que la configuración de seguridad es correcta.

#### Acerca de esta tarea

Una configuración de seguridad mostrada puede ser el valor predeterminado para ese objeto o un valor no predeterminado que se configura mediante la CLI de ONTAP o mediante objetos de directiva de grupo de Active Directory (GPO).

No utilice la `vserver cifs security show` Comando para servidores SMB en modo de grupo de trabajo, porque algunas de las opciones no son válidas.

#### Paso

1. Ejecute una de las siguientes acciones:

| Si desea mostrar información acerca de...                           | Introduzca el comando...                                                                                                                                                             |
|---------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Toda la configuración de seguridad en una SVM especificada          | <code>vserver cifs security show -vserver <i>vserver_name</i></code>                                                                                                                 |
| Una configuración o configuración de seguridad específica en la SVM | <code>vserver cifs security show -vserver <i>_vserver_name_</i> -fields [fieldname,...]</code><br>Puede entrar <code>-fields ?</code> para determinar qué campos se pueden utilizar. |

#### Ejemplo

En el siguiente ejemplo, se muestran todas las opciones de seguridad de la SVM vs1:

```
cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

Kerberos Clock Skew: 5 minutes
Kerberos Ticket Age: 10 hours
Kerberos Renewal Age: 7 days
Kerberos KDC Timeout: 3 seconds
Is Signing Required: false
Is Password Complexity Required: true
Use start_tls For AD LDAP connection: false
Is AES Encryption Enabled: false
LM Compatibility Level: lm-ntlm-ntlmv2-krb
Is SMB Encryption Required: false
Client Session Security: none
SMB1 Enabled for DC Connections: false
SMB2 Enabled for DC Connections: system-default
LDAP Referral Enabled For AD LDAP connections: false
Use LDAPS for AD LDAP connection: false
Encryption is required for DC Connections: false
AES session key enabled for NetLogon channel: false
Try Channel Binding For AD LDAP Connections: false
```

Tenga en cuenta que la configuración mostrada depende de la versión de ONTAP en ejecución.

En el siguiente ejemplo, se muestra el desfase de reloj de Kerberos para SVM vs1:

```
cluster1::> vserver cifs security show -vserver vs1 -fields kerberos-
clock-skew

vserver kerberos-clock-skew

vs1 5
```

## Información relacionada

[Mostrar información acerca de las configuraciones de GPO](#)

## Habilitar o deshabilitar la complejidad de contraseña requerida para los usuarios locales de la SMB

La complejidad de contraseña necesaria proporciona una seguridad mejorada para los usuarios de SMB locales en sus máquinas virtuales de almacenamiento (SVM). La función de complejidad de contraseña necesaria está activada de forma predeterminada. Puede deshabilitarla y volver a habilitarla en cualquier momento.

## Antes de empezar

Los usuarios locales, los grupos locales y la autenticación de usuarios locales deben estar habilitados en el servidor CIFS.



**Acerca de esta tarea**

No debe utilizar el `vserver cifs security modify` Comando para un servidor CIFS en modo de grupo de trabajo debido a que algunas de las opciones no son válidas.

**Pasos**

- 1. Ejecute una de las siguientes acciones:

| Si desea que la complejidad de contraseña requerida para los usuarios locales de la SMB sea... | Introduzca el comando...                                                                                |
|------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| Activado                                                                                       | <code>vserver cifs security modify -vserver vserver_name -is-password-complexity -required true</code>  |
| Deshabilitado                                                                                  | <code>vserver cifs security modify -vserver vserver_name -is-password-complexity -required false</code> |

- 2. Compruebe la configuración de seguridad para conocer la complejidad de la contraseña necesaria:  
`vserver cifs security show -vserver vserver_name`

**Ejemplo**

El siguiente ejemplo muestra que la complejidad de contraseña necesaria está habilitada para los usuarios locales de SMB para SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-password
-complexity-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-password-
complexity-required
vserver is-password-complexity-required

vs1 true
```

**Información relacionada**

- [Mostrar información acerca de la configuración de seguridad del servidor CIFS](#)
- [Uso de usuarios y grupos locales para autenticación y autorización](#)
- [Requisitos para las contraseñas de usuario local](#)
- [Cambio de contraseñas de cuenta de usuario local](#)

**Modifique la configuración de seguridad Kerberos del servidor CIFS**

Puede modificar ciertos ajustes de seguridad Kerberos del servidor CIFS, incluyendo la hora de desfase de reloj de Kerberos máxima permitida, la duración de la incidencia de Kerberos y el número máximo de días de renovación de incidencias.

**Acerca de esta tarea**

Modificar la configuración de Kerberos del servidor CIFS mediante el `vserver cifs security modify` El comando modifica la configuración solo en la máquina virtual de almacenamiento única (SVM) que se especifica con el `-vserver` parámetro. Puede administrar de forma centralizada la configuración de seguridad Kerberos para todas las SVM del clúster que pertenecen al mismo dominio de Active Directory mediante objetos de directiva de grupo (GPO) de Active Directory.

**Pasos**

1. Ejecute una o varias de las siguientes acciones:

| Si desea...                                                                                                                                  | Introduzca...                                                                                                                                        |
|----------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| Especifique el tiempo máximo permitido de inclinación del reloj Kerberos en minutos (9.13.1 y posteriores) o segundos (9.12.1 o anteriores). | <pre>vserver cifs security modify -vserver vserver_name -kerberos-clock-skew integer_in_minutes</pre> <p>El valor predeterminado es 5 minutos.</p>   |
| Especifique la duración del billete Kerberos en horas.                                                                                       | <pre>vserver cifs security modify -vserver vserver_name -kerberos-ticket-age integer_in_hours</pre> <p>El valor predeterminado es 10 horas.</p>      |
| Especifique el número máximo de días de renovación de la tarjeta.                                                                            | <pre>vserver cifs security modify -vserver vserver_name -kerberos-renew-age integer_in_days</pre> <p>El valor predeterminado es 7 días.</p>          |
| Especifique el tiempo de espera para los sockets de los KDC después de lo cual todos los KDC están marcados como inaccesibles.               | <pre>vserver cifs security modify -vserver vserver_name -kerberos-kdc-timeout integer_in_seconds</pre> <p>El valor predeterminado es 3 segundos.</p> |

2. Compruebe la configuración de seguridad de Kerberos:

```
vserver cifs security show -vserver vserver_name
```

**Ejemplo**

En el ejemplo siguiente se realizan los cambios siguientes en la seguridad de Kerberos: «'Kerberos Clock Skew'» se establece en 3 minutos y «'Kerberos Ticket Age'» se establece en 8 horas para SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock-skew 3 -kerberos-ticket-age 8
```

```
cluster1::> vserver cifs security show -vserver vs1
```

Vserver: vs1

|                                       |                    |
|---------------------------------------|--------------------|
| Kerberos Clock Skew:                  | 3 minutes          |
| Kerberos Ticket Age:                  | 8 hours            |
| Kerberos Renewal Age:                 | 7 days             |
| Kerberos KDC Timeout:                 | 3 seconds          |
| Is Signing Required:                  | false              |
| Is Password Complexity Required:      | true               |
| Use start_tls For AD LDAP connection: | false              |
| Is AES Encryption Enabled:            | false              |
| LM Compatibility Level:               | lm-ntlm-ntlmv2-krb |
| Is SMB Encryption Required:           | false              |

#### Información relacionada

["Mostrar información acerca de la configuración de seguridad del servidor CIFS"](#)

["Objetos de normativa de grupo compatibles"](#)

["Aplicación de objetos de directiva de grupo a servidores CIFS"](#)

#### Establezca el nivel de seguridad de autenticación mínimo del servidor SMB

Puede establecer el nivel de seguridad mínimo del servidor SMB, también conocido como *LMCompatibilityLevel*, en el servidor SMB para satisfacer los requisitos de seguridad del negocio para el acceso de cliente SMB. El nivel de seguridad mínimo es el nivel mínimo de los tokens de seguridad que acepta el servidor SMB de los clientes SMB.



#### Acerca de esta tarea

- Los servidores SMB en modo de grupo de trabajo sólo admiten la autenticación NTLM. La autenticación Kerberos no es compatible.
- LmCompatibilityLevel se aplica sólo a la autenticación de cliente SMB, no a la autenticación de administrador.

Es posible configurar el nivel de seguridad de autenticación mínimo en uno de los cuatro niveles de seguridad compatibles.

| Valor                               | Descripción                                                                                         |
|-------------------------------------|-----------------------------------------------------------------------------------------------------|
| lm-ntlm-ntlmv2-krb (predeterminado) | La máquina virtual de almacenamiento (SVM) acepta seguridad de autenticación LM, NTLMv2 y Kerberos. |

| Valor           | Descripción                                                                                                      |
|-----------------|------------------------------------------------------------------------------------------------------------------|
| ntlm-ntlmv2-krb | La SVM acepta la seguridad de autenticación NTLM, NTLMv2 y Kerberos. La SVM rechaza la autenticación LM.         |
| ntlmv2-krb      | La SVM acepta la seguridad de autenticación NTLMv2 y Kerberos. La SVM rechaza la autenticación LM y NTLM.        |
| krb             | La SVM solo acepta la seguridad de autenticación de Kerberos. La SVM deniega la autenticación LM, NTLM y NTLMv2. |

## Pasos

1. Configure el nivel de seguridad de autenticación mínimo: `vserver cifs security modify -vserver vserver_name -lm-compatibility-level {lm-ntlm-ntlmv2-krb|ntlm-ntlmv2-krb|ntlmv2-krb|krb}`
2. Compruebe que el nivel de seguridad de autenticación se haya establecido en el nivel deseado: `vserver cifs security show -vserver vserver_name`

## Información relacionada

[Habilitar o deshabilitar el cifrado AES para la comunicación basada en Kerberos](#)

### Configure una seguridad segura para la comunicación basada en Kerberos mediante el cifrado AES

Para obtener la mayor seguridad con la comunicación basada en Kerberos, puede habilitar el cifrado AES-256 y AES-128 en el servidor SMB. De manera predeterminada, cuando crea un servidor SMB en la SVM, el cifrado Advanced Encryption Standard (AES) está deshabilitado. Debe habilitarla para aprovechar la seguridad robusta proporcionada por el cifrado AES.

La comunicación relacionada con Kerberos para SMB se utiliza durante la creación del servidor SMB en la SVM, así como durante la fase de configuración de la sesión SMB. El servidor SMB es compatible con los siguientes tipos de cifrado para la comunicación de Kerberos:

- AES 256
- AES 128
- DES
- RC4-HMAC

Si desea utilizar el tipo de cifrado de seguridad más alto para la comunicación de Kerberos, debe habilitar el cifrado AES para la comunicación de Kerberos en la SVM.

Cuando se crea el servidor SMB, el controlador de dominio crea una cuenta de equipo en Active Directory. En este momento, el KDC se da cuenta de las capacidades de cifrado de la cuenta de equipo en particular. Posteriormente, se selecciona un tipo de cifrado concreto para cifrar el ticket de servicio que el cliente presenta al servidor durante la autenticación.

A partir de ONTAP 9.12.1, puede especificar los tipos de cifrado que desea anunciar en el KDC de Active Directory (AD). Puede utilizar el `-advertised-enc-types` opción para activar los tipos de cifrado recomendados y puede utilizarlo para desactivar los tipos de cifrado más débiles. Aprenda cómo ["Habilite y deshabilite tipos de cifrado para la comunicación basada en Kerberos"](#).



Las nuevas instrucciones de AES (Intel AES ni) están disponibles en SMB 3.0, mejorando el algoritmo AES y acelerando el cifrado de datos con las familias de procesadores compatibles.a partir de SMB 3.1.1, AES-128-GCM reemplaza a AES-128-CCM como el algoritmo hash utilizado por el cifrado SMB.

**Información relacionada**

[Modificar la configuración de seguridad Kerberos del servidor CIFS](#)

**Habilite o deshabilite el cifrado AES para la comunicación basada en Kerberos**

Para aprovechar la seguridad más fuerte con la comunicación basada en Kerberos, debe utilizar el cifrado AES-256 y AES-128 en el servidor SMB. A partir de ONTAP 9.13.1, el cifrado AES está habilitado de forma predeterminada. Si no desea que el servidor SMB seleccione los tipos de cifrado AES para la comunicación basada en Kerberos con el KDC de Active Directory (AD), puede deshabilitar el cifrado AES.

Si el cifrado AES está habilitado de forma predeterminada y si tiene la opción de especificar tipos de cifrado depende de su versión de ONTAP.

| Versión de ONTAP    | El cifrado AES está activado... | ¿Puede especificar tipos de cifrado? |
|---------------------|---------------------------------|--------------------------------------|
| 9.13.1 y posterior  | De forma predeterminada         | Sí                                   |
| 9.12.1              | Manualmente                     | Sí                                   |
| 9.11.1 y anteriores | Manualmente                     | No                                   |

A partir de ONTAP 9.12.1, el cifrado AES está habilitado y deshabilitado mediante el `-advertised-enc-types` Opción, que permite especificar los tipos de cifrado anunciados en AD KDC. El valor predeterminado es `rc4 y.. des`, Pero cuando se especifica un tipo AES, el cifrado AES está activado. También puede utilizar la opción para desactivar explícitamente los tipos de cifrado RC4 y DES más débiles. En ONTAP 9.11.1 y versiones anteriores, debe utilizar el `-is-aes-encryption-enabled` Opción para habilitar y deshabilitar el cifrado AES, y no se pueden especificar los tipos de cifrado.

Para mejorar la seguridad, la máquina virtual de almacenamiento (SVM) cambia su contraseña de cuenta de máquina en AD cada vez que se modifica la opción de seguridad AES. El cambio de la contraseña podría requerir credenciales AD administrativas para la unidad organizativa (OU) que contiene la cuenta del equipo.

Si una SVM se configura como un destino de recuperación ante desastres donde no se conserva la identidad (la `-identity-preserve` opción establecida en `false` En la configuración SnapMirror), las opciones de seguridad del servidor SMB no predeterminadas no se replican en el destino. Si habilitó el cifrado AES en la SVM de origen, debe habilitarla manualmente.



## Ejemplo 5. Pasos

### ONTAP 9.12.1 y versiones posteriores

1. Ejecute una de las siguientes acciones:

| Si desea que los tipos de cifrado AES para la comunicación Kerberos sean... | Introduzca el comando...                                                                                     |
|-----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| Activado                                                                    | <pre>vserver cifs security modify<br/>-vserver vserver_name -advertised<br/>-enc-types aes-128,aes-256</pre> |
| Deshabilitado                                                               | <pre>vserver cifs security modify<br/>-vserver vserver_name -advertised<br/>-enc-types des,rc4</pre>         |

**Nota:** la `-is-aes-encryption-enabled` La opción quedó obsoleta en ONTAP 9.12.1 y se puede quitar en una versión posterior.

2. Compruebe que el cifrado AES está habilitado o deshabilitado como desee: `vserver cifs security show -vserver vserver_name -fields advertised-enc-types`

### Ejemplos

En el siguiente ejemplo, se habilitan los tipos de cifrado AES para el servidor SMB en la SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -advertised-enc
-types aes-128,aes-256

cluster1::> vserver cifs security show -vserver vs1 -fields advertised-
enc-types

vserver advertised-enc-types

vs1 aes-128,aes-256
```

En el ejemplo siguiente se habilitan los tipos de cifrado AES para el servidor SMB en la SVM vs2. Se solicita al administrador que introduzca las credenciales AD administrativas para la unidad organizativa que contiene el servidor SMB.

```
cluster1::> vsriver cifs security modify -vsriver vs2 -advertised-enc
-types aes-128,aes-256
```

Info: In order to enable SMB AES encryption, the password for the SMB server machine account must be reset. Enter the username and password for the SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

```
cluster1::> vsriver cifs security show -vsriver vs2 -fields advertised-
enc-types
```

```
vsriver advertised-enc-types
----- -----
vs2 aes-128,aes-256
```

## ONTAP 9.11.1 y anteriores

1. Ejecute una de las siguientes acciones:

| Si desea que los tipos de cifrado AES para la comunicaci3n Kerberos sean... | Introduzca el comando...                                                                        |
|-----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| Activado                                                                    | <pre>vsriver cifs security modify -vsriver vsriver_name -is-aes -encryption-enabled true</pre>  |
| Deshabilitado                                                               | <pre>vsriver cifs security modify -vsriver vsriver_name -is-aes -encryption-enabled false</pre> |

2. Compruebe que el cifrado AES est3 habilitado o deshabilitado como desee: 

```
vsriver cifs security show -vsriver vsriver_name -fields is-aes-encryption-enabled
```

La `is-aes-encryption-enabled` se muestra el campo `true` Si el cifrado AES est3 habilitado y `false` si est3 desactivada.

## Ejemplos

En el siguiente ejemplo, se habilitan los tipos de cifrado AES para el servidor SMB en la SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-aes
-encryption-enabled true

cluster1::> vserver cifs security show -vserver vs1 -fields is-aes-
encryption-enabled

vserver is-aes-encryption-enabled

vs1 true
```

En el ejemplo siguiente se habilitan los tipos de cifrado AES para el servidor SMB en la SVM vs2. Se solicita al administrador que introduzca las credenciales AD administrativas para la unidad organizativa que contiene el servidor SMB.

```
cluster1::> vserver cifs security modify -vserver vs2 -is-aes
-encryption-enabled true

Info: In order to enable SMB AES encryption, the password for the CIFS
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields is-aes-
encryption-enabled

vserver is-aes-encryption-enabled

vs2 true
```

**Utilice la firma SMB para mejorar la seguridad de la red**

**Utilice la firma SMB para mejorar la información general sobre seguridad de red**

La firma SMB ayuda a garantizar que el tráfico de red entre el servidor SMB y el cliente no se vea comprometido; esto evita los ataques de repetición. De forma predeterminada, ONTAP admite la firma SMB cuando lo solicita el cliente. De manera opcional, el administrador de almacenamiento puede configurar el servidor SMB para que requiera la firma SMB.

## Cómo afectan las políticas de firma SMB a la comunicación con un servidor CIFS

Además de la configuración de seguridad de firma SMB del servidor CIFS, dos políticas de firma SMB en clientes de Windows controlan la firma digital de las comunicaciones entre clientes y el servidor CIFS. Puede configurar el ajuste que cumpla con sus requisitos empresariales.

Las directivas SMB de cliente se controlan a través de la configuración de la directiva de seguridad local de Windows, que se configuran mediante Microsoft Management Console (MMC) o los GPO de Active Directory. Para obtener más información acerca de los problemas de firma SMB de cliente y de seguridad, consulte la documentación de Microsoft Windows.

A continuación, se muestran descripciones de las dos políticas de firma SMB en los clientes de Microsoft:

- `Microsoft network client: Digitally sign communications (if server agrees)`

Esta configuración controla si la capacidad de firma SMB del cliente está habilitada. Está activado de forma predeterminada. Cuando se deshabilita esta configuración en el cliente, las comunicaciones del cliente con el servidor CIFS dependen de la configuración de firma SMB en el servidor CIFS.

- `Microsoft network client: Digitally sign communications (always)`

Esta configuración controla si el cliente requiere la firma SMB para comunicarse con un servidor. Está desactivado de forma predeterminada. Cuando esta configuración está deshabilitada en el cliente, el comportamiento de firma SMB se basa en la configuración de directiva para `Microsoft network client: Digitally sign communications (if server agrees)` Y la configuración en el servidor CIFS.



Si el entorno incluye clientes de Windows configurados para requerir la firma SMB, debe habilitar la firma SMB en el servidor CIFS. Si no lo hace, el servidor CIFS no puede proporcionar datos a estos sistemas.

Los resultados efectivos de la configuración de firma SMB del cliente y del servidor CIFS dependen de si las sesiones SMB utilizan SMB 1.0 o SMB 2.x y versiones posteriores.

En la tabla siguiente se resume el comportamiento efectivo de la firma SMB si la sesión utiliza SMB 1.0:

| Cliente                          | No se requiere firma con ONTAP | Se requiere firma ONTAP |
|----------------------------------|--------------------------------|-------------------------|
| Firma desactivada y no requerida | No firmado                     | Firmado                 |
| Firma habilitada y no requerida  | No firmado                     | Firmado                 |
| Firma desactivada y obligatoria  | Firmado                        | Firmado                 |
| Firma habilitada y requerida     | Firmado                        | Firmado                 |



Es posible que los clientes Windows SMB 1 anteriores y algunos clientes SMB 1 distintos de Windows no puedan conectarse si la firma está deshabilitada en el cliente, pero es necesaria en el servidor CIFS.

En la tabla siguiente se resume el comportamiento efectivo de la firma SMB si la sesión utiliza SMB 2.x o SMB 3.0:



Para los clientes SMB 2.x y SMB 3.0, la firma SMB siempre está habilitada. No se puede deshabilitar.

| Cliente              | No se requiere firma con ONTAP | Se requiere firma ONTAP |
|----------------------|--------------------------------|-------------------------|
| No se requiere firma | No firmado                     | Firmado                 |
| Se requiere firma    | Firmado                        | Firmado                 |

En la tabla siguiente se resume el comportamiento de firma SMB de servidor y cliente de Microsoft predeterminado:

| Protocolo | Algoritmo hash | Puede activar/desactivar | Se puede requerir o no se puede requerir | Valor predeterminado del cliente | Valor predeterminado del servidor | DC predeterminado |
|-----------|----------------|--------------------------|------------------------------------------|----------------------------------|-----------------------------------|-------------------|
| SMB 1,0   | MD5            | Sí                       | Sí                                       | Habilitado (no es necesario)     | Deshabilitado (no obligatorio)    | Obligatorio       |
| SMB 2.x   | HMAC SHA-256   | No                       | Sí                                       | No es obligatorio                | No es obligatorio                 | Obligatorio       |
| SMB 3,0   | AES-CMAC.      | No                       | Sí                                       | No es obligatorio                | No es obligatorio                 | Obligatorio       |



Microsoft ya no recomienda su uso `Digitally sign communications (if client agrees)` o `Digitally sign communications (if server agrees)` Configuración de la directiva de grupo. Microsoft tampoco recomienda utilizar más `EnableSecuritySignature` configuración del registro. Estas opciones solo afectan al comportamiento de SMB 1 y pueden ser sustituidas por `Digitally sign communications (always)` Configuración de directiva de grupo o la `RequireSecuritySignature` configuración del registro. También puede obtener más información en el blog de Microsoft. Conceptos básicos de [The para la firma de SMB \(cubriendo tanto SMB1 como SMB2\)](#)

## Impacto en el rendimiento de la firma SMB

Cuando las sesiones SMB utilizan la firma SMB, todas las comunicaciones SMB a y desde clientes de Windows experimentan un impacto en el rendimiento, lo cual afecta tanto a los clientes como al servidor (es decir, los nodos del clúster que ejecuta la SVM que contiene el servidor SMB).

El impacto en el rendimiento muestra que el uso de CPU ha aumentado tanto en los clientes como en el servidor, aunque la cantidad de tráfico de red no cambia.

La magnitud del impacto en el rendimiento depende de la versión de ONTAP 9 que esté ejecutando. A partir de ONTAP 9.7, un nuevo algoritmo de descarga del cifrado puede permitir un mejor rendimiento en el tráfico de SMB firmado. La descarga de firma SMB se habilita de forma predeterminada cuando se habilita la firma SMB.

El rendimiento mejorado de la firma SMB requiere la funcionalidad de descarga de AES-ni. Consulte el Hardware Universe (HWU) para verificar que la descarga AES-ni es compatible con su plataforma.

Otras mejoras de rendimiento también son posibles si usted es capaz de utilizar SMB versión 3,11 que admite el algoritmo GCM mucho más rápido.

Según la red, la versión de ONTAP 9, la versión de SMB y la implementación de SVM, el impacto en el rendimiento de la firma SMB puede variar enormemente; puede verificarlo únicamente mediante pruebas en el entorno de red.

La mayoría de los clientes de Windows negocian la firma SMB de forma predeterminada si está habilitada en el servidor. Si necesita protección SMB para algunos de sus clientes Windows y la firma SMB está provocando problemas de rendimiento, puede deshabilitar la firma SMB en cualquiera de sus clientes Windows que no necesiten protección contra ataques de repetición. Para obtener información sobre cómo deshabilitar la firma SMB en clientes Windows, consulte la documentación de Microsoft Windows.

**Recomendaciones para configurar la firma SMB**

Puede configurar un comportamiento de firma SMB entre clientes SMB y el servidor CIFS para satisfacer sus requisitos de seguridad. La configuración que elija al configurar la firma SMB en el servidor CIFS depende de cuáles sean sus requisitos de seguridad.

Es posible configurar la firma SMB en el cliente o en el servidor CIFS. Tenga en cuenta las siguientes recomendaciones al configurar la firma SMB:

| Si...                                                                                                            | Recomendación...                                                                                                                                    |
|------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| Desea aumentar la seguridad de la comunicación entre el cliente y el servidor                                    | Haga que se requiera la firma SMB en el cliente al habilitar el <code>Require Option (Sign always)</code> configuración de seguridad en el cliente. |
| Es conveniente que todo el tráfico de SMB esté firmado a una determinada máquina virtual de almacenamiento (SVM) | Para requerir la firma SMB en el servidor CIFS, configure la configuración de seguridad para requerir la firma SMB.                                 |

Consulte la documentación de Microsoft para obtener más información acerca de la configuración de la seguridad del cliente de Windows.

**Directrices para la firma SMB cuando se configuran varias LIF de datos**

Si habilita o deshabilita la firma SMB requerida en el servidor SMB, debe tener en cuenta las directrices para varias configuraciones de LIF de datos para una SVM.

Cuando configura un servidor SMB, puede haber varios LIF de datos configurados. Si es así, el servidor DNS contiene varios A Registre las entradas del servidor CIFS utilizando el mismo nombre de host del servidor SMB, pero cada una con una dirección IP única. Por ejemplo, un servidor SMB que tiene dos LIF de datos configuradas puede tener el siguiente DNS A entradas de registro:

```
10.1.1.128 A VS1.IEPUB.LOCAL VS1
10.1.1.129 A VS1.IEPUB.LOCAL VS1
```

El comportamiento normal es que, al cambiar la configuración de firma SMB necesaria, solo las nuevas conexiones de clientes se ven afectadas por el cambio en la configuración de firma SMB. Sin embargo, hay una excepción a este comportamiento. Existe un caso en el que un cliente tiene una conexión existente con un recurso compartido y éste crea una nueva conexión con el mismo recurso compartido después de cambiar la configuración, manteniendo la conexión original. En este caso, tanto la conexión SMB nueva como la existente adoptan los nuevos requisitos de firma SMB.

Observe el siguiente ejemplo:

1. CLIENTE1 se conecta a un recurso compartido sin la firma SMB requerida mediante la ruta de acceso `O:\`.
2. El administrador de almacenamiento modifica la configuración del servidor SMB para requerir la firma SMB.
3. CLIENTE1 se conecta al mismo recurso compartido con la firma SMB requerida mediante la ruta de acceso `S:\` (mientras mantiene la conexión utilizando la ruta `O:\`).
4. El resultado es que se utiliza la firma SMB al acceder a datos a través de ambos `O:\` y `S:\` unidades.

### Habilite o deshabilite la firma SMB requerida para el tráfico entrante de SMB

Puede aplicar el requisito de que los clientes firmen mensajes SMB habilitando la firma SMB requerida. Si está habilitada, ONTAP solo acepta mensajes SMB si tienen firmas válidas. Si desea permitir la firma SMB, pero no la requiere, puede deshabilitar la firma SMB requerida.

#### Acerca de esta tarea

De manera predeterminada, la firma SMB requerida está deshabilitada. Es posible habilitar o deshabilitar la firma SMB requerida en cualquier momento.



La firma SMB no está deshabilitada de forma predeterminada en las siguientes circunstancias:

1. La firma SMB necesaria está habilitada y el clúster se revierte a una versión de ONTAP que no admite la firma SMB.
2. Posteriormente, el clúster se actualiza a una versión de ONTAP que admite la firma SMB.

En estas circunstancias, la configuración de firma SMB configurada originalmente en una versión compatible de ONTAP se conserva mediante la reversión y la posterior actualización.

Al configurar una relación de recuperación ante desastres de máquina virtual de almacenamiento (SVM), el valor que seleccione para `-identity-preserve` opción de `snapmirror create` El comando determina los detalles de configuración que se replican en la SVM de destino.

Si establece la `-identity-preserve` opción a `true` (ID-preserve), la configuración de seguridad de firma SMB se replica en el destino.

Si establece la `-identity-preserve` opción a `false` (Que no sea una conservación de ID), la configuración de seguridad de firma SMB no se replica en el destino. En este caso, la configuración de seguridad del servidor CIFS en el destino se establece en los valores predeterminados. Si habilitó la firma SMB requerida en la SVM de origen, debe habilitar manualmente la firma SMB requerida en la SVM de destino.

**Pasos**

- 1. Ejecute una de las siguientes acciones:

| Si desea que la firma SMB sea... | Introduzca el comando...                                                                   |
|----------------------------------|--------------------------------------------------------------------------------------------|
| Activado                         | <code>vserver cifs security modify -vserver vserver_name -is-signing-required true</code>  |
| Deshabilitado                    | <code>vserver cifs security modify -vserver vserver_name -is-signing-required false</code> |

- 2. Compruebe que la firma SMB necesaria está habilitada o deshabilitada determinando si el valor de la `Is Signing Required` el campo del resultado del comando siguiente está establecido en el valor deseado:  
`vserver cifs security show -vserver vserver_name -fields is-signing-required`

**Ejemplo**

En el siguiente ejemplo, se habilita la firma SMB requerida para SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-signing-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-signing-required
vserver is-signing-required
----- -
vs1 true
```



Los cambios en la configuración de cifrado surten efecto para las nuevas conexiones. Las conexiones existentes no se ven afectadas.

**Determinar si se han firmado las sesiones SMB**

Puede ver información sobre las sesiones SMB conectadas en el servidor CIFS. Puede usar esta información para determinar si las sesiones SMB están firmadas. Esto puede resultar útil para determinar si las sesiones de cliente SMB se conectan con la configuración de seguridad deseada.

**Pasos**

- 1. Ejecute una de las siguientes acciones:



| Si desea mostrar información acerca de...                                             | Introduzca el comando...                                                                          |
|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| Todas las sesiones firmados en una máquina virtual de almacenamiento (SVM) específica | <code>vserver cifs session show -vserver <i>vserver_name</i> -is-session-signed true</code>       |
| Detalles de una sesión firmada con un ID de sesión específico en la SVM               | <code>vserver cifs session show -vserver <i>vserver_name</i> -session-id integer -instance</code> |

## Ejemplos

El siguiente comando muestra información de sesión sobre las sesiones firmadas en la SVM vs1. El resultado de resumen predeterminado no muestra el campo de salida "is Session Signed":

```
cluster1::> vserver cifs session show -vserver vs1 -is-session-signed true
Node: node1
Vserver: vs1
Connection Session
ID ID Workstation Windows User Open Idle

3151272279 1 10.1.1.1 DOMAIN\joe 2 23s
```

El siguiente comando muestra información detallada de sesión, incluido si la sesión está firmada, en una sesión SMB con un ID de sesión de 2:

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
Node: node1
Vserver: vs1
Session ID: 2
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation: 10.1.1.2
Authentication Mechanism: Kerberos
Windows User: DOMAIN\joe
UNIX User: pcuser
Open Shares: 1
Open Files: 1
Open Other: 0
Connected Time: 10m 43s
Idle Time: 1m 19s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: true
User Authenticated as: domain-user
NetBIOS Name: CIFS_ALIAS1
SMB Encryption Status: Unencrypted
```

## Información relacionada

[Supervisar estadísticas de sesión firmada por SMB](#)

## Supervise las estadísticas de la sesión firmada de SMB

Es posible supervisar las estadísticas de sesiones SMB y determinar qué sesiones establecidas se han firmado y cuáles no.

### Acerca de esta tarea

La `statistics` en el nivel de privilegio avanzado, proporciona el `signed_sessions` Contador que puede utilizar para supervisar el número de sesiones SMB firmadas. La `signed_sessions` counter está disponible con los siguientes objetos de estadísticas:

- `cifs` Permite supervisar la firma SMB en todas las sesiones SMB.
- `smb1` Permite supervisar la firma SMB para sesiones SMB 1.0.
- `smb2` Permite supervisar la firma SMB para las sesiones SMB 2.x y SMB 3.0.

Las estadísticas de SMB 3.0 se incluyen en el resultado del `smb2` objeto.

Si desea comparar el número de sesiones firmadas con el número total de sesiones, puede comparar el resultado de `signed_sessions` contador con la salida para el `established_sessions` contador.

Debe iniciar una colección de ejemplos de estadísticas para poder ver los datos resultantes. Puede ver los datos de la muestra si no detiene la recopilación de datos. Al detener la recopilación de datos, se proporciona

una muestra fija. No detener la recopilación de datos le ofrece la posibilidad de obtener datos actualizados que puede utilizar para compararlos con consultas anteriores. La comparación puede ayudarle a identificar tendencias.

**Pasos**

- 1. Establezca el nivel de privilegio en Advanced:  
`set -privilege advanced`
- 2. Iniciar una recopilación de datos:  
`statistics start -object {cifs|smb1|smb2} -instance instance -sample-id sample_ID [-node node_name]`

Si no especifica el `-sample-id` Parámetro, el comando genera un identificador de muestra para usted y define esta muestra como la muestra predeterminada para la sesión CLI. Valor para `-sample-id` es una cadena de texto. Si ejecuta este comando durante la misma sesión CLI y no especifica el `-sample-id` parámetro, el comando sobrescribe la muestra predeterminada anterior.

Opcionalmente, puede especificar el nodo en el que se desea recoger estadísticas. Si no especifica el nodo, la muestra recopila estadísticas para todos los nodos del clúster.

- 3. Utilice la `statistics stop` comando para detener la recogida de datos de la muestra.
- 4. Ver estadísticas de firma SMB:

| Si desea ver información acerca de...                             | Introduzca...                                                     |
|-------------------------------------------------------------------|-------------------------------------------------------------------|
| Sesiones firmadas                                                 | <code>`show -sample-id sample_ID -counter signed_sessions`</code> |
| <code>node_name [-node node_name]</code>                          | Sesiones firmadas y sesiones establecidas                         |
| <code>`show -sample-id sample_ID -counter signed_sessions`</code> | <code>established_sessions</code>                                 |

Si solo desea mostrar información de un solo nodo, especifique la opción `-node` parámetro.

- 5. Vuelva al nivel de privilegio de administrador:  
`set -privilege admin`

## Ejemplos

El siguiente ejemplo muestra cómo se pueden supervisar las estadísticas de firma de SMB 2.x y SMB 3.0 en vs1 de la máquina virtual de almacenamiento (SVM).

El siguiente comando cambia al nivel de privilegio avanzado:

```
cluster1::> set -privilege advanced
```

```
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
```

```
Do you want to continue? {y|n}: y
```

El siguiente comando inicia la recogida de datos de una nueva muestra:

```
cluster1::*> statistics start -object smb2 -sample-id smbsigning_sample
-vserver vs1
```

```
Statistics collection is being started for Sample-id: smbsigning_sample
```

El siguiente comando detiene la recogida de datos de la muestra:

```
cluster1::*> statistics stop -sample-id smbsigning_sample
```

```
Statistics collection is being stopped for Sample-id: smbsigning_sample
```

El siguiente comando muestra sesiones SMB firmadas y sesiones SMB establecidas por nodo a partir de la muestra:

```
cluster1::*> statistics show -sample-id smbSigning_sample -counter
signed_sessions|established_sessions|node_name
```

Object: smb2

Instance: vs1

Start-time: 2/6/2013 01:00:00

End-time: 2/6/2013 01:03:04

Cluster: cluster1

| Counter              | Value |
|----------------------|-------|
| -----                | ----- |
| established_sessions | 0     |
| node_name            | node1 |
| signed_sessions      | 0     |
| established_sessions | 1     |
| node_name            | node2 |
| signed_sessions      | 1     |
| established_sessions | 0     |
| node_name            | node3 |
| signed_sessions      | 0     |
| established_sessions | 0     |
| node_name            | node4 |
| signed_sessions      | 0     |

En el siguiente comando, se muestran las sesiones SMB firmadas para el nodo 2 en la muestra:

```
cluster1::*> statistics show -sample-id smbSigning_sample -counter
signed_sessions|node_name -node node2
```

Object: smb2

Instance: vs1

Start-time: 2/6/2013 01:00:00

End-time: 2/6/2013 01:22:43

Cluster: cluster1

| Counter         | Value |
|-----------------|-------|
| -----           | ----- |
| node_name       | node2 |
| signed_sessions | 1     |

El siguiente comando vuelve a pasar al nivel de privilegios de administrador:

```
cluster1::*> set -privilege admin
```

**Información relacionada**

[Determinar si se firmaron las sesiones SMB](#)

["Información general sobre la gestión y el control del rendimiento"](#)

**Configurar el cifrado SMB necesario en servidores SMB para las transferencias de datos a través de SMB**

**Información general de cifrado de SMB**

El cifrado SMB para las transferencias de datos a través de SMB es una mejora de seguridad que se puede habilitar o deshabilitar en servidores SMB. También puede configurar el valor de cifrado SMB deseado de forma compartida mediante una configuración de propiedad de recurso compartido.

De forma predeterminada, cuando crea un servidor SMB en la máquina virtual de almacenamiento (SVM), el cifrado SMB se deshabilita. Debe habilitarla para aprovechar la seguridad mejorada proporcionada por el cifrado SMB.

Para crear una sesión SMB cifrada, el cliente SMB debe admitir el cifrado SMB. Los clientes de Windows que empiezan con Windows Server 2012 y Windows 8 admiten el cifrado SMB.

El cifrado SMB en la SVM se controla mediante dos opciones de configuración:

- Una opción de seguridad del servidor SMB que habilita la funcionalidad en la SVM
- Una propiedad de recurso compartido SMB que configura la configuración de cifrado SMB de recurso compartido

Puede decidir si se requiere el cifrado para acceder a todos los datos en la SVM o si se requiere el cifrado SMB para acceder solo a los datos en recursos compartidos seleccionados. La configuración a nivel de SVM tiene preferencia en la configuración a nivel de recurso compartido.

La configuración efectiva del cifrado SMB depende de la combinación de las dos opciones y se describe en la siguiente tabla:

| Cifrado SMB Server habilitado | Configuración de cifrado compartido de datos activada | Comportamiento de cifrado del servidor                                                                                                                                                                                       |
|-------------------------------|-------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Verdadero                     | Falso                                                 | El cifrado a nivel de servidor está habilitado para todos los recursos compartidos de la SVM. Con esta configuración, se produce el cifrado en toda la sesión SMB.                                                           |
| Verdadero                     | Verdadero                                             | El cifrado a nivel de servidor se habilita para todos los recursos compartidos de la SVM, independientemente del cifrado a nivel de recurso compartido. Con esta configuración, se produce el cifrado en toda la sesión SMB. |

| <b>Cifrado SMB Server habilitado</b> | <b>Configuración de cifrado compartido de datos activada</b> | <b>Comportamiento de cifrado del servidor</b>                                                                                                                                 |
|--------------------------------------|--------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Falso                                | Verdadero                                                    | El cifrado a nivel de recurso compartido está habilitado para los recursos compartidos específicos. Con esta configuración, el cifrado se produce desde la conexión de árbol. |
| Falso                                | Falso                                                        | No hay ningún cifrado activado.                                                                                                                                               |

Los clientes SMB que no admiten cifrado no pueden conectarse a un servidor SMB o recurso compartido que requiera cifrado.

Los cambios en la configuración de cifrado surten efecto para las nuevas conexiones. Las conexiones existentes no se ven afectadas.

### **Impacto en el rendimiento del cifrado SMB**

Cuando las sesiones SMB utilizan el cifrado SMB, todas las comunicaciones SMB a y desde clientes de Windows experimentan un impacto en el rendimiento, lo cual afecta tanto a los clientes como al servidor (es decir, los nodos del clúster que ejecuta la SVM que contiene el servidor SMB).

El impacto en el rendimiento muestra que el uso de CPU ha aumentado tanto en los clientes como en el servidor, aunque la cantidad de tráfico de red no cambia.

La magnitud del impacto en el rendimiento depende de la versión de ONTAP 9 que esté ejecutando. A partir de ONTAP 9.7, un nuevo algoritmo de descarga del cifrado puede permitir un mejor rendimiento en el tráfico SMB cifrado. La descarga de cifrado SMB se habilita de forma predeterminada cuando se habilita el cifrado SMB.

El rendimiento del cifrado SMB mejorado requiere la capacidad de descarga de AES-ni. Consulte el Hardware Universe (HWU) para verificar que la descarga AES-ni es compatible con su plataforma.

Otras mejoras de rendimiento también son posibles si usted es capaz de utilizar SMB versión 3,11 que admite el algoritmo GCM mucho más rápido.

Según la red, la versión de ONTAP 9, la versión de SMB y la implementación de SVM, el impacto en el rendimiento del cifrado SMB puede variar enormemente; puede verificarlo únicamente mediante pruebas en su entorno de red.

El cifrado SMB está deshabilitado de forma predeterminada en el servidor SMB. Debe habilitar el cifrado SMB solo en aquellos recursos compartidos SMB o servidores SMB que requieran cifrado. Con el cifrado SMB, ONTAP realiza un procesamiento adicional de descifrar las solicitudes y cifrar las respuestas para cada solicitud. Por tanto, el cifrado SMB solo debe habilitarse cuando sea necesario.

### **Habilite o deshabilite el cifrado SMB requerido para el tráfico SMB entrante**

Si desea requerir el cifrado SMB para el tráfico SMB entrante puede habilitarla en el servidor CIFS o en el nivel de recurso compartido. De manera predeterminada, no es

necesario el cifrado SMB.

**Acerca de esta tarea**

Puede habilitar el cifrado SMB en el servidor CIFS, que se aplica a todos los recursos compartidos del servidor CIFS. Si no desea usar el cifrado SMB necesario para todos los recursos compartidos en el servidor CIFS o si desea habilitar el cifrado SMB necesario para el tráfico SMB entrante de acuerdo con recurso compartido por recurso, puede deshabilitar el cifrado SMB requerido en el servidor CIFS.

Al configurar una relación de recuperación ante desastres de máquina virtual de almacenamiento (SVM), el valor seleccionado para `-identity-preserve` opción de `snapmirror create` El comando determina los detalles de configuración que se replican en la SVM de destino.

Si establece la `-identity-preserve` opción a. `true` (ID-preserve), la configuración de seguridad de cifrado SMB se replica en el destino.

Si establece la `-identity-preserve` opción a. `false` (Que no sea ID-preserve), la configuración de seguridad de cifrado SMB no se replica en el destino. En este caso, la configuración de seguridad del servidor CIFS en el destino se establece en los valores predeterminados. Si ha habilitado el cifrado SMB en la SVM de origen, debe habilitar manualmente el cifrado SMB del servidor CIFS en el destino.

**Pasos**

- 1. Ejecute una de las siguientes acciones:

| Si desea que el cifrado SMB para el tráfico SMB entrante en el servidor CIFS sea... | Introduzca el comando...                                                                           |
|-------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| Activado                                                                            | <code>vserver cifs security modify -vserver vserver_name -is-smb-encryption -required true</code>  |
| Deshabilitado                                                                       | <code>vserver cifs security modify -vserver vserver_name -is-smb-encryption -required false</code> |

- 2. Compruebe que el cifrado SMB necesario en el servidor CIFS está habilitado o deshabilitado de la forma deseada:`vserver cifs security show -vserver vserver_name -fields is-smb-encryption-required`

La `is-smb-encryption-required` se muestra el campo `true` Si es necesario, el cifrado SMB se habilita en el servidor CIFS y. `false` si está desactivada.

**Ejemplo**

En el ejemplo siguiente se habilita el cifrado SMB requerido para el tráfico SMB entrante para el servidor CIFS en la SVM vs1:



```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption
-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-
encryption-required
vserver is-smb-encryption-required

vs1 true
```

## Determine si los clientes están conectados mediante sesiones SMB cifradas

Puede mostrar información sobre las sesiones SMB conectadas para determinar si los clientes están utilizando conexiones SMB cifradas. Esto puede resultar útil para determinar si las sesiones de cliente SMB se conectan con la configuración de seguridad deseada.

### Acerca de esta tarea

Las sesiones de clientes de SMB pueden tener uno de tres niveles de cifrado:

- `unencrypted`

La sesión SMB no está cifrada. No se configura ni el cifrado a nivel de equipo virtual de almacenamiento (SVM) ni el nivel de recurso compartido.

- `partially-encrypted`

El cifrado se inicia cuando se produce la conexión de árbol. Se configuró el cifrado a nivel de recurso compartido. El cifrado a nivel de SVM no está habilitado.

- `encrypted`

La sesión SMB está totalmente cifrada. El cifrado de la SVM está habilitado. Es posible que el cifrado de nivel de recurso compartido esté habilitado o no. La configuración de cifrado a nivel de SVM sustituye la configuración de cifrado a nivel de recurso compartido.

### Pasos

1. Ejecute una de las siguientes acciones:

| Si desea mostrar información acerca de...                                                    | Introduzca el comando...                                                          |
|----------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| Sesiones con una configuración de cifrado especificada para sesiones en una SVM especificada | <code>`vserver cifs session show -vserver <i>vserver_name</i> {unencrypted</code> |
| <code>partially-encrypted</code>                                                             | <code>encrypted} -instance`</code>                                                |

| Si desea mostrar información acerca de...                                           | Introduzca el comando...                                                                                 |
|-------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| La configuración de cifrado para un ID de sesión específico en una SVM especificada | <code>vserver cifs session show -vserver <i>vserver_name</i> -session-id <i>integer</i> -instance</code> |

## Ejemplos

El siguiente comando muestra información detallada de la sesión, incluida la configuración de cifrado, en una sesión SMB con un ID de sesión de 2:

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
Node: node1
Vserver: vs1
Session ID: 2
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation: 10.1.1.2
Authentication Mechanism: Kerberos
Windows User: DOMAIN\joe
UNIX User: pcuser
Open Shares: 1
Open Files: 1
Open Other: 0
Connected Time: 10m 43s
Idle Time: 1m 19s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: true
User Authenticated as: domain-user
NetBIOS Name: CIFS_ALIAS1
SMB Encryption Status: Unencrypted
```

## Supervise las estadísticas de cifrado SMB

Es posible supervisar las estadísticas de cifrado SMB y determinar qué sesiones establecidas y conexiones de uso compartido están cifradas y cuáles no lo están.

### Acerca de esta tarea

La `statistics` En el nivel de privilegio avanzado, proporciona los siguientes contadores, que puede utilizar para supervisar el número de sesiones de SMB cifradas y conexiones compartidas:

| Nombre del contador             | Descripciones                                      |
|---------------------------------|----------------------------------------------------|
| <code>encrypted_sessions</code> | Proporciona el número de sesiones cifradas SMB 3.0 |

| Nombre del contador                        | Descripciones                                                                                                                  |
|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <code>encrypted_share_connections</code>   | Proporciona el número de recursos compartidos cifrados en los que se ha producido una conexión de árbol                        |
| <code>rejected_unencrypted_sessions</code> | Da el número de configuraciones de sesión rechazadas debido a la falta de capacidad de cifrado del cliente                     |
| <code>rejected_unencrypted_shares</code>   | Proporciona el número de asignaciones de recursos compartidos rechazadas debido a la falta de capacidad de cifrado del cliente |

Estos contadores están disponibles con los siguientes objetos de estadísticas:

- `cifs` Permite supervisar el cifrado SMB para todas las sesiones SMB 3.0.

Las estadísticas de SMB 3.0 se incluyen en el resultado del `cifs` objeto. Si desea comparar el número de sesiones cifradas con el número total de sesiones, puede comparar la salida de `encrypted_sessions` contador con la salida para el `established_sessions` contador.

Si desea comparar el número de conexiones de recursos compartidos cifradas con el número total de conexiones de recursos compartidos, puede comparar la salida de `encrypted_share_connections` contador con la salida para el `connected_shares` contador.

- `rejected_unencrypted_sessions` Proporciona el número de veces que se ha intentado establecer una sesión SMB que requiere cifrado de un cliente que no admite cifrado SMB.
- `rejected_unencrypted_shares` Proporciona el número de veces que se intenta conectar con un recurso compartido de SMB que requiere cifrado de un cliente que no admite cifrado SMB.

Debe iniciar una colección de ejemplos de estadísticas para poder ver los datos resultantes. Puede ver los datos de la muestra si no detiene la recopilación de datos. Al detener la recopilación de datos, se proporciona una muestra fija. No detener la recopilación de datos le ofrece la posibilidad de obtener datos actualizados que puede utilizar para compararlos con consultas anteriores. La comparación puede ayudarle a identificar tendencias.

## Pasos

1. Establezca el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Iniciar una recopilación de datos:

```
statistics start -object {cifs|smb1|smb2} -instance instance -sample-id sample_ID [-node node_name]
```

Si no especifica el `-sample-id` Parámetro, el comando genera un identificador de muestra para usted y define esta muestra como la muestra predeterminada para la sesión CLI. Valor para `-sample-id` es una cadena de texto. Si ejecuta este comando durante la misma sesión CLI y no especifica el `-sample-id` parámetro, el comando sobrescribe la muestra predeterminada anterior.

Opcionalmente, puede especificar el nodo en el que se desea recoger estadísticas. Si no especifica el nodo, la muestra recopila estadísticas para todos los nodos del clúster.

3. Utilice la `statistics stop` comando para detener la recogida de datos de la muestra.

4. Ver estadísticas de cifrado SMB:

| Si desea ver información acerca de...                                                | Introduzca...                                                                          |
|--------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| Sesiones cifradas                                                                    | <code>`show -sample-id <i>sample_ID</i> -counter encrypted_sessions`</code>            |
| <code>node_name [-node <i>node_name</i>]</code>                                      | Sesiones cifradas y sesiones establecidas                                              |
| <code>`show -sample-id <i>sample_ID</i> -counter encrypted_sessions`</code>          | <code>established_sessions</code>                                                      |
| <code>node_name [-node <i>node_name</i>]</code>                                      | Conexiones de recursos compartidos cifradas                                            |
| <code>`show -sample-id <i>sample_ID</i> -counter encrypted_share_connections`</code> | <code>node_name [-node <i>node_name</i>]</code>                                        |
| Conexiones de recursos compartidos cifradas y recursos compartidos conectados        | <code>`show -sample-id <i>sample_ID</i> -counter encrypted_share_connections`</code>   |
| <code>connected_shares</code>                                                        | <code>node_name [-node <i>node_name</i>]</code>                                        |
| Sesiones no cifradas rechazadas                                                      | <code>`show -sample-id <i>sample_ID</i> -counter rejected_unencrypted_sessions`</code> |
| <code>node_name [-node <i>node_name</i>]</code>                                      | Se han rechazado conexiones compartidas sin cifrar                                     |
| <code>`show -sample-id <i>sample_ID</i> -counter rejected_unencrypted_share`</code>  | <code>node_name [-node <i>node_name</i>]</code>                                        |

Si desea mostrar información solo para un solo nodo, especifique la opción `-node` parámetro.

5. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

## Ejemplos

El ejemplo siguiente muestra cómo se pueden supervisar las estadísticas de cifrado de SMB 3.0 en vs1 de la máquina virtual de almacenamiento (SVM).

El siguiente comando cambia al nivel de privilegio avanzado:

```
cluster1::> set -privilege advanced
```

```
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
```

```
Do you want to continue? {y|n}: y
```

El siguiente comando inicia la recogida de datos de una nueva muestra:

```
cluster1::*> statistics start -object cifs -sample-id
smbencryption_sample -vserver vs1
Statistics collection is being started for Sample-id:
smbencryption_sample
```

El siguiente comando detiene la recogida de datos de esa muestra:

```
cluster1::*> statistics stop -sample-id smbencryption_sample
Statistics collection is being stopped for Sample-id:
smbencryption_sample
```

El siguiente comando muestra sesiones SMB cifradas y sesiones SMB establecidas por el nodo a partir de la muestra:

```
cluster2::*> statistics show -object cifs -counter
established_sessions|encrypted_sessions|node_name -node node_name
```

Object: cifs

Instance: [proto\_ctx:003]

Start-time: 4/12/2016 11:17:45

End-time: 4/12/2016 11:21:45

Scope: vsim2

| Counter              | Value |
|----------------------|-------|
| established_sessions | 1     |
| encrypted_sessions   | 1     |

2 entries were displayed

El siguiente comando muestra el número de sesiones SMB no cifradas rechazadas por el nodo a partir de la muestra:

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_sessions -node node_name
```

Object: cifs

Instance: [proto\_ctx:003]

Start-time: 4/12/2016 11:17:45

End-time: 4/12/2016 11:21:51

Scope: vsim2

| Counter                       | Value |
|-------------------------------|-------|
| rejected_unencrypted_sessions | 1     |

1 entry was displayed.

El siguiente comando muestra el número de recursos compartidos de SMB conectados y recursos compartidos de SMB cifrados mediante el nodo de la muestra:

```
clus-2::*> statistics show -object cifs -counter
connected_shares|encrypted_share_connections|node_name -node node_name
```

Object: cifs  
Instance: [proto\_ctx:003]  
Start-time: 4/12/2016 10:41:38  
End-time: 4/12/2016 10:41:43  
Scope: vsim2

| Counter                     | Value |
|-----------------------------|-------|
| connected_shares            | 2     |
| encrypted_share_connections | 1     |

2 entries were displayed.

El siguiente comando muestra el número de conexiones de recursos compartidos SMB no cifradas rechazadas por el nodo a partir de la muestra:

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_shares -node node_name
```

Object: cifs  
Instance: [proto\_ctx:003]  
Start-time: 4/12/2016 10:41:38  
End-time: 4/12/2016 10:42:06  
Scope: vsim2

| Counter                     | Value |
|-----------------------------|-------|
| rejected_unencrypted_shares | 1     |

1 entry was displayed.

## Información relacionada

[Determinar qué objetos de estadísticas y contadores están disponibles](#)

["Información general sobre la gestión y el control del rendimiento"](#)

**Comunicación segura de sesiones LDAP**

**Conceptos de firma y sellado LDAP**

A partir de ONTAP 9, puede configurar la firma y el sellado para habilitar la seguridad de la sesión LDAP en consultas a un servidor de Active Directory (AD). Debe configurar los

ajustes de seguridad del servidor CIFS en la máquina virtual de almacenamiento (SVM) para que se correspondan con los del servidor LDAP.

La firma comprueba la integridad de la carga de datos LDAP mediante una tecnología de clave secreta. El sellado cifra la carga de datos LDAP para impedir la transmisión de información confidencial en texto sin cifrar. Una opción *LDAP Security Level* indica si es necesario firmar, firmar y sellar el tráfico LDAP o no. El valor predeterminado es `none`.

La firma y el sellado LDAP en el tráfico CIFS están habilitados en la SVM con el `-session-security-for-ad-ldap` de la `vserver cifs security modify` comando.

## Habilite la firma y el sellado LDAP en el servidor CIFS

Antes de que el servidor CIFS pueda utilizar la firma y el sellado para establecer una comunicación segura con un servidor LDAP de Active Directory, debe modificar la configuración de seguridad del servidor CIFS para habilitar la firma y el sellado LDAP.

### Antes de empezar

Debe consultar al administrador del servidor AD para determinar los valores de configuración de seguridad adecuados.

### Pasos

1. Configure la configuración de seguridad del servidor CIFS que permita el tráfico firmado y sellado con los servidores LDAP de Active Directory: `vserver cifs security modify -vserver vserver_name -session-security-for-ad-ldap {none|sign|seal}`

Puede habilitar la firma (`sign`, integridad de los datos), firma y sellado (`seal`, integridad y cifrado de los datos), o ninguno de los dos `none`, sin firma ni sellado). El valor predeterminado es `none`.

2. Compruebe que la configuración de seguridad de firma y sellado LDAP está configurada correctamente: `vserver cifs security show -vserver vserver_name`



Si la SVM utiliza el mismo servidor LDAP para consultar la asignación de nombres u otra información de UNIX, como usuarios, grupos y netgroups, debe habilitar el valor correspondiente con el `-session-security` opción de `vserver services name-service ldap client modify` comando.

## Configure LDAP sobre TLS

### Exporte una copia del certificado de CA raíz autofirmado

Para utilizar LDAP sobre SSL/TLS para proteger la comunicación de Active Directory, primero debe exportar una copia del certificado raíz autofirmado del Servicio de certificados de Active Directory a un archivo de certificado y convertirlo en un archivo de texto ASCII. ONTAP utiliza este archivo de texto para instalar el certificado en la máquina virtual de almacenamiento (SVM).

### Antes de empezar

El servicio de certificados de Active Directory ya debe estar instalado y configurado para el dominio al que pertenece el servidor CIFS. Puede encontrar información acerca de la instalación y configuración de Active



Director Certificate Services consultando la biblioteca de Microsoft TechNet.

"Biblioteca de Microsoft TechNet: [technet.microsoft.com](http://technet.microsoft.com)"

## Paso

1. Obtenga un certificado de CA raíz del controlador de dominio que se encuentra en .pem formato de texto.

"Biblioteca de Microsoft TechNet: [technet.microsoft.com](http://technet.microsoft.com)"

## Después de terminar

Instale el certificado en la SVM.

## Información relacionada

"Biblioteca de Microsoft TechNet"

## Instale el certificado de CA raíz autofirmado en la SVM

Si se requiere la autenticación LDAP con TLS al enlazar con servidores LDAP, primero debe instalar el certificado de CA raíz autofirmado en la SVM.

## Acerca de esta tarea

Cuando LDAP over TLS está habilitado, el cliente LDAP de ONTAP en la SVM no admite certificados revocados en ONTAP 9.0 y 9.1.

A partir de ONTAP 9.2, todas las aplicaciones de ONTAP que utilizan comunicaciones TLS pueden comprobar el estado de certificado digital mediante el protocolo de estado de certificado en línea (OCSP). Si OCSP está habilitado para LDAP over TLS, se rechazan los certificados revocados y la conexión falla.

## Pasos

1. Instale el certificado de CA raíz autofirmado:

- a. Comience la instalación del certificado: `security certificate install -vserver vserver_name -type server-ca`

El resultado de la consola muestra el siguiente mensaje: Please enter Certificate: Press <Enter> when done

- b. Abra el certificado .pem archivo con un editor de texto, copie el certificado, incluidas las líneas que empiezan por -----BEGIN CERTIFICATE----- y terminar con `-----END CERTIFICATE-----`, a continuación, pegue el certificado después del símbolo del sistema.
- c. Compruebe que el certificado se muestra correctamente.
- d. Para completar la instalación, pulse Intro.

2. Compruebe que el certificado esté instalado: `security certificate show -vserver vserver_name`

## Habilite LDAP sobre TLS en el servidor

Antes de que el servidor SMB pueda utilizar TLS para obtener comunicación segura con un servidor LDAP de Active Directory, debe modificar la configuración de seguridad del servidor SMB para habilitar LDAP over TLS.

A partir de ONTAP 9.10.1, el enlace de canal LDAP se admite de forma predeterminada tanto para las conexiones LDAP de Active Directory (AD) como de los servicios de nombres. ONTAP intentará establecer la vinculación de canal con las conexiones LDAP solo si Start-TLS o LDAPS está habilitado junto con la seguridad de la sesión establecida en Sign o Seal. Para deshabilitar o volver a habilitar el enlace de canal LDAP con servidores AD, utilice `-try-channel-binding-for-ad-ldap` con el `vserver cifs security modify` comando.

Para obtener más información, consulte:

- ["Descripción general de LDAP"](#)
- ["2020 requisitos de enlace de canal LDAP y firma LDAP para Windows"](#).

## Pasos

1. Configure la opción de seguridad del servidor SMB que permite una comunicación LDAP segura con servidores LDAP de Active Directory: `vserver cifs security modify -vserver vserver_name -use-start-tls-for-ad-ldap true`
2. Compruebe que la configuración de seguridad de LDAP over TLS está establecida en `true`: `vserver cifs security show -vserver vserver_name`



Si la SVM utiliza el mismo servidor LDAP para consultar la asignación de nombres u otra información de UNIX (como usuarios, grupos y grupos de red), también debe modificar el `-use-start-tls` mediante el `vserver services name-service ldap client modify` comando.

## Configure multicanal de SMB para un mayor rendimiento y redundancia

A partir de ONTAP 9.4, puede configurar SMB MultiChannel para proporcionar varias conexiones entre ONTAP y clientes en una sola sesión SMB. Al hacerlo, se mejora el rendimiento y la tolerancia a fallos.

### Antes de empezar

Solo se puede utilizar la funcionalidad multicanal de SMB cuando los clientes negocian en SMB 3.0 o versiones posteriores. De forma predeterminada, SMB 3.0 y las versiones posteriores se encuentran habilitadas en el servidor SMB de ONTAP.

### Acerca de esta tarea

Los clientes de SMB detectan y utilizan automáticamente varias conexiones de red si se identifica una configuración adecuada en el clúster de ONTAP.

El número de conexiones simultáneas en una sesión SMB depende de las NIC que haya implementado:

- **1G NIC en el cluster ONTAP y cliente**

El cliente establece una conexión por NIC y enlaza la sesión a todas las conexiones.

- **NIC 10G y mayor capacidad en cluster ONTAP y cliente**

El cliente establece hasta cuatro conexiones por NIC y enlaza la sesión a todas las conexiones. El cliente puede establecer conexiones en varias NIC de 10 G y de mayor capacidad.

También puede modificar los siguientes parámetros (privilegios avanzados):

- **-max-connections-per-session**

El número máximo de conexiones permitidas por sesión multicanal. El valor predeterminado es 32 conexiones.

Si desea habilitar más conexiones que las predeterminadas, debe realizar ajustes comparables a la configuración del cliente, que también tiene un valor predeterminado de 32 conexiones.

- **-max-lifs-per-session**

Número máximo de interfaces de red anunciadas por sesión multicanal. El valor predeterminado es 256 interfaces de red.

## Pasos

1. Configure el nivel de privilegio en Advanced: `set -privilege advanced`
2. Habilite multicanal de SMB en el servidor SMB: `vserver cifs options modify -vserver vserver_name -is-multichannel-enabled true`
3. Compruebe que ONTAP informa de sesiones multicanal de SMB: `vserver cifs session show options`
4. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

## Ejemplo

En el siguiente ejemplo, se muestra información sobre todas las sesiones SMB, donde se muestran varias conexiones para una sola sesión:

```
cluster1::> vserver cifs session show
Node: node1
Vserver: vs1
Connection Session Open
Idle
IDs ID Workstation Windows User Files
Time

138683,
138684,
138685 1 10.1.1.1 DOMAIN\
4s Administrator 0
```

En el siguiente ejemplo, se muestra información detallada sobre una sesión SMB con el ID de sesión 1:

```
cluster1::> vserver cifs session show -session-id 1 -instance
```

```
Vserver: vs1
```

```
 Node: node1
 Session ID: 1
 Connection IDs: 138683,138684,138685
 Connection Count: 3
Incoming Data LIF IP Address: 192.1.1.1
 Workstation IP Address: 10.1.1.1
 Authentication Mechanism: NTLMv1
 User Authenticated as: domain-user
 Windows User: DOMAIN\administrator
 UNIX User: root
 Open Shares: 2
 Open Files: 5
 Open Other: 0
 Connected Time: 5s
 Idle Time: 5s
 Protocol Version: SMB3
 Continuously Available: No
 Is Session Signed: false
 NetBIOS Name: -
```

## Configurar los mapas de usuario UNIX predeterminados de usuario de Windows en el servidor SMB

### Configure el usuario UNIX predeterminado

Puede configurar el usuario UNIX predeterminado para que lo utilice si fallan todos los demás intentos de asignación para un usuario o si no desea asignar usuarios individuales entre UNIX y Windows. De manera alternativa, si desea que la autenticación de usuarios no asignados falle, no debe configurar el usuario UNIX predeterminado.

### Acerca de esta tarea

De forma predeterminada, el nombre del usuario UNIX predeterminado es "pcuser", lo que significa que, de forma predeterminada, se activa la asignación de usuarios al usuario UNIX predeterminado. Puede especificar otro nombre que se utilizará como usuario UNIX predeterminado. El nombre que especifique debe existir en las bases de datos del servicio de nombres configuradas para la máquina virtual de almacenamiento (SVM). Si esta opción está establecida en una cadena nula, nadie puede acceder al servidor CIFS como usuario predeterminado de UNIX. Es decir, cada usuario debe tener una cuenta en la base de datos de contraseñas para poder acceder al servidor CIFS.

Para que un usuario pueda conectarse al servidor CIFS con la cuenta de usuario UNIX predeterminada, el usuario debe cumplir los siguientes requisitos previos:

- El usuario se autentica.
- El usuario se encuentra en la base de datos de usuarios Windows local del servidor CIFS, en el dominio principal del servidor CIFS o en un dominio de confianza (si las búsquedas de asignación de nombres

multidominio están activadas en el servidor CIFS).

- El nombre de usuario no se asigna explícitamente a una cadena nula.

## Pasos

1. Configure el usuario UNIX predeterminado:

| Si desea ...                                                    | Introduzca ...                                                         |
|-----------------------------------------------------------------|------------------------------------------------------------------------|
| Utilizar el usuario UNIX predeterminado "pcuser"                | <code>vserver cifs options modify -default -unix-user pcuser</code>    |
| Utilice otra cuenta de usuario UNIX como usuario predeterminado | <code>vserver cifs options modify -default -unix-user user_name</code> |
| Desactive el usuario UNIX predeterminado                        | <code>vserver cifs options modify -default -unix-user ""</code>        |

```
vserver cifs options modify -default-unix-user pcuser
```

2. Compruebe que el usuario UNIX predeterminado está configurado correctamente: `vserver cifs options show -vserver vserver_name`

En el siguiente ejemplo, tanto el usuario UNIX predeterminado como el usuario UNIX invitado en SVM vs1 están configurados para utilizar el usuario UNIX "pcuser":

```
vserver cifs options show -vserver vs1
```

```
Vserver: vs1
```

```
Client Session Timeout : 900
Default Unix Group : -
Default Unix User : pcuser
Guest Unix User : pcuser
Read Grants Exec : disabled
Read Only Delete : disabled
WINS Servers : -
```

## Configure el usuario UNIX invitado

Configurar la opción de usuario UNIX invitado significa que los usuarios que inician sesión desde dominios que no son de confianza se asignan al usuario UNIX invitado y pueden conectarse al servidor CIFS. Como alternativa, si desea que la autenticación de usuarios de dominios que no son de confianza falle, no debe configurar el usuario UNIX invitado. El valor predeterminado es no permitir que los usuarios de dominios que no son de confianza se conecten al servidor CIFS (la cuenta UNIX invitada no está configurada).

**Acerca de esta tarea**

Debe tener en cuenta lo siguiente al configurar la cuenta de UNIX de invitado:

- Si el servidor CIFS no puede autenticar al usuario en un controlador de dominio para el dominio principal, un dominio de confianza o la base de datos local y esta opción está habilitada, el servidor CIFS considera al usuario como un usuario invitado y lo asigna al usuario UNIX especificado.
- Si esta opción se establece en una cadena nula, el usuario UNIX invitado estará deshabilitado.
- Debe crear un usuario UNIX para usarlo como usuario UNIX invitado en una de las bases de datos del servicio de nombres de máquina virtual de almacenamiento (SVM).
- Un usuario que inició sesión como usuario invitado es automáticamente miembro del grupo BUILTIN\guest en el servidor CIFS.
- La opción 'homedirs-public' se aplica sólo a los usuarios autenticados. Un usuario que ha iniciado sesión como usuario invitado no tiene un directorio principal y no puede acceder a los directorios principales de otros usuarios.

**Pasos**

1. Ejecute una de las siguientes acciones:

| Si desea...                          | Introduzca...                                                               |
|--------------------------------------|-----------------------------------------------------------------------------|
| Configure el usuario UNIX invitado   | <code>vserver cifs options modify -guest -unix-user <i>unix_name</i></code> |
| Deshabilite el usuario UNIX invitado | <code>vserver cifs options modify -guest -unix-user ""</code>               |

```
vserver cifs options modify -guest-unix-user pcuser
```

2. Verifique que el usuario UNIX invitado esté configurado correctamente: `vserver cifs options show -vserver vserver_name`

En el siguiente ejemplo, tanto el usuario UNIX predeterminado como el usuario UNIX invitado en SVM vs1 están configurados para utilizar el usuario UNIX "pcuser":

```
vserver cifs options show -vserver vs1
```

```
Vserver: vs1

Client Session Timeout : 900
Default Unix Group : -
Default Unix User : pcuser
Guest Unix User : pcuser
Read Grants Exec : disabled
Read Only Delete : disabled
WINS Servers : -
```

**Asigne el grupo de administradores a raíz**

Si solo tiene clientes CIFS en su entorno y su máquina virtual de almacenamiento (SVM) está configurada como un sistema de almacenamiento multiprotocolo, debe tener al menos una cuenta de Windows con privilegios raíz para acceder a los archivos en la SVM; De lo contrario, no puede gestionar la SVM porque no tiene suficientes derechos de usuario.

**Acerca de esta tarea**

Si el sistema de almacenamiento se configuró como sólo NTFS, no obstante, el /etc el directorio tiene una ACL a nivel de archivo que permite que el grupo de administradores acceda a los archivos de configuración de ONTAP.

**Pasos**

- 1. Configure el nivel de privilegio en Advanced: `set -privilege advanced`
- 2. Configure la opción del servidor CIFS que asigna el grupo de administradores a la raíz, según corresponda:

| Si desea...                                                                    | Realice lo siguiente...                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Asigne los miembros del grupo de administradores a la raíz                     | <code>vserver cifs options modify -vserver vserver_name -is-admin-users-mapped-to -root-enabled true</code> Todas las cuentas del grupo de administradores se consideran root, aunque no tenga /etc/usermap.cfg introduzca la asignación de las cuentas a root. Si crea un archivo utilizando una cuenta que pertenece al grupo de administradores, el archivo es propiedad de root cuando ve el archivo desde un cliente UNIX. |
| Desactive la asignación de los miembros del grupo de administradores a la raíz | <code>vserver cifs options modify -vserver vserver_name -is-admin-users-mapped-to -root-enabled false</code> Las cuentas del grupo de administradores ya no se asignan a la raíz. Sólo se puede asignar explícitamente un solo usuario a la raíz.                                                                                                                                                                               |

- 3. Compruebe que la opción está establecida en el valor deseado: `vserver cifs options show -vserver vserver_name`
- 4. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

**Muestra información sobre los tipos de usuarios que están conectados a través de sesiones SMB**

Puede ver información acerca del tipo de usuarios que están conectados en sesiones SMB. Esto puede ayudarle a asegurarse de que solo el tipo adecuado de usuario se conecte a través de sesiones SMB en la máquina virtual de almacenamiento (SVM).

**Acerca de esta tarea**

Los siguientes tipos de usuarios pueden conectarse a través de sesiones SMB:

- local-user

Se autentica como usuario CIFS local

- domain-user

Autenticado como usuario de dominio (ya sea desde el dominio principal del servidor CIFS o desde un dominio de confianza)

- guest-user

Autenticado como usuario invitado

- anonymous-user

Autenticado como usuario anónimo o nulo

Pasos

1. Determinar qué tipo de usuario está conectado en una sesión SMB: `vserver cifs session show -vserver vserver_name -windows-user windows_user_name -fields windows-user,address,lif-address,user-type`

| Si desea mostrar información sobre tipos de usuario para las sesiones establecidas... | Introduzca el siguiente comando...                                                   |
|---------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| Para todas las sesiones con un tipo de usuario especificado                           | <code>`vserver cifs session show -vserver vserver_name -user-type {local-user</code> |
| domain-user                                                                           | guest-user                                                                           |
| anonymous-user}`                                                                      | Para un usuario específico                                                           |

Ejemplos

El siguiente comando muestra información de sesión sobre el tipo de usuario para las sesiones en SVM vs1 establecidas por el usuario " iepubs\user1":

```
cluster1::> vserver cifs session show -vserver publ -windows-user
iepubs\user1 -fields windows-user,address,lif-address,user-type
node vserver session-id connection-id lif-address address
windows-user user-type

publnode1 publ 1 3439441860 10.0.0.1 10.1.1.1
IEPUBS\user1 domain-user
```

Opciones de comando para limitar el consumo excesivo de recursos de cliente de Windows

Opciones para `vserver cifs options modify` Comando le permite controlar el



consumo de recursos para clientes Windows. Esto puede ser útil si algún cliente está fuera de los límites normales del consumo de recursos, por ejemplo, si hay un número inusualmente alto de archivos abiertos, sesiones abiertas o peticiones de notificación de cambio.

Las siguientes opciones para `vserver cifs options modify` Se ha agregado el comando para controlar el consumo de recursos del cliente de Windows. Si se supera el valor máximo de cualquiera de estas opciones, se deniega la solicitud y se envía un mensaje EMS. También se envía un mensaje de advertencia EMS cuando se alcanza el 80 % del límite configurado para estas opciones.

- `-max-opens-same-file-per-tree`

Número máximo de apertura en el mismo archivo por árbol CIFS

- `-max-same-user-sessions-per-connection`

Número máximo de sesiones abiertas por el mismo usuario por conexión

- `-max-same-tree-connect-per-session`

Número máximo de conexiones de árbol en el mismo recurso compartido por sesión

- `-max-watches-set-per-tree`

Número máximo de relojes (también conocido como *change notifications*) establecido por árbol

Consulte las páginas de manual para ver los límites predeterminados y para mostrar la configuración actual.

A partir de ONTAP 9.4, los servidores que ejecutan SMB versión 2 o posterior pueden limitar el número de solicitudes pendientes (*créditos SMB*) que el cliente puede enviar al servidor en una conexión SMB. La gestión de créditos SMB es iniciada por el cliente y controlada por el servidor.

El número máximo de solicitudes pendientes que se pueden conceder en una conexión SMB está controlado por la `-max-credits` opción. El valor predeterminado de esta opción es 128.

## **Mejore el rendimiento del cliente con los bloqueos oportunistas tradicionales y de arrendamiento**

### **Mejore el rendimiento del cliente con la información general sobre los bloqueos oportunistas tradicionales y de arrendamiento**

Los bloqueos oportunistas tradicionales (bloqueos oportunistas oportunistas oportunistas) y los bloqueos oportunistas de arrendamiento habilitan un cliente SMB en determinados escenarios de uso compartido de archivos para realizar el almacenamiento en caché en el lado del cliente de información de lectura anticipada, escritura subyacente y bloqueo. A continuación, un cliente puede leer o escribir en un archivo sin recordar periódicamente al servidor que necesita acceso al archivo en cuestión. Esto mejora el rendimiento al reducir el tráfico de red.

Los bloqueos oportunistas del arrendamiento son una forma mejorada de bloqueos oportunistas disponibles con el protocolo SMB 2.1 y versiones posteriores. Los bloqueos oportunistas de arrendamiento permiten a un cliente obtener y conservar el estado de almacenamiento en caché del cliente en múltiples abiertos de SMB originados por sí mismo.

Los bloqueos oportunistas pueden controlarse de dos formas:

- Mediante una propiedad de recurso compartido, mediante `vserver cifs share create` cuando se crea el recurso compartido, o el `vserver share properties` comando después de su creación.
- Mediante una propiedad Qtree, se usa la `volume qtree create` cuando se crea el qtree o la `volume qtree oplock` después de crear.

#### **Consideraciones de pérdida de datos de la caché de escritura cuando se usan bloqueos oportunistas**

En determinadas circunstancias, si un proceso tiene un oplock exclusivo en un archivo y un segundo proceso intenta abrir el archivo, el primer proceso debe invalidar los datos almacenados en caché y vaciar las escrituras y los bloqueos. A continuación, el cliente debe renunciar al oplock y acceder al archivo. Si hay un fallo de red durante este vaciado, se pueden perder los datos de escritura en caché.

- Posibilidades de pérdida de datos

Cualquier aplicación que tenga datos en la caché de la escritura puede perder esos datos en el siguiente conjunto de circunstancias:

- La conexión se realiza mediante SMB 1.0.
  - Tiene un oplock exclusivo en el archivo.
  - Se le indica que rompa ese oplock o cierre el archivo.
  - Durante el proceso de vaciado de la caché de escritura, la red o el sistema de destino genera un error.
- Gestión de errores y finalización de escritura

La caché en sí no tiene ningún control de errores: Las aplicaciones sí. Cuando la aplicación realiza una escritura en la caché, siempre se completa la escritura. Si la caché, a su vez, realiza una escritura en el sistema de destino a través de una red, debe asumir que la escritura se completa porque, si no lo hace, los datos se pierden.

#### **Habilite o deshabilite los bloqueos oportunistas al crear recursos compartidos de SMB**

Los bloqueos oportunistas permiten a los clientes bloquear archivos y contenido de la caché localmente, lo que puede aumentar el rendimiento de las operaciones de archivos. Los bloqueos oportunistas están habilitados en los recursos compartidos de SMB que residen en máquinas virtuales de almacenamiento (SVM). En algunas circunstancias, es posible que desee deshabilitar los bloqueos oportunistas. Puede habilitar o deshabilitar los bloqueos oportunistas de acuerdo con el recurso compartido por recurso compartido.

#### **Acerca de esta tarea**

Si los bloqueos oportunistas están habilitados en el volumen que contiene un recurso compartido pero la propiedad de recurso compartido de oplock para ese recurso compartido está deshabilitada, los bloqueos oportunistas se deshabilitan para ese recurso compartido. La deshabilitación de los bloqueos oportunistas en un recurso compartido tiene prioridad sobre la configuración de oplock de volumen. Al deshabilitar los bloqueos oportunistas del recurso compartido, se deshabilitan los bloqueos oportunistas oportunistas de arrendamiento y oportunistas.

Puede especificar otras propiedades de recursos compartidos además de especificar la propiedad de recursos

compartidos de oplock mediante una lista delimitada por comas. También puede especificar otros parámetros de recursos compartidos.

**Pasos**

- 1. Realice la acción correspondiente:

| Si desea...                                                                                              | Realice lo siguiente...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Habilite los bloqueos oportunistas del recurso compartido durante la creación de recursos compartidos    | <div>Introduzca el siguiente comando: <code>vserver cifs share create -vserver _vserver_name_ -share-name share_name -path path_to_share -share-properties [oplocks,...]</code></div> <div><div>Si desea que el recurso compartido tenga solo las propiedades de recurso compartido predeterminadas, que son <code>oplocks</code>, <code>browsable</code>, y <code>changenotify</code> habilitada, no tiene que especificar el <code>-share-properties</code> Parámetro al crear un recurso compartido de SMB. Si desea una combinación de propiedades de recurso compartido que no sea la predeterminada, debe especificar el <code>-share-properties</code> parámetro con la lista de propiedades de recurso compartido que se van a utilizar para ese recurso compartido.</div></div> |
| Deshabilite los bloqueos oportunistas del recurso compartido durante la creación de recursos compartidos | <div>Introduzca el siguiente comando: <code>vserver cifs share create -vserver _vserver_name_ -share-name _share_name_ -path _path_to_share_ -share-properties [other_share_property,...]</code></div> <div><div>Al deshabilitar los bloqueos oportunistas, debe especificar una lista de propiedades de recursos compartidos al crear el recurso compartido, pero no debe especificar el <code>oplocks</code> propiedad.</div></div>                                                                                                                                                                                                                                                                                                                                                  |

**Información relacionada**

[Habilitar o deshabilitar los bloqueos oportunistas en los recursos compartidos de SMB existentes](#)

[Control del estado del plock](#)

Los bloqueos oportunistas permiten a los clientes bloquear archivos y contenido de la caché localmente, lo que puede aumentar el rendimiento de las operaciones de archivos. Debe conocer los comandos para habilitar o deshabilitar los bloqueos oportunistas en volúmenes o qtrees. También debe saber cuándo puede habilitar o deshabilitar los bloqueos oportunistas de los volúmenes y qtrees.

- Los bloqueos oportunistas están habilitados en los volúmenes de forma predeterminada.
  - No se pueden deshabilitar los bloqueos oportunistas cuando crea un volumen.
  - Puede habilitar o deshabilitar los bloqueos oportunistas de los volúmenes existentes de las SVM en cualquier momento.
  - Puede habilitar los bloqueos oportunistas en qtrees para SVM.
- La configuración del modo oplock es una propiedad del ID de qtree 0, el qtree predeterminado que tienen todos los volúmenes. Si no se especifica una configuración de oplock al crear un qtree, el qtree hereda la configuración oplock del volumen principal, que se habilita de forma predeterminada. Sin embargo, si se especifica una configuración de oplock en el nuevo qtree, tendrá prioridad sobre la configuración de oplock en el volumen.

| Si desea...                                                 | Se usa este comando...                                                                                           |
|-------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Habilite los bloqueos oportunistas en volúmenes o qtrees    | <code>volume qtree oplocks</code> con la <code>-oplock-mode</code> parámetro establecido en <code>enable</code>  |
| Deshabilite los bloqueos oportunistas en volúmenes o qtrees | <code>volume qtree oplocks</code> con la <code>-oplock-mode</code> parámetro establecido en <code>disable</code> |

Información relacionada

[Control del estado del plock](#)

Habilite o deshabilite los bloqueos oportunistas en los recursos compartidos de SMB existentes



Los bloqueos oportunistas están habilitados en recursos compartidos de SMB en máquinas virtuales de almacenamiento (SVM) de forma predeterminada. En algunas circunstancias, puede que desee deshabilitar los bloqueos oportunistas; de forma alternativa, si ha deshabilitado los bloqueos oportunistas en un recurso compartido anteriormente, puede que desee volver a habilitar los bloqueos oportunistas.

Acerca de esta tarea

Si los bloqueos oportunistas están habilitados en el volumen que contiene un recurso compartido, pero la propiedad de recurso compartido oplock de ese recurso compartido está deshabilitada, los bloqueos oportunistas se deshabilitan para ese recurso compartido. La deshabilitación de los bloqueos oportunistas en un recurso compartido tiene prioridad sobre el hecho de habilitar los bloqueos oportunistas en el volumen. Al deshabilitar los bloqueos oportunistas del recurso compartido, se deshabilitan los bloqueos oportunistas oportunistas de arrendamiento y oportunistas. Puede habilitar o deshabilitar los bloqueos oportunistas de los recursos compartidos existentes en cualquier momento.

Paso

1. Realice la acción correspondiente:

| Si desea...                                                                                                | Realice lo siguiente...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Habilite los bloqueos oportunistas del recurso compartido modificando un recurso compartido existente      | <p>Introduzca el siguiente comando: <code>vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties oplocks</code></p> <div><p>Puede especificar propiedades de recursos compartidos adicionales que desea agregar mediante una lista delimitada por comas.</p></div> <p>Las propiedades recién agregadas se agregan a la lista existente de propiedades de recursos compartidos. Todas las propiedades de recurso compartido que haya especificado anteriormente permanecen vigentes.</p>                                           |
| Deshabilite los bloqueos oportunistas de un recurso compartido modificando un recurso compartido existente | <p>Introduzca el siguiente comando: <code>vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties oplocks</code></p> <div><p>Puede especificar propiedades de recursos compartidos adicionales que desea quitar mediante una lista delimitada por comas.</p></div> <p>Las propiedades de recursos compartidos que se quitan se eliminan de la lista existente de propiedades de recursos compartidos; sin embargo, las propiedades de recursos compartidos configuradas previamente que no se quitan permanecen vigentes.</p> |

### Ejemplos

El siguiente comando habilita los bloqueos oportunistas del recurso compartido denominado «'Engineering» en la máquina virtual de almacenamiento (SVM, antes conocida como Vserver) vs1:

```
cluster1::> vsriver cifs share properties add -vsriver vs1 -share-name Engineering -share-properties oplocks
```

```
cluster1::> vsriver cifs share properties show
```

| Vsriver | Share       | Properties                                           |
|---------|-------------|------------------------------------------------------|
| vs1     | Engineering | oplocks<br>browsable<br>changenotify<br>showsnapshot |

El siguiente comando deshabilita los bloqueos oportunistas del recurso compartido denominado "Engineering" en SVM vs1:

```
cluster1::> vsriver cifs share properties remove -vsriver vs1 -share-name Engineering -share-properties oplocks
```

```
cluster1::> vsriver cifs share properties show
```

| Vsriver | Share       | Properties                                |
|---------|-------------|-------------------------------------------|
| vs1     | Engineering | browsable<br>changenotify<br>showsnapshot |

## Información relacionada

[Habilitar o deshabilitar los bloqueos oportunistas al crear recursos compartidos de SMB](#)

[Control del estado del plock](#)

[Agregar o quitar propiedades de recursos compartidos en un recurso compartido SMB existente](#)

## Controlar el estado del plock

Puede supervisar y mostrar información sobre el estado de los plock. Puede usar esta información para determinar qué archivos tienen bloqueos oportunistas, cuál son el nivel de plock y el nivel de estado de plock y si se utiliza el leasing de plock. También puede determinar la información acerca de los bloqueos que podría necesitar interrumpir manualmente.

## Acerca de esta tarea

Puede mostrar información acerca de todos los bloqueos oportunistas en un formulario de resumen o en un formulario de lista detallado. También puede utilizar parámetros opcionales para mostrar información sobre un subconjunto más pequeño de bloqueos existentes. Por ejemplo, puede especificar que la salida devuelva solo los bloqueos con la dirección IP del cliente especificada o con la ruta especificada.

Puede mostrar la siguiente información acerca de los bloqueos oportunistas tradicionales y de arrendamiento:

- SVM, nodo, volumen y LIF en los que se establece el oplock
- Bloquear UUID
- Dirección IP del cliente con el oplock
- Ruta en la que se establece el oplock
- Protocolo de bloqueo (SMB) y tipo (oplock)
- Estado de bloqueo
- Nivel de plock
- Estado de la conexión y tiempo de caducidad del bloque de mensajes del servidor
- Abra el código de grupo si se concede un seguro de arrendamiento

Consulte `vserver oplocks show` manual para obtener una descripción detallada de cada parámetro.

## Pasos

1. Mostrar el estado de plock mediante el `vserver locks show` comando.

## Ejemplos

El siguiente comando muestra información predeterminada sobre todos los bloqueos. El oplock del archivo mostrado se concede con un `read-batch` nivel de plock:

```
cluster1::> vserver locks show
```

Vserver: vs0

| Volume | Object Path                            | LIF         | Protocol | Lock Type   | Client      |
|--------|----------------------------------------|-------------|----------|-------------|-------------|
| vol1   | /vol1/notes.txt                        | node1_data1 |          |             |             |
|        |                                        |             | cifs     | share-level | 192.168.1.5 |
|        | Sharelock Mode: read_write-deny_delete |             |          |             |             |
|        |                                        |             |          | op-lock     | 192.168.1.5 |
|        | Oplock Level: read-batch               |             |          |             |             |

En el ejemplo siguiente se muestra información más detallada sobre el bloqueo de un archivo con la ruta `/data2/data2_2/intro.pptx`. Un `lease oplock` se concede en el archivo con un `batch` Oplock nivel a un cliente con una dirección IP de `10.3.1.3`:



Al mostrar información detallada, el comando proporciona una salida independiente para la información de plock y sharelock. En este ejemplo sólo se muestra la salida de la sección de plock.

```
cluster1::> vserver lock show -instance -path /data2/data2_2/intro.pptx
```

```

 Vserver: vs1
 Volume: data2_2
Logical Interface: lif2
 Object Path: /data2/data2_2/intro.pptx
 Lock UUID: ff1cbf29-bfef-4d91-ae06-062bf69212c3
 Lock Protocol: cifs
 Lock Type: op-lock
Node Holding Lock State: node3
 Lock State: granted
Bytelock Starting Offset: -
 Number of Bytes Locked: -
 Bytelock is Mandatory: -
 Bytelock is Exclusive: -
 Bytelock is Superlock: -
 Bytelock is Soft: -
 Oplock Level: batch
Shared Lock Access Mode: -
 Shared Lock is Soft: -
 Delegation Type: -
 Client Address: 10.3.1.3
 SMB Open Type: -
 SMB Connect State: connected
SMB Expiration Time (Secs): -
 SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

## Información relacionada

[Habilitar o deshabilitar los bloqueos oportunistas al crear recursos compartidos de SMB](#)

[Habilitar o deshabilitar los bloqueos oportunistas en los recursos compartidos de SMB existentes](#)

[Comandos para habilitar o deshabilitar los bloqueos oportunistas en volúmenes y qtrees](#)

## Aplicar objetos de directiva de grupo a servidores SMB

### Aplicar objetos de directiva de grupo a la información general de los servidores SMB

El servidor SMB admite objetos de directiva de grupo (GPO), un conjunto de reglas conocidas como atributos de directiva de grupo\_ que se aplican a equipos de un entorno de Active Directory. Puede utilizar los GPO para gestionar de forma centralizada la configuración de todas las máquinas virtuales de almacenamiento (SVM) del clúster que pertenece al mismo dominio de Active Directory.

Cuando se habilitan los GPO en el servidor SMB, ONTAP envía consultas LDAP al servidor de Active Directory que solicita información de GPO. Si hay definiciones de GPO aplicables al servidor SMB, el servidor



Active Directory devuelve la siguiente información de GPO:

- Nombre de GPO
- Versión de GPO actual
- Ubicación de la definición de GPO
- Listas de UUID (identificadores universales únicos) para conjuntos de directivas de GPO

### Información relacionada

[Protección del acceso a los archivos mediante el control de acceso dinámico \(DAC\)](#)

["Seguimiento de seguridad y auditoría de SMB y NFS"](#)

### Objetos de normativa de grupo compatibles

Aunque no todos los objetos de políticas de grupo (GPO) se aplican a las máquinas virtuales de almacenamiento (SVM) habilitadas para CIFS, las SVM pueden reconocer y procesar el conjunto de objetos de normativa de grupo correspondiente.

Actualmente, los siguientes GPO son compatibles con las SVM:

- Ajustes de configuración de directivas de auditoría avanzadas:

Acceso a objetos: Escalonamiento de la directiva de acceso central

Especifica el tipo de eventos que se auditarán para la configuración provisional de la directiva de acceso central (CAP), incluida la siguiente configuración:

- No auditar
- Auditar solo los eventos de éxito
- Auditar solo los eventos de fallo
- Auditar eventos de éxito y fallo



Si se establece cualquiera de las tres opciones de auditoría (sólo eventos de éxito de auditoría, auditar sólo eventos de fallo, auditar eventos de éxito y de fallo), ONTAP audita tanto eventos de éxito como de fallo.

Establecer mediante la `Audit Central Access Policy Staging` ajuste en la `Advanced Audit Policy Configuration/Audit Policies/Object Access GPO`.



Para utilizar las opciones de GPO de configuración de directivas de auditoría avanzadas, la auditoría debe configurarse en la SVM habilitada para CIFS a la que desee aplicar estas opciones. Si la auditoría no está configurada en la SVM, la configuración de GPO no se aplicará y se descarta.

- Configuración del registro:
  - Intervalo de actualización de la directiva de grupo para la SVM habilitada para CIFS

Establecer mediante la `Registry GPO`.

- Actualización aleatoria de directivas de grupo

Establecer mediante la Registry GPO.

- Publicación de hash para BranchCache

El GPO Hash Publication para BranchCache corresponde al modo operativo de BranchCache. Se admiten los tres modos de funcionamiento compatibles siguientes:

- Por recurso compartido
  - Todos los recursos compartidos
  - Deshabilitado
- Establecer mediante la Registry GPO.

- Compatibilidad de la versión de hash para BranchCache

Se admiten las tres configuraciones de la siguiente versión de hash:

- BranchCache, versión 1
  - BranchCache versión 2
  - BranchCache versiones 1 y 2
- Establecer mediante la Registry GPO.



Para usar la configuración de GPO de BranchCache, BranchCache debe configurarse en la SVM habilitada para CIFS a la que desea aplicar esta configuración. Si no se configura BranchCache en la SVM, no se aplicará la configuración de GPO y se descarta.

- Configuración de seguridad

- Política de auditoría y registro de eventos

- Auditar eventos de inicio de sesión

Especifica el tipo de eventos de inicio de sesión que se van a auditar, incluida la siguiente configuración:

- No auditar
- Auditar solo los eventos de éxito
- Auditoría de eventos de fallo
- Auditar eventos de éxito y fallo

Establecer mediante la Audit logon events ajuste en la Local Policies/Audit Policy GPO.



Si se establece cualquiera de las tres opciones de auditoría (sólo eventos de éxito de auditoría, auditar sólo eventos de fallo, auditar eventos de éxito y de fallo), ONTAP audita tanto eventos de éxito como de fallo.

- Auditar el acceso a objetos

Especifica el tipo de acceso al objeto que se va a auditar, incluida la siguiente configuración:

- No auditar
- Auditar solo los eventos de éxito
- Auditoría de eventos de fallo
- Auditar eventos de éxito y fallo

Establecer mediante la `Audit object access` ajuste en la `Local Policies/Audit Policy` GPO.



Si se establece cualquiera de las tres opciones de auditoría (sólo eventos de éxito de auditoría, auditar sólo eventos de fallo, auditar eventos de éxito y de fallo), ONTAP audita tanto eventos de éxito como de fallo.

- Método de retención de registros

Especifica el método de retención del registro de auditoría, incluida la siguiente configuración:

- Sobrescribir el registro de eventos cuando el tamaño del archivo de registro supere el tamaño máximo del registro
- No sobrescribir el registro de eventos (borrar el registro manualmente)  
Establecer mediante la `Retention method for security log` ajuste en la `Event Log` GPO.

- Tamaño máximo del registro

Especifica el tamaño máximo del registro de auditoría.

Establecer mediante la `Maximum security log size` ajuste en la `Event Log` GPO.



Para utilizar la configuración de directiva de auditoría y GPO de registro de eventos, la auditoría debe configurarse en la SVM habilitada para CIFS a la que desea aplicar esta configuración. Si la auditoría no está configurada en la SVM, la configuración de GPO no se aplicará y se descarta.

- Seguridad del sistema de archivos

Especifica una lista de archivos o directorios en los que se aplica la seguridad de archivos a través de un GPO.

Establecer mediante la `File System` GPO.



Debe existir la ruta de acceso del volumen donde se configura el GPO de seguridad del sistema de archivos en la SVM.

- Política de Kerberos

- Desviación máxima del reloj

Especifica la tolerancia máxima en minutos para la sincronización del reloj del equipo.

Establecer mediante la `Maximum tolerance for computer clock synchronization` ajuste en la `Account Policies/Kerberos Policy` GPO.

- Antigüedad máxima del billete

Especifica la duración máxima en horas para el ticket de usuario.

Establecer mediante la `Maximum lifetime for user ticket` ajuste en la `Account Policies/Kerberos Policy` GPO.

- Antigüedad máxima de renovación del boleto

Especifica la duración máxima en días para la renovación de la tarjeta de usuario.

Establecer mediante la `Maximum lifetime for user ticket renewal` ajuste en la `Account Policies/Kerberos Policy` GPO.

- Asignación de derechos de usuario (derechos de privilegio)

- Asuma la propiedad

Especifica la lista de usuarios y grupos que tienen derecho a asumir la propiedad de cualquier objeto asegurable.

Establecer mediante la `Take ownership of files or other objects` ajuste en la `Local Policies/User Rights Assignment` GPO.

- Privilegio de seguridad

Especifica la lista de usuarios y grupos que pueden especificar opciones de auditoría para el acceso a objetos de recursos individuales, como archivos, carpetas y objetos de Active Directory.

Establecer mediante la `Manage auditing and security log` ajuste en la `Local Policies/User Rights Assignment` GPO.

- Cambiar privilegio de notificación (comprobación de recorrido de derivación)

Especifica la lista de usuarios y grupos que pueden recorrer los árboles de directorios aunque los usuarios y los grupos puedan no tener permisos en el directorio de recorrido.

El mismo privilegio es necesario para que los usuarios reciban notificaciones de cambios en archivos y directorios. Establecer mediante la `Bypass traverse checking` ajuste en la `Local Policies/User Rights Assignment` GPO.

- Valores del Registro

- Firma Configuración requerida

Especifica si la firma SMB necesaria está habilitada o deshabilitada.

Establecer mediante la `Microsoft network server: Digitally sign communications (always)` ajuste en la `Security Options` GPO.

- Restringir anónimo

Especifica cuáles son las restricciones para los usuarios anónimos e incluye las tres configuraciones de GPO siguientes:

- No hay enumeración de cuentas del Administrador de cuentas de seguridad (SAM):

Esta configuración de seguridad determina qué permisos adicionales se conceden para las conexiones anónimas al equipo. Esta opción se muestra como `no-enumeration` En ONTAP si está habilitado.

Establecer mediante la `Network access: Do not allow anonymous enumeration of SAM accounts` ajuste en la `Local Policies/Security Options` GPO.

- No hay enumeración de cuentas y recursos compartidos de SAM

Esta configuración de seguridad determina si se permite la enumeración anónima de cuentas SAM y recursos compartidos. Esta opción se muestra como `no-enumeration` En ONTAP si está habilitado.

Establecer mediante la `Network access: Do not allow anonymous enumeration of SAM accounts and shares` ajuste en la `Local Policies/Security Options` GPO.

- Restringir el acceso anónimo a recursos compartidos y canalizaciones con nombre

Esta configuración de seguridad restringe el acceso anónimo a recursos compartidos y tuberías. Esta opción se muestra como `no-access` En ONTAP si está habilitado.

Establecer mediante la `Network access: Restrict anonymous access to Named Pipes and Shares` ajuste en la `Local Policies/Security Options` GPO.

Cuando se muestra información acerca de las directivas de grupo definidas y aplicadas, la `Resultant restriction for anonymous user` El campo salida proporciona información sobre la restricción resultante de las tres configuraciones de GPO anónimo de restricción. Las posibles restricciones resultantes son las siguientes:

- `no-access`

Al usuario anónimo se le deniega el acceso a los recursos compartidos especificados y a las canalizaciones con nombre, y no se puede utilizar la enumeración de cuentas y recursos compartidos SAM. Esta restricción resultante se observa si el `Network access: Restrict anonymous access to Named Pipes and Shares` GPO está habilitado.

- `no-enumeration`

El usuario anónimo tiene acceso a los recursos compartidos y canalizaciones con nombre especificados, pero no puede utilizar la enumeración de cuentas y recursos compartidos SAM. Esta restricción resultante se observa si se cumplen las dos condiciones siguientes:

- La `Network access: Restrict anonymous access to Named Pipes and Shares` GPO deshabilitado.
- O bien la `Network access: Do not allow anonymous enumeration of SAM accounts` o la `Network access: Do not allow anonymous enumeration of SAM accounts and shares` Los GPO están habilitados.

- `no-restriction`

El usuario anónimo tiene acceso completo y puede utilizar la enumeración. Esta restricción resultante se observa si se cumplen las dos condiciones siguientes:

- La `Network access: Restrict anonymous access to Named Pipes and Shares`

GPO deshabilitado.

- **Ambas Network access:** Do not allow anonymous enumeration of SAM accounts y.. **Network access:** Do not allow anonymous enumeration of SAM accounts and shares Los GPO están deshabilitados.
- Grupos restringidos

Puede configurar grupos restringidos para administrar de forma centralizada la pertenencia a grupos integrados o definidos por el usuario. Cuando aplica un grupo restringido a través de una directiva de grupo, la pertenencia a un grupo local de servidor CIFS se establece automáticamente para que coincida con la configuración de la lista de miembros definida en la directiva de grupo aplicada.

Establecer mediante la `Restricted Groups` GPO.

- Configuración de la directiva de acceso central

Especifica una lista de directivas de acceso central. Las políticas de acceso central y las reglas de política de acceso central asociadas determinan los permisos de acceso para varios archivos en la SVM.

### Información relacionada

[Habilitar o deshabilitar la compatibilidad de GPO en un servidor CIFS](#)

[Protección del acceso a los archivos mediante el control de acceso dinámico \(DAC\)](#)

["Seguimiento de seguridad y auditoría de SMB y NFS"](#)

[Modificar la configuración de seguridad Kerberos del servidor CIFS](#)

[Uso de BranchCache para almacenar en caché contenido compartido de SMB en una sucursal](#)

[Utilizar la firma SMB para mejorar la seguridad de la red](#)

[Configuración de la comprobación de recorrido de derivación](#)

[Configuración de restricciones de acceso para usuarios anónimos](#)

### Requisitos para usar GPO con el servidor SMB

Para utilizar objetos de directiva de grupo (GPO) con el servidor SMB, el sistema debe cumplir varios requisitos.

- Las licencias de SMB deben estar en el clúster. La licencia SMB se incluye con **"ONTAP One"**. Si no tiene ONTAP One y la licencia no está instalada, póngase en contacto con su representante de ventas.
- Debe haber un servidor SMB configurado y Unido a un dominio de Windows Active Directory.
- El estado del administrador del servidor SMB debe ser on.
- Los GPO deben configurarse y aplicarse a la unidad organizativa (OU) de Active Directory de Windows que contiene el objeto de equipo servidor SMB.
- La compatibilidad con GPO debe estar habilitada en el servidor SMB.

**Habilite o deshabilite la compatibilidad de GPO en un servidor CIFS**

Puede habilitar o deshabilitar la compatibilidad con objetos de directiva de grupo (GPO) en un servidor CIFS. Si habilita la compatibilidad de GPO en un servidor CIFS, los GPO aplicables definidos en la directiva de grupo (la directiva que se aplica a la unidad organizativa (OU) que contiene el objeto de equipo del servidor CIFS) se aplican al servidor CIFS.



**Acerca de esta tarea**

Los GPO no pueden habilitarse en servidores CIFS en modo de grupo de trabajo.

**Pasos**

1. Ejecute una de las siguientes acciones:

| Si desea...      | Introduzca el comando...                                                             |
|------------------|--------------------------------------------------------------------------------------|
| Habilite los GPO | <code>vserver cifs group-policy modify -vserver vserver_name -status enabled</code>  |
| Deshabilitar GPO | <code>vserver cifs group-policy modify -vserver vserver_name -status disabled</code> |

2. Compruebe que la compatibilidad con GPO está en el estado deseado: `vserver cifs group-policy show -vserver +vserver_name_`

El estado de la directiva de grupo de los servidores CIFS en el modo de grupo se muestra como "desactivado".

**Ejemplo**

En el siguiente ejemplo, se habilita la compatibilidad de GPO en máquinas virtuales de almacenamiento (SVM) vs1:

```
cluster1::> vserver cifs group-policy modify -vserver vs1 -status enabled

cluster1::> vserver cifs group-policy show -vserver vs1

 Vserver: vs1
Group Policy Status: enabled
```

**Información relacionada**

[Objetos de normativa de grupo compatibles](#)

[Requisitos para el uso de GPO con su servidor CIFS](#)

[Cómo se actualizan los GPO en el servidor CIFS](#)

[Actualizar manualmente la configuración de GPO en el servidor CIFS](#)

**Cómo se actualizan los GPO en el servidor SMB**

**Cómo se actualizan los GPO en la información general del servidor CIFS**

De forma predeterminada, ONTAP recupera y aplica los cambios de objeto de directiva de grupo (GPO) cada 90 minutos. La configuración de seguridad se actualiza cada 16 horas. Si desea actualizar GPO para aplicar nuevas configuraciones de directivas de GPO antes de que ONTAP las actualice automáticamente, puede activar una actualización manual en un servidor CIFS con un comando ONTAP.

- De forma predeterminada, todos los GPO se verifican y actualizan según sea necesario cada 90 minutos.

Este intervalo se puede configurar y se puede establecer mediante la `Refresh interval` y `Random offset` Configuración de GPO.

ONTAP consulta a Active Directory los cambios realizados en los GPO. Si los números de versión de GPO registrados en Active Directory son superiores a los del servidor CIFS, ONTAP recupera y aplica los nuevos GPO. Si los números de versión son los mismos, los GPO en el servidor CIFS no se actualizan.

- Configuración de seguridad los GPO se actualizan cada 16 horas.

ONTAP recupera y aplica los GPO de configuración de seguridad cada 16 horas, independientemente de que estos GPO hayan cambiado o no.



El valor predeterminado de 16 horas no se puede cambiar en la versión actual de ONTAP. Es una configuración predeterminada del cliente Windows.

- Todos los GPO se pueden actualizar manualmente con un comando ONTAP.

Este comando simula Windows ``gpupdate.exe`` comando `/force`.

**Información relacionada**

[Actualizar manualmente la configuración de GPO en el servidor CIFS](#)

**Actualizar manualmente la configuración de GPO en el servidor CIFS**

Si desea actualizar inmediatamente la configuración del objeto de directiva de grupo (GPO) en el servidor CIFS, puede actualizar manualmente la configuración. Sólo puede actualizar los ajustes modificados o puede forzar una actualización para todos los ajustes, incluidos los que se aplicaron anteriormente pero no se han modificado.

**Paso**

1. Ejecute la acción adecuada:

| Si desea actualizar...              | Introduzca el comando...                                                            |
|-------------------------------------|-------------------------------------------------------------------------------------|
| Ha cambiado la configuración de GPO | <code>vserver cifs group-policy update</code><br><code>-vserver vserver_name</code> |



| Si desea actualizar...           | Introduzca el comando...                                                                                      |
|----------------------------------|---------------------------------------------------------------------------------------------------------------|
| Todas las configuraciones de GPO | <code>vserver cifs group-policy update<br/>-vserver vserver_name -force-reapply<br/>-all-settings true</code> |

## Información relacionada

[Cómo se actualizan los GPO en el servidor CIFS](#)

## Mostrar información acerca de las configuraciones de GPO

Puede mostrar información acerca de las configuraciones de objeto de directiva de grupo (GPO) definidas en Active Directory y acerca de las configuraciones de GPO aplicadas al servidor CIFS.

## Acerca de esta tarea

Puede mostrar información acerca de todas las configuraciones de GPO definidas en Active Directory del dominio al que pertenece el servidor CIFS o solo puede mostrar información acerca de las configuraciones de GPO aplicadas a un servidor CIFS.

## Pasos

1. Mostrar información acerca de las configuraciones de GPO realizando una de las siguientes acciones:

| Si desea mostrar información acerca de todas las configuraciones de directiva de grupo... | Introduzca el comando...                                                      |
|-------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| Definido en Active Directory                                                              | <code>vserver cifs group-policy show-defined<br/>-vserver vserver_name</code> |
| Aplicado a una máquina virtual de almacenamiento (SVM) habilitada para CIFS               | <code>vserver cifs group-policy show-applied<br/>-vserver vserver_name</code> |

## Ejemplo

En el siguiente ejemplo, se muestran las configuraciones de GPO definidas en Active Directory al que pertenece la SVM habilitada para CIFS con el nombre vs1:

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1
```

```
Vserver: vs1
```

```

```

```
 GPO Name: Default Domain Policy
```

```
 Level: Domain
```

```
 Status: enabled
```

```
 Advanced Audit Settings:
```

```
 Object Access:
```

```
 Central Access Policy Staging: failure
```

Registry Settings:

Refresh Time Interval: 22  
Refresh Random Offset: 8  
Hash Publication Mode for BranchCache: per-share  
Hash Version Support for BranchCache : version1

Security Settings:

Event Audit and Event Log:

Audit Logon Events: none  
Audit Object Access: success  
Log Retention Method: overwrite-as-needed  
Max Log Size: 16384

File Security:

/vol1/home  
/vol1/dir1

Kerberos:

Max Clock Skew: 5  
Max Ticket Age: 10  
Max Renew Age: 7

Privilege Rights:

Take Ownership: usr1, usr2  
Security Privilege: usr1, usr2  
Change Notify: usr1, usr2

Registry Values:

Signing Required: false

Restrict Anonymous:

No enumeration of SAM accounts: true  
No enumeration of SAM accounts and shares: false  
Restrict anonymous access to shares and named pipes: true  
Combined restriction for anonymous user: no-access

Restricted Groups:

gpr1  
gpr2

Central Access Policy Settings:

Policies: cap1  
cap2

GPO Name: Resultant Set of Policy

Status: enabled

Advanced Audit Settings:

Object Access:

Central Access Policy Staging: failure

Registry Settings:

Refresh Time Interval: 22  
Refresh Random Offset: 8  
Hash Publication for Mode BranchCache: per-share  
Hash Version Support for BranchCache: version1

#### Security Settings:

##### Event Audit and Event Log:

Audit Logon Events: none  
Audit Object Access: success  
Log Retention Method: overwrite-as-needed  
Max Log Size: 16384

##### File Security:

/vol1/home  
/vol1/dirl

##### Kerberos:

Max Clock Skew: 5  
Max Ticket Age: 10  
Max Renew Age: 7

##### Privilege Rights:

Take Ownership: usr1, usr2  
Security Privilege: usr1, usr2  
Change Notify: usr1, usr2

##### Registry Values:

Signing Required: false

##### Restrict Anonymous:

No enumeration of SAM accounts: true  
No enumeration of SAM accounts and shares: false  
Restrict anonymous access to shares and named pipes: true  
Combined restriction for anonymous user: no-access

##### Restricted Groups:

gpr1  
gpr2

#### Central Access Policy Settings:

Policies: cap1  
cap2

En el siguiente ejemplo, se muestran las configuraciones de GPO aplicadas a la SVM vs1 habilitada para CIFS:

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1
```

Vserver: vs1

-----

GPO Name: Default Domain Policy

Level: Domain

Status: enabled

##### Advanced Audit Settings:

Object Access:

Central Access Policy Staging: failure

##### Registry Settings:

Refresh Time Interval: 22

```
Refresh Random Offset: 8
Hash Publication Mode for BranchCache: per-share
Hash Version Support for BranchCache: all-versions
Security Settings:
 Event Audit and Event Log:
 Audit Logon Events: none
 Audit Object Access: success
 Log Retention Method: overwrite-as-needed
 Max Log Size: 16384
 File Security:
 /vol1/home
 /vol1/dir1
 Kerberos:
 Max Clock Skew: 5
 Max Ticket Age: 10
 Max Renew Age: 7
 Privilege Rights:
 Take Ownership: usr1, usr2
 Security Privilege: usr1, usr2
 Change Notify: usr1, usr2
 Registry Values:
 Signing Required: false
 Restrict Anonymous:
 No enumeration of SAM accounts: true
 No enumeration of SAM accounts and shares: false
 Restrict anonymous access to shares and named pipes: true
 Combined restriction for anonymous user: no-access
 Restricted Groups:
 gpr1
 gpr2
Central Access Policy Settings:
 Policies: cap1
 cap2

GPO Name: Resultant Set of Policy
Level: RSOP
Advanced Audit Settings:
 Object Access:
 Central Access Policy Staging: failure
Registry Settings:
 Refresh Time Interval: 22
 Refresh Random Offset: 8
 Hash Publication Mode for BranchCache: per-share
 Hash Version Support for BranchCache: all-versions
Security Settings:
 Event Audit and Event Log:
```

```
Audit Logon Events: none
Audit Object Access: success
Log Retention Method: overwrite-as-needed
Max Log Size: 16384
File Security:
 /vol1/home
 /vol1/dir1
Kerberos:
 Max Clock Skew: 5
 Max Ticket Age: 10
 Max Renew Age: 7
Privilege Rights:
 Take Ownership: usr1, usr2
 Security Privilege: usr1, usr2
 Change Notify: usr1, usr2
Registry Values:
 Signing Required: false
Restrict Anonymous:
 No enumeration of SAM accounts: true
 No enumeration of SAM accounts and shares: false
 Restrict anonymous access to shares and named pipes: true
 Combined restriction for anonymous user: no-access
Restricted Groups:
 gpr1
 gpr2
Central Access Policy Settings:
 Policies: cap1
 cap2
```

## Información relacionada

[Habilitar o deshabilitar la compatibilidad de GPO en un servidor CIFS](#)

### Mostrar información detallada acerca de los GPO de grupo restringidos

Puede mostrar información detallada sobre los grupos restringidos que se definen como objetos de directiva de grupo (GPO) en Active Directory y que se aplican al servidor CIFS.

### Acerca de esta tarea

De forma predeterminada, se muestra la siguiente información:

- Nombre de la política de grupo
- Versión de la directiva de grupo
- Enlace

Especifica el nivel en el que se configura la directiva de grupo. Los valores de salida posibles incluyen los siguientes:

- **Local** Cuando se configura la política de grupo en ONTAP
- **Site** cuando la directiva de grupo se configura a nivel de sitio en el controlador de dominio
- **Domain** cuando la directiva de grupo se configura en el nivel de dominio en el controlador de dominio
- **OrganizationalUnit** Cuando la directiva de grupo se configura en el nivel Unidad organizativa (OU) del controlador de dominio
- **RSOP** para el conjunto resultante de directivas derivadas de todas las directivas de grupo definidas en varios niveles

- Nombre de grupo restringido
- Los usuarios y grupos que pertenecen al grupo restringido y que no pertenecen al mismo
- Lista de grupos a los que se agrega el grupo restringido

Un grupo puede ser miembro de grupos distintos de los que se enumeran aquí.

## Paso

1. Muestre información acerca de todos los GPO de grupo restringidos realizando una de las siguientes acciones:

| Si desea mostrar información sobre todos los GPO de grupo restringidos... | Introduzca el comando...                                                                   |
|---------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| Definido en Active Directory                                              | <code>vserver cifs group-policy restricted-group show-defined -vserver vserver_name</code> |
| Aplicado a un servidor CIFS                                               | <code>vserver cifs group-policy restricted-group show-applied -vserver vserver_name</code> |

## Ejemplo

En el siguiente ejemplo, se muestra información sobre los objetos de normativa de grupo restringidos definidos en el dominio de Active Directory al que pertenece la SVM habilitada para CIFS, llamada vs1:

```
cluster1::> vsserver cifs group-policy restricted-group show-defined
-vsserver vs1
```

```
Vserver: vs1
```

```

```

```
Group Policy Name: gp01
Version: 16
Link: OrganizationalUnit
Group Name: group1
Members: user1
MemberOf: EXAMPLE\group9

Group Policy Name: Resultant Set of Policy
Version: 0
Link: RSOP
Group Name: group1
Members: user1
MemberOf: EXAMPLE\group9
```

En el siguiente ejemplo, se muestra información sobre los objetos de normativa de grupo restringidos aplicados a la SVM vs1 habilitada para CIFS:

```
cluster1::> vsserver cifs group-policy restricted-group show-applied
-vsserver vs1
```

```
Vserver: vs1
```

```

```

```
Group Policy Name: gp01
Version: 16
Link: OrganizationalUnit
Group Name: group1
Members: user1
MemberOf: EXAMPLE\group9

Group Policy Name: Resultant Set of Policy
Version: 0
Link: RSOP
Group Name: group1
Members: user1
MemberOf: EXAMPLE\group9
```

## Información relacionada


Muestra información sobre las políticas de acceso central

Puede mostrar información detallada acerca de las directivas de acceso central definidas en Active Directory. También puede mostrar información sobre las políticas de acceso central que se aplican al servidor CIFS a través de objetos de política de grupo (GPO).

Acerca de esta tarea

De forma predeterminada, se muestra la siguiente información:

- Nombre de SVM
- Nombre de la política de acceso central
- SID
- Descripción
- Hora de creación
- Tiempo de modificación
- Normas de los miembros



Los servidores CIFS en el modo de grupo de trabajo no se muestran porque no admiten los GPO.

Paso

1. Muestre información acerca de las directivas de acceso central realizando una de las siguientes acciones:

| Si desea mostrar información sobre todas las directivas de acceso central... | Introduzca el comando...                                                                               |
|------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| Definido en Active Directory                                                 | <code>vserver cifs group-policy central-access-policy show-defined -vserver <i>vserver_name</i></code> |
| Aplicado a un servidor CIFS                                                  | <code>vserver cifs group-policy central-access-policy show-applied -vserver <i>vserver_name</i></code> |

Ejemplo

El siguiente ejemplo muestra información de todas las directivas de acceso central definidas en Active Directory:



```
cluster1::> vservers cifs group-policy central-access-policy show-defined
```

```
Vserver Name SID
----- -

vs1 p1 S-1-17-3386172923-1132988875-3044489393-
3993546205
 Description: policy #1
 Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
 Member Rules: r1

vs1 p2 S-1-17-1885229282-1100162114-134354072-
822349040
 Description: policy #2
 Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
 Member Rules: r1
 r2
```

El siguiente ejemplo muestra información de todas las políticas de acceso central que se aplican a las máquinas virtuales de almacenamiento (SVM) del clúster:

```
cluster1::> vservers cifs group-policy central-access-policy show-applied
```

```
Vserver Name SID
----- -

vs1 p1 S-1-17-3386172923-1132988875-3044489393-
3993546205
 Description: policy #1
 Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
 Member Rules: r1

vs1 p2 S-1-17-1885229282-1100162114-134354072-
822349040
 Description: policy #2
 Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
 Member Rules: r1
 r2
```

## Información relacionada

**Muestra información acerca de las reglas de la política de acceso central**

Puede mostrar información detallada acerca de las reglas de directiva de acceso central asociadas a las directivas de acceso central definidas en Active Directory. También puede mostrar información sobre las reglas de políticas de acceso central que se aplican al servidor CIFS a través de los GPO de la política de acceso central (objetos de política de grupo).

**Acerca de esta tarea**

Puede mostrar información detallada acerca de las reglas de directiva de acceso central definidas y aplicadas. De forma predeterminada, se muestra la siguiente información:

- Nombre del Vserver
- Nombre de la regla de acceso central
- Descripción
- Hora de creación
- Tiempo de modificación
- Permisos actuales
- Permisos propuestos
- Recursos objetivo

| Si desea mostrar información acerca de todas las reglas de directiva de acceso central asociadas con las directivas de acceso central... | Introduzca el comando...                                                                      |
|------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| Definido en Active Directory                                                                                                             | <code>vserver cifs group-policy central-access-rule show-defined -vserver vserver_name</code> |
| Aplicado a un servidor CIFS                                                                                                              | <code>vserver cifs group-policy central-access-rule show-applied -vserver vserver_name</code> |

**Ejemplo**

En el siguiente ejemplo se muestra información de todas las reglas de directiva de acceso central asociadas a las directivas de acceso central definidas en Active Directory:

```
cluster1::> vservers cifs group-policy central-access-rule show-defined
```

| Vserver | Name                                                                 |
|---------|----------------------------------------------------------------------|
| vs1     | r1                                                                   |
|         | Description: rule #1                                                 |
|         | Creation Time: Tue Oct 22 09:33:48 2013                              |
|         | Modification Time: Tue Oct 22 09:33:48 2013                          |
|         | Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)                        |
|         | Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY) |
| vs1     | r2                                                                   |
|         | Description: rule #2                                                 |
|         | Creation Time: Tue Oct 22 10:27:57 2013                              |
|         | Modification Time: Tue Oct 22 10:27:57 2013                          |
|         | Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)                        |
|         | Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY) |

El siguiente ejemplo muestra información de todas las reglas de políticas de acceso central asociadas con las políticas de acceso centrales aplicadas a las máquinas virtuales de almacenamiento (SVM) en el clúster:

```
cluster1::> vservers cifs group-policy central-access-rule show-applied
```

| Vserver | Name                                                                 |
|---------|----------------------------------------------------------------------|
| vs1     | r1                                                                   |
|         | Description: rule #1                                                 |
|         | Creation Time: Tue Oct 22 09:33:48 2013                              |
|         | Modification Time: Tue Oct 22 09:33:48 2013                          |
|         | Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)                        |
|         | Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY) |
| vs1     | r2                                                                   |
|         | Description: rule #2                                                 |
|         | Creation Time: Tue Oct 22 10:27:57 2013                              |
|         | Modification Time: Tue Oct 22 10:27:57 2013                          |
|         | Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)                        |
|         | Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY) |

## Información relacionada

[Protección del acceso a los archivos mediante el control de acceso dinámico \(DAC\)](#)

[Mostrar información acerca de las configuraciones de GPO](#)

[Visualización de información acerca de las políticas de acceso central](#)

## Comandos para gestionar las contraseñas de cuentas de equipos de servidores SMB

Debe conocer los comandos para cambiar, restablecer y deshabilitar contraseñas, así como para configurar las programaciones de actualización automática. También puede configurar una programación en el servidor SMB para que la actualice automáticamente.

| Si desea...                                                                             | Se usa este comando...                                                                                     |
|-----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| Cambie o restablezca la contraseña de la cuenta de dominio y sabrá la contraseña        | <code>vserver cifs domain password change</code>                                                           |
| Restablezca la contraseña de la cuenta de dominio y no conoce la contraseña             | <code>vserver cifs domain password reset</code>                                                            |
| Configurar servidores SMB para cambios automáticos de contraseña de cuenta de equipo    | <code>vserver cifs domain password schedule modify -vserver vserver_name -is -schedule-enabled true</code> |
| Deshabilite los cambios automáticos de contraseña de cuenta de equipo en servidores SMB | <code>vserver cifs domain password schedule modify -vserver vs1 -is-schedule-enabled false</code>          |

Consulte la página de manual de cada comando para obtener más información.

## Gestione las conexiones del controlador de dominio

### Muestra información sobre los servidores detectados

Puede mostrar información relacionada con los servidores LDAP y las controladoras de dominio detectados en el servidor CIFS.

### Paso

1. Para mostrar información relacionada con los servidores detectados, introduzca el siguiente comando:  
`vserver cifs domain discovered-servers show`

### Ejemplo

En el siguiente ejemplo, se muestran los servidores detectados para la SVM vs1:

```
cluster1::> vserver cifs domain discovered-servers show
```

Node: node1

Vserver: vs1

| Domain Name | Type    | Preference | DC-Name | DC-Address | Status |
|-------------|---------|------------|---------|------------|--------|
| example.com | MS-LDAP | adequate   | DC-1    | 1.1.3.4    | OK     |
| example.com | MS-LDAP | adequate   | DC-2    | 1.1.3.5    | OK     |
| example.com | MS-DC   | adequate   | DC-1    | 1.1.3.4    | OK     |
| example.com | MS-DC   | adequate   | DC-2    | 1.1.3.5    | OK     |

## Información relacionada

[Restablecer y volver a descubrir servidores](#)

[Detener o iniciar el servidor CIFS](#)

## Restablecer y volver a detectar servidores

La restauración y la nueva detección de servidores en el servidor CIFS permite que el servidor CIFS deseche la información almacenada sobre los servidores LDAP y las controladoras de dominio. Tras descartar información del servidor, el servidor CIFS vuelve a adquirir la información actual de estos servidores externos. Esto puede ser útil cuando los servidores conectados no responden adecuadamente.

## Pasos

1. Introduzca el siguiente comando: `vserver cifs domain discovered-servers reset-servers -vserver vserver_name`
2. Mostrar información sobre los servidores que se han redescubierto recientemente: `vserver cifs domain discovered-servers show -vserver vserver_name`

## Ejemplo

En el siguiente ejemplo, se restablecen y vuelven a detectar los servidores para la máquina virtual de almacenamiento (SVM, antes denominada Vserver) vs1:

```
cluster1::> vserver cifs domain discovered-servers reset-servers -vserver vs1
```

```
cluster1::> vserver cifs domain discovered-servers show
```

```
Node: node1
Vserver: vs1
```

| Domain Name | Type    | Preference | DC-Name | DC-Address | Status |
|-------------|---------|------------|---------|------------|--------|
| example.com | MS-LDAP | adequate   | DC-1    | 1.1.3.4    | OK     |
| example.com | MS-LDAP | adequate   | DC-2    | 1.1.3.5    | OK     |
| example.com | MS-DC   | adequate   | DC-1    | 1.1.3.4    | OK     |
| example.com | MS-DC   | adequate   | DC-2    | 1.1.3.5    | OK     |

## Información relacionada

[Mostrar información sobre los servidores detectados](#)

[Detener o iniciar el servidor CIFS](#)

## Administrar la detección del controlador de dominio

A partir de ONTAP 9.3, puede modificar el proceso predeterminado por el que se detectan los controladores de dominio (DC). Esto le permite limitar la detección a sus instalaciones o a un conjunto de centros de datos preferidos, lo que puede mejorar el rendimiento en función del entorno.

## Acerca de esta tarea

De forma predeterminada, el proceso de detección dinámica detecta todos los centros de datos disponibles, incluidos los centros de datos preferidos, todos los centros de datos del sitio local y todos los centros de datos remotos. Esta configuración puede provocar latencia en autenticación y acceder a recursos compartidos en determinados entornos. Si ya ha determinado el grupo de DC que desea utilizar o si los DC remotos son inadecuados o inaccesibles, puede cambiar el método de descubrimiento.

En ONTAP 9.3 y versiones posteriores, el `discovery-mode` parámetro de `cifs domain discovered-servers` comando permite seleccionar una de las siguientes opciones de detección:

- Se descubren todos los DC del dominio.
- Sólo se descubren los centros de datos del sitio local.

La `default-site` El parámetro del servidor SMB se puede definir para utilizar este modo con LIF que no están asignadas a un sitio en `sites-and-services`.

- No se realiza la detección del servidor, la configuración del servidor SMB depende únicamente de los centros de datos preferidos.

Para utilizar este modo, primero debe definir los DC preferidos para el servidor SMB.

## Paso

1. Especifique la opción de detección deseada: `vserver cifs domain discovered-servers discovery-mode modify -vserver vserver_name -mode {all|site|none}`

Opciones para mode parámetro:

- all

Descubrir todos los DC disponibles (predeterminado).

- site

Limite el descubrimiento de DC a su sitio.

- none

Utilice sólo los centros de datos preferidos y no realice la detección.

## Añada controladores de dominio preferidos

ONTAP detecta automáticamente controladoras de dominio a través de DNS. Opcionalmente, puede añadir uno o varios controladores de dominio a la lista de controladores de dominio preferidos para un dominio específico.

### Acerca de esta tarea

Si ya existe una lista de controladores de dominio preferido para el dominio especificado, la nueva lista se combina con la lista existente.

## Paso

1. Para agregar a la lista de controladores de dominio preferidos, introduzca el siguiente comando:  
`vserver cifs domain preferred-dc add -vserver vserver_name -domain domain_name -preferred-dc IP_address, ...+`  
  
`-vserver vserver_name` Especifica el nombre de la máquina virtual de almacenamiento (SVM).  
  
`-domain domain_name` Especifica el nombre completo de Active Directory del dominio al que pertenecen los controladores de dominio especificados.  
  
`-preferred-dc IP_address,...` Especifica una o varias direcciones IP de los controladores de dominio preferidos, como una lista delimitada por comas, en orden de preferencia.

## Ejemplo

El siguiente comando añade los controladores de dominio 172.17.102.25 y 172.17.102.24 a la lista de controladores de dominio preferidos que el servidor SMB en SVM vs1 utiliza para gestionar el acceso externo al dominio cifs.lab.example.com.

```
cluster1::> vserver cifs domain preferred-dc add -vserver vs1 -domain
cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

## Información relacionada

### Comandos para gestionar controladoras de dominio preferidas

Debe conocer los comandos para añadir, mostrar y eliminar controladoras de dominio preferidas.

| Si desea...                                     | Se usa este comando...                               |
|-------------------------------------------------|------------------------------------------------------|
| Agregar un controlador de dominio preferido     | <code>vserver cifs domain preferred-dc add</code>    |
| Mostrar los controladores de dominio preferidos | <code>vserver cifs domain preferred-dc show</code>   |
| Quite una controladora de dominio preferida     | <code>vserver cifs domain preferred-dc remove</code> |

Consulte la página de manual de cada comando para obtener más información.

### Información relacionada

[Adición de controladores de dominio preferidos](#)

### Habilite conexiones SMB2 a controladores de dominio

A partir de ONTAP 9.1, es posible habilitar SMB versión 2.0 para conectarse a un controlador de dominio. Hacerlo es necesario si ha deshabilitado SMB 1.0 en controladores de dominio. A partir de ONTAP 9.2, SMB2 está habilitado de forma predeterminada.

### Acerca de esta tarea

La `smb2-enabled-for-dc-connections` Opción de comando habilita la opción predeterminada del sistema para la versión de ONTAP que está usando. El valor predeterminado del sistema para ONTAP 9.1 está habilitado para SMB 1.0 y deshabilitado para SMB 2.0. El valor predeterminado del sistema para ONTAP 9.2 está habilitado para SMB 1.0 y habilitado para SMB 2.0. Si la controladora de dominio no puede negociar inicialmente SMB 2.0, utiliza SMB 1.0.

SMB 1.0 puede deshabilitarse desde ONTAP a un controlador de dominio. En ONTAP 9.1, si se ha deshabilitado SMB 1.0, se debe habilitar SMB 2.0 para poder comunicarse con un controlador de dominio.

Más información sobre:

- ["Verificación de las versiones habilitadas del SMB"](#).
- ["Funcionalidades y versiones de SMB compatibles"](#).



Si `-smb1-enabled-for-dc-connections` se establece en `false` aunque `-smb1-enabled` se establece en `true`, ONTAP deniega las conexiones SMB 1.0 como cliente, pero continúa aceptando conexiones SMB 1.0 entrantes como servidor.

### Pasos

1. Antes de cambiar la configuración de seguridad de SMB, compruebe qué versiones de SMB están habilitadas: `vserver cifs security show`



2. Desplácese hacia abajo por la lista para ver las versiones de SMB.
3. Ejecute el comando apropiado con el `smb2-enabled-for-dc-connections` opción.

| Si desea que SMB2 sea... | Introduzca el comando...                                                                              |
|--------------------------|-------------------------------------------------------------------------------------------------------|
| Activado                 | <pre>vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc -connections true</pre>  |
| Deshabilitado            | <pre>vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc -connections false</pre> |

#### Habilite conexiones cifradas con controladores de dominio

A partir de ONTAP 9.8, puede especificar que se cifren las conexiones a los controladores de dominio.

#### Acerca de esta tarea

ONTAP requiere cifrado para las comunicaciones del controlador de dominio (DC) cuando el `-encryption -required-for-dc-connection` opción establecida en `true`; el valor predeterminado es `false`. Cuando se establece la opción, solo se utilizará el protocolo SMB3 para las conexiones ONTAP-DC, ya que el cifrado solo es compatible con SMB3.

Cuando se necesitan comunicaciones de DC cifradas, la `-smb2-enabled-for-dc-connections` Se ignora la opción, ya que ONTAP solo negocia las conexiones de SMB3. Si un controlador de dominio no admite SMB3 y cifrado, ONTAP no se conectará a él.

#### Paso

1. Habilitar la comunicación cifrada con el controlador de dominio: 

```
vserver cifs security modify
-vserver svm_name -encryption-required-for-dc-connection true
```

#### Utilice sesiones nulas para acceder al almacenamiento en entornos que no sean de Kerberos

##### Utilice sesiones nulas para acceder al almacenamiento en la información general de entornos que no sean Kerberos

El acceso de sesión nulo proporciona permisos para recursos de red, como datos del sistema de almacenamiento, y para servicios basados en cliente que se ejecutan en el sistema local. Una sesión nula se produce cuando un proceso de cliente utiliza la cuenta "system" para acceder a un recurso de red. La configuración de sesión nula es específica para la autenticación que no es de Kerberos.

##### Cómo el sistema de almacenamiento proporciona acceso nulo a una sesión

Debido a que los recursos compartidos de sesión nulos no requieren autenticación, los clientes que requieren acceso de sesión nulo deben tener sus direcciones IP asignadas en el sistema de almacenamiento.

De forma predeterminada, los clientes de sesión nula sin asignar pueden acceder a determinados servicios

del sistema ONTAP, como la enumeración de recursos compartidos, pero se limitan a acceder a cualquier dato del sistema de almacenamiento.



ONTAP admite los valores de configuración del Registro RestrictAnónimo de Windows con `-restrict-anonymous` opción. Esto permite controlar hasta qué punto los usuarios nulos no asignados pueden ver o acceder a los recursos del sistema. Por ejemplo, puede deshabilitar la enumeración de recursos compartidos y el acceso al recurso compartido IPC\$ (recurso compartido de canalizaciones con nombre oculto). La `vserver cifs options modify` y `vserver cifs options show` las páginas de manual proporcionan más información sobre el `-restrict-anonymous` opción.

A menos que se configure lo contrario, un cliente que ejecute un proceso local que solicite acceso al sistema de almacenamiento a través de una sesión nula sólo es miembro de grupos no restrictivos, como «'todos'». Para limitar el acceso de sesión nulo a los recursos del sistema de almacenamiento seleccionados, es posible que desee crear un grupo al que pertenecen todos los clientes de sesión nulos; al crear este grupo se le permite restringir el acceso al sistema de almacenamiento y establecer permisos de recursos del sistema de almacenamiento que se aplican específicamente a clientes de sesión nulos.

ONTAP proporciona una sintaxis de asignación en `vserver name-mapping`. El conjunto de comandos permite especificar la dirección IP de los clientes que pueden acceder a los recursos del sistema de almacenamiento mediante una sesión de usuario nula. Después de crear un grupo para usuarios nulos, puede especificar restricciones de acceso para los recursos del sistema de almacenamiento y permisos de recursos que se apliquen solo a sesiones nulas. El usuario nulo se identifica como inicio de sesión anónimo. Los usuarios nulos no tienen acceso a ningún directorio principal.

Todos los usuarios nulos que acceden al sistema de almacenamiento desde una dirección IP asignada se conceden permisos de usuario asignado. Considere las precauciones adecuadas para evitar el acceso no autorizado a sistemas de almacenamiento asignados con usuarios nulos. Para obtener la máxima protección, coloque el sistema de almacenamiento y todos los clientes que necesiten un acceso nulo al sistema de almacenamiento de usuarios en una red independiente, con el fin de eliminar la posibilidad de que se produzca una dirección IP «posing».

### Información relacionada

[Configuración de restricciones de acceso para usuarios anónimos](#)

### Conceda a usuarios nulos acceso a recursos compartidos del sistema de archivos

Puede permitir el acceso a los recursos del sistema de almacenamiento por parte de clientes de sesión nulos asignando un grupo para que lo utilicen clientes de sesión nulos y registrando las direcciones IP de clientes de sesión nulos para añadirlas a la lista de clientes a los que el sistema de almacenamiento puede acceder a los datos mediante sesiones nulas.

### Pasos

1. Utilice la `vserver name-mapping create` Comando para asignar el usuario nulo a cualquier usuario válido de Windows, con un calificador IP.

El siguiente comando asigna el usuario nulo al usuario1 con un nombre de host válido google.com:

```
vserver name-mapping create -direction win-unix -position 1 -pattern
"ANONYMOUS LOGON" -replacement user1 - hostname google.com
```

El siguiente comando asigna el usuario nulo a user1 con una dirección IP válida 10.238.2.54/32:

```
vserver name-mapping create -direction win-unix -position 2 -pattern
"ANONYMOUS LOGON" -replacement user1 -address 10.238.2.54/32
```

2. Utilice la `vserver name-mapping show` comando para confirmar la asignación de nombres.

```
vserver name-mapping show

Vserver: vs1
Direction: win-unix
Position Hostname IP Address/Mask

1 - 10.72.40.83/32 Pattern: anonymous logon
 Replacement: user1
```

3. Utilice la `vserver cifs options modify -win-name-for-null-user` Comando para asignar la pertenencia a Windows al usuario nulo.

Esta opción sólo se aplica cuando hay una asignación de nombres válida para el usuario nulo.

```
vserver cifs options modify -win-name-for-null-user user1
```

4. Utilice la `vserver cifs options show` Comando para confirmar la asignación del usuario nulo al usuario o grupo de Windows.

```
vserver cifs options show

Vserver :vs1

Map Null User to Windows User of Group: user1
```

## Administrar alias NetBIOS para servidores SMB

### Información general sobre la administración de alias NetBIOS para servidores SMB

Los alias NetBIOS son nombres alternativos para el servidor SMB que los clientes SMB pueden utilizar al conectarse con el servidor SMB. La configuración de alias NetBIOS para un servidor SMB puede ser útil cuando está consolidando datos de otros servidores

de archivos en el servidor SMB y desea que el servidor SMB responda a los nombres de los servidores de archivos originales.

Puede especificar una lista de alias NetBIOS cuando cree el servidor SMB o en cualquier momento después de crear el servidor SMB. Puede agregar o quitar alias NetBIOS de la lista en cualquier momento. Puede conectarse al servidor SMB utilizando cualquiera de los nombres de la lista de alias NetBIOS.

### Información relacionada

[Visualización de información acerca de NetBIOS sobre conexiones TCP](#)

### Agregue una lista de alias NetBIOS al servidor SMB

Si desea que los clientes SMB se conecten al servidor SMB mediante un alias, puede crear una lista de alias NetBIOS o agregar alias NetBIOS a una lista existente de alias NetBIOS.

### Acerca de esta tarea

- El nombre del alias NetBIOS puede tener una longitud máxima de 15 caracteres.
- Puede configurar hasta 200 alias NetBIOS en el servidor SMB.
- No se permiten los siguientes caracteres:

@ # \* ( ) = + [ ] | ; : ' , < > \ / ?

### Pasos

1. Agregue los alias NetBIOS:

```
vserver cifs add-netbios-aliases -vserver vserver_name -netbios-aliases
NetBIOS_alias,...
```

```
vserver cifs add-netbios-aliases -vserver vs1 -netbios-aliases
alias_1,alias_2,alias_3
```

- Puede especificar uno o varios alias NetBIOS utilizando una lista delimitada por comas.
- Los alias NetBIOS especificados se agregan a la lista existente.
- Se crea una nueva lista de alias NetBIOS si la lista está vacía actualmente.

2. Compruebe que los alias NetBIOS se han agregado correctamente: `vserver cifs show -vserver vserver_name -display-netbios-aliases`

```
vserver cifs show -vserver vs1 -display-netbios-aliases
```

```
Vserver: vs1
```

```
Server Name: CIFS_SERVER
```

```
NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

### Información relacionada

[Quitar alias NetBIOS de la lista de alias NetBIOS](#)

Se muestra la lista de alias NetBIOS en los servidores CIFS

Eliminar alias NetBIOS de la lista de alias NetBIOS

Si no necesita alias NetBIOS específicos para un servidor CIFS, puede eliminar esos alias NetBIOS de la lista. También puede quitar todos los alias NetBIOS de la lista.

Acerca de esta tarea

Puede quitar más de un alias NetBIOS utilizando una lista delimitada por comas. Puede eliminar todos los alias NetBIOS de un servidor CIFS especificando - como valor para -netbios-aliases parámetro.

Pasos

- 1. Ejecute una de las siguientes acciones:

| Si desea quitar...                    | Introduzca...                                                                                                 |
|---------------------------------------|---------------------------------------------------------------------------------------------------------------|
| Alias NetBIOS específicos de la lista | <code>vserver cifs remove-netbios-aliases -vserver _vserver_name_ -netbios-aliases _NetBIOS_alias_,...</code> |
| Todos los alias NetBIOS de la lista   | <code>vserver cifs remove-netbios-aliases -vserver vserver_name -netbios-aliases -</code>                     |

```
vserver cifs remove-netbios-aliases -vserver vs1 -netbios-aliases alias_1
```

- 2. Compruebe que se han eliminado los alias NetBIOS especificados: `vserver cifs show -vserver vserver_name -display-netbios-aliases`

```
vserver cifs show -vserver vs1 -display-netbios-aliases
```

```
Vserver: vs1

Server Name: CIFS_SERVER
NetBIOS Aliases: ALIAS_2, ALIAS_3
```

Muestre la lista de alias NetBIOS en los servidores CIFS

Puede mostrar la lista de alias NetBIOS. Esto puede resultar útil cuando desea determinar la lista de nombres a través de la cual los clientes SMB pueden realizar conexiones con el servidor CIFS.

Paso

- 1. Ejecute una de las siguientes acciones:

| Si desea mostrar información acerca de...                                          | Introduzca...                                            |
|------------------------------------------------------------------------------------|----------------------------------------------------------|
| Alias de NetBIOS de un servidor CIFS                                               | <code>vserver cifs show -display-netbios -aliases</code> |
| La lista de alias NetBIOS como parte de la información detallada del servidor CIFS | <code>vserver cifs show -instance</code>                 |

En el siguiente ejemplo, se muestra información sobre los alias NetBIOS de un servidor CIFS:

```
vserver cifs show -display-netbios-aliases
```

```
Vserver: vs1
```

```
Server Name: CIFS_SERVER
```

```
NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

En el siguiente ejemplo, se muestra la lista de alias NetBIOS como parte de la información detallada del servidor CIFS:

```
vserver cifs show -instance
```

```

Vserver: vs1
CIFS Server NetBIOS Name: CIFS_SERVER
NetBIOS Domain/Workgroup Name: EXAMPLE
Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
Authentication Style: domain
CIFS Server Administrative Status: up
CIFS Server Description:
List of NetBIOS Aliases: ALIAS_1, ALIAS_2,
ALIAS_3
```

Consulte la página man de los comandos para obtener más información.

## Información relacionada

[Agregando una lista de alias NetBIOS al servidor CIFS](#)

[Comandos para gestionar servidores CIFS](#)

## Determine si los clientes SMB están conectados mediante alias NetBIOS

Puede determinar si los clientes SMB están conectados mediante alias NetBIOS y, si es así, qué alias NetBIOS se utiliza para realizar la conexión. Esto puede ser útil para solucionar problemas de conexión.

**Acerca de esta tarea**

Debe utilizar el `-instance` Parámetro para mostrar el alias NetBIOS (si lo hay) asociado a una conexión SMB. Si se utiliza el nombre del servidor CIFS o una dirección IP para realizar la conexión SMB, el resultado del NetBIOS Name el campo es `-` (guión).

**Paso**

- 1. Realice la acción deseada:

| Si desea mostrar información de NetBIOS para...        | Introduzca...                                                                      |
|--------------------------------------------------------|------------------------------------------------------------------------------------|
| Conexiones SMB                                         | <code>vserver cifs session show -instance</code>                                   |
| Conexiones que utilizan un alias NetBIOS especificado: | <code>vserver cifs session show -instance -netbios-name <i>netbios_name</i></code> |

En el siguiente ejemplo se muestra información sobre el alias NetBIOS utilizado para establecer la conexión SMB con el ID de sesión 1:

```
vserver cifs session show -session-id 1 -instance
```

```
Node: node1
Vserver: vs1
Session ID: 1
Connection ID: 127834
Incoming Data LIF IP Address: 10.1.1.25
Workstation: 10.2.2.50
Authentication Mechanism: NTLMv2
Windows User: EXAMPLE\user1
UNIX User: user1
Open Shares: 2
Open Files: 2
Open Other: 0
Connected Time: 1d 1h 10m 5s
Idle Time: 22s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: true
User Authenticated as: domain-user
NetBIOS Name: ALIAS1
SMB Encryption Status: Unencrypted
```

**Administrar varias tareas del servidor SMB**

**Detenga o inicie el servidor CIFS**

Puede detener el servidor CIFS en una SVM, que puede ser útil a la hora de realizar

tareas mientras los usuarios no acceden a datos a través de recursos compartidos SMB. Puede reiniciar el acceso SMB iniciando el servidor CIFS. Al detener el servidor CIFS, también puede modificar los protocolos permitidos en la máquina virtual de almacenamiento (SVM).

**Pasos**

1. Ejecute una de las siguientes acciones:

| Si desea...                                                               | Introduzca el comando...                                                 |
|---------------------------------------------------------------------------|--------------------------------------------------------------------------|
| Detenga el servidor CIFS                                                  | <code>`vserver cifs stop -vserver vserver_name [-foreground {true</code> |
| <code>false}]]`</code>                                                    | Inicie el servidor CIFS                                                  |
| <code>`vserver cifs start -vserver vserver_name [-foreground {true</code> | <code>false}]]`</code>                                                   |

-foreground especifica si el comando debe ejecutarse en primer plano o fondo. Si no se introduce este parámetro, se configura en true, y el comando se ejecuta en primer plano.

2. Compruebe que el estado administrativo del servidor CIFS es correcto mediante el `vserver cifs show` comando.

**Ejemplo**

Los siguientes comandos inician el servidor CIFS en la SVM vs1:

```

cluster1::> vserver cifs start -vserver vs1

cluster1::> vserver cifs show -vserver vs1

 Vserver: vs1
 CIFS Server NetBIOS Name: VS1
 NetBIOS Domain/Workgroup Name: DOMAIN
 Fully Qualified Domain Name: DOMAIN.LOCAL
Default Site Used by LIFs Without Site Membership:
 Authentication Style: domain
 CIFS Server Administrative Status: up

```

**Información relacionada**

[Mostrar información sobre los servidores detectados](#)

[Restablecer y volver a descubrir servidores](#)

**Mueva servidores CIFS a unidades organizativas diferentes**

El proceso de creación del servidor CIFS utiliza la unidad organizativa (OU)



CN=Computers predeterminada durante la instalación, a menos que especifique una unidad organizativa diferente. Puede mover servidores CIFS a unidades organizativas diferentes tras la configuración.

### Pasos

1. En el servidor Windows, abra el árbol **usuarios y equipos de Active Directory**.
2. Busque el objeto de Active Directory para la máquina virtual de almacenamiento (SVM).
3. Haga clic con el botón derecho del ratón en el objeto y seleccione **mover**.
4. Seleccione la unidad organizativa que desea asociar con la SVM

### Resultados

El objeto SVM se coloca en la unidad organizativa seleccionada.

### Modifique el dominio DNS dinámico en la SVM antes de mover el servidor SMB

Si desea que el servidor DNS integrado en Active Directory registre de forma dinámica los registros DNS del servidor SMB en DNS cuando mueve el servidor SMB a otro dominio, debe modificar el DNS dinámico (DDNS) en la máquina virtual de almacenamiento (SVM) antes de mover el servidor SMB.

### Antes de empezar

Los servicios de nombres DNS se deben modificar en la SVM para utilizar el dominio DNS que contiene los registros de ubicación del servicio para el nuevo dominio que contendrá la cuenta de equipo del servidor SMB. Si utiliza DDNS seguro, debe utilizar servidores de nombres DNS integrados en Active Directory.

### Acerca de esta tarea

Si bien DDNS (si se configura en la SVM) agrega automáticamente los registros DNS de las LIF de datos al dominio nuevo, los registros DNS del dominio original no se eliminan automáticamente del servidor DNS original. Debe eliminarlos manualmente.

Para completar las modificaciones de DDNS antes de mover el servidor SMB, consulte el siguiente tema:

["Configure los servicios DNS dinámicos"](#)

### Una SVM a un dominio de Active Directory

Puede unirse a una máquina virtual de almacenamiento (SVM) a un dominio de Active Directory sin eliminar el servidor SMB existente modificando el dominio mediante el `vserver cifs modify` comando. Puede volver a unirse al dominio actual o unirse a uno nuevo.

### Antes de empezar

- La SVM ya debe tener una configuración de DNS.
- La configuración de DNS para la SVM debe poder servir el dominio de destino.

Los servidores DNS deben contener los registros de ubicación de servicio (SRV) para el LDAP de dominio y los servidores del controlador de dominio.

### Acerca de esta tarea

- El estado administrativo del servidor CIFS debe definirse en «dirección» para proceder con la modificación de dominio de Active Directory.
- Si el comando se completa correctamente, el estado administrativo se establece automáticamente en "up".
- Al unirse a un dominio, este comando puede tardar varios minutos en completarse.

## Pasos

1. Una la SVM al dominio de servidor CIFS: `vserver cifs modify -vserver vserver_name -domain domain_name -status-admin down`

Para obtener más información, consulte la página de manual de `vserver cifs modify` comando. Si necesita volver a configurar DNS para el nuevo dominio, consulte la página `man` de `vserver dns modify` comando.

Para crear una cuenta de equipo de Active Directory para el servidor SMB, debe proporcionar el nombre y la contraseña de una cuenta de Windows con privilegios suficientes para agregar equipos al `ou=example` ou contenedor dentro de `example` dominio .com.

A partir de ONTAP 9.7, el administrador de AD puede proporcionarle un URI a un archivo keytab como alternativa a proporcionarle un nombre y una contraseña a una cuenta de Windows con privilegios. Cuando reciba el URI, inclúyalo en el `-keytab-uri` con el `vserver cifs` comandos.

2. Compruebe que el servidor CIFS esté en el dominio de Active Directory deseado: `vserver cifs show`

## Ejemplo

En el siguiente ejemplo, el servidor SMB «CIFSSERVER1» de la SVM `vs1` se une al dominio `example.com` mediante la autenticación keytab:

```
cluster1::> vserver cifs modify -vserver vs1 -domain example.com -status
-admin down -keytab-uri http://admin.example.com/ontap1.keytab
```

```
cluster1::> vserver cifs show
```

|         | Server      | Status | Domain/Workgroup | Authentication |
|---------|-------------|--------|------------------|----------------|
| Vserver | Name        | Admin  | Name             | Style          |
| -----   | -----       | -----  | -----            | -----          |
| vs1     | CIFSSERVER1 | up     | EXAMPLE          | domain         |

## Muestra información acerca de NetBIOS sobre conexiones TCP

Puede mostrar información acerca de las conexiones NetBIOS sobre TCP (NBT). Esto puede ser útil para solucionar problemas relacionados con NetBIOS.

## Paso

1. Utilice la `vserver cifs nbtstat` Comando para mostrar información acerca de NetBIOS sobre conexiones TCP.



No se admite el servicio de nombres NetBIOS (NBNS) sobre IPv6.

Ejemplo

En el siguiente ejemplo se muestra la información del servicio de nombres NetBIOS que se muestra para "cluster1":

```
cluster1::> vserver cifs nbtstat

Vserver: vs1
Node: cluster1-01
Interfaces:
 10.10.10.32
 10.10.10.33
Servers:
 17.17.1.2 (active)
NBT Scope:
 []
NBT Mode:
 [h]
NBT Name NetBIOS Suffix State Time Left Type

CLUSTER_1 00 wins 57
CLUSTER_1 20 wins 57

Vserver: vs1
Node: cluster1-02
Interfaces:
 10.10.10.35
Servers:
 17.17.1.2 (active)
CLUSTER_1 00 wins 58
CLUSTER_1 20 wins 58
4 entries were displayed.
```

Comandos para gestionar servidores SMB

Debe conocer los comandos para crear, mostrar, modificar, detener, iniciar, Y eliminando servidores SMB. También hay comandos para restablecer y volver a detectar servidores, cambiar o restablecer contraseñas de cuentas de equipo, programar cambios para contraseñas de cuentas de equipo y agregar o quitar alias de NetBIOS.

|                                               |                        |
|-----------------------------------------------|------------------------|
| Si desea...                                   | Se usa este comando... |
| Cree un servidor SMB                          | vserver cifs create    |
| Muestra información acerca de un servidor SMB | vserver cifs show      |

|                                                                                       |                                                                       |
|---------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| Modificar un servidor SMB                                                             | <code>vserver cifs modify</code>                                      |
| Mover un servidor SMB a otro dominio                                                  | <code>vserver cifs modify</code>                                      |
| Detener un servidor SMB                                                               | <code>vserver cifs stop</code>                                        |
| Inicie un servidor SMB                                                                | <code>vserver cifs start</code>                                       |
| Suprimir un servidor SMB                                                              | <code>vserver cifs delete</code>                                      |
| Restablecer y volver a detectar servidores para el servidor SMB                       | <code>vserver cifs domain discovered-servers<br/>reset-servers</code> |
| Cambiar la contraseña de la cuenta de equipo del servidor SMB                         | <code>vserver cifs domain password change</code>                      |
| Restablezca la contraseña de la cuenta de máquina del servidor SMB                    | <code>vserver cifs domain password change</code>                      |
| Programar cambios automáticos de contraseña para la cuenta de equipo del servidor SMB | <code>vserver cifs domain password schedule<br/>modify</code>         |
| Agregue alias NetBIOS para el servidor SMB                                            | <code>vserver cifs add-netbios-aliases</code>                         |
| Elimine los alias de NetBIOS para el servidor SMB                                     | <code>vserver cifs remove-netbios-aliases</code>                      |

Consulte la página de manual de cada comando para obtener más información.

### Información relacionada

["Qué sucede a los usuarios locales y grupos al eliminar servidores SMB"](#)

### Habilite el servicio de nombres NetBIOS

A partir de ONTAP 9, el servicio de nombres NetBIOS (NBNS, a veces denominado Servicio de nombres Internet de Windows o WINS) está deshabilitado de forma predeterminada. Anteriormente, las máquinas virtuales de almacenamiento (SVM) habilitadas para CIFS enviaron registros de nombres independientemente de si se habilitó WINS en una red. Para limitar dichas emisiones a configuraciones en las que se necesita NBNS, debe habilitar NBNS explícitamente para servidores CIFS nuevos.

### Antes de empezar

- Si ya está utilizando NBNS y actualiza a ONTAP 9, no es necesario completar esta tarea. NBNS continuará trabajando como antes.
- NBNS está habilitado en UDP (puerto 137).
- No se admite NBNS sobre IPv6.

## Pasos

1. Configure el nivel de privilegio en Advanced.

```
set -privilege advanced
```

2. Habilite NBNS en un servidor CIFS.

```
vserver cifs options modify -vserver <vserver name> -is-nbns-enabled true
```

3. Vuelva al nivel de privilegio de administrador.

```
set -privilege admin
```

## Utilice IPv6 para el acceso a SMB y los servicios SMB

### Requisitos para usar IPv6

Antes de poder utilizar IPv6 en el servidor SMB, debe saber qué versiones de ONTAP y SMB admiten y cuáles son los requisitos de licencia.

### Requisitos para la licencia de ONTAP

No se requiere ninguna licencia especial para IPv6 cuando SMB tiene licencia. La licencia SMB se incluye con "ONTAP One". Si no tiene ONTAP One y la licencia no está instalada, póngase en contacto con su representante de ventas.

### Requisitos de la versión del protocolo SMB

- Para las SVM, ONTAP es compatible con IPv6 en todas las versiones del protocolo SMB.



No se admite el servicio de nombres NetBIOS (NBNS) sobre IPv6.

### Compatibilidad con IPv6 con acceso SMB y servicios CIFS

Si desea usar IPv6 en el servidor CIFS, debe saber cómo ONTAP admite IPv6 para el acceso SMB y la comunicación de redes para servicios CIFS.

### Compatibilidad con clientes y servidores Windows

ONTAP ofrece compatibilidad con los servidores y clientes de Windows que admiten IPv6. A continuación se describe la compatibilidad con IPv6 del cliente Microsoft Windows y el servidor:

- Windows 7, Windows 8, Windows Server 2008, Windows Server 2012 y versiones posteriores admiten IPv6 tanto para el uso compartido de archivos SMB como para los servicios de Active Directory, incluidos los servicios DNS, LDAP, CLDAP y Kerberos.

Si se han configurado direcciones IPv6, Windows 7 y Windows Server 2008 y versiones posteriores utilizan IPv6 de forma predeterminada para los servicios de Active Directory. Se admiten tanto la autenticación NTLM como la autenticación Kerberos a través de conexiones IPv6.

Todos los clientes de Windows compatibles con ONTAP pueden conectarse a recursos compartidos de SMB mediante direcciones IPv6.

Para obtener la información más reciente sobre los clientes de Windows compatibles con ONTAP, consulte la ["Matriz de interoperabilidad"](#).



Los dominios NT no son compatibles con IPv6.

### **Compatibilidad adicional con servicios CIFS**

Además de la compatibilidad con IPv6 para recursos compartidos de archivos SMB y servicios de Active Directory, ONTAP ofrece compatibilidad con IPv6 para lo siguiente:

- Servicios de cliente, incluidas carpetas sin conexión, perfiles de itinerancia, redirección de carpetas y versiones anteriores
- Servicios del lado del servidor, incluidos directorios iniciales dinámicos (funcionalidad de Home Directory), enlaces simbólicos y widgets, BranchCache, descarga de copias ODX, referencias automáticas a nodos, Y versiones anteriores
- Servicios de administración de acceso a archivos, incluido el uso de usuarios y grupos locales de Windows para el control de acceso y la administración de derechos, la configuración de permisos de archivos y políticas de auditoría mediante la CLI, el seguimiento de seguridad, la gestión de bloqueos de archivos y la supervisión de la actividad de SMB
- Auditoría multiprotocolo de NAS
- FPolicy
- Recursos compartidos disponibles de forma continua, protocolo de observación y VSS remoto (utilizado con configuraciones de Hyper-V en SMB)

### **Servicio de nombres y soporte del servicio de autenticación**

La comunicación con los siguientes servicios de nombres se admite con IPv6:

- Controladores de dominio
- Servidores DNS
- Servidores LDAP
- Servidores KDC
- Servidores NIS

### **Cómo los servidores CIFS utilizan IPv6 para conectarse a servidores externos**

Para crear una configuración que cumpla con sus requisitos, debe saber cómo usan IPv6 los servidores CIFS a la hora de realizar conexiones a servidores externos.

- Selección de direcciones de origen

Si se intenta conectarse a un servidor externo, la dirección de origen seleccionada debe ser del mismo

tipo que la dirección de destino. Por ejemplo, si se conecta a una dirección IPv6, la máquina virtual de almacenamiento (SVM) que aloja el servidor CIFS debe tener una LIF de datos o una LIF de gestión que tenga una dirección IPv6 que se usará como dirección de origen. Del mismo modo, si se conecta a una dirección IPv4, la SVM debe tener una LIF de datos o una LIF de gestión que tenga una dirección IPv4 que se usará como dirección de origen.

- Para los servidores detectados dinámicamente mediante DNS, la detección de servidores se realiza de la siguiente manera:
  - Si IPv6 está deshabilitado en el clúster, solo se detectan direcciones de los servidores IPv4.
  - Si IPv6 está habilitado en el clúster, se detectan tanto las direcciones de los servidores IPv4 como IPv6. Cualquiera de los dos tipos puede utilizarse en función de la idoneidad del servidor al que pertenece la dirección y de la disponibilidad de LIF de gestión o datos IPv6 o IPv4.  
La detección dinámica de servidores se utiliza para detectar controladores de dominio y sus servicios asociados, como LSA, NETLOGON, Kerberos y LDAP.

- **Conectividad del servidor DNS**

Si la SVM utiliza IPv6 al conectarse a un servidor DNS depende de la configuración de los servicios de nombres DNS. Si los servicios DNS se configuran para usar direcciones IPv6, las conexiones se realizan mediante IPv6. Si lo desea, la configuración de los servicios de nombres DNS puede usar direcciones IPv4, de modo que las conexiones con los servidores DNS sigan usando direcciones IPv4. Al configurar los servicios de nombres DNS, se pueden especificar combinaciones de direcciones IPv4 e IPv6.

- **Conectividad del servidor LDAP**

Si la SVM utiliza IPv6 al conectarse a un servidor LDAP depende de la configuración del cliente LDAP. Si el cliente LDAP está configurado para usar direcciones IPv6, las conexiones se realizan mediante IPv6. Si lo desea, la configuración del cliente LDAP puede usar direcciones IPv4 a fin de que las conexiones con servidores LDAP sigan usando direcciones IPv4. Al configurar la configuración del cliente LDAP, se pueden especificar las combinaciones de direcciones IPv4 e IPv6.



La configuración del cliente LDAP se utiliza al configurar LDAP para los servicios de nombre de usuario, grupo y grupo de redes de UNIX.

- **Conectividad del servidor NIS**

Si la SVM utiliza IPv6 al conectarse a un servidor NIS depende de la configuración de los servicios de nombres NIS. Si los servicios NIS se configuran para utilizar direcciones IPv6, las conexiones se realizan mediante IPv6. Si lo desea, la configuración de los servicios de nombres NIS puede utilizar direcciones IPv4 para que las conexiones con los servidores NIS sigan usando direcciones IPv4. Las combinaciones de direcciones IPv4 e IPv6 pueden especificarse al configurar los servicios de nombres NIS.



Los servicios de nombres NIS se utilizan para almacenar y administrar objetos de usuario, grupo, grupo de red y nombre de host de UNIX.

## **Información relacionada**

[Habilitar IPv6 para SMB \(solo administradores de clúster\)](#)

[Supervisar y mostrar información acerca de las sesiones SMB de IPv6](#)

**Habilitar IPv6 para SMB (solo administradores de clúster)**

Las redes IPv6 no se habilitan durante la configuración del clúster. Un administrador de

clúster debe habilitar IPv6 después de que la configuración del clúster se haya completado a fin de usar IPv6 para SMB. Cuando el administrador de clúster habilita IPv6, se habilita para todo el clúster.

**Paso**

- 1. Habilitar IPv6: `network options ipv6 modify -enabled true`

Para obtener más información acerca de cómo habilitar IPv6 en el clúster y configurar LIF IPv6, consulte *Network Management Guide*.

IPv6 está habilitado. Se pueden configurar LIF de datos IPv6 para el acceso SMB.

**Información relacionada**

[Supervisar y mostrar información acerca de las sesiones SMB de IPv6](#)

["Gestión de redes"](#)

**Deshabilite IPv6 para SMB**

Aunque IPv6 esté habilitado en el clúster mediante una opción de red, no puede deshabilitar IPv6 para SMB con el mismo comando. En su lugar, ONTAP deshabilita IPv6 cuando el administrador de clúster deshabilita la última interfaz habilitada para IPv6 en el clúster. Debe comunicarse con el administrador de clúster acerca de la gestión de las interfaces IPv6 habilitadas.

Para obtener más información acerca de cómo deshabilitar IPv6 en el clúster, consulte *Network Management Guide*.

**Información relacionada**

["Gestión de redes"](#)

**Supervisar y mostrar información acerca de las sesiones SMB de IPv6**

Puede supervisar y mostrar información sobre las sesiones SMB conectadas mediante redes IPv6. Esta información es útil para determinar qué clientes se conectan mediante IPv6, así como otra información útil sobre las sesiones SMB de IPv6.

**Paso**

- 1. Realice la acción deseada:

| Si desea determinar si...                                                                | Introduzca el comando...                                               |
|------------------------------------------------------------------------------------------|------------------------------------------------------------------------|
| Las sesiones SMB a una máquina virtual de almacenamiento (SVM) se conectan mediante IPv6 | <code>vserver cifs session show -vserver vserver_name -instance</code> |



| Si desea determinar si...                                                    | Introduzca el comando...                                                                                                                                               |
|------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IPv6 se utiliza para sesiones SMB a través de una dirección LIF especificada | <pre>vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address -instance</pre> <p><i>LIF_IP_address</i> Es la dirección IPv6 de la LIF de datos.</p> |

## Configure el acceso a archivos mediante SMB

### Configurar estilos de seguridad

#### Cómo afectan los estilos de seguridad al acceso a los datos

#### Cuáles son los estilos de seguridad y sus efectos

Hay cuatro estilos de seguridad diferentes: UNIX, NTFS, mixto y unificado. Cada estilo de seguridad tiene un efecto diferente sobre cómo se gestionan los permisos para los datos. Debe comprender los diferentes efectos para asegurarse de que selecciona el estilo de seguridad adecuado para sus propósitos.

Es importante entender que los estilos de seguridad no determinan qué tipos de clientes pueden o no pueden tener acceso a los datos. Los estilos de seguridad sólo determinan el tipo de permisos que ONTAP utiliza para controlar el acceso a los datos y qué tipo de cliente puede modificar estos permisos.

Por ejemplo, si un volumen utiliza el estilo de seguridad UNIX, los clientes SMB todavía pueden acceder a los datos (siempre y cuando estos se autenticuen y autoricen correctamente) debido a la naturaleza multiprotocolo de ONTAP. Sin embargo, ONTAP utiliza permisos UNIX que sólo los clientes UNIX pueden modificar mediante herramientas nativas.

| Estilo de seguridad | Clientes que pueden modificar permisos | Permisos que pueden utilizar los clientes | El estilo de seguridad efectivo resultante | Clientes que pueden acceder a los ficheros |
|---------------------|----------------------------------------|-------------------------------------------|--------------------------------------------|--------------------------------------------|
| UNIX                | NFS                                    | Bits del modo NFSv3                       | UNIX                                       | NFS y SMB                                  |
| NFSv4.x ACL         | UNIX                                   | NTFS                                      | SMB                                        | ACL de NTFS                                |
| NTFS                | Mixto                                  | NFS o SMB                                 | Bits del modo NFSv3                        | UNIX                                       |
| NFSv4.x ACL         | UNIX                                   | ACL de NTFS                               | NTFS                                       | Unificado                                  |
| NFS o SMB           | Bits del modo NFSv3                    | UNIX                                      | ACL de NFSv4.1                             | UNIX                                       |

| Estilo de seguridad | Clientes que pueden modificar permisos | Permisos que pueden utilizar los clientes                                   | El estilo de seguridad efectivo resultante | Clientes que pueden acceder a los ficheros |
|---------------------|----------------------------------------|-----------------------------------------------------------------------------|--------------------------------------------|--------------------------------------------|
| ACL de NTFS         | NTFS                                   | Unificado (Solo para Infinite Volume, en ONTAP 9,4 y versiones anteriores). | NFS o SMB                                  | Bits del modo NFSv3                        |
| UNIX                | ACL de NFSv4.1                         |                                                                             |                                            | ACL de NTFS                                |

Los volúmenes de FlexVol son compatibles con UNIX, NTFS y estilos de seguridad mixtos. Cuando el estilo de seguridad es mixto o unificado, los permisos efectivos dependen del tipo de cliente que modificó por última vez los permisos porque los usuarios establecen el estilo de seguridad de forma individual. Si el último cliente que modificó permisos era un cliente NFSv3, los permisos son bits del modo NFSv3 de UNIX. Si el último cliente era un cliente NFSv4, los permisos son ACL de NFSv4. Si el último cliente era un cliente SMB, los permisos son ACL de Windows NTFS.

El estilo de seguridad unificado solo está disponible en Infinite Volume, que ya no son compatibles con ONTAP 9.5 y versiones posteriores. Para obtener más información, consulte ["Información general de gestión de volúmenes de FlexGroup"](#).

A partir de ONTAP 9,2, el `show-effective-permissions` parámetro de la `vserver security file-directory` El comando le permite mostrar permisos efectivos otorgados a un usuario de Windows o UNIX en la ruta de archivo o carpeta especificada. Además, el parámetro opcional `-share-name` permite mostrar el permiso de uso compartido efectivo.



ONTAP establece inicialmente algunos permisos de archivo predeterminados. De forma predeterminada, el estilo de seguridad efectivo de todos los datos de los volúmenes de estilo de seguridad mixto y unificado es UNIX y el tipo de permisos efectivos es bits de modo UNIX (0755 a menos que se especifique lo contrario) hasta que un cliente lo configure como permite el estilo de seguridad predeterminado. De forma predeterminada, el estilo de seguridad efectivo en todos los datos de los volúmenes de estilo de seguridad NTFS es NTFS y tiene una ACL que permite un control total para todos.

## Dónde y cuándo establecer estilos de seguridad

Los estilos de seguridad se pueden establecer en volúmenes de FlexVol (tanto volúmenes raíz como de datos) y qtrees. Los estilos de seguridad se pueden configurar manualmente en el momento de la creación, heredados automáticamente o modificados posteriormente.

## Decida qué estilo de seguridad se utilizará en las SVM

Para ayudar a decidir qué estilo de seguridad se debe usar en un volumen, se deben tener en cuenta dos factores. El factor principal es el tipo de administrador que administra el sistema de archivos. El factor secundario es el tipo de usuario o servicio que tiene acceso a los datos del volumen.

Al configurar el estilo de seguridad en un volumen, debe tener en cuenta las necesidades del entorno para garantizar que selecciona el mejor estilo de seguridad y evitar problemas con la gestión de permisos. Las siguientes consideraciones pueden ayudarle a decidir:

| Estilo de seguridad | Elija si...                                                                                                                                                                                                                                                                      |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| UNIX                | <ul style="list-style-type: none"> <li>• Un administrador de UNIX gestiona el sistema de ficheros.</li> <li>• La mayoría de los usuarios son clientes NFS.</li> <li>• Una aplicación que accede a los datos utiliza un usuario UNIX como cuenta de servicio.</li> </ul>          |
| NTFS                | <ul style="list-style-type: none"> <li>• Un administrador de Windows gestiona el sistema de archivos.</li> <li>• La mayoría de los usuarios son clientes SMB.</li> <li>• Una aplicación que accede a los datos utiliza un usuario de Windows como cuenta de servicio.</li> </ul> |
| Mixto               | El sistema de archivos lo gestionan administradores de UNIX y Windows, y los usuarios están formados por clientes NFS y SMB.                                                                                                                                                     |

### Cómo funciona la herencia de estilos de seguridad

Si no especifica el estilo de seguridad al crear un nuevo volumen de FlexVol o un qtree, hereda su estilo de seguridad de formas diferentes.

Los estilos de seguridad se heredan de la siguiente manera:

- Un volumen FlexVol hereda el estilo de seguridad del volumen raíz de su SVM que contiene.
- Un qtree hereda el estilo de seguridad del volumen FlexVol que contiene.
- Un archivo o un directorio hereda el estilo de seguridad de su volumen o qtree de FlexVol.

### Cómo ONTAP conserva los permisos de UNIX

Cuando las aplicaciones Windows editan y guardan archivos de un volumen FlexVol que actualmente tienen permisos UNIX, ONTAP puede preservar los permisos UNIX.

Cuando las aplicaciones de clientes de Windows editan y guardan archivos, leen las propiedades de seguridad del archivo, crean un nuevo archivo temporal, aplican esas propiedades al archivo temporal y, a continuación, asignan al archivo temporal el nombre de archivo original.

Cuando los clientes de Windows realizan una consulta para las propiedades de seguridad, reciben una ACL construida que representa exactamente los permisos de UNIX. El único propósito de esta ACL construida es preservar los permisos UNIX del archivo a medida que las aplicaciones de Windows actualizan los archivos para garantizar que los archivos resultantes tengan los mismos permisos UNIX. ONTAP no establece ninguna ACL de NTFS usando la ACL construida.

### Administre los permisos de UNIX mediante la ficha Seguridad de Windows

Si desea manipular los permisos de UNIX de archivos o carpetas en volúmenes o qtrees de estilo de seguridad mixtos en las SVM, puede utilizar la pestaña Seguridad en clientes

de Windows. También puede utilizar aplicaciones que puedan consultar y establecer ACL de Windows.

- **Modificación de permisos de UNIX**

Puede usar la pestaña Seguridad de Windows para ver y cambiar los permisos de UNIX para un volumen o un qtree de estilo de seguridad mixto. Si utiliza la ficha Seguridad de Windows principal para cambiar los permisos de UNIX, primero debe quitar la ACE existente que desea editar (esto establece los bits de modo en 0) antes de realizar los cambios. De forma alternativa, puede utilizar el editor avanzado para cambiar los permisos.

Si se utilizan permisos de modo, puede cambiar directamente los permisos de modo para el UID, GID y otros (todos los demás con una cuenta en el equipo) de la lista. Por ejemplo, si el UID mostrado tiene permisos r-x, puede cambiar los permisos de UID a rwx.

- **Cambiar los permisos de UNIX a los permisos NTFS**

Puede usar la pestaña Seguridad de Windows para reemplazar objetos de seguridad UNIX por objetos de seguridad de Windows en un volumen o qtree de estilo de seguridad mixto donde los archivos y carpetas tienen un estilo de seguridad efectivo de UNIX.

Primero debe quitar todas las entradas de permisos de UNIX enumeradas antes de que pueda reemplazarlas con los objetos de usuario y grupo de Windows deseados. A continuación, puede configurar ACL basados en NTFS en los objetos Usuario y Grupo de Windows. Si quita todos los objetos de seguridad de UNIX y agrega sólo usuarios y grupos de Windows a un archivo o carpeta de un volumen o qtree de estilo de seguridad mixto, cambie el estilo de seguridad efectivo del archivo o carpeta de UNIX a NTFS.

Al cambiar los permisos de una carpeta, el comportamiento predeterminado de Windows es propagar estos cambios a todas las subcarpetas y archivos. Por lo tanto, debe cambiar la opción de propagación a la configuración deseada si no desea propagar un cambio en el estilo de seguridad a todas las carpetas secundarias, subcarpetas y archivos.

### **Configurar estilos de seguridad en volúmenes raíz de SVM**

El estilo de seguridad del volumen raíz de la máquina virtual de almacenamiento (SVM) se configura para determinar el tipo de permisos utilizados para los datos en el volumen raíz de la SVM.

#### **Pasos**

1. Utilice la `vserver create` con el `-rootvolume-security-style` parámetro para definir el estilo de seguridad.

Las opciones posibles para el estilo de seguridad del volumen raíz son `unix`, `ntfs`, o `mixed`.

2. Mostrar y verificar la configuración, incluido el estilo de seguridad del volumen raíz de la SVM que creó:

```
vserver show -vserver vserver_name
```

### **Configurar estilos de seguridad en volúmenes FlexVol**

El estilo de seguridad del volumen FlexVol se configura para determinar el tipo de permisos utilizados para los datos en volúmenes FlexVol de la máquina virtual de almacenamiento (SVM).

## Pasos

1. Ejecute una de las siguientes acciones:

| Si el volumen de FlexVol... | Usar el comando...                                                                                                      |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Aún no existe               | <code>volume create</code> e incluya la <code>-security-style</code> parámetro para especificar el estilo de seguridad. |
| Ya existe                   | <code>volume modify</code> e incluya la <code>-security-style</code> parámetro para especificar el estilo de seguridad. |

Las posibles opciones para el estilo de seguridad del volumen FlexVol son `unix`, `ntfs`, o `mixed`.

Si no se especifica un estilo de seguridad al crear un volumen FlexVol, el volumen hereda el estilo de seguridad del volumen raíz.

Para obtener más información acerca de `volume create` o `volume modify` comandos, consulte ["Gestión de almacenamiento lógico"](#).

2. Para ver la configuración, incluido el estilo de seguridad del volumen FlexVol que se creó, escriba el siguiente comando:

```
volume show -volume volume_name -instance
```

## Configurar estilos de seguridad en qtrees

El estilo de seguridad del volumen de qtrees se configura para determinar el tipo de permisos utilizados para los datos en qtrees.

## Pasos

1. Ejecute una de las siguientes acciones:

| Si el qtree... | Usar el comando...                                                                                                            |
|----------------|-------------------------------------------------------------------------------------------------------------------------------|
| Aún no existe  | <code>volume qtree create</code> e incluya la <code>-security-style</code> parámetro para especificar el estilo de seguridad. |
| Ya existe      | <code>volume qtree modify</code> e incluya la <code>-security-style</code> parámetro para especificar el estilo de seguridad. |

Las posibles opciones para el estilo de seguridad para qtrees son `unix`, `ntfs`, o `mixed`.

Si no se especifica un estilo de seguridad al crear un qtree, el estilo de seguridad predeterminado es `mixed`.

Para obtener más información acerca de `volume qtree create` o `volume qtree modify` comandos, consulte ["Gestión de almacenamiento lógico"](#).

2. Para ver la configuración, incluido el estilo de seguridad del qtree que ha creado, escriba el siguiente comando: `volume qtree show -qtree qtree_name -instance`

## Cree y gestione volúmenes de datos en espacios de nombres NAS

### Creación y administración de volúmenes de datos en espacios de nombres NAS Información general

Para gestionar el acceso a archivos en un entorno NAS, debe gestionar volúmenes de datos y puntos de unión en la máquina virtual de almacenamiento (SVM). Esto incluye planificar la arquitectura de espacios de nombres, crear volúmenes con o sin puntos de unión, montar o desmontar volúmenes, y mostrar información sobre volúmenes de datos y espacios de nombres de servidores NFS o servidores CIFS.

#### Cree volúmenes de datos con puntos de unión especificados

Puede especificar el punto de unión cuando crea un volumen de datos. El volumen resultante se monta automáticamente en el punto de unión y se puede configurar inmediatamente para el acceso NAS.

#### Antes de empezar

El agregado en el que desea crear el volumen ya debe existir.



Los siguientes caracteres no se pueden utilizar en la ruta de unión: `* # " > < | ? \`

Además, la longitud de la ruta de unión no puede ser superior a 255 caracteres.

#### Pasos

1. Cree el volumen con un punto de unión: `volume create -vserver vservers_name -volume volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed} -junction-path junction_path`

La ruta de unión debe comenzar con la raíz (/) y puede contener tanto directorios como volúmenes con conexiones. No es necesario que la ruta de unión contenga el nombre del volumen. Las rutas de unión son independientes del nombre del volumen.

Es opcional especificar un estilo de seguridad del volumen. Si no se especifica un estilo de seguridad, ONTAP crea el volumen con el mismo estilo de seguridad que se aplica al volumen raíz de la máquina virtual de almacenamiento (SVM). Sin embargo, es posible que el estilo de seguridad del volumen raíz no sea el estilo de seguridad que se desea aplicar al volumen de datos que se crea. La recomendación es especificar el estilo de seguridad al crear el volumen para minimizar los problemas de acceso a archivos difíciles de solucionar.

La ruta de unión no distingue mayúsculas y minúsculas; /ENG es igual que /eng. Si crea un recurso compartido CIFS, Windows trata la ruta de unión como si fuera sensible a mayúsculas de minúsculas. Por ejemplo, si la unión es /ENG, La ruta de acceso de un recurso compartido CIFS debe comenzar con /ENG, no /eng.

Existen muchos parámetros opcionales que se pueden usar para personalizar un volumen de datos. Para aprender más sobre ellos, consulte las páginas de manual de `volume create` comando.

2. Compruebe que el volumen se ha creado con el punto de unión deseado: `volume show -vserver`

```
vserver_name -volume volume_name -junction
```

## Ejemplo

En el siguiente ejemplo se crea un volumen denominado «home4» ubicado en la SVM vs1 que tiene una ruta de unión /eng/home:

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1 -volume home4 -junction
```

|         |        | Junction |               | Junction  |        |
|---------|--------|----------|---------------|-----------|--------|
| Vserver | Volume | Active   | Junction Path | Path      | Source |
| -----   | -----  | -----    | -----         | -----     | -----  |
| vs1     | home4  | true     | /eng/home     | RW_volume |        |

## Cree volúmenes de datos sin especificar puntos de unión

Puede crear un volumen de datos sin especificar un punto de unión. El volumen resultante no se monta automáticamente y no se puede configurar para acceso NAS. Debe montar el volumen para poder configurar los recursos compartidos de SMB o las exportaciones de NFS de ese volumen.

## Antes de empezar

El agregado en el que desea crear el volumen ya debe existir.

## Pasos

1. Cree el volumen sin un punto de unión mediante el siguiente comando: `volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed}`

Es opcional especificar un estilo de seguridad del volumen. Si no se especifica un estilo de seguridad, ONTAP crea el volumen con el mismo estilo de seguridad que se aplica al volumen raíz de la máquina virtual de almacenamiento (SVM). Sin embargo, es posible que el estilo de seguridad del volumen raíz no sea el estilo de seguridad que se desea aplicar al volumen de datos. La recomendación es especificar el estilo de seguridad al crear el volumen para minimizar los problemas de acceso a archivos difíciles de solucionar.

Existen muchos parámetros opcionales que se pueden usar para personalizar un volumen de datos. Para aprender más sobre ellos, consulte las páginas de manual de `volume create` comando.

2. Compruebe que el volumen se ha creado sin un punto de unión: `volume show -vserver vserver_name -volume volume_name -junction`

## Ejemplo

En el siguiente ejemplo se crea un volumen denominado «números» ubicado en la SVM vs1 que no se monta en un punto de unión:

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1 -junction
```

| Vserver | Volume   | Active | Junction Path | Junction Path Source |
|---------|----------|--------|---------------|----------------------|
| vs1     | data     | true   | /data         | RW_volume            |
| vs1     | home4    | true   | /eng/home     | RW_volume            |
| vs1     | vs1_root | -      | /             | -                    |
| vs1     | sales    | -      | -             | -                    |

## Monte o desmonte volúmenes existentes en el espacio de nombres NAS

Un volumen se debe montar en el espacio de nombres NAS para poder configurar el acceso de clientes NAS a los datos contenidos en los volúmenes de la máquina virtual de almacenamiento (SVM). Puede montar un volumen en un punto de unión si no está montado actualmente. También es posible desmontar volúmenes.

### Acerca de esta tarea

Si desmonta y desconecta un volumen, los clientes NAS no pueden acceder a todos los datos dentro del punto de unión, incluidos los datos en los volúmenes con puntos de unión ubicados en el espacio de nombres del volumen sin montar.



Para interrumpir el acceso de un cliente NAS a un volumen, no basta con desmontar el volumen. Debe desconectar el volumen o realizar otros pasos para garantizar que las cachés del identificador de archivos del cliente se invaliden. Para obtener más información, consulte el siguiente artículo de la base de conocimientos: ["Los clientes NFSv3 siguen teniendo acceso a un volumen después de eliminarse del espacio de nombres de ONTAP"](#)

Cuando desmonta y desconecta un volumen, no se pierden datos dentro del volumen. Además, se conservan las políticas de exportación de volúmenes existentes y los recursos compartidos de SMB creados en el volumen o en directorios y puntos de unión dentro del volumen desmontado. Si vuelve a montar el volumen desmontado, los clientes NAS pueden acceder a los datos contenidos en el volumen mediante políticas de exportación y recursos compartidos SMB existentes.

### Pasos

1. Realice la acción deseada:

| Si desea...       | Introduzca los comandos...                                                                 |
|-------------------|--------------------------------------------------------------------------------------------|
| Montar un volumen | <pre>volume mount -vserver svm_name -volume volume_name -junction-path junction_path</pre> |



| Si desea...          | Introduzca los comandos...                                                                                            |
|----------------------|-----------------------------------------------------------------------------------------------------------------------|
| Desmontar un volumen | <pre>volume unmount -vserver svm_name -volume volume_name  volume offline -vserver svm_name -volume volume_name</pre> |

2. Compruebe que el volumen esté en el estado de montaje deseado:

```
volume show -vserver svm_name -volume volume_name -fields state,junction-
path,junction-active
```

## Ejemplos

El siguiente ejemplo monta un volumen llamado “sales” ubicado en SVM “VS1” al punto de unión “/sales”:

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active
```

| vserver | volume | state  | junction-path | junction-active |
|---------|--------|--------|---------------|-----------------|
| vs1     | data   | online | /data         | true            |
| vs1     | home4  | online | /eng/home     | true            |
| vs1     | sales  | online | /sales        | true            |

El siguiente ejemplo desmonta y desconecta un volumen llamado “data” ubicado en la SVM “VS1”:

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active
```

| vserver | volume | state   | junction-path | junction-active |
|---------|--------|---------|---------------|-----------------|
| vs1     | data   | offline | -             | -               |
| vs1     | home4  | online  | /eng/home     | true            |
| vs1     | sales  | online  | /sales        | true            |

## Muestra información sobre el montaje del volumen y los puntos de unión

Puede ver información sobre los volúmenes montados para las máquinas virtuales de almacenamiento (SVM) y los puntos de unión a los que están montados los volúmenes. También puede determinar qué volúmenes no están montados en un punto de unión.

Esta información se puede usar para comprender y gestionar el espacio de nombres de la SVM.

**Pasos**

1. Realice la acción deseada:

| Si desea mostrar...                                                         | Introduzca el comando...                                                                                                                                                                                                                                                                                                |
|-----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Información resumida sobre los volúmenes montados y desmontados en la SVM   | <code>volume show -vserver vserver_name -junction</code>                                                                                                                                                                                                                                                                |
| Información detallada sobre los volúmenes montados y desmontados en la SVM  | <code>volume show -vserver vserver_name -volume volume_name -instance</code>                                                                                                                                                                                                                                            |
| Información específica sobre los volúmenes montados y desmontados en la SVM | <div>a. Si es necesario, puede mostrar campos válidos para <code>-fields</code> parámetro con el comando siguiente: <code>volume show -fields ?</code></div> <div>b. Muestre la información deseada mediante <code>-fields</code> parámetro: <code>volume show -vserver vserver_name -fields fieldname,...</code></div> |

**Ejemplos**

En el siguiente ejemplo, se muestra un resumen de los volúmenes montados y desmontados en la SVM vs1:

```
cluster1::> volume show -vserver vs1 -junction
```

| Vserver | Volume   | Active | Junction Path | Junction Path Source |
|---------|----------|--------|---------------|----------------------|
| vs1     | data     | true   | /data         | RW_volume            |
| vs1     | home4    | true   | /eng/home     | RW_volume            |
| vs1     | vs1_root | -      | /             | -                    |
| vs1     | sales    | true   | /sales        | RW_volume            |

En el siguiente ejemplo, se muestra información sobre campos especificados para los volúmenes ubicados en la SVM vs2:

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume aggregate size state type security-style junction-path
junction-parent node

vs2 data1 aggr3 2GB online RW unix - -
node3
vs2 data2 aggr3 1GB online RW ntfs /data2
vs2_root node3
vs2 data2_1 aggr3 8GB online RW ntfs /data2/d2_1
data2 node3
vs2 data2_2 aggr3 8GB online RW ntfs /data2/d2_2
data2 node3
vs2 pubs aggr1 1GB online RW unix /publications
vs2_root node1
vs2 images aggr3 2TB online RW ntfs /images
vs2_root node3
vs2 logs aggr1 1GB online RW unix /logs
vs2_root node1
vs2 vs2_root aggr3 1GB online RW ntfs / -
node3
```

## Configurar las asignaciones de nombres

### Configure la información general de asignaciones de nombres

ONTAP utiliza la asignación de nombres para asignar identidades de CIFS a identidades de UNIX, identidades de Kerberos a identidades de UNIX e identidades de UNIX a identidades de CIFS. Necesita esta información para obtener credenciales de usuario y proporcionar un acceso adecuado a los archivos, independientemente de si se conectan desde un cliente NFS o un cliente CIFS.

Existen dos excepciones en las que no es necesario utilizar la asignación de nombres:

- Puede configurar un entorno UNIX puro y no tiene previsto utilizar el estilo de seguridad NTFS o acceso CIFS en los volúmenes.
- En su lugar, puede configurar el usuario predeterminado que se utilizará.

En este escenario, no es necesario asignar nombres porque en lugar de asignar cada credencial de cliente individual todas las credenciales de cliente se asignan al mismo usuario predeterminado.

Tenga en cuenta que sólo puede utilizar la asignación de nombres para usuarios, no para grupos.

Sin embargo, puede asignar un grupo de usuarios individuales a un usuario específico. Por ejemplo, puede asignar todos los usuarios de AD que comiencen o terminen con la palabra SALES a un usuario UNIX

específico y al UID del usuario.

### **Cómo funciona la asignación de nombres**

Cuando ONTAP tiene que asignar credenciales para un usuario, primero comprueba la base de datos de asignación de nombres local y el servidor LDAP para buscar una asignación existente. Si comprueba uno o ambos y en qué orden se determina mediante la configuración del servicio de nombres de la SVM.

- Para la asignación de Windows a UNIX

Si no se encuentra ninguna asignación, ONTAP comprueba si el nombre de usuario de Windows en minúsculas es un nombre de usuario válido en el dominio UNIX. Si esto no funciona, utiliza el usuario UNIX predeterminado siempre que esté configurado. Si el usuario UNIX predeterminado no está configurado y ONTAP no puede obtener una asignación de esta manera, se produce un error en la asignación y se devuelve un error.

- De asignación de UNIX a Windows

Si no se encuentra ninguna asignación, ONTAP intenta encontrar una cuenta de Windows que coincida con el nombre UNIX en el dominio SMB. Si esto no funciona, utiliza el usuario SMB predeterminado, siempre que esté configurado. Si el usuario CIFS predeterminado no está configurado y ONTAP no puede obtener una asignación de esta manera, la asignación falla y se devuelve un error.

Las cuentas de equipo se asignan al usuario UNIX predeterminado especificado de forma predeterminada. Si no se especifica ningún usuario UNIX predeterminado, las asignaciones de cuentas de equipo fallan.

- A partir de ONTAP 9.5, puede asignar cuentas de equipo a usuarios distintos del usuario UNIX predeterminado.
- En ONTAP 9.4 y versiones anteriores, no es posible asignar cuentas de equipo a otros usuarios.

Incluso si se definen las asignaciones de nombre para las cuentas de equipo, las asignaciones se omiten.

### **Busca usuarios de UNIX a través de multidominio para mapeos de nombres de usuario de Windows**

ONTAP admite las búsquedas multidominio al asignar usuarios de UNIX a usuarios de Windows. Se buscan todos los dominios de confianza detectados para que coincidan con el patrón de reemplazo hasta que se devuelva un resultado coincidente. También puede configurar una lista de dominios de confianza preferidos, que se utiliza en lugar de la lista de dominios de confianza detectados y se busca en orden hasta que se devuelve un resultado coincidente.

### **Cómo afectan las confianzas de dominio a las búsquedas de asignación de nombres de usuario de UNIX a Windows**

Para comprender cómo funciona la asignación de nombres de usuario multidominio, debe comprender cómo funcionan las relaciones de confianza de dominios con ONTAP. Las relaciones de confianza de Active Directory con el dominio principal del servidor CIFS pueden ser una confianza bidireccional o pueden ser uno de dos tipos de confianzas unidireccionales, ya sea una confianza de entrada o una confianza de salida. El dominio inicial es el dominio al que pertenece el servidor CIFS de la SVM.

- *Confianza bidireccional*

Con confianzas bidireccionales, ambos dominios confían entre sí. Si el dominio principal del servidor CIFS tiene una confianza bidireccional con otro dominio, el dominio principal puede autenticar y autorizar a un usuario que pertenezca al dominio de confianza, y viceversa.

Las búsquedas de asignación de nombres de usuario de UNIX a usuario de Windows sólo se pueden realizar en dominios con relaciones de confianza bidireccionales entre el dominio principal y el otro dominio.

- *Confianza saliente*

Con una confianza saliente, el dominio principal confía en el otro dominio. En este caso, el dominio principal puede autenticar y autorizar a un usuario que pertenezca al dominio de confianza saliente.

Se realiza una búsqueda en un dominio con una confianza saliente con el dominio principal al realizar búsquedas de asignación de nombres de usuario de UNIX a usuario de Windows.

- *Confianza entrante*


Con una confianza de entrada, el otro dominio confía en el dominio principal del servidor CIFS. En este caso, el dominio principal no puede autenticar ni autorizar a un usuario que pertenezca al dominio de confianza entrante.

Se busca un dominio con una confianza entrante con el dominio principal cuando se realizan búsquedas de asignación de nombres de usuario de UNIX a nombre de usuario de Windows.

## **Cómo se utilizan los comodines (\*) para configurar las búsquedas multidominio para la asignación de nombres**

Las búsquedas de asignación de nombres multidominio se facilitan mediante el uso de caracteres comodín en la sección de dominio del nombre de usuario de Windows. En la siguiente tabla se muestra cómo utilizar comodines en la parte de dominio de una entrada de asignación de nombres para habilitar las búsquedas multidominio:

| Patrón | Sustitución      | Resultado                                                                                                                                                                                                             |
|--------|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| raíz   | *\\administrador | El usuario UNIX «'root'» está asignado al usuario denominado «'Administrator'». Todos los dominios de confianza se buscan en orden hasta que se encuentre el primer usuario coincidente denominado «'Administrator'». |

| Patrón | Sustitución | Resultado                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| *      | *\\*        | <p>Los usuarios UNIX válidos se asignan a los usuarios de Windows correspondientes. Todos los dominios de confianza se buscan en orden hasta que se encuentre el primer usuario que coincida con ese nombre.</p> <div>  <p>El patrón *\\* sólo es válido para la asignación de nombres de UNIX a Windows, no al revés.</p> </div> |

### Cómo se realizan las búsquedas de nombres multidominio

Puede elegir uno de los dos métodos para determinar la lista de dominios de confianza utilizados para las búsquedas de nombres multidominio:

- Utilice la lista de confianza bidireccional detectada automáticamente compilada por ONTAP
- Utilice la lista de dominios de confianza preferida que compila

Si un usuario de UNIX se asigna a un usuario de Windows con un comodín utilizado para la sección de dominio del nombre de usuario, se busca al usuario de Windows en todos los dominios de confianza de la siguiente manera:

- Si se configura una lista de dominio de confianza preferido, el usuario de Windows asignado se busca sólo en esta lista de búsqueda, en orden.
- Si no se configura una lista preferida de dominios de confianza, se busca al usuario de Windows en todos los dominios de confianza bidireccionales del dominio principal.
- Si no hay dominios de confianza bidireccional para el dominio principal, se busca al usuario en el dominio principal.

Si un usuario de UNIX está asignado a un usuario de Windows sin una sección de dominio en el nombre de usuario, se busca al usuario de Windows en el dominio principal.

### Reglas de conversión de asignación de nombres

Un sistema ONTAP mantiene un conjunto de reglas de conversión para cada SVM. Cada regla consta de dos piezas: Un *pattern* y un *substitut*. Las conversiones comienzan al principio de la lista apropiada y realizan una sustitución basada en la primera regla de coincidencia. El patrón es una expresión regular de estilo UNIX. El reemplazo es una cadena que contiene secuencias de escape que representan subexpresiones del patrón, como en UNIX `sed` programa.

## Cree una asignación de nombres

Puede utilizar el `vserver name-mapping create` comando para crear una asignación de nombres. Se usan asignaciones de nombres para habilitar a los usuarios de Windows a fin de acceder a los volúmenes de estilo de seguridad de UNIX y al revés.

### Acerca de esta tarea

Con cada SVM, ONTAP admite hasta 12,500 asignaciones de nombres para cada dirección.

### Paso

1. Crear una asignación de nombres: `vserver name-mapping create -vserver vserver_name -direction {krb-unix|win-unix|unix-win} -position integer -pattern text -replacement text`



La `-pattern` y `-replacement` las declaraciones se pueden formular como expresiones regulares. También puede utilizar el `-replacement` instrucción para denegar explícitamente una asignación al usuario mediante la cadena de reemplazo nula " " (el carácter de espacio). Consulte `vserver name-mapping create` manual para más detalles.

Cuando se crean las asignaciones de Windows a UNIX, todos los clientes de SMB que tengan conexiones abiertas al sistema ONTAP en el momento en el que se creen las nuevas asignaciones deben cerrar e iniciar sesión para ver las nuevas asignaciones.

### Ejemplos

El siguiente comando crea un mapa de nombre en la SVM llamada `vs1`. La asignación es una asignación de UNIX a Windows en la posición 1 de la lista de prioridades. La asignación asigna el usuario UNIX `johnd` al usuario de Windows `ENG\JohnDoe`.

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\JohnDoe"
```

El siguiente comando crea otra asignación de nombre en la SVM llamada `vs1`. La asignación es una asignación de Windows a UNIX en la posición 1 de la lista de prioridades. Aquí el patrón y reemplazo incluyen expresiones regulares. La asignación asigna cada usuario CIFS del dominio `ENG` a los usuarios del dominio LDAP asociado con la SVM.

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\\1"
```

El siguiente comando crea otra asignación de nombre en la SVM llamada `vs1`. Aquí el patrón incluye `"$"` como elemento del nombre de usuario de Windows que debe escaparse. La asignación asigna al usuario de Windows `ENG\john$OPS` al usuario UNIX `john OPS`.

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\${ops}
-replacement john_ops
```

### Configure el usuario predeterminado

Puede configurar un usuario predeterminado para que lo utilice si todos los demás intentos de asignación fallan para un usuario o si no desea asignar usuarios individuales entre UNIX y Windows. Si desea que la autenticación de usuarios no asignados falle, no debe configurar un usuario predeterminado.

### Acerca de esta tarea

Para la autenticación CIFS, si no desea asignar cada usuario de Windows a un usuario individual de UNIX, puede especificar un usuario predeterminado de UNIX.

Para la autenticación NFS, si no desea asignar cada usuario UNIX a un usuario individual de Windows, puede especificar un usuario predeterminado de Windows.

### Pasos

1. Ejecute una de las siguientes acciones:


| Si desea...                                    | Introduzca el siguiente comando...                                            |
|------------------------------------------------|-------------------------------------------------------------------------------|
| Configure el usuario UNIX predeterminado       | <code>vserver cifs options modify -default -unix-user <i>user_name</i></code> |
| Configure el usuario predeterminado de Windows | <code>vserver nfs modify -default-win-user <i>user_name</i></code>            |

### Comandos para gestionar las asignaciones de nombres

Hay comandos de la ONTAP específicos para gestionar las asignaciones de nombres.

| Si desea...                                                  | Se usa este comando...                   |
|--------------------------------------------------------------|------------------------------------------|
| Cree una asignación de nombres                               | <code>vserver name-mapping create</code> |
| Inserte una asignación de nombres en una posición específica | <code>vserver name-mapping insert</code> |
| Mostrar asignaciones de nombres                              | <code>vserver name-mapping show</code>   |



| Si desea...                                                                                                                                                                                           | Se usa este comando...                                                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
|  <p>No se permite un intercambio cuando se configura la asignación de nombres con una entrada de calificador ip.</p> | <code>vserver name-mapping swap</code>                                                                                            |
| Modificar una asignación de nombres                                                                                                                                                                   | <code>vserver name-mapping modify</code>                                                                                          |
| Eliminar una asignación de nombres                                                                                                                                                                    | <code>vserver name-mapping delete</code>                                                                                          |
| Validar la asignación de nombre correcta                                                                                                                                                              | <code>vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1</code> |

Consulte la página de manual de cada comando para obtener más información.

## Configurar las búsquedas de asignación de nombres multidominio

### Habilitar o deshabilitar las búsquedas de asignación de nombres multidominio

Con las búsquedas de asignación de nombres multidominio, puede utilizar una tarjeta comodín (\*) en la parte de dominio de un nombre de Windows al configurar la asignación de nombres de usuario de UNIX a Windows. El uso de un comodín (\*) en la parte de dominio del nombre permite a ONTAP buscar en todos los dominios que tienen una confianza bidireccional con el dominio que contiene la cuenta de equipo del servidor CIFS.

### Acerca de esta tarea

Como alternativa a la búsqueda en todos los dominios de confianza bidireccional, puede configurar una lista de dominios de confianza preferidos. Cuando se configura una lista de dominios de confianza preferidos, ONTAP utiliza la lista de dominios de confianza preferidos en lugar de los dominios de confianza en ambas direcciones detectados para realizar búsquedas de asignación de nombres multidominio.

- Las búsquedas de asignación de nombres multidominio están activadas de manera predeterminada.
- Esta opción está disponible en el nivel de privilegio avanzado.

### Pasos

1. Configure el nivel de privilegio en Advanced: `set -privilege advanced`
2. Ejecute una de las siguientes acciones:

| Si desea que las búsquedas de asignación de nombres multidominio sean... | Introduzca el comando...                                                                                     |
|--------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| Activado                                                                 | <code>vserver cifs options modify -vserver vserver_name -is-trusted-domain-enum -search-enabled true</code>  |
| Deshabilitado                                                            | <code>vserver cifs options modify -vserver vserver_name -is-trusted-domain-enum -search-enabled false</code> |

3. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

### Información relacionada

[Opciones disponibles del servidor SMB](#)

### Restablecer y volver a detectar dominios de confianza

Puede forzar la redetección de todos los dominios de confianza. Esto puede ser útil cuando los servidores de dominio de confianza no responden adecuadamente o las relaciones de confianza han cambiado. Solo se detectan los dominios con una confianza bidireccional con el dominio principal, que es el dominio que contiene la cuenta de equipo del servidor CIFS.

### Paso

1. Restablezca y vuelva a detectar dominios de confianza mediante el `vserver cifs domain trusts rediscover` comando.

```
vserver cifs domain trusts rediscover -vserver vs1
```

### Información relacionada

[Visualización de información acerca de los dominios de confianza detectados](#)

### Muestra información sobre los dominios de confianza detectados

Puede mostrar información acerca de los dominios de confianza detectados para el dominio principal del servidor CIFS, que es el dominio que contiene la cuenta de equipo del servidor CIFS. Esto puede ser útil si desea saber qué dominios de confianza se descubren y cómo se ordenan dentro de la lista de dominios de confianza detectados.

### Acerca de esta tarea

Sólo se descubren los dominios con confianzas bidireccionales con el dominio principal. Dado que el controlador de dominio (DC) del dominio principal devuelve la lista de dominios de confianza en un orden determinado por el DC, no se puede predecir el orden de los dominios de la lista. Al mostrar la lista de dominios de confianza, puede determinar el orden de búsqueda para las búsquedas de asignación de nombres multidominio.

La información que se muestra sobre el dominio de confianza se agrupa por nodos y máquina virtual de almacenamiento (SVM).

## Paso

1. Muestra información sobre los dominios de confianza detectados mediante el `vserver cifs domain trusts show` comando.

```
vserver cifs domain trusts show -vserver vs1
```

```
Node: node1
Vserver: vs1

Home Domain Trusted Domain

EXAMPLE.COM CIFS1.EXAMPLE.COM,
 CIFS2.EXAMPLE.COM
 EXAMPLE.COM

Node: node2
Vserver: vs1

Home Domain Trusted Domain

EXAMPLE.COM CIFS1.EXAMPLE.COM,
 CIFS2.EXAMPLE.COM
 EXAMPLE.COM
```

## Información relacionada

[Restablecer y volver a detectar dominios de confianza](#)

### Agregar, quitar o reemplazar dominios de confianza en las listas de dominios de confianza preferidas

Puede agregar o quitar dominios de confianza de la lista de dominios de confianza preferidos para el servidor SMB o puede modificar la lista actual. Si configura una lista de dominios de confianza preferidos, esta lista se utiliza en lugar de los dominios de confianza bidireccionales detectados al realizar búsquedas de asignación de nombres multidominio.

### Acerca de esta tarea

- Si va a agregar dominios de confianza a una lista existente, la nueva lista se combina con la lista existente con las nuevas entradas colocadas al final. Los dominios de confianza se buscan en el orden en que aparecen en la lista de dominios de confianza.
- Si va a quitar dominios de confianza de la lista existente y no especifica una lista, se elimina toda la lista de dominios de confianza de la máquina virtual de almacenamiento (SVM) especificada.
- Si modifica la lista existente de dominios de confianza, la nueva lista sobrescribe la lista existente.



Debe introducir solo los dominios de confianza bidireccional en la lista de dominios de confianza preferidos. Aunque puede introducir dominios de confianza de salida o de entrada en la lista de dominios preferidos, no se utilizan al realizar búsquedas de asignación de nombres multidominio. ONTAP omite la entrada para el dominio unidireccional y pasa al siguiente dominio de confianza bidireccional de la lista.

## Paso

1. Ejecute una de las siguientes acciones:

| Si desea hacer lo siguiente con la lista de dominios de confianza preferidos... | Usar el comando...                                                                                             |
|---------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| Agregar dominios de confianza a la lista                                        | <code>vserver cifs domain name-mapping-search add -vserver _vserver_name_-trusted-domains FQDN, ...</code>     |
| Quitar dominios de confianza de la lista                                        | <code>vserver cifs domain name-mapping-search remove -vserver _vserver_name_-trusted-domains FQDN, ...]</code> |
| Modifique la lista existente                                                    | <code>vserver cifs domain name-mapping-search modify -vserver _vserver_name_-trusted-domains FQDN, ...</code>  |

## Ejemplos

El siguiente comando añade dos dominios de confianza (cifs1.example.com y cifs2.example.com) a la lista de dominios de confianza preferida utilizada por SVM vs1:

```
cluster1::> vserver cifs domain name-mapping-search add -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

El siguiente comando quita dos dominios de confianza de la lista utilizada por SVM vs1:

```
cluster1::> vserver cifs domain name-mapping-search remove -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

El siguiente comando modifica la lista de dominios de confianza utilizada por SVM vs1. La nueva lista sustituye a la lista original:

```
cluster1::> vserver cifs domain name-mapping-search modify -vserver vs1
-trusted-domains cifs3.example.com
```

## Información relacionada

[Muestra información acerca de la lista de dominios de confianza preferidos](#)

**Muestra información sobre la lista de dominios de confianza preferidos**

Puede mostrar información acerca de los dominios de confianza que se encuentran en la lista de dominios de confianza preferidos y el orden en que se realizan búsquedas si las búsquedas de asignación de nombres multidominio están habilitadas. Puede configurar una lista de dominios de confianza preferida como alternativa al uso de la lista de dominios de confianza detectados automáticamente.

**Pasos**

- 1. Ejecute una de las siguientes acciones:

| Si desea mostrar información sobre lo siguiente...                                                                | Usar el comando...                                                                     |
|-------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| Todos los dominios de confianza preferidos en el clúster agrupados por máquinas virtuales de almacenamiento (SVM) | <code>vserver cifs domain name-mapping-search show</code>                              |
| Todos los dominios de confianza preferidos para una SVM especificada                                              | <code>vserver cifs domain name-mapping-search show -vserver <i>vserver_name</i></code> |

El siguiente comando muestra información sobre todos los dominios de confianza preferidos en el clúster:

```
cluster1::> vserver cifs domain name-mapping-search show
Vserver Trusted Domains

vs1 CIFS1.EXAMPLE.COM
```

**Información relacionada**

[Agregar, quitar o reemplazar dominios de confianza en las listas de dominios de confianza preferidas](#)

**Crear y configurar recursos compartidos de SMB**

**Crear y configurar la información general sobre recursos compartidos de SMB**

Antes de que los usuarios y las aplicaciones puedan acceder a los datos en el servidor CIFS mediante SMB, debe crear y configurar recursos compartidos de SMB, que es un punto de acceso con nombre en un volumen. Puede personalizar los recursos compartidos especificando parámetros de recurso compartido y propiedades de recurso compartido. Puede modificar un recurso compartido existente en cualquier momento.

Cuando se crea un recurso compartido de SMB, ONTAP crea una ACL predeterminada para el recurso compartido con permisos de control completo para todos.

Los recursos compartidos de SMB están ligados al servidor CIFS en la máquina virtual de almacenamiento (SVM). Los recursos compartidos de SMB se eliminan si la SVM se elimina o el servidor CIFS con el que está asociado se elimina de la SVM. Si vuelve a crear el servidor CIFS en la SVM, debe volver a crear los recursos compartidos SMB.

## Información relacionada

[Gestione el acceso a archivos mediante SMB](#)

["Configuración de SMB para Microsoft Hyper-V y SQL Server"](#)

[Configurar la asignación de caracteres para la traducción de nombres de archivo SMB en volúmenes](#)

### Cuáles son los recursos compartidos administrativos predeterminados

Cuando se crea un servidor CIFS en la máquina virtual de almacenamiento (SVM), los recursos compartidos administrativos predeterminados se crean automáticamente. Debe comprender cuáles son esos recursos compartidos predeterminados y cómo se utilizan.

ONTAP crea los siguientes recursos compartidos administrativos predeterminados al crear el servidor CIFS:



A partir de ONTAP 9.8, el recurso compartido admin\$ ya no se crea de forma predeterminada.

- ipc\$
- Admin\$ (solo ONTAP 9.7 y versiones anteriores)
- r\$

Puesto que los recursos compartidos que terminan con el carácter \$ son recursos compartidos ocultos, los recursos compartidos administrativos predeterminados no son visibles desde Mi PC, pero puede verlos utilizando carpetas compartidas.

### Cómo se utilizan los recursos compartidos predeterminados ipc\$ y admin\$

Los recursos compartidos ipc\$ y admin\$ los utilizan ONTAP y los administradores de Windows no pueden utilizarlos para acceder a los datos que residen en la SVM.

- ipc\$ share

el recurso compartido ipc\$ es un recurso que comparte las canalizaciones con nombre que son esenciales para la comunicación entre programas. el recurso compartido ipc\$ se utiliza durante la administración remota de un equipo y cuando se visualizan los recursos compartidos de un equipo. No puede cambiar la configuración de recursos compartidos, las propiedades de recursos compartidos ni las ACL del recurso compartido ipc\$. Tampoco puede cambiar el nombre del recurso compartido ipc\$ ni eliminarlo.

- Recurso compartido admin\$ (solo ONTAP 9.7 y versiones anteriores)



A partir de ONTAP 9.8, el recurso compartido admin\$ ya no se crea de forma predeterminada.

El recurso compartido admin\$ se usa durante la administración remota de la SVM. La ruta de este recurso siempre es la ruta al raíz de SVM. No se pueden cambiar las configuraciones de recursos compartidos, las propiedades de recursos compartidos ni las ACL del recurso compartido admin\$. Tampoco puede cambiar el nombre del recurso compartido admin\$ ni eliminarlo.

### Cómo se utiliza el recurso compartido c\$ predeterminado

El recurso compartido c\$ es un recurso compartido administrativo que puede usar el administrador de clústeres o SVM para acceder al volumen raíz de SVM y administrarlo.

A continuación se muestran las características de la cuota c\$:

- La ruta de este recurso compartido siempre es la ruta al volumen raíz de la SVM y no se puede modificar.
- La ACL predeterminada para el recurso compartido c\$ es Administrator / Full Control.

Este usuario es BUILTIN\Administrator. De forma predeterminada, BUILTIN\Administrator puede asignar al recurso compartido y ver, crear, modificar o eliminar archivos y carpetas en el directorio raíz asignado. Se debe tener cuidado al administrar archivos y carpetas en este directorio.

- Es posible cambiar la ACL del recurso compartido de c\$.
- Puede cambiar la configuración de c\$ share y las propiedades share.
- No se puede eliminar el recurso compartido c\$.
- El administrador de SVM puede acceder al resto del espacio de nombres de la SVM desde el recurso compartido c\$ asignado cruzando las uniones del espacio de nombres.
- Se puede acceder al recurso compartido c\$ mediante Microsoft Management Console.

### Información relacionada

[Configuración de permisos de archivo NTFS avanzados mediante la ficha Seguridad de Windows](#)

### Requisitos de nomenclatura de recursos compartidos de SMB

Tenga en cuenta los requisitos de nomenclatura de los recursos compartidos de ONTAP al crear recursos compartidos de SMB en el servidor de SMB.

Las convenciones de nomenclatura de los recursos compartidos para ONTAP son las mismas que para Windows e incluyen los siguientes requisitos:

- El nombre de cada recurso compartido debe ser exclusivo para el servidor SMB.
- Los nombres de recurso compartido no distinguen mayúsculas de minúsculas.
- La longitud máxima del nombre compartido es de 80 caracteres.
- Se admiten los nombres de los recursos compartidos Unicode.
- Los nombres de los recursos compartidos que terminan con el carácter \$ son recursos compartidos ocultos.
- Para ONTAP 9.7 y anteriores, los recursos compartidos administrativos admin\$, ipc\$ y c\$ se crean automáticamente en cada servidor CIFS y son nombres de recursos compartidos reservados. A partir de ONTAP 9.8, el recurso compartido admin\$ ya no se crea automáticamente.
- No se puede usar el nombre del recurso compartido ONTAP\_ADMIN\$ al crear un recurso compartido.
- Se admiten los nombres de uso compartido que contienen espacios:
  - No puede utilizar un espacio como primer carácter ni como último carácter en un nombre de recurso compartido.
  - Los nombres de los recursos compartidos deben escribirse entre comillas.



Las comillas simples se consideran parte del nombre del recurso compartido y no se pueden utilizar en lugar de comillas.

- Los siguientes caracteres especiales se admiten cuando se asigna el nombre a los recursos compartidos de SMB:

!@#\$%&'\_-~(){}.

- Los siguientes caracteres especiales no se admiten cuando se asigna el nombre a los recursos compartidos de SMB:
  - "/\:;|<>,?\* =

#### Requisitos de distinción entre mayúsculas y minúsculas de directorio al crear recursos compartidos en un entorno multiprotocolo

Si crea recursos compartidos en una SVM donde se utiliza el esquema de nomenclatura 8.3 para distinguir entre nombres de directorio donde solo hay diferencias de mayúsculas y minúsculas entre los nombres, debe utilizar el nombre 8.3 en la ruta de acceso compartido para garantizar que el cliente se conecte a la ruta de directorio deseada.

En el siguiente ejemplo, se crearon dos directorios llamados "testdir" y "TESTDIR" en un cliente Linux. La ruta de unión del volumen que contiene los directorios es /home. La primera salida es de un cliente Linux y la segunda es de un cliente SMB.

```
ls -l
drwxrwxr-x 2 user1 group1 4096 Apr 17 11:23 testdir
drwxrwxr-x 2 user1 group1 4096 Apr 17 11:24 TESTDIR
```

```
dir

Directory of Z:\

04/17/2015 11:23 AM <DIR> testdir
04/17/2015 11:24 AM <DIR> TESTDI~1
```

Al crear un recurso compartido en el segundo directorio, debe utilizar el nombre 8.3 en la ruta de acceso al recurso compartido. En este ejemplo, la ruta del recurso compartido al primer directorio es /home/testdir y la ruta del recurso compartido al segundo directorio es /home/TESTDI~1.

#### Utilizar las propiedades de recursos compartidos de SMB

##### Usar la información general de propiedades compartidas de SMB

Puede personalizar las propiedades de los recursos compartidos SMB.

Las propiedades de recursos compartidos disponibles son las siguientes:

| Comparta propiedades | Descripción                                                                                                                                      |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| oplocks              | Esta propiedad especifica que el recurso compartido utiliza bloqueos oportunistas, también conocidos como almacenamiento en caché en el cliente. |



| Comparta propiedades     | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| browsable                | Esta propiedad permite a los clientes de Windows examinar el recurso compartido.                                                                                                                                                                                                                                                                                                                                                                                                                     |
| showsnapshot             | Esta propiedad especifica que los clientes pueden ver y conocer copias Snapshot.                                                                                                                                                                                                                                                                                                                                                                                                                     |
| changenotify             | Esta propiedad especifica que el recurso compartido admite peticiones de notificación de cambio. Para los recursos compartidos en una SVM, esta es una propiedad inicial predeterminada.                                                                                                                                                                                                                                                                                                             |
| attributecache           | Esta propiedad permite que el atributo de archivo que almacena en caché en el recurso compartido SMB proporcione un acceso más rápido a los atributos. El valor predeterminado es deshabilitar el almacenamiento en caché de atributos. Esta propiedad debe estar habilitada sólo si hay clientes que se conectan a recursos compartidos a través de SMB 1.0. Esta propiedad de recurso compartido no es aplicable si los clientes se conectan a recursos compartidos a través de SMB 2.x o SMB 3.0. |
| continuously-available   | Esta propiedad permite a los clientes SMB que lo admiten abrir archivos de una forma persistente. Los archivos abiertos de esta manera están protegidos contra eventos disruptivos, como la conmutación por error y la devolución.                                                                                                                                                                                                                                                                   |
| branchcache              | Esta propiedad especifica que el recurso compartido permite a los clientes solicitar hash de BranchCache en los archivos dentro de este recurso compartido. Esta opción solo es útil si se especifica «'por recurso compartido» como modo operativo en la configuración de BranchCache CIFS.                                                                                                                                                                                                         |
| access-based-enumeration | Esta propiedad especifica que <i>Access Based Enumeration</i> (ABE) está habilitado en este recurso compartido. Las carpetas compartidas filtradas POR ABE son visibles para un usuario en función de los derechos de acceso de ese usuario individual, lo que impide la visualización de carpetas u otros recursos compartidos a los que el usuario no tiene derechos de acceso.                                                                                                                    |

| Comparta propiedades | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| namespace-caching    | Esta propiedad especifica que los clientes SMB que se conectan a este recurso compartido pueden almacenar en caché los resultados de enumeración de directorios que devuelven los servidores CIFS, lo que puede proporcionar un mejor rendimiento. De forma predeterminada, los clientes de SMB 1 no almacenan en caché los resultados de la enumeración de directorios. Dado que los resultados de enumeración de directorios de caché de los clientes SMB 2 y SMB 3 son los mismos, al especificar esta propiedad de recurso compartido, se proporcionan ventajas de rendimiento solo para las conexiones de cliente SMB 1. |
| encrypt-data         | Esta propiedad especifica que se debe utilizar el cifrado SMB al acceder a este recurso compartido. Los clientes de SMB que no admiten cifrado al acceder a los datos de SMB no podrán acceder a este recurso compartido.                                                                                                                                                                                                                                                                                                                                                                                                     |

### Agregar o quitar propiedades de recursos compartidos en un recurso compartido SMB existente

Puede personalizar un recurso compartido SMB existente agregando o quitando propiedades de recurso compartido. Esto puede ser útil para cambiar la configuración de recursos compartidos con el fin de satisfacer los requisitos en constante cambio del entorno.

#### Antes de empezar

Debe existir el recurso compartido cuyas propiedades desea modificar.

#### Acerca de esta tarea

Directrices para añadir propiedades de recurso compartido:

- Puede agregar una o más propiedades de recursos compartidos mediante una lista delimitada por comas.
- Todas las propiedades de recurso compartido que haya especificado anteriormente permanecen vigentes.

Las propiedades recién agregadas se agregan a la lista existente de propiedades de recursos compartidos.

- Si especifica un nuevo valor para las propiedades de recurso compartido que ya se han aplicado al recurso compartido, el valor recién especificado reemplazará al valor original.
- No se pueden quitar las propiedades compartidas mediante la `vserver cifs share properties add` comando.

Puede utilizar el `vserver cifs share properties remove` comando para quitar propiedades de recurso compartido.

Directrices para eliminar propiedades de recurso compartido:

- Puede quitar una o varias propiedades de recursos compartidos mediante una lista delimitada por comas.
- Las propiedades de recurso compartido que ha especificado previamente pero no las quita permanecen vigentes.

## Pasos

1. Introduzca el comando correspondiente:

| Si desea...                             | Introduzca el comando...                                                                                                              |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| Añada propiedades de recurso compartido | <code>vserver cifs share properties add -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...</code>    |
| Quite las propiedades de uso compartido | <code>vserver cifs share properties remove -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...</code> |

2. Compruebe la configuración de propiedades compartidas: `vserver cifs share show -vserver vserver_name -share-name share_name`

## Ejemplos

El siguiente comando añade el `showsnapshot` Comparta la propiedad con una participación denominada «shara1» en la SVM vs1:

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name share1 -share-properties showsnapshot
```

```
cluster1::> vserver cifs share show -vserver vs1
```

| Vserver | Share  | Path    | Properties   | Comment | ACL             |
|---------|--------|---------|--------------|---------|-----------------|
| -----   | -----  | -----   | -----        | -----   | -----           |
| vs1     | share1 | /share1 | oplocks      | -       | Everyone / Full |
| Control |        |         | browsable    |         |                 |
|         |        |         | changenotify |         |                 |
|         |        |         | showsnapshot |         |                 |

El siguiente comando quita el `browsable` Compartir la propiedad de una acción denominada «shara2» en la SVM vs1:

```
cluster1::> vsriver cifs share properties remove -vsriver vs1 -share-name
share2 -share-properties browsable

cluster1::> vsriver cifs share show -vsriver vs1
Vserver Share Path Properties Comment ACL

vs1 share2 /share2 oplocks - Everyone / Full
Control
 changenotify
```

## Información relacionada

### Comandos para gestionar los recursos compartidos de SMB

#### Optimice el acceso de los usuarios de SMB con la configuración de recursos compartidos de grupos forzada

Cuando se crea un recurso compartido desde la línea de comandos de ONTAP a datos con seguridad efectiva de UNIX, se puede especificar que todos los archivos creados por los usuarios de SMB en ese recurso compartido pertenecen al mismo grupo, conocido como el *force-group*, que debe ser un grupo predefinido en la base de datos de grupos UNIX. El uso de un grupo de fuerza facilita el acceso de los usuarios SMB que pertenecen a varios grupos a los archivos.

Especificar un grupo de fuerza solo es significativo si el recurso compartido está en un qtree UNIX o mixto. No es necesario establecer un grupo forzado para los recursos compartidos de un volumen NTFS o un qtree ya que el acceso a los archivos de estos recursos compartidos está determinado por permisos de Windows, no por GID de UNIX.

Si se ha especificado un grupo de fuerza para un recurso compartido, lo siguiente se convierte en verdadero del recurso compartido:

- Los usuarios de SMB del grupo de fuerza que acceden a este recurso compartido se cambian temporalmente al GID del grupo de fuerza.

Este GID permite acceder a los archivos de este recurso compartido a los que no se puede acceder normalmente con su GID o UID principal.

- Todos los archivos de este recurso compartido creados por usuarios SMB pertenecen al mismo grupo de fuerzas, independientemente del GID primario del propietario del archivo.

Cuando los usuarios de SMB intentan acceder a un archivo creado por NFS, los GID principales de los usuarios de SMB determinan los derechos de acceso.

El grupo de fuerza no afecta al modo en que los usuarios NFS acceden a los archivos de este recurso compartido. Un archivo creado por NFS adquiere el GID del propietario del archivo. La determinación de los permisos de acceso se basa en el UID y el GID primario del usuario NFS que intenta acceder al archivo.

El uso de un grupo de fuerza facilita el acceso de los usuarios SMB que pertenecen a varios grupos a los archivos. Por ejemplo, si desea crear un recurso compartido para almacenar las páginas web de la empresa y proporcionar acceso de escritura a los usuarios de los departamentos de Ingeniería y Marketing, puede crear un recurso compartido y proporcionar acceso de escritura a un grupo de fuerza denominado "webgroup1".

Debido al grupo de fuerza, todos los archivos creados por los usuarios de SMB en este recurso compartido son propiedad del grupo "webgroup1". Además, a los usuarios se les asigna automáticamente el GID del grupo "webgroup1" al acceder al recurso compartido. Como resultado, todos los usuarios pueden escribir en este recurso compartido sin necesidad de gestionar los derechos de acceso de los usuarios en los departamentos de ingeniería y marketing.

#### Información relacionada

[Crear un recurso compartido de SMB con la configuración de recurso compartido de grupo forzado](#)

#### Cree un recurso compartido SMB con la configuración force-group share

Puede crear un recurso compartido de SMB con la configuración de recurso compartido de grupo forzado si desea que los usuarios de SMB que acceden a datos de volúmenes o qtrees con seguridad de archivos UNIX consideren que ONTAP pertenece al mismo grupo UNIX.

#### Paso

1. Cree el recurso compartido de SMB: `vserver cifs share create -vserver vserver_name -share-name share_name -path path -force-group-for-create UNIX_group_name`

Si la ruta UNC (\\servername\sharename\filepath) del recurso compartido contiene más de 256 caracteres (excluyendo el inicial "\\") en la ruta UNC), la ficha **Seguridad** del cuadro Propiedades de Windows no está disponible. Se trata de un problema del cliente Windows y no de un problema de ONTAP. Para evitar este problema, no cree recursos compartidos con rutas UNC con más de 256 caracteres.

Si desea quitar el grupo de fuerza después de crear el recurso compartido, puede modificar el recurso compartido en cualquier momento y especificar una cadena vacía ("") como valor para `-force-group` `-for-create` parámetro. Si quita el grupo de fuerza modificando el recurso compartido, todas las conexiones existentes a este recurso compartido siguen teniendo el grupo de fuerza establecido anteriormente como GID primario.

#### Ejemplo

El siguiente comando crea un recurso compartido "webpages" al que se puede acceder en la web del /corp/companyinfo directorio en el que todos los archivos que crean los usuarios SMB se asignan al grupo webgroup1:

```
vserver cifs share create -vserver vs1 -share-name webpages -path /corp/companyinfo -force-group-for-create webgroup1
```

#### Información relacionada

[Optimice el acceso de los usuarios de SMB con la configuración de recursos compartidos de grupos forzada](#)

#### Consulte información sobre los recursos compartidos de SMB mediante MMC

Puede ver información sobre los recursos compartidos de SMB en la SVM y realizar algunas tareas de gestión con Microsoft Management Console (MMC). Antes de ver los recursos compartidos, tiene que conectar MMC a la SVM.

#### Acerca de esta tarea

Puede realizar las siguientes tareas en recursos compartidos contenidos en las SVM mediante MMC:

- Ver recursos compartidos
- Ver sesiones activas
- Ver archivos abiertos
- Enumera la lista de sesiones, archivos y conexiones de árbol del sistema
- Cierre los archivos abiertos en el sistema
- Cierre las sesiones abiertas
- Cree/gestione recursos compartidos



Las vistas que muestran las capacidades anteriores son específicas de los nodos y no del clúster. Por lo tanto, cuando utiliza MMC para conectarse al nombre de host del servidor SMB (es decir, cifs01.domain.local), se le enrutará, en función de cómo haya configurado DNS, a una única LIF dentro del clúster.

MMC para ONTAP no admite las siguientes funciones:

- Creación de nuevos usuarios/grupos locales
- Gestión/visualización de usuarios/grupos locales existentes
- Ver eventos o registros de rendimiento
- Reducida
- Servicios y aplicaciones

Es posible que tenga experiencia cuando no se admite la operación `remote procedure call failed` errores.

### "Preguntas más frecuentes: Uso de MMC de Windows con ONTAP"

#### Pasos

1. Para abrir la MMC de Administración de equipos en cualquier servidor de Windows, en **Panel de control**, seleccione **Herramientas administrativas > Administración de equipos**.
2. Seleccione **Acción > conectar a otro ordenador**.

Aparece el cuadro de diálogo Seleccionar equipo.

3. Escriba el nombre del sistema de almacenamiento o haga clic en **examinar** para buscar el sistema de almacenamiento.
4. Haga clic en **Aceptar**.

MMC se conecta a SVM.

5. En el panel de navegación, haga clic en **carpetas compartidas > recursos compartidos**.

Se muestra una lista de recursos compartidos de la SVM en el panel de visualización derecho.

6. Para mostrar las propiedades de uso compartido de un recurso compartido, haga doble clic en él para abrir el cuadro de diálogo **Propiedades**.
7. Si no puede conectarse al sistema de almacenamiento mediante MMC, puede agregar al usuario al grupo BUILTIN\Administrators o BUILTIN\Power Users mediante uno de los siguientes comandos del sistema de almacenamiento:

```
cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name BUILTIN\Administrators -member-names <domainuser>

cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name "BUILTIN\Power Users" -member-names <domainuser>
```

## Comandos para gestionar los recursos compartidos de SMB

Utilice la `vserver cifs share y.. vserver cifs share properties` Comandos para gestionar los recursos compartidos de SMB.

| Si desea...                                                                 | Se usa este comando...                            |
|-----------------------------------------------------------------------------|---------------------------------------------------|
| Cree un recurso compartido de SMB                                           | <code>vserver cifs share create</code>            |
| Mostrar los recursos compartidos de SMB                                     | <code>vserver cifs share show</code>              |
| Modificar un recurso compartido de SMB                                      | <code>vserver cifs share modify</code>            |
| Eliminar un recurso compartido de SMB                                       | <code>vserver cifs share delete</code>            |
| Agregar propiedades de recurso compartido a un recurso compartido existente | <code>vserver cifs share properties add</code>    |
| Quitar propiedades de recurso compartido de un recurso compartido existente | <code>vserver cifs share properties remove</code> |
| Muestra información sobre las propiedades de uso compartido                 | <code>vserver cifs share properties show</code>   |

Consulte la página de manual de cada comando para obtener más información.

## Acceso seguro a archivos mediante ACL de uso compartido de SMB

### Directrices para gestionar las ACL de nivel de recurso compartido de SMB

Puede cambiar las ACL de nivel compartido para otorgar a los usuarios más o menos derechos de acceso al recurso compartido. Puede configurar ACL de nivel compartido usando usuarios y grupos de Windows o usuarios y grupos de UNIX.

Después de crear un recurso compartido, de forma predeterminada, la ACL de nivel compartido proporciona acceso de lectura al grupo estándar denominado Everyone. El acceso de lectura en la ACL significa que todos los usuarios del dominio y todos los dominios de confianza tienen acceso de sólo lectura al recurso compartido.

Puede cambiar una ACL de nivel de recurso compartido mediante la Consola de administración de Microsoft

(MMC) en un cliente de Windows o la línea de comandos de ONTAP.

Las siguientes directrices se aplican cuando se utiliza MMC:

- Los nombres de usuario y de grupo especificados deben ser nombres de Windows.
- Sólo puede especificar permisos de Windows.

Cuando se utiliza la línea de comandos de ONTAP, se aplican las siguientes directrices:

- Los nombres de usuario y de grupo especificados pueden ser nombres de Windows o nombres UNIX.

Si no se especifica un tipo de usuario y grupo al crear o modificar ACL, el tipo predeterminado es usuarios y grupos de Windows.

- Sólo puede especificar permisos de Windows.

**Cree listas de control de acceso a recursos compartidos de SMB**

La configuración de permisos de uso compartido mediante la creación de listas de control de acceso (ACL) para recursos compartidos de SMB permite controlar el nivel de acceso a un recurso compartido para usuarios y grupos.

**Acerca de esta tarea**

Puede configurar ACL de nivel compartido utilizando nombres de usuarios o grupos locales o de dominio de Windows o nombres de usuarios o grupos de UNIX.

Antes de crear una ACL nueva, debe eliminar la ACL de recurso compartido predeterminada `Everyone / Full Control`, lo que supone un riesgo para la seguridad.

En modo de grupo de trabajo, el nombre de dominio local es el nombre del servidor SMB.

**Pasos**

1. Elimine la ACL de uso compartido predeterminada: `vserver cifs share access-control delete -vserver vserver_NAME -share share_name -user-or-group Everyone`
2. Configure la nueva ACL:

| Si desea configurar las ACL utilizando... | Introduzca el comando...                                                                                                                                                                                          |
|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Usuario de Windows                        | <code>vserver cifs share access-control<br/>create -vserver vserver_name -share<br/>share_name -user-group-type windows<br/>-user-or-group<br/>Windows_domain_name\user_name<br/>-permission access_right</code>  |
| Grupo Windows                             | <code>vserver cifs share access-control<br/>create -vserver vserver_name -share<br/>share_name -user-group-type windows<br/>-user-or-group<br/>Windows_domain_name\group_name<br/>-permission access_right</code> |



| Si desea configurar las ACL utilizando... | Introduzca el comando...                                                                                                                                                                          |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Usuario UNIX                              | <code>vserver cifs share access-control<br/>create -vserver vserver_name -share<br/>share_name -user-group-type unix-user<br/>-user-or-group UNIX_user_name<br/>-permission access_right</code>   |
| Grupo UNIX                                | <code>vserver cifs share access-control<br/>create -vserver vserver_name -share<br/>share_name -user-group-type unix-group<br/>-user-or-group UNIX_group_name<br/>-permission access_right</code> |

3. Compruebe que la ACL aplicada al recurso compartido sea correcta mediante el `vserver cifs share access-control show` comando.

**Ejemplo**

El siguiente comando da Change Permisos al grupo «equipo de ventas» de Windows para la participación «números» en «SVM» de «vs1.example.com»:

```
cluster1::> vserver cifs share access-control create -vserver
vs1.example.com -share sales -user-or-group "DOMAIN\Sales Team"
-permission Change

cluster1::> vserver cifs share access-control show -vserver
vs1.example.com
```

| Vserver         | Share | User/Group             | User/Group | Access |
|-----------------|-------|------------------------|------------|--------|
| Permission      | Name  | Name                   | Type       |        |
| -----           | ----- | -----                  | -----      |        |
| -----           |       |                        |            |        |
| vs1.example.com | c\$   | BUILTIN\Administrators | windows    |        |
| Full_Control    |       |                        |            |        |
| vs1.example.com | sales | DOMAIN\Sales Team      | windows    | Change |

El siguiente comando da Read Permiso para el grupo UNIX «'engineering» de la cuota «'eng'» del «vs2.example.com» «SVM»:

```
cluster1::> vsriver cifs share access-control create -vsriver
vs2.example.com -share eng -user-group-type unix-group -user-or-group
engineering -permission Read

cluster1::> vsriver cifs share access-control show -vsriver
vs2.example.com
```

| Vsriver         | Share | User/Group             | User/Group | Access |
|-----------------|-------|------------------------|------------|--------|
| Permission      | Name  | Name                   | Type       |        |
| -----           | ----- | -----                  | -----      |        |
| -----           |       |                        |            |        |
| vs2.example.com | c\$   | BUILTIN\Administrators | windows    |        |
| Full_Control    |       |                        |            |        |
| vs2.example.com | eng   | engineering            | unix-group | Read   |

Los siguientes comandos dan Change Permiso para el grupo local de Windows llamado "Tiger Team" and Full\_Control Permiso para el usuario local de Windows denominado «Sue Chang» para la participación «en la versión «.avol5» en «SVM:

```
cluster1::> vsriver cifs share access-control create -vsriver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vsriver cifs share access-control create -vsriver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vsriver cifs share access-control show -vsriver vs1
```

| Vsriver      | Share    | User/Group             | User/Group | Access       |
|--------------|----------|------------------------|------------|--------------|
| Permission   | Name     | Name                   | Type       |              |
| -----        | -----    | -----                  | -----      |              |
| -----        |          |                        |            |              |
| vs1          | c\$      | BUILTIN\Administrators | windows    |              |
| Full_Control |          |                        |            |              |
| vs1          | datavol5 | Tiger Team             | windows    | Change       |
| vs1          | datavol5 | Sue Chang              | windows    | Full_Control |

#### Comandos para gestionar las listas de control de acceso a recursos compartidos de SMB

Debe conocer los comandos para gestionar las listas de control de acceso (ACL) de SMB, lo que incluye crear, mostrar, modificar y eliminar dichas listas.

| Si desea...        | Se usa este comando...                                |
|--------------------|-------------------------------------------------------|
| Cree una nueva ACL | <code>vserver cifs share access-control create</code> |
| Mostrar ACL        | <code>vserver cifs share access-control show</code>   |
| Modificar una ACL  | <code>vserver cifs share access-control modify</code> |
| Eliminar una ACL   | <code>vserver cifs share access-control delete</code> |

## Acceso seguro a archivos mediante permisos de archivo

Configure los permisos de archivo NTFS avanzados mediante la ficha **Seguridad de Windows**

Puede configurar permisos de archivo NTFS estándar en archivos y carpetas mediante la ficha **Seguridad de Windows** de la ventana Propiedades de Windows.

### Antes de empezar

El administrador que realiza esta tarea debe tener suficientes permisos NTFS para cambiar los permisos en los objetos seleccionados.

### Acerca de esta tarea

La configuración de los permisos de archivo NTFS se realiza en un host de Windows agregando entradas a las listas de control de acceso discrecional NTFS (DACL) asociadas con un descriptor de seguridad NTFS. El descriptor de seguridad se aplica entonces a los archivos y directorios NTFS. La interfaz gráfica de usuario de Windows se encarga automáticamente de estas tareas.

### Pasos

1. En el menú **Herramientas** del Explorador de Windows, seleccione **asignar unidad de red**.
2. Complete el cuadro de diálogo **asignar unidad de red**:
  - a. Seleccione una letra **Unidad**.
  - b. En el cuadro **carpeta**, escriba el nombre del servidor CIFS que contiene el recurso compartido que contiene los datos a los que desea aplicar permisos y el nombre del recurso compartido.

Si el nombre de su servidor CIFS es «CIFS\_SERVER» y su cuota se llama «shara1», debería escribir \\CIFS\_SERVER\share1.



Puede especificar la dirección IP de la interfaz de datos para el servidor CIFS en lugar del nombre del servidor CIFS.

- c. Haga clic en **Finalizar**.

La unidad seleccionada está montada y lista con la ventana del Explorador de Windows que muestra archivos y carpetas contenidos en el recurso compartido.

3. Seleccione el archivo o directorio para el que desea establecer los permisos de archivo NTFS.
4. Haga clic con el botón secundario del ratón en el archivo o directorio y seleccione **Propiedades**.
5. Seleccione la ficha **Seguridad**.

La ficha **Seguridad** muestra la lista de usuarios y grupos para los que se ha establecido el permiso NTFS. El cuadro **permisos para** muestra una lista de permisos permitir y denegar que están en vigor para cada usuario o grupo seleccionado.

6. Haga clic en **Avanzado**.

La ventana Propiedades de Windows muestra información sobre los permisos de archivo existentes asignados a usuarios y grupos.

7. Haga clic en **Cambiar permisos**.

Se abrirá la ventana permisos.

8. Realice las acciones deseadas:

| Si desea...                                                     | Haga lo siguiente...                                                                                                                                                                                                                                                     |
|-----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configure permisos NTFS avanzados para un nuevo usuario o grupo | <ol style="list-style-type: none"> <li>a. Haga clic en <b>Agregar</b>.</li> <li>b. En el cuadro <b>Escriba el nombre del objeto que desea seleccionar</b> , escriba el nombre del usuario o grupo que desea agregar.</li> <li>c. Haga clic en <b>Aceptar</b>.</li> </ol> |
| Cambiar los permisos NTFS avanzados de un usuario o grupo       | <ol style="list-style-type: none"> <li>a. En el cuadro <b>permisos de entrada:</b> , seleccione el usuario o grupo cuyos permisos avanzados desea cambiar.</li> <li>b. Haga clic en <b>Editar</b>.</li> </ol>                                                            |
| Quitar permisos NTFS avanzados para un usuario o grupo          | <ol style="list-style-type: none"> <li>a. En el cuadro <b>Entradas de permisos:</b> , seleccione el usuario o grupo que desea quitar.</li> <li>b. Haga clic en <b>Quitar</b>.</li> <li>c. Vaya al paso 13.</li> </ol>                                                    |

Si va a agregar permisos NTFS avanzados en un nuevo usuario o grupo o si va a cambiar los permisos avanzados de NTFS en un usuario o grupo existente, se abrirá el cuadro Entrada de permisos para <Object> .

9. En el cuadro **aplicar a**, seleccione cómo desea aplicar esta entrada de permiso de archivo NTFS.

Si está configurando permisos de archivo NTFS en un solo archivo, el cuadro **aplicar a** no está activo. El valor **aplicar a** se establece de forma predeterminada en **este objeto sólo**.

10. En el cuadro **permisos** , seleccione los cuadros **permitir** o **Denegar** para los permisos avanzados que desea establecer en este objeto.
  - Para permitir el acceso especificado, seleccione el cuadro **permitir**.

- Para no permitir el acceso especificado, seleccione el cuadro **Denegar**.

Puede establecer permisos en los siguientes derechos avanzados:

- **Control total**

Si elige este derecho avanzado, todos los demás derechos avanzados se seleccionan automáticamente (permitir o denegar derechos).

- **Carpeta Traverse / archivo de ejecución**

- **Lista de carpetas / lectura de datos**

- **Leer atributos**

- **Leer atributos extendidos**

- **Crear archivos / escribir datos**

- **Crear carpetas / anexar datos**

- **Escribir atributos**

- **Escriba atributos extendidos**

- **Eliminar subcarpetas y archivos**

- **Eliminar**

- **Leer permisos**

- **Cambiar permisos**

- **Tome la propiedad**



Si alguno de los cuadros de permisos avanzados no se puede seleccionar, se debe a que los permisos se heredan del objeto primario.

11. Si desea que las subcarpetas y los archivos de este objeto hereden estos permisos, seleccione la casilla **aplicar estos permisos a objetos y/o contenedores dentro de este contenedor únicamente**.

12. Haga clic en **Aceptar**.

13. Después de terminar de agregar, quitar o editar permisos NTFS, especifique la configuración de herencia para este objeto:

- Seleccione el cuadro **incluir permisos heredables del primario de este objeto**.

Este es el valor predeterminado.

- Seleccione el cuadro **Reemplazar todos los permisos de objeto secundario con permisos heredables de este objeto**.

Esta configuración no está presente en el cuadro permisos si está estableciendo permisos de archivo NTFS en un solo archivo.



Tenga cuidado al seleccionar este ajuste. Esta configuración quita todos los permisos existentes en todos los objetos secundarios y los reemplaza con la configuración de permisos de este objeto. Podría quitar sin darse cuenta los permisos que no desea quitar. Especialmente importante cuando se configuran permisos en un volumen o un qtree de estilo de seguridad mixto. Si los objetos secundarios tienen un estilo de seguridad efectivo de UNIX, al propagar los permisos NTFS a esos objetos secundarios, ONTAP cambia estos objetos del estilo de seguridad de UNIX al estilo de seguridad NTFS y todos los permisos de UNIX de esos objetos secundarios se sustituyen por permisos NTFS.

- Seleccione ambas casillas.
- Seleccione ninguna casilla.

14. Haga clic en **Aceptar** para cerrar el cuadro **permisos**.

15. Haga clic en **Aceptar** para cerrar el cuadro **Configuración avanzada de seguridad para <Object>**.

Para obtener más información acerca de cómo establecer permisos NTFS avanzados, consulte la documentación de Windows.

### Información relacionada

[Configurar y aplicar la seguridad de archivos en archivos y carpetas NTFS mediante la CLI](#)

[Mostrar información acerca de la seguridad de archivos en volúmenes de estilo de seguridad NTFS](#)

[Mostrar información sobre la seguridad de archivos en volúmenes mixtos de estilo de seguridad](#)

[Visualización de información acerca de la seguridad de archivos en volúmenes de estilo de seguridad de UNIX](#)

### Configure los permisos del archivo NTFS mediante la interfaz de línea de comandos de ONTAP

Puede configurar los permisos de archivo NTFS en archivos y directorios mediante la interfaz de línea de comandos de ONTAP. Esto le permite configurar permisos de archivo NTFS sin necesidad de conectarse a los datos mediante un recurso compartido SMB en un cliente Windows.

Puede configurar los permisos de archivo NTFS agregando entradas a las listas de control de acceso discrecional (DACL) de NTFS que están asociadas con un descriptor de seguridad de NTFS. El descriptor de seguridad se aplica entonces a los archivos y directorios NTFS.

Sólo puede configurar permisos de archivo NTFS mediante la línea de comandos. No puede configurar las ACL de NFSv4 mediante la CLI.

### Pasos

1. Cree un descriptor de seguridad NTFS.

```
vserver security file-directory ntfs create -vserver svm_name -ntfs-sd
ntfs_security_descriptor_name -owner owner_name -group primary_group_name
-control-flags-raw raw_control_flags
```

2. Agregue DACL al descriptor de seguridad NTFS.

```
vserver security file-directory ntfs dacl add -vserver svm_name -ntfs-sd
ntfs_security_descriptor_name -access-type {deny|allow} -account account_name
```

```
-rights {no-access|full-control|modify|read-and-execute|read|write} -apply-to
{this-folder|sub-folders|files}
```

### 3. Cree una directiva de seguridad de archivos/directorios.

```
vserver security file-directory policy create -vserver svm_name -policy-name
policy_name
```

#### Cómo proporcionan los permisos de archivos UNIX el control de acceso al acceder a archivos a través de SMB

Un volumen FlexVol puede tener uno de los tres tipos de estilo de seguridad: NTFS, UNIX o mixto. Es posible acceder a los datos a través de SMB independientemente del estilo de seguridad; no obstante, se necesitan permisos adecuados de archivos UNIX para acceder a los datos con una seguridad efectiva de UNIX.

Cuando se accede a los datos a través de SMB, existen varios controles de acceso que se utilizan para determinar si un usuario está autorizado a realizar una acción solicitada:

- Permisos de exportación

La configuración de los permisos de exportación para el acceso SMB es opcional.

- Comparta los permisos
- Permisos de archivo

Los siguientes tipos de permisos de archivo se pueden aplicar a los datos en los que el usuario desea realizar una acción:

- NTFS
- ACL de UNIX NFSv4
- Bits de modo UNIX

En el caso de los datos con ACL de NFSv4 o conjuntos de bits de modo UNIX, se utilizan permisos de estilo UNIX para determinar los derechos de acceso a los archivos de los datos. El administrador de SVM debe establecer el permiso de archivo adecuado para garantizar que los usuarios tienen derechos para realizar la acción deseada.



Los datos de un volumen de estilo de seguridad mixto pueden tener un estilo de seguridad efectivo NTFS o UNIX. Si los datos tienen un estilo de seguridad efectivo de UNIX, se utilizan los permisos de NFSv4 o bits de modo UNIX al determinar los derechos de acceso a los datos.

#### Acceso seguro a archivos mediante control de acceso dinámico (DAC)

##### Acceso seguro a archivos mediante la información general de control de acceso dinámico (DAC)

Puede proteger el acceso mediante el control de acceso dinámico y mediante la creación de directivas de acceso central en Active Directory y su aplicación a archivos y carpetas en las SVM mediante objetos de directiva de grupo aplicados (GPO). Puede configurar la auditoría para utilizar los eventos de configuración de directivas de acceso central para ver los efectos de los cambios en las directivas de acceso central antes de aplicarlas.

## Adiciones a las credenciales CIFS

Antes del control dinámico de acceso, una credencial CIFS incluía la identidad de los principales de seguridad (el usuario) y la pertenencia al grupo Windows. Con el control dinámico de acceso, se agregan tres tipos más de información a la credencial: Identidad del dispositivo, reclamos del dispositivo y reclamos del usuario:

- Identidad del dispositivo

El análogo de la información de identidad del usuario, excepto que es la identidad y pertenencia de grupo del dispositivo desde el que el usuario inicia sesión.

- Reclamaciones de dispositivos

Afirmaciones acerca de una entidad de seguridad del dispositivo. Por ejemplo, una reclamación de dispositivo podría ser que es miembro de una unidad organizativa específica.

- Reclamaciones del usuario

Afirmaciones acerca de una entidad de seguridad de usuario. Por ejemplo, una reclamación de usuario podría ser que su cuenta AD es miembro de una unidad organizativa específica.

## Políticas de acceso central

Las políticas de acceso central para archivos permiten a las organizaciones implementar y administrar de forma centralizada políticas de autorización que incluyen expresiones condicionales mediante grupos de usuarios, reclamaciones de usuarios, reclamaciones de dispositivos y propiedades de recursos.

Por ejemplo, para acceder a datos de alto impacto empresarial, un usuario necesita ser un empleado a tiempo completo y solo tener acceso a los datos desde un dispositivo gestionado. Las directivas de acceso central se definen en Active Directory y se distribuyen a servidores de archivos mediante el mecanismo GPO.

## Configuración de directivas de acceso central con auditoría avanzada

Las políticas centrales de acceso pueden ser «más favorables», en cuyo caso se evalúan de forma «qué sucede si» durante los controles de acceso a los archivos. Los resultados de lo que habría ocurrido si la directiva estaba en vigor y cómo difiere de lo que está configurado actualmente se registran como un evento de auditoría. De esta forma, los administradores pueden utilizar registros de eventos de auditoría para estudiar el impacto de un cambio de directiva de acceso antes de poner la directiva en juego. Tras evaluar el impacto de un cambio de política de acceso, la política se puede implementar a través de GPO en las SVM deseadas.

## Información relacionada

[Objetos de normativa de grupo compatibles](#)

[Aplicación de objetos de directiva de grupo a servidores CIFS](#)

[Habilitar o deshabilitar la compatibilidad de GPO en un servidor CIFS](#)

[Mostrar información acerca de las configuraciones de GPO](#)

[Visualización de información acerca de las políticas de acceso central](#)

[Mostrar información acerca de las reglas de la política de acceso central](#)

[Configuración de políticas de acceso centrales para proteger los datos en servidores CIFS](#)



["Seguimiento de seguridad y auditoría de SMB y NFS"](#)

**Funcionalidad de control de acceso dinámico compatible**

Si desea utilizar el control de acceso dinámico (DAC) en un servidor CIFS, debe comprender cómo ONTAP admite la funcionalidad de control de acceso dinámico en entornos Active Directory.

**Compatible con el control de acceso dinámico**

ONTAP admite la siguiente funcionalidad cuando está habilitado el control de acceso dinámico en el servidor CIFS:

| Funcionalidad                                                                   | Comentarios                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Reclamaciones en el sistema de archivos                                         | Las reclamaciones son pares simples de nombre y valor que indican cierta verdad acerca de un usuario. Las credenciales de usuario contienen información de reclamación y los descriptores de seguridad de los archivos pueden realizar comprobaciones de acceso que incluyen comprobaciones de reclamaciones. De este modo, los administradores disponen de un mayor nivel de control sobre quién puede acceder a los archivos.                                                             |
| Expresiones condicionales para comprobaciones de acceso a archivos              | Al modificar los parámetros de seguridad de un archivo, los usuarios pueden agregar expresiones condicionales arbitrariamente complejas al descriptor de seguridad del archivo. La expresión condicional puede incluir comprobaciones para las reclamaciones.                                                                                                                                                                                                                               |
| Control centralizado de acceso a ficheros mediante directivas de acceso central | Las directivas de acceso central son un tipo de ACL almacenadas en Active Directory que se pueden etiquetar a un archivo. El acceso al archivo sólo se concede si el acceso comprueba tanto el descriptor de seguridad del disco como la directiva de acceso central etiquetada permiten el acceso.esto proporciona a los administradores la capacidad de controlar el acceso a los archivos desde una ubicación central (AD) sin tener que modificar el descriptor de seguridad del disco. |
| Configuración de políticas de acceso central                                    | Agrega la capacidad de probar los cambios de seguridad sin afectar el acceso real a los archivos, mediante un «envejecimiento» de las políticas de acceso centrales y viendo el efecto del cambio en un informe de auditoría.                                                                                                                                                                                                                                                               |

| Funcionalidad                                                                                                                             | Comentarios                                                                                                                                                             |
|-------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Soporte para mostrar información sobre la seguridad de las políticas de acceso central mediante la interfaz de línea de comandos de ONTAP | Amplía la <code>vserver security file-directory show</code> comando para mostrar información acerca de las directivas de acceso central aplicadas.                      |
| Seguimiento de la seguridad que incluye políticas de acceso central                                                                       | Amplía la <code>vserver security trace</code> familia de comandos para mostrar los resultados que incluyen información sobre las políticas de acceso central aplicadas. |

### No compatible con el control de acceso dinámico

ONTAP no admite la siguiente funcionalidad cuando el control de acceso dinámico está habilitado en el servidor CIFS:

| Funcionalidad                                                                 | Comentarios                                                                                                    |
|-------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| Clasificación automática de objetos del sistema de archivos NTFS              | Esta es una extensión de la infraestructura de clasificación de archivos de Windows que no se admite en ONTAP. |
| Auditoría avanzada que no sea la configuración de políticas de acceso central | Sólo se admite la configuración de directivas de acceso central para la auditoría avanzada.                    |

### Consideraciones que tener en cuenta al utilizar el control de acceso dinámico y las políticas de acceso central con servidores CIFS

Hay ciertas consideraciones que debe tener en cuenta al utilizar el control de acceso dinámico (DAC) y las políticas de acceso central para proteger los archivos y las carpetas en los servidores CIFS.

#### Se puede denegar el acceso NFS a la raíz si la regla de directiva se aplica al usuario de dominio\administrador

En determinadas circunstancias, puede denegarse el acceso NFS a root cuando se aplica la seguridad de la política de acceso central a los datos a los que el usuario raíz intenta acceder. El problema se produce cuando la directiva de acceso central contiene una regla que se aplica al dominio\administrador y la cuenta raíz se asigna a la cuenta de dominio\administrador.

En lugar de aplicar una regla al usuario de dominio\administrador, debe aplicar la regla a un grupo con privilegios administrativos, como el dominio\grupo de administradores. De esta forma, puede asignar root a la cuenta de dominio\administrador sin que este problema afecte a root.

#### El grupo BUILTIN\Administrators del servidor CIFS tiene acceso a los recursos cuando la directiva de acceso central aplicada no se encuentra en Active Directory

Es posible que los recursos contenidos en el servidor CIFS tengan políticas de acceso central aplicadas a ellos, pero cuando el servidor CIFS usa el SID de la política de acceso central para intentar recuperar información de Active Directory, el SID no coincide con ningún SID de política de acceso central existente en Active Directory. En estas circunstancias, el servidor CIFS aplica la política de recuperación predeterminada

local para ese recurso.

La directiva de recuperación predeterminada local permite el acceso de grupo BUILTIN\Administrators del servidor CIFS a ese recurso.

**Active o desactive la descripción general de Dynamic Access Control**

La opción que permite utilizar el control de acceso dinámico (DAC) para proteger objetos en el servidor CIFS está deshabilitada de forma predeterminada. Debe habilitar la opción si desea utilizar el control de acceso dinámico en el servidor CIFS. Si más adelante decide que no desea utilizar el control de acceso dinámico para proteger los objetos almacenados en el servidor CIFS, puede deshabilitar la opción.

**Acerca de esta tarea**

Una vez que el control de acceso dinámico está activado, el sistema de archivos puede contener ACL con entradas relacionadas con el control de acceso dinámico. Si el control de acceso dinámico está desactivado, se ignorarán las entradas actuales del control de acceso dinámico y no se permitirán las nuevas.

Esta opción solo está disponible en el nivel de privilegios avanzado.

**Paso**

- 1. Configure el nivel de privilegio en Advanced: `set -privilege advanced`
- 2. Ejecute una de las siguientes acciones:

| Si desea que el control de acceso dinámico sea... | Introduzca el comando...                                                             |
|---------------------------------------------------|--------------------------------------------------------------------------------------|
| Activado                                          | <code>vserver cifs options modify -vserver vserver_name -is-dac-enabled true</code>  |
| Deshabilitado                                     | <code>vserver cifs options modify -vserver vserver_name -is-dac-enabled false</code> |

- 3. Devolver al nivel de privilegio del administrador: `set -privilege admin`

**Información relacionada**

[Configuración de políticas de acceso centrales para proteger los datos en servidores CIFS](#)

**Administrar ACL que contienen ACE de control de acceso dinámico cuando el Control de acceso dinámico está desactivado**

Si tiene recursos que tienen ACL aplicados a ACE de control de acceso dinámico y deshabilita el control de acceso dinámico en la máquina virtual de almacenamiento (SVM), debe quitar las ACE de control de acceso dinámico antes de poder gestionar las ACE que no son de control de acceso dinámico en ese recurso.

**Acerca de esta tarea**

Una vez que el control dinámico de acceso está desactivado, no puede quitar los ACE de control de acceso no dinámico existentes ni agregar nuevos ACE de control de acceso no dinámico hasta que haya eliminado los ACE de control dinámico de acceso existentes.

Puede utilizar cualquier herramienta que utilice normalmente para administrar ACL para realizar estos pasos.

## Pasos

1. Determine qué ACE de control dinámico de acceso se aplican al recurso.
2. Quite los ACE de control de acceso dinámico del recurso.
3. Agregue o quite ACE de control de acceso no dinámico según lo desee del recurso.

## Configuración de políticas de acceso centrales para proteger los datos en servidores CIFS

Hay varios pasos que debe dar para garantizar el acceso seguro a los datos en el servidor CIFS mediante políticas de acceso centrales, incluida la habilitación del control de acceso dinámico (DAC) en el servidor CIFS, la configuración de políticas de acceso centrales en Active Directory y la aplicación de las políticas de acceso centrales a los contenedores de Active Directory con GPO, Y habilitar los GPO en el servidor CIFS.

### Antes de empezar

- Active Directory debe estar configurado para utilizar las directivas de acceso central.
- Debe tener suficiente acceso en los controladores de dominio de Active Directory para crear políticas de acceso centrales y crear y aplicar GPO a los contenedores que contienen los servidores CIFS.
- Debe tener suficiente acceso administrativo en la máquina virtual de almacenamiento (SVM) para ejecutar los comandos necesarios.

### Acerca de esta tarea

Las directivas de acceso central se definen y aplican a los objetos de directiva de grupo (GPO) en Active Directory. Puede consultar la biblioteca de Microsoft TechNet para obtener instrucciones sobre la configuración de directivas de acceso central y GPO.

["Biblioteca de Microsoft TechNet"](#)

## Pasos

1. Habilite el control de acceso dinámico en la SVM si aún no está habilitado mediante el `vserver cifs options modify` comando.

```
vserver cifs options modify -vserver vs1 -is-dac-enabled true
```

2. Habilite los objetos de política de grupo (GPO) en el servidor CIFS si todavía no están habilitados mediante el `vserver cifs group-policy modify` comando.

```
vserver cifs group-policy modify -vserver vs1 -status enabled
```

3. Crear reglas de acceso central y políticas de acceso central en Active Directory.
4. Cree un objeto de directiva de grupo (GPO) para implementar las directivas de acceso central en Active Directory.
5. Aplique el GPO al contenedor donde se encuentra la cuenta de equipo servidor CIFS.
6. Actualice manualmente los GPO aplicados al servidor CIFS mediante el `vserver cifs group-policy update` comando.

```
vserver cifs group-policy update -vserver vs1
```

7. Compruebe que la directiva de acceso central de GPO se aplica a los recursos del servidor CIFS mediante `vserver cifs group-policy show-applied` comando.

El siguiente ejemplo muestra que la política de dominio predeterminada tiene dos políticas de acceso centrales que se aplican al servidor CIFS:

```
vserver cifs group-policy show-applied
```

```
Vserver: vs1

GPO Name: Default Domain Policy
 Level: Domain
 Status: enabled
Advanced Audit Settings:
 Object Access:
 Central Access Policy Staging: failure
Registry Settings:
 Refresh Time Interval: 22
 Refresh Random Offset: 8
 Hash Publication Mode for BranchCache: per-share
 Hash Version Support for BranchCache: all-versions
Security Settings:
 Event Audit and Event Log:
 Audit Logon Events: none
 Audit Object Access: success
 Log Retention Method: overwrite-as-needed
 Max Log Size: 16384
 File Security:
 /vol1/home
 /vol1/dirl
 Kerberos:
 Max Clock Skew: 5
 Max Ticket Age: 10
 Max Renew Age: 7
 Privilege Rights:
 Take Ownership: usr1, usr2
 Security Privilege: usr1, usr2
 Change Notify: usr1, usr2
 Registry Values:
 Signing Required: false
 Restrict Anonymous:
 No enumeration of SAM accounts: true
 No enumeration of SAM accounts and shares: false
 Restrict anonymous access to shares and named pipes: true
 Combined restriction for anonymous user: no-access
 Restricted Groups:
 gpr1
```

```
gpr2
Central Access Policy Settings:
 Policies: cap1
 cap2

GPO Name: Resultant Set of Policy
Level: RSOP
Advanced Audit Settings:
 Object Access:
 Central Access Policy Staging: failure
Registry Settings:
 Refresh Time Interval: 22
 Refresh Random Offset: 8
 Hash Publication Mode for BranchCache: per-share
 Hash Version Support for BranchCache: all-versions
Security Settings:
 Event Audit and Event Log:
 Audit Logon Events: none
 Audit Object Access: success
 Log Retention Method: overwrite-as-needed
 Max Log Size: 16384
 File Security:
 /vol1/home
 /vol1/dir1
 Kerberos:
 Max Clock Skew: 5
 Max Ticket Age: 10
 Max Renew Age: 7
 Privilege Rights:
 Take Ownership: usr1, usr2
 Security Privilege: usr1, usr2
 Change Notify: usr1, usr2
 Registry Values:
 Signing Required: false
 Restrict Anonymous:
 No enumeration of SAM accounts: true
 No enumeration of SAM accounts and shares: false
 Restrict anonymous access to shares and named pipes: true
 Combined restriction for anonymous user: no-access
 Restricted Groups:
 gpr1
 gpr2
Central Access Policy Settings:
 Policies: cap1
 cap2

2 entries were displayed.
```

**Información relacionada**

[Mostrar información acerca de las configuraciones de GPO](#)

[Visualización de información acerca de las políticas de acceso central](#)

[Mostrar información acerca de las reglas de la política de acceso central](#)

[Activación o desactivación del control de acceso dinámico](#)

**Mostrar información acerca de la seguridad del control de acceso dinámico**

Puede mostrar información acerca de la seguridad DAC (Dynamic Access Control) en volúmenes NTFS y en datos con seguridad efectiva NTFS en volúmenes mixtos de estilo de seguridad. Esto incluye información sobre ACE condicionales, ACE de recursos y ACE de políticas de acceso central. Puede utilizar los resultados para validar la configuración de seguridad o solucionar problemas de acceso a archivos.

**Acerca de esta tarea**

Debe proporcionar el nombre de la máquina virtual de almacenamiento (SVM) y la ruta a los datos cuya información de seguridad de archivo o carpeta desee mostrar. Puede mostrar el resultado en forma de resumen o como una lista detallada.

**Paso**

- 1. Mostrar la configuración de seguridad de archivos y directorios con el nivel de detalle deseado:

| Si desea mostrar información...                                                                                                                       | Introduzca el siguiente comando...                                                                             |
|-------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| En forma de resumen                                                                                                                                   | <code>vserver security file-directory show<br/>-vserver vserver_name -path path</code>                         |
| Con detalle ampliado                                                                                                                                  | <code>vserver security file-directory show<br/>-vserver vserver_name -path path<br/>-expand-mask true</code>   |
| Donde se muestra la salida con los SID de grupo y usuario                                                                                             | <code>vserver security file-directory show<br/>-vserver vserver_name -path path<br/>-lookup-names false</code> |
| Acerca de la seguridad de archivos y directorios para archivos y directorios en los que la máscara de bits hexadecimal se traduce al formato de texto | <code>vserver security file-directory show<br/>-vserver vserver_name -path path<br/>-textual-mask true</code>  |

**Ejemplos**

En el ejemplo siguiente se muestra información de seguridad de Dynamic Access Control sobre la ruta de acceso /vol11 En SVM vs1:

```

cluster1::> vserver security file-directory show -vserver vs1 -path /vol1
 Vserver: vs1
 File Path: /vol1
 File Inode Number: 112
 Security Style: mixed
 Effective Style: ntfs
 DOS Attributes: 10
 DOS Attributes in Text: ----D---
 Expanded Dos Attribute: -
 Unix User Id: 0
 Unix Group Id: 1
 Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
 ACLs: NTFS Security Descriptor
 Control:0xbf14
 Owner:CIFS1\Administrator
 Group:CIFS1\Domain Admins
 SACL - ACEs
 ALL-Everyone-0xf01ff-OI|CI|SA|FA
 RESOURCE ATTRIBUTE-Everyone-0x0

 ("Department_MS",TS,0x10020,"Finance")
 POLICY ID-All resources - No Write-
0x0-OI|CI
 DACL - ACEs
 ALLOW-CIFS1\Administrator-0x1f01ff-
OI|CI
 ALLOW-Everyone-0x1f01ff-OI|CI
 ALLOW CALLBACK-DAC\user1-0x1200a9-
OI|CI

 ((@User.department==@Resource.Department_MS&&@Resource.Impact_MS>1000)&&@D
evice.department==@Resource.Department_MS)

```

## Información relacionada

[Mostrar información acerca de las configuraciones de GPO](#)

[Visualización de información acerca de las políticas de acceso central](#)

[Mostrar información acerca de las reglas de la política de acceso central](#)

## Consideraciones de reversión para el control de acceso dinámico

Debe ser consciente de lo que sucede al volver a una versión de ONTAP que no admite el control de acceso dinámico (DAC) y lo que debe hacer antes y después de revertir.



Si desea revertir el clúster a una versión de ONTAP que no admite el control de acceso dinámico y que el control de acceso dinámico está habilitado en una o varias máquinas virtuales de almacenamiento (SVM), debe hacer lo siguiente antes de revertir:

- Debe deshabilitar el control de acceso dinámico en todas las SVM que tengan habilitado en el clúster.
- Debe modificar cualquier configuración de auditoría del clúster que contenga el `cap-staging` tipo de evento para utilizar únicamente la `file-op` tipo de evento.

Debe comprender y actuar sobre algunas consideraciones importantes de reversión para archivos y carpetas con los ACE de control de acceso dinámico:

- Si se revierte el clúster, los ACE existentes de Dynamic Access Control no se eliminan; sin embargo, se ignorarán en las comprobaciones de acceso a archivos.
- Dado que los ACE de control de acceso dinámico se ignoran después de la nueva versión, el acceso a los archivos cambiará en archivos con ACE de control de acceso dinámico.

Esto podría permitir a los usuarios acceder a los archivos que no podían obtener anteriormente o no tener acceso a los que podían acceder anteriormente.

- Debería aplicar ACE de control de acceso no dinámico a los archivos afectados para restaurar su nivel anterior de seguridad.

Esto puede hacerse antes de revertir o inmediatamente después de que finaliza la reversión.



Puesto que los ACE de control dinámico de acceso se ignoran después de volver a verlos, no es necesario eliminarlos cuando se aplican los ACE de control de acceso no dinámico a los archivos afectados. Sin embargo, si lo desea, puede eliminarlos manualmente.

#### **Dónde encontrar información adicional acerca de cómo configurar y utilizar el control dinámico de acceso y las directivas de acceso central**

Hay recursos adicionales disponibles para ayudarle a configurar y utilizar el control dinámico de acceso y las políticas de acceso central.

Puede encontrar información acerca de cómo configurar el control dinámico de acceso y las directivas de acceso central en Active Directory en la biblioteca de Microsoft TechNet.

["Microsoft TechNet: Información general sobre el escenario de control de acceso dinámico"](#)

["Microsoft TechNet: Escenario de política de acceso central"](#)

Las siguientes referencias pueden ayudarle a configurar el servidor SMB para que utilice y admita el control de acceso dinámico y las políticas de acceso centrales:

- **Uso de GPO en el servidor SMB**

[Aplicar objetos de directiva de grupo a servidores SMB](#)

- **Configuración de la auditoría NAS en el servidor SMB**

["Seguimiento de seguridad y auditoría de SMB y NFS"](#)

## Acceso seguro a SMB mediante políticas de exportación

### Cómo se usan las políticas de exportación con el acceso de SMB

Si se habilitan las políticas de exportación para el acceso de SMB en el servidor SMB, se utilizan las políticas de exportación cuando se controla el acceso a los volúmenes de SVM mediante clientes SMB. Para acceder a los datos, puede crear una política de exportación que permita el acceso a SMB y, a continuación, asociar la política con los volúmenes que contienen recursos compartidos de SMB.

Una política de exportación tiene una o varias reglas que se le aplican para especificar qué clientes pueden acceder a los datos y qué protocolos de autenticación son compatibles con el acceso de solo lectura y de lectura y escritura. Puede configurar directivas de exportación para permitir el acceso a través de SMB a todos los clientes, a una subred de clientes o a un cliente específico y para permitir la autenticación mediante autenticación Kerberos, autenticación NTLM o autenticación Kerberos y NTLM al determinar el acceso de sólo lectura y escritura a los datos.

Tras procesar todas las reglas de exportación aplicadas a la política de exportación, ONTAP puede determinar si el cliente obtiene acceso y qué nivel de acceso se concede. Las reglas de exportación se aplican a los equipos cliente, no a los usuarios y grupos de Windows. Las reglas de exportación no reemplazan la autenticación y autorización basada en usuarios y grupos de Windows. Las reglas de exportación proporcionan otra capa de seguridad de acceso, además de permisos de uso compartido y acceso a archivos.

Se asocia exactamente una política de exportación a cada volumen para configurar el acceso de los clientes al volumen. Cada SVM puede contener varias políticas de exportación. Esto le permite hacer lo siguiente para las SVM con varios volúmenes:

- Asigne diferentes políticas de exportación a cada volumen de la SVM para controlar el acceso de clientes individuales a cada volumen de la SVM.
- Asigne la misma política de exportación a varios volúmenes del SVM para un control de acceso de clientes idéntico sin que tenga que crear una nueva política de exportación para cada volumen.

Cada SVM tiene, como mínimo, una política de exportación denominada «default», que no contiene reglas. No puede eliminar esta política de exportación, pero puede cambiarla ni cambiar el nombre. Cada volumen de la SVM está asociado de forma predeterminada con la política de exportación predeterminada. Si en la SVM se deshabilitan las políticas de exportación de acceso SMB, la política de exportación «predeterminado» no tendrá efecto en el acceso de las pymes.

Puede configurar reglas que proporcionen acceso a los hosts NFS y SMB y asociarlos con una política de exportación, que se puede asociar al volumen que contiene datos a los que necesitan acceder los hosts NFS y SMB. De forma alternativa, si hay algunos volúmenes en los que solo los clientes SMB necesitan acceso, puede configurar una directiva de exportación con reglas que solo permitan el acceso mediante el protocolo SMB y que sólo utilice Kerberos o NTLM (o ambos) para la autenticación de solo lectura y acceso de escritura. La política de exportación se asocia entonces a los volúmenes en los que solo se desea acceso a SMB.

Si se habilitan las políticas de exportación de SMB y un cliente realiza una solicitud de acceso que no permite la política de exportación correspondiente, la solicitud genera un mensaje de permiso denegado. Si un cliente no coincide con ninguna regla de la política de exportación del volumen, se deniega el acceso. Si una política de exportación está vacía, se deniegan implícitamente todos los accesos. Esto es cierto incluso si los permisos de recurso compartido y archivo de lo contrario permitirían el acceso. Esto significa que debe configurar la política de exportación para permitir, como mínimo, el siguiente valor en los volúmenes que contengan recursos compartidos de SMB:

- Permitir el acceso a todos los clientes o al subconjunto apropiado de clientes
- Permitir el acceso a través de SMB
- Permitir el acceso de sólo lectura y escritura adecuado mediante autenticación Kerberos o NTLM (o ambos)

Descubra "[configuración y gestión de políticas de exportación](#)".

### Cómo funcionan las reglas de exportación

Las reglas de exportación son los elementos funcionales de una política de exportación. Las reglas de exportación coinciden con las solicitudes de acceso de los clientes a un volumen con los parámetros específicos que se configuran para determinar cómo se manejan las solicitudes de acceso de los clientes.

La política de exportación debe contener al menos una regla de exportación para permitir el acceso a los clientes. Si una política de exportación contiene más de una regla, se procesan las reglas en el orden en que aparecen en la política de exportación. El orden de las reglas viene determinado por el número de índice de reglas. Si una regla coincide con un cliente, se utilizan los permisos de esa regla y no se procesan otras reglas. Si no hay reglas que coincidan, se deniega el acceso al cliente.

Puede configurar reglas de exportación para determinar los permisos de acceso de clientes con los siguientes criterios:

- El protocolo de acceso a archivos que utiliza el cliente para enviar la solicitud, por ejemplo, NFSv4 o SMB.
- Un identificador de cliente, por ejemplo, un nombre de host o una dirección IP.

El tamaño máximo de `-clientmatch` el campo tiene 4096 caracteres.

- Tipo de seguridad utilizado por el cliente para autenticar, por ejemplo, Kerberos v5, NTLM o AUTH\_SYS.

Si una regla especifica varios criterios, el cliente debe coincidir con todos ellos para que se aplique la regla.

### Ejemplo

La política de exportación contiene una regla de exportación con los siguientes parámetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

La solicitud de acceso del cliente se envía mediante el protocolo NFSv3 y el cliente tiene la dirección IP 10.1.17.37.

Aunque el protocolo de acceso del cliente coincida, la dirección IP del cliente se encuentra en una subred diferente de la especificada en la regla de exportación. Por lo tanto, la coincidencia de cliente falla y esta regla no se aplica a este cliente.

### Ejemplo

La política de exportación contiene una regla de exportación con los siguientes parámetros:

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

La solicitud de acceso del cliente se envía con el protocolo NFSv4 y el cliente tiene la dirección IP 10.1.16.54.

El protocolo de acceso del cliente coincide y la dirección IP del cliente se encuentra en la subred especificada. Por lo tanto, la coincidencia de cliente es correcta y esta regla se aplica a este cliente. El cliente obtiene acceso de lectura y escritura independientemente de su tipo de seguridad.

### Ejemplo

La política de exportación contiene una regla de exportación con los siguientes parámetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`

El cliente n.º 1 tiene la dirección IP 10.1.16.207, envía una solicitud de acceso con el protocolo NFSv3 y se autentica con Kerberos v5.

El cliente #2 tiene la dirección IP 10.1.16.211, envía una solicitud de acceso con el protocolo NFSv3 y se autentica con AUTH\_SYS.

El protocolo de acceso del cliente y la dirección IP coinciden con los dos clientes. El parámetro de solo lectura permite un acceso de solo lectura a todos los clientes independientemente del tipo de seguridad con el que se autenticuen. Por lo tanto, ambos clientes obtienen acceso de solo lectura. Sin embargo, sólo el cliente #1 obtiene acceso de lectura y escritura porque utilizó el tipo de seguridad aprobado Kerberos v5 para autenticar. El cliente n.º 2 no obtiene acceso de lectura/escritura.

### Ejemplos de reglas de política de exportación que restringen o permiten el acceso a través de SMB

Los ejemplos muestran cómo crear reglas de política de exportación que restringen o permiten el acceso a través de SMB en una SVM que tiene habilitadas políticas de exportación para el acceso a SMB.

Las políticas de exportación para acceso a SMB están deshabilitadas de forma predeterminada. Debe configurar reglas de políticas de exportación que restrinjan o permitan el acceso mediante SMB solo si ha habilitado políticas de exportación para el acceso a SMB.

### Regla de exportación solo para acceso SMB

El siguiente comando crea una regla de exportación en la SVM denominada "vs1" que tiene la siguiente configuración:

- Nombre de la directiva: Cifs1
- Número de índice: 1
- Coincidencia de cliente: Sólo coincide con los clientes de la red 192.168.1.0/24

- Protocol: Solo habilita el acceso SMB
- Acceso de sólo lectura: A clientes que utilizan autenticación NTLM o Kerberos
- Acceso de lectura y escritura: A clientes que utilizan autenticación Kerberos

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifs1 -ruleindex 1 -protocol cifs -clientmatch 192.168.1.0/255.255.255.0
-rorule krb5,ntlm -rwrule krb5
```

## Regla de exportación para el acceso a SMB y NFS

El siguiente comando crea una regla de exportación en el SVM denominado 'vs1' que tiene la siguiente configuración:

- Nombre de la directiva: Cifssnfs1
- Número de índice: 2
- Coincidencia de cliente: Coincide con todos los clientes
- Protocolo: Acceso SMB y NFS
- Acceso de sólo lectura: A todos los clientes
- Acceso de lectura y escritura: A clientes que utilizan Kerberos (NFS y SMB) o autenticación NTLM (SMB)
- Asignación para el ID de usuario de UNIX 0 (cero): Se asigna al ID de usuario 65534 (que normalmente asigna al nombre de usuario nobody)
- Acceso suid y sgid: Permite

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifs1nfs1 -ruleindex 2 -protocol cifs,nfs -clientmatch 0.0.0.0/0 -rorule any
-rwrule krb5,ntlm -anon 65534 -allow-suid true
```

## Regla de exportación para acceso SMB únicamente mediante NTLM

El siguiente comando crea una regla de exportación en la SVM denominada 'vs1' que tiene la siguiente configuración:

- Nombre de la política: Ntlm1
- Número de índice: 1
- Coincidencia de cliente: Coincide con todos los clientes
- Protocol: Solo habilita el acceso SMB
- Acceso de sólo lectura: Sólo para clientes que utilizan NTLM
- Acceso de lectura y escritura: Sólo para clientes que utilizan NTLM



Si configura la opción de sólo lectura o la opción de lectura y escritura para el acceso NTLM, debe utilizar las entradas basadas en dirección IP en la opción de coincidencia de cliente. De lo contrario, recibirá `access denied` errores. Esto se debe a que ONTAP utiliza los nombres principales de servicios (SPN) de Kerberos al utilizar un nombre de host para comprobar los derechos de acceso del cliente. La autenticación NTLM no admite nombres SPN.

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
ntlm1 -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule ntlm
-rwrule ntlm
```

### Habilite o deshabilite las políticas de exportación para el acceso de SMB

Puede habilitar o deshabilitar las políticas de exportación para acceso de SMB en máquinas virtuales de almacenamiento (SVM). El uso de políticas de exportación para controlar el acceso de SMB a los recursos es opcional.

#### Antes de empezar

A continuación, se muestran los requisitos para habilitar las políticas de exportación para SMB:

- El cliente debe tener un registro "PTR" en DNS antes de crear las reglas de exportación para ese cliente.
- Se necesita un conjunto adicional de registros «'A'» y «'PTR'» para los nombres de host si la SVM proporciona acceso a los clientes NFS y el nombre de host que desea utilizar para el acceso NFS es diferente al nombre del servidor CIFS.

#### Acerca de esta tarea

Al configurar un nuevo servidor CIFS en la SVM, el uso de políticas de exportación para acceso de SMB está deshabilitado de forma predeterminada. Puede habilitar las políticas de exportación para el acceso de SMB si desea controlar el acceso en función del protocolo de autenticación o en direcciones IP de cliente o nombres de host. Es posible habilitar o deshabilitar las políticas de exportación para el acceso de SMB en cualquier momento.

#### Pasos

1. Configure el nivel de privilegio en Advanced: `set -privilege advanced`
2. Habilite o deshabilite políticas de exportación:
  - Habilitar políticas de exportación: `vserver cifs options modify -vserver vserver_name -is-exportpolicy-enabled true`
  - Desactivar las políticas de exportación: `vserver cifs options modify -vserver vserver_name -is-exportpolicy-enabled false`
3. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

#### Ejemplo

El siguiente ejemplo permite el uso de políticas de exportación para controlar el acceso de clientes SMB a los recursos en SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-exportpolicy
-enabled true

cluster1::*> set -privilege admin
```

## Acceso seguro a archivos mediante Storage-Level Access Guard

### Acceso seguro a archivos mediante Storage-Level Access Guard

Además de proteger el acceso mediante el uso nativo a nivel de archivo y la seguridad de exportación y uso compartido, puede configurar la protección de acceso a nivel de almacenamiento, una tercera capa de seguridad aplicada por ONTAP a nivel de volumen. El servicio de protección de acceso a nivel de almacenamiento se aplica para acceder desde todos los protocolos NAS al objeto de almacenamiento al que se aplica.

Sólo se admiten permisos de acceso NTFS. Para que ONTAP realice comprobaciones de seguridad en los usuarios de UNIX con el fin de acceder a los datos de los volúmenes para los que se ha aplicado la protección de acceso a nivel de almacenamiento, el usuario de UNIX debe asignar a un usuario de Windows en la SVM propietaria del volumen.

### Comportamiento de protección del acceso al nivel de almacenamiento

- Storage-Level Access Guard se aplica a todos los archivos o todos los directorios de un objeto de almacenamiento.

Puesto que todos los archivos o directorios de un volumen están sujetos a la configuración de Storage-Level Access Guard, no se requiere la herencia a través de la propagación.

- Puede configurar Storage-Level Access Guard para que se aplique sólo a archivos, sólo a directorios o a los archivos y directorios de un volumen.

- Seguridad de archivos y directorios

Se aplica a todos los directorios y archivos del objeto de almacenamiento. Esta es la configuración predeterminada.

- Seguridad de archivos

Se aplica a cada archivo dentro del objeto de almacenamiento. Aplicar esta seguridad no afecta al acceso a los directorios o a la auditoría de ellos.

- Seguridad del directorio

Se aplica a cada directorio dentro del objeto de almacenamiento. Aplicar esta seguridad no afecta al acceso a los archivos ni a la auditoría de ellos.

- Se utiliza Storage-Level Access Guard para restringir los permisos.

Nunca dará permisos de acceso adicionales.

- Si ve la configuración de seguridad en un archivo o un directorio desde un cliente NFS o SMB, no verá la seguridad de Access Guard a nivel de almacenamiento.

Se aplica en el nivel de objeto de almacenamiento y se almacena en los metadatos que se usan para determinar la efectividad de los permisos.

- La seguridad a nivel de almacenamiento no puede ser revocada desde un cliente, incluso por un administrador de sistema (Windows o UNIX)

Está diseñado para que lo modifiquen únicamente administradores del almacenamiento.

- Se puede aplicar Access Guard en el nivel de almacenamiento a volúmenes con un estilo de seguridad NTFS o mixto.
- Es posible aplicar una protección de acceso al nivel de almacenamiento a los volúmenes con estilo de seguridad UNIX siempre que la SVM que contiene el volumen tenga configurado un servidor CIFS.
- Cuando los volúmenes se montan en una ruta de unión de volúmenes y, si existe la función Storage-Level Access Guard en esa ruta, no se propagará a los volúmenes montados bajo ella.
- El descriptor de seguridad de Storage-Level Access Guard se replica con la replicación de datos de SnapMirror y con la replicación de SVM.
- Hay una dispensación especial para los escáneres de virus.

Estos servidores pueden acceder de forma excepcional a los archivos y directorios de pantalla, incluso si Storage-Level Access Guard deniega el acceso al objeto.

- Las notificaciones de FPolicy no se envían si se deniega el acceso debido a la protección de acceso al nivel de almacenamiento.

## **Orden de las comprobaciones de acceso**

El acceso a un archivo o directorio se determina por el efecto combinado de los permisos de exportación o uso compartido, los permisos de Storage-Level Access Guard configurados en volúmenes y los permisos de archivo nativos aplicados a archivos y/o directorios. Se evalúan todos los niveles de seguridad para determinar los permisos efectivos que tiene un archivo o directorio. Las comprobaciones de acceso de seguridad se realizan en el siguiente orden:

1. Permisos a nivel de exportación de SMB o NFS
2. Protección de acceso al nivel de almacenamiento
3. Listas de control de acceso a carpetas/archivos NTFS (ACL), ACL de NFSv4 o bits de modo UNIX

## **Casos de uso para usar Storage-Level Access Guard**

El servicio de protección de acceso a nivel de almacenamiento proporciona una seguridad adicional a nivel de almacenamiento, que no puede verse en el lado del cliente; por lo tanto, no puede ser revocado por ninguno de los usuarios o administradores de sus escritorios. Existen determinados casos de uso en los que es conveniente la capacidad de controlar el acceso en el nivel de almacenamiento.



Los casos de uso típicos de esta función incluyen las siguientes situaciones:

- Protección de la propiedad intelectual mediante la auditoría y el control del acceso de todos los usuarios a nivel de almacenamiento
- Almacenamiento para empresas de servicios financieros, incluidos grupos bancarios y comerciales
- Servicios gubernamentales con almacenamiento de ficheros independiente para departamentos individuales
- Universidades que protegen todos los archivos de los estudiantes

#### **Flujo de trabajo para configurar Storage-Level Access Guard**

El flujo de trabajo para configurar la protección de acceso al nivel de almacenamiento (SSLAG) utiliza los mismos comandos de la CLI de ONTAP que utiliza para configurar permisos de archivos NTFS y directivas de auditoría. En lugar de configurar el acceso a archivos y directorios en un destino designado, debe configurar SLAG en el volumen de máquina virtual de almacenamiento designado.



#### Información relacionada

[Configuración de Storage-Level Access Guard](#)

Configure Storage-Level Access Guard

Hay una serie de pasos que se deben seguir para configurar la protección del acceso al nivel de almacenamiento en un volumen o un qtree. El protector de acceso al nivel de almacenamiento ofrece un nivel de seguridad de acceso que se establece en el nivel de almacenamiento. Proporciona seguridad que se aplica a todos los accesos desde todos los protocolos NAS al objeto de almacenamiento al que se ha aplicado.

Pasos

- 1. Cree un descriptor de seguridad mediante `vserver security file-directory ntfs create` comando.

```
vserver security file-directory ntfs create -vserver vs1 -ntfs-sd sd1 vserver security file-directory ntfs show -vserver vs1
```

Vserver: vs1

| NTFS Security Descriptor Name | Owner Name |
|-------------------------------|------------|
| sd1                           | -          |

Se crea un descriptor de seguridad con las siguientes cuatro entradas predeterminadas de control de acceso de DACL (ACE):

Vserver: vs1

NTFS Security Descriptor Name: sd1

| Account Name           | Access Type | Access Rights | Apply To                        |
|------------------------|-------------|---------------|---------------------------------|
| BUILTIN\Administrators | allow       | full-control  | this-folder, sub-folders, files |
| BUILTIN\Users          | allow       | full-control  | this-folder, sub-folders, files |
| CREATOR OWNER          | allow       | full-control  | this-folder, sub-folders, files |
| NT AUTHORITY\SYSTEM    | allow       | full-control  | this-folder, sub-folders, files |

Si no desea utilizar las entradas predeterminadas al configurar Storage-Level Access Guard, puede eliminarlas antes de crear y agregar sus propias ACE al descriptor de seguridad.

- 2. Quite cualquiera de los ACE de DACL predeterminados del descriptor de seguridad que no desea

configurar con la seguridad Storage-Level Access Guard:

- a. Elimine los ACE de DACL no deseados mediante `vserver security file-directory ntfs dacl remove` comando.

En este ejemplo, se quitan tres ACE de DACL predeterminados del descriptor de seguridad: BUILTIN\Administrators, BUILTIN\Users y CREATOR OWNER.

```
vserver security file-directory ntfs dacl remove -vserver vs1 -ntfs-sd sd1
-access-type allow -account builtin\users vserver security file-directory
ntfs dacl remove -vserver vs1 -ntfs-sd sd1 -access-type allow -account
builtin\administrators vserver security file-directory ntfs dacl remove
-vserver vs1 -ntfs-sd sd1 -access-type allow -account "creator owner"
```

- b. Compruebe que los ACE DACL que no desea utilizar para la seguridad de Access Guard de nivel de almacenamiento se quitan del descriptor de seguridad mediante el `vserver security file-directory ntfs dacl show` comando.

En este ejemplo, la salida del comando verifica que se han eliminado tres ACE de DACL predeterminados del descriptor de seguridad, dejando sólo la entrada de ACE de DACL predeterminada de NT AUTHORITY\SYSTEM:

```
vserver security file-directory ntfs dacl show -vserver vs1
```

Vserver: vs1

NTFS Security Descriptor Name: sd1

| Account Name        | Access Type | Access Rights | Apply To                        |
|---------------------|-------------|---------------|---------------------------------|
| NT AUTHORITY\SYSTEM | allow       | full-control  | this-folder, sub-folders, files |

3. Agregue una o varias entradas DACL a un descriptor de seguridad mediante `vserver security file-directory ntfs dacl add` comando.

En este ejemplo, se agregan dos ACE DACL al descriptor de seguridad:

```
vserver security file-directory ntfs dacl add -vserver vs1 -ntfs-sd sd1
-access-type allow -account example\engineering -rights full-control -apply-to
this-folder,sub-folders,files vserver security file-directory ntfs dacl add
-vserver vs1 -ntfs-sd sd1 -access-type allow -account "example\Domain Users"
-rights read -apply-to this-folder,sub-folders,files
```

4. Agregue una o más entradas de SACL a un descriptor de seguridad mediante `vserver security file-directory ntfs sacl add` comando.

En este ejemplo, se agregan dos ACE de SACL al descriptor de seguridad:

```
vserver security file-directory ntfs sacl add -vserver vs1 -ntfs-sd sd1
```

```
-access-type failure -account "example\Domain Users" -rights read -apply-to
this-folder,sub-folders,files vserver security file-directory ntfs sacl add
-vserver vs1 -ntfs-sd sd1 -access-type success -account example\engineering
-rights full-control -apply-to this-folder,sub-folders,files
```

5. Compruebe que los ACE DACL y SACL están configurados correctamente mediante el `vserver security file-directory ntfs dacl show y. vserver security file-directory ntfs sacl show` comandos, respectivamente.

En este ejemplo, el siguiente comando muestra información acerca de las entradas DACL del descriptor de seguridad "sD1":

```
vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
```

Vserver: vs1

NTFS Security Descriptor Name: sd1

| Account Name         | Access Type | Access Rights | Apply To                        |
|----------------------|-------------|---------------|---------------------------------|
| -----                | -----       | -----         | -----                           |
| EXAMPLE\Domain Users | allow       | read          | this-folder, sub-folders, files |
| EXAMPLE\engineering  | allow       | full-control  | this-folder, sub-folders, files |
| NT AUTHORITY\SYSTEM  | allow       | full-control  | this-folder, sub-folders, files |

En este ejemplo, el siguiente comando muestra información sobre las entradas de SACL para el descriptor de seguridad "D1":

```
vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
```

```
Vserver: vs1
```

```
NTFS Security Descriptor Name: sd1
```

| Account Name         | Access Type | Access Rights | Apply To                        |
|----------------------|-------------|---------------|---------------------------------|
| -----                | -----       | -----         | -----                           |
| EXAMPLE\Domain Users | failure     | read          | this-folder, sub-folders, files |
| EXAMPLE\engineering  | success     | full-control  | this-folder, sub-folders, files |

6. Cree una política de seguridad mediante `vserver security file-directory policy create` comando.

En el siguiente ejemplo se crea una directiva denominada «'póliza 1'»:

```
vserver security file-directory policy create -vserver vs1 -policy-name policy1
```

7. Compruebe que la directiva está correctamente configurada mediante el `vserver security file-directory policy show` comando.

```
vserver security file-directory policy show
```

| Vserver | Policy Name |
|---------|-------------|
| -----   | -----       |
| vs1     | policy1     |

8. Agregue una tarea con un descriptor de seguridad asociado a la directiva de seguridad mediante `vserver security file-directory policy task add` con el `-access-control` parámetro establecido en `slag`.

Aunque una directiva puede contener más de una tarea de Storage-Level Access Guard, no puede configurar una directiva para que contenga tareas de directorio de archivos y de Storage-Level Access Guard. Una política debe contener todas las tareas de Storage-Level Access Guard o todas las tareas de directorio de archivos.

En este ejemplo, se agrega una tarea a la política denominada "poly1", que se asigna al descriptor de seguridad "sD1". Está asignado a `/datavol1` ruta con el tipo de control de acceso establecido en "retardo".

```
vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /datavol1 -access-control slag -security-type ntfs -ntfs-mode propagate -ntfs-sd sd1
```

9. Compruebe que la tarea está configurada correctamente mediante el `vserver security file-`

directory policy task show comando.

```
vserver security file-directory policy task show -vserver vs1 -policy-name policy1
```

```
Vserver: vs1
Policy: policy1
```

| Index    | File/Folder | Access  | Security | NTFS      | NTFS       |
|----------|-------------|---------|----------|-----------|------------|
| Security | Path        | Control | Type     | Mode      | Descriptor |
| Name     |             |         |          |           |            |
| -----    | -----       | -----   | -----    | -----     |            |
| -----    |             |         |          |           |            |
| 1        | /datavol1   | slag    | ntfs     | propagate | sd1        |

10. Aplique la directiva de seguridad de protección de acceso al nivel de almacenamiento mediante `vserver security file-directory apply` comando.

```
vserver security file-directory apply -vserver vs1 -policy-name policy1
```

El trabajo que se va a aplicar la directiva de seguridad está programado.

11. Compruebe que la configuración de seguridad aplicada de la protección del acceso al nivel de almacenamiento sea correcta mediante `vserver security file-directory show` comando.

En este ejemplo, el resultado del comando muestra que la seguridad Storage-Level Access Guard se ha aplicado al volumen NTFS /datavol1. Aunque el DACL predeterminado que permite el control total para todos permanece, la seguridad de Storage-Level Access Guard restringe (y audita) el acceso a los grupos definidos en la configuración de Storage-Level Access Guard.

```
vserver security file-directory show -vserver vs1 -path /datavol1
```

```

 Vserver: vs1
 File Path: /datavol1
File Inode Number: 77
 Security Style: ntfs
 Effective Style: ntfs
 DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
 Unix User Id: 0
 Unix Group Id: 0
 Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
 ACLs: NTFS Security Descriptor
 Control:0x8004
 Owner:BUILTIN\Administrators
 Group:BUILTIN\Administrators
 DACL - ACEs
 ALLOW-Everyone-0x1f01ff
 ALLOW-Everyone-0x10000000-OI|CI|IO

Storage-Level Access Guard security
SACL (Applies to Directories):
 AUDIT-EXAMPLE\Domain Users-0x120089-FA
 AUDIT-EXAMPLE\engineering-0x1f01ff-SA
DACL (Applies to Directories):
 ALLOW-EXAMPLE\Domain Users-0x120089
 ALLOW-EXAMPLE\engineering-0x1f01ff
 ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
SACL (Applies to Files):
 AUDIT-EXAMPLE\Domain Users-0x120089-FA
 AUDIT-EXAMPLE\engineering-0x1f01ff-SA
DACL (Applies to Files):
 ALLOW-EXAMPLE\Domain Users-0x120089
 ALLOW-EXAMPLE\engineering-0x1f01ff
 ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

## Información relacionada

[Gestión de la seguridad de archivos NTFS, políticas de auditoría NTFS y Storage-Level Access Guard en SVM mediante la CLI](#)

[Flujo de trabajo para configurar Storage-Level Access Guard](#)

[Se muestra información acerca de Storage-Level Access Guard](#)

[Extracción de la protección de acceso a nivel de almacenamiento](#)



#### Matriz de ESCORIA efectiva

Puede configurar ESCORIA en un volumen, en un qtree o en ambos. La matriz DE ESCORIA define en qué volumen o qtree es la configuración DE ESCORIA aplicable en varios escenarios enumerados en la tabla.

|                                                                                     | ESCORIA de volumen en un AFS | ESCORIA de volumen en una copia snapshot | ESCORIA Qtree en un AFS | ESCORIA de qtree en una copia snapshot |
|-------------------------------------------------------------------------------------|------------------------------|------------------------------------------|-------------------------|----------------------------------------|
| Acceso de volumen en un sistema de archivos de acceso (AFS)                         | SÍ                           | NO                                       | N.A.                    | N.A.                                   |
| Acceso de volúmenes en una copia Snapshot                                           | SÍ                           | NO                                       | N.A.                    | N.A.                                   |
| Acceso Qtree en un AFS (cuando HAY ESCORIA en el qtree)                             | NO                           | NO                                       | SÍ                      | NO                                     |
| Acceso Qtree en un AFS (cuando LA ESCORIA no está presente en qtree)                | SÍ                           | NO                                       | NO                      | NO                                     |
| Acceso de qtree en la copia snapshot (cuando HAY ESCORIA en el AFS de qtree)        | NO                           | NO                                       | SÍ                      | NO                                     |
| Acceso de qtree en la copia snapshot (cuando NO hay ESCORIA en el AFS para qtrees). | SÍ                           | NO                                       | NO                      | NO                                     |

#### Muestra información sobre Storage-Level Access Guard

El servicio de protección del acceso a nivel de almacenamiento es una tercera capa de seguridad aplicada en un volumen o un qtree. La configuración de Storage-Level Access Guard no se puede ver mediante la ventana Propiedades de Windows. Es necesario usar la interfaz de línea de comandos de ONTAP para ver información sobre la seguridad de protección del acceso a nivel de almacenamiento, que se puede utilizar para validar la configuración o solucionar problemas de acceso a archivos.

**Acerca de esta tarea**

Se debe proporcionar el nombre de la máquina virtual de almacenamiento (SVM) y la ruta al volumen o qtree cuya información de seguridad de protección de acceso de nivel de almacenamiento desea mostrar. Puede mostrar el resultado en forma de resumen o como una lista detallada.

**Paso**

- 1. Mostrar la configuración de seguridad de protección de acceso a nivel de almacenamiento con el nivel de detalle deseado:

| Si desea mostrar información... | Introduzca el siguiente comando...                                                                                 |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------|
| En forma de resumen             | <code>vserver security file-directory show -vserver <i>vserver_name</i> -path <i>path</i></code>                   |
| Con detalle ampliado            | <code>vserver security file-directory show -vserver <i>vserver_name</i> -path <i>path</i> -expand-mask true</code> |

**Ejemplos**

En el siguiente ejemplo, se muestra información de seguridad de Storage-Level Access Guard para el volumen de estilo de seguridad NTFS con la ruta /datavol1 En SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1
```

```

 Vserver: vs1
 File Path: /datavol1
 File Inode Number: 77
 Security Style: ntfs
 Effective Style: ntfs
 DOS Attributes: 10
 DOS Attributes in Text: ----D---
 Expanded Dos Attributes: -
 Unix User Id: 0
 Unix Group Id: 0
 Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
 ACLs: NTFS Security Descriptor
 Control:0x8004
 Owner: BUILTIN\Administrators
 Group: BUILTIN\Administrators
 DACL - ACEs
 ALLOW-Everyone-0x1f01ff
 ALLOW-Everyone-0x10000000-OI|CI|IO

 Storage-Level Access Guard security
 SACL (Applies to Directories):
 AUDIT-EXAMPLE\Domain Users-0x120089-FA
 AUDIT-EXAMPLE\engineering-0x1f01ff-SA
 DACL (Applies to Directories):
 ALLOW-EXAMPLE\Domain Users-0x120089
 ALLOW-EXAMPLE\engineering-0x1f01ff
 ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
 SACL (Applies to Files):
 AUDIT-EXAMPLE\Domain Users-0x120089-FA
 AUDIT-EXAMPLE\engineering-0x1f01ff-SA
 DACL (Applies to Files):
 ALLOW-EXAMPLE\Domain Users-0x120089
 ALLOW-EXAMPLE\engineering-0x1f01ff
 ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

En el siguiente ejemplo, se muestra información de Storage-Level Access Guard acerca del volumen de estilo de seguridad mixto en la ruta /datavol15. En SVM vs1. El nivel superior de este volumen tiene una seguridad efectiva para UNIX. El volumen tiene seguridad de protección de acceso en el nivel de almacenamiento.

```

cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5

 Vserver: vs1
 File Path: /datavol5
 File Inode Number: 3374
 Security Style: mixed
 Effective Style: unix
 DOS Attributes: 10
 DOS Attributes in Text: ----D---
 Expanded Dos Attributes: -
 Unix User Id: 0
 Unix Group Id: 0
 Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
 ACLs: Storage-Level Access Guard security
 SACL (Applies to Directories):
 AUDIT-EXAMPLE\Domain Users-0x120089-FA
 AUDIT-EXAMPLE\engineering-0xf01ff-SA
 DACL (Applies to Directories):
 ALLOW-EXAMPLE\Domain Users-0x120089
 ALLOW-EXAMPLE\engineering-0xf01ff
 ALLOW-NT AUTHORITY\SYSTEM-0xf01ff
 SACL (Applies to Files):
 AUDIT-EXAMPLE\Domain Users-0x120089-FA
 AUDIT-EXAMPLE\engineering-0xf01ff-SA
 DACL (Applies to Files):
 ALLOW-EXAMPLE\Domain Users-0x120089
 ALLOW-EXAMPLE\engineering-0xf01ff
 ALLOW-NT AUTHORITY\SYSTEM-0xf01ff

```

#### Quite la protección de acceso al nivel de almacenamiento

Puede quitar la protección de acceso al nivel de almacenamiento en un volumen o qtree si ya no desea establecer la seguridad de acceso en el nivel de almacenamiento. La eliminación de la protección de acceso a nivel de almacenamiento no modifica ni quita la seguridad normal de archivos NTFS y directorios.

#### Pasos

1. Compruebe que el volumen o qtree tengan una protección de acceso al nivel de almacenamiento configurada mediante el `vserver security file-directory show` comando.

```
vserver security file-directory show -vserver vs1 -path /datavol2
```

```

 Vserver: vs1
 File Path: /datavol2
 File Inode Number: 99
 Security Style: ntfs
 Effective Style: ntfs
 DOS Attributes: 10
 DOS Attributes in Text: ----D---
 Expanded Dos Attributes: -
 Unix User Id: 0
 Unix Group Id: 0
 Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
 ACLs: NTFS Security Descriptor
 Control:0xbf14
 Owner:BUILTIN\Administrators
 Group:BUILTIN\Administrators
 SACL - ACEs
 AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
 DACL - ACEs
 ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
 ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI

 Storage-Level Access Guard security
 DACL (Applies to Directories):
 ALLOW-BUILTIN\Administrators-0x1f01ff
 ALLOW-CREATOR OWNER-0x1f01ff
 ALLOW-EXAMPLE\Domain Admins-0x1f01ff
 ALLOW-EXAMPLE\Domain Users-0x120089
 ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
 DACL (Applies to Files):
 ALLOW-BUILTIN\Administrators-0x1f01ff
 ALLOW-CREATOR OWNER-0x1f01ff
 ALLOW-EXAMPLE\Domain Admins-0x1f01ff
 ALLOW-EXAMPLE\Domain Users-0x120089
 ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

2. Retire el protector de acceso a nivel de almacenamiento mediante el `vserver security file-directory remove-slag` comando.

```
vserver security file-directory remove-slag -vserver vs1 -path /datavol2
```

3. Compruebe que la protección de acceso al nivel de almacenamiento se haya quitado del volumen o qtree mediante el `vserver security file-directory show` comando.

```
vserver security file-directory show -vserver vs1 -path /datavol2
```

```

Vserver: vs1
File Path: /datavol2
File Inode Number: 99
Security Style: ntfs
Effective Style: ntfs
DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
Unix User Id: 0
Unix Group Id: 0
Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
ACLs: NTFS Security Descriptor
Control:0xbf14
Owner:BUILTIN\Administrators
Group:BUILTIN\Administrators
SACL - ACEs
AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
DACL - ACEs
ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI

```

## Gestione el acceso a archivos mediante SMB

### Utilice usuarios y grupos locales para autenticación y autorización

#### Cómo utiliza ONTAP usuarios y grupos locales

#### Conceptos de usuarios locales y grupos

Debe saber cuáles son los usuarios y grupos locales, así como alguna información básica sobre ellos, antes de determinar si configurar y utilizar usuarios y grupos locales en su entorno.

- **Usuario local**

Una cuenta de usuario con un identificador de seguridad único (SID) que solo tiene visibilidad en la máquina virtual de almacenamiento (SVM) donde se crea. Las cuentas de usuario local tienen un conjunto de atributos, incluidos el nombre de usuario y el SID. Una cuenta de usuario local autentica de forma local en el servidor CIFS mediante la autenticación NTLM.

Las cuentas de usuario tienen varios usos:

- Se utiliza para otorgar privilegios *User Rights Management* a un usuario.
- Se usa para controlar el acceso a nivel de recurso compartido y de archivo a los recursos de archivos y carpetas que posee la SVM.

- **Grupo local**

Un grupo con un SID exclusivo tiene visibilidad solo en la SVM donde se crea. Los grupos contienen un conjunto de miembros. Los miembros pueden ser usuarios locales, usuarios de dominio, grupos de dominio y cuentas de equipos de dominio. Los grupos se pueden crear, modificar o eliminar.

Los grupos tienen varios usos:

- Se utiliza para otorgar privilegios *User Rights Management* a sus miembros.
- Se usa para controlar el acceso a nivel de recurso compartido y de archivo a los recursos de archivos y carpetas que posee la SVM.

- **Dominio local**

Un dominio que tiene un alcance local, delimitado por la SVM. El nombre del dominio local es el nombre del servidor CIFS. Los usuarios y grupos locales se encuentran dentro del dominio local.

- **Identificador de seguridad (SID)**

Un SID es un valor numérico de longitud variable que identifica los principios de seguridad de estilo Windows. Por ejemplo, un SID típico toma la siguiente forma: S-1-5-21-3139654847-1303905135-2517279418-123456.

- **Autenticación NTLM**

Un método de seguridad de Microsoft Windows que se utiliza para autenticar usuarios en un servidor CIFS.

- **Base de datos replicada en cluster (RDB)**

Base de datos replicada con una instancia en cada nodo de un clúster. Los objetos de usuario local y de grupo se almacenan en el RDB.

## **Motivos para crear usuarios locales y grupos locales**

Hay varias razones para crear usuarios locales y grupos locales en la máquina virtual de almacenamiento (SVM). Por ejemplo, puede tener acceso a un servidor SMB utilizando una cuenta de usuario local si los controladores de dominio (DC) no están disponibles, es posible que desee utilizar grupos locales para asignar privilegios o que el servidor SMB esté en un grupo de trabajo.

Es posible crear una o varias cuentas de usuario locales por los siguientes motivos:

- El servidor SMB está en un grupo de trabajo y los usuarios del dominio no están disponibles.

Los usuarios locales son necesarios en configuraciones de grupos de trabajo.

- Puede autenticar e iniciar sesión en el servidor SMB si las controladoras de dominio no están disponibles.

Los usuarios locales pueden autenticarse con el servidor SMB mediante la autenticación NTLM cuando el controlador de dominio está inactivo o cuando los problemas de red impiden que el servidor SMB se ponga en contacto con el controlador de dominio.

- Desea asignar privilegios *User Rights Management* a un usuario local.

*User Rights Management* es la capacidad de un administrador de servidor SMB para controlar los derechos que tienen los usuarios y los grupos en la SVM. Puede asignar privilegios a un usuario asignando los privilegios a la cuenta del usuario o haciendo que el usuario sea miembro de un grupo local que tenga esos privilegios.

Se pueden crear uno o varios grupos locales por los siguientes motivos:

- El servidor SMB está en un grupo de trabajo y los grupos de dominio no están disponibles.

Los grupos locales no son necesarios en las configuraciones de grupos de trabajo, pero pueden ser útiles para administrar privilegios de acceso para los usuarios de grupos de trabajo locales.

- Desea controlar el acceso a los recursos de archivos y carpetas mediante grupos locales para controlar el uso compartido y el acceso a archivos.
- Desea crear grupos locales con privilegios *User Rights Management* personalizados.

Algunos grupos de usuarios integrados tienen privilegios predefinidos. Para asignar un conjunto personalizado de privilegios, puede crear un grupo local y asignar los privilegios necesarios a ese grupo. A continuación, puede agregar usuarios locales, usuarios de dominio y grupos de dominio al grupo local.

## Información relacionada

[Cómo funciona la autenticación de usuarios locales](#)

[Lista de privilegios compatibles](#)

## Cómo funciona la autenticación de usuarios locales

Para que un usuario local pueda acceder a los datos en un servidor CIFS, el usuario debe crear una sesión autenticada.

Debido a que el bloque de mensajes del servidor se basa en sesiones, la identidad del usuario se puede determinar una sola vez cuando se configura la sesión por primera vez. El servidor CIFS utiliza autenticación basada en NTLM al autenticar usuarios locales. Se admiten tanto NTLMv1 como NTLMv2.

ONTAP utiliza autenticación local en tres casos de uso. Cada caso de uso depende de si la parte del dominio del nombre de usuario (con el formato de DOMINIO\usuario) coincide con el nombre de dominio local del servidor CIFS (el nombre del servidor CIFS):

- La parte del dominio coincide

Los usuarios que proporcionan credenciales de usuario local al solicitar acceso a los datos se autentican localmente en el servidor CIFS.

- La parte del dominio no coincide

ONTAP intenta utilizar la autenticación NTLM con un controlador de dominio del dominio al que pertenece el servidor CIFS. Si la autenticación se realiza correctamente, se completa el inicio de sesión. Si no se realiza correctamente, lo que sucede a continuación depende de por qué la autenticación no se ha realizado correctamente.

Por ejemplo, si el usuario existe en Active Directory pero la contraseña no es válida o ha caducado, ONTAP no intenta utilizar la cuenta de usuario local correspondiente en el servidor CIFS. En su lugar, la autenticación genera errores. Hay otros casos en los que ONTAP utiliza la cuenta local correspondiente en



el servidor CIFS, si existe, para la autenticación, aunque los nombres de dominio NetBIOS no coincidan. Por ejemplo, si existe una cuenta de dominio coincidente pero está deshabilitada, ONTAP utiliza la cuenta local correspondiente en el servidor CIFS para la autenticación.

- No se ha especificado la parte del dominio

ONTAP intenta primero la autenticación como usuario local. Si la autenticación como usuario local falla, ONTAP autentica al usuario con una controladora de dominio en el dominio al que pertenece el servidor CIFS.

Una vez que la autenticación de usuario local o de dominio se ha completado correctamente, ONTAP crea un token de acceso de usuario completo, que tiene en cuenta la pertenencia a grupos locales y los privilegios.

Para obtener más información acerca de la autenticación NTLM para usuarios locales, consulte la documentación de Microsoft Windows.

### Información relacionada

[Habilitar o deshabilitar la autenticación de usuario local](#)

### Cómo se construyen los tokens de acceso de usuario

Cuando un usuario asigna un recurso compartido, se establece una sesión SMB autenticada y se crea un token de acceso de usuario que contiene información acerca del usuario, la pertenencia al grupo del usuario y los privilegios acumulativos, así como el usuario UNIX asignado.

A menos que la funcionalidad esté deshabilitada, la información de grupo y de usuario local también se agrega al token de acceso de usuario. La forma en que se crean los tokens de acceso depende de si el inicio de sesión es para un usuario local o un usuario de dominio de Active Directory:

- Inicio de sesión de usuario local

Aunque los usuarios locales pueden ser miembros de diferentes grupos locales, los grupos locales no pueden ser miembros de otros grupos locales. El token de acceso de usuario local se compone de una unión de todos los privilegios asignados a grupos a los que pertenece un usuario local determinado.

- Inicio de sesión de usuario de dominio

Cuando un usuario de dominio inicia sesión, ONTAP obtiene un token de acceso de usuario que contiene el SID y SID de usuario para todos los grupos de dominio a los que pertenece el usuario. ONTAP utiliza la unión del token de acceso de usuario de dominio con el token de acceso proporcionado por las membresías locales de los grupos de dominio del usuario (si los hay), así como todos los privilegios directos asignados al usuario de dominio o cualquiera de sus pertenencias a grupos de dominio.

Tanto para el inicio de sesión local como para el usuario de dominio, el RID de grupo principal también está configurado para el token de acceso de usuario. EL RID predeterminado es `Domain Users` (RID 513). No puede cambiar el valor predeterminado.

El proceso de asignación de nombres de Windows a UNIX y UNIX a Windows sigue las mismas reglas para las cuentas locales y de dominio.



No hay ningún mapeo implícito y automático de un usuario UNIX a una cuenta local. Si es necesario, se debe especificar una regla de asignación explícita mediante los comandos de asignación de nombres existentes.

### **Directrices para usar SnapMirror en SVM que contienen grupos locales**

Debe tener en cuenta las directrices al configurar SnapMirror en los volúmenes que son propiedad de las SVM que contienen grupos locales.

No se pueden utilizar grupos locales en ACE aplicados a archivos, directorios o recursos compartidos replicados por SnapMirror en otra SVM. Si utiliza la función SnapMirror para crear un reflejo de recuperación ante desastres en un volumen en otra SVM y el volumen tiene una ACE para un grupo local, la ACE no es válida en el reflejo. Si los datos se replican en una SVM diferente, estos se cruzan realmente en un dominio local diferente. Los permisos concedidos a los usuarios y grupos locales solo son válidos dentro del ámbito de la SVM en la que se crearon originalmente.

### **Lo que sucede a los usuarios locales y los grupos al eliminar servidores CIFS**

El conjunto predeterminado de usuarios y grupos locales se crea cuando se crea un servidor CIFS y está asociado con las máquinas virtuales de almacenamiento (SVM) que alojan el servidor CIFS. Los administradores de SVM pueden crear usuarios y grupos locales en cualquier momento. Debe saber qué sucede con los usuarios locales y los grupos al eliminar el servidor CIFS.

Los usuarios y grupos locales están asociados a las SVM; por lo tanto, no se eliminan cuando los servidores CIFS se eliminan debido a consideraciones de seguridad. Aunque los usuarios y grupos locales no se eliminan al eliminar el servidor CIFS, sí se ocultan. No se pueden ver ni gestionar usuarios y grupos locales hasta que se vuelva a crear un servidor CIFS en la SVM.



El estado administrativo del servidor CIFS no afecta a la visibilidad de los grupos o usuarios locales.

### **Cómo puede utilizar Microsoft Management Console con usuarios y grupos locales**

Puede ver información acerca de los usuarios y grupos locales desde la Consola de administración de Microsoft. Con esta versión de ONTAP, no puede realizar otras tareas de administración para usuarios y grupos locales desde la Consola de administración de Microsoft.

### **Directrices para revertir**

Si piensa revertir el clúster a una versión de ONTAP que no da soporte a usuarios y grupos locales y se están utilizando grupos y usuarios locales para gestionar los derechos de usuario o el acceso a los archivos, debe tener en cuenta ciertas consideraciones.

- Debido a motivos de seguridad, no se elimina la información sobre usuarios locales, grupos y privilegios configurados cuando ONTAP se revierte a una versión que no admite la funcionalidad de usuarios y grupos locales.

- Al volver a una versión principal anterior de ONTAP, ONTAP no utiliza usuarios ni grupos locales durante la autenticación ni la creación de credenciales.
- Los usuarios y grupos locales no se quitan de las ACL de archivos y carpetas.
- Se deniegan las solicitudes de acceso a archivos que dependen de que se conceda el acceso debido a los permisos concedidos a los usuarios o grupos locales.

Para permitir el acceso, debe volver a configurar los permisos de archivo para permitir el acceso basado en objetos de dominio en lugar de objetos de usuario local y de grupo.

#### Qué privilegios locales son

#### Lista de privilegios compatibles

ONTAP tiene un conjunto predefinido de privilegios admitidos. Algunos grupos locales predefinidos tienen algunos de estos privilegios añadidos de forma predeterminada. También puede agregar o quitar privilegios de los grupos predefinidos o crear nuevos usuarios o grupos locales y agregar privilegios a los grupos que creó o a los usuarios y grupos de dominio existentes.

En la siguiente tabla se enumeran los privilegios admitidos en la máquina virtual de almacenamiento (SVM) y se proporciona una lista de los grupos BUILTIN con privilegios asignados:

| Nombre del privilegio    | Configuración de seguridad predeterminada           | Descripción                                                                                                                              |
|--------------------------|-----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| SeTcbPrivilege           | Ninguno                                             | Actuar como parte del sistema operativo                                                                                                  |
| SeBackupPrivilege        | BUILTIN\Administrators,<br>BUILTIN\Backup Operators | Realice copias de seguridad de archivos y directorios, anulando cualquier ACL                                                            |
| SeRestorePrivilege       | BUILTIN\Administrators,<br>BUILTIN\Backup Operators | Restaurar archivos y directorios, anulando cualquier ACL establecer cualquier SID de usuario o grupo válido como propietario del archivo |
| SeTakeOwnershipPrivilege | BUILTIN\Administrators                              | Tomar posesión de archivos u otros objetos                                                                                               |
| SeSecurityPrivilege      | BUILTIN\Administrators                              | Gestionar auditoría<br><br>Esto incluye ver, volcar y borrar el registro de seguridad.                                                   |

| Nombre del privilegio   | Configuración de seguridad predeterminada                                                               | Descripción                                                                                                                                                                                 |
|-------------------------|---------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SeChangeNotifyPrivilege | BUILTIN\Administrators,<br>BUILTIN\Backup Operators,<br>BUILTIN\Power Users,<br>BUILTIN\Users, Everyone | Comprobación de desvío transversal<br><br>No es necesario que los usuarios con este privilegio tengan permisos de desplazamiento (x) para recorrer carpetas, vínculos simbólicos o uniones. |

#### Información relacionada

- [Asigne privilegios locales](#)
- [Configuración de la comprobación de recorrido de derivación](#)

#### Asigne privilegios

Es posible asignar privilegios directamente a usuarios locales o a usuarios de dominio. También puede asignar usuarios a grupos locales cuyos privilegios asignados coincidan con las capacidades que desea que tengan esos usuarios.

- Puede asignar un conjunto de privilegios a un grupo que cree.

A continuación, agregue un usuario al grupo que tenga los privilegios que desea que tenga ese usuario.

- También puede asignar usuarios locales y usuarios de dominio a grupos predefinidos cuyos privilegios predeterminados coincidan con los privilegios que desea conceder a esos usuarios.

#### Información relacionada

- [Adición de privilegios a usuarios o grupos locales o de dominio](#)
- [Quitar privilegios de usuarios o grupos locales o de dominio](#)
- [Restableciendo privilegios para usuarios y grupos locales o de dominio](#)
- [Configuración de la comprobación de recorrido de derivación](#)

#### Directrices para el uso de grupos BUILTIN y la cuenta de administrador local

Hay ciertas pautas que debe tener en cuenta cuando utilice los grupos BUILTIN y la cuenta de administrador local. Por ejemplo, puede cambiar el nombre de la cuenta de administrador local, pero no puede eliminar esta cuenta.

- Se puede cambiar el nombre de la cuenta Administrador, pero no se puede eliminar.
- La cuenta de administrador no se puede quitar del grupo BUILTIN\Administrators.
- Se puede cambiar el nombre de los grupos INTEGRADOS, pero no se pueden eliminar.

Después de cambiar el nombre del grupo BUILTIN, se puede crear otro objeto local con el nombre bien conocido; sin embargo, al objeto se le asigna UN NUEVO RID.

- No hay una cuenta de invitado local.

**Información relacionada**

[Grupos BUILTIN predefinidos y privilegios predeterminados](#)

**Requisitos para las contraseñas de usuario local**

De manera predeterminada, las contraseñas de usuario local deben cumplir con los requisitos complejos. Los requisitos de complejidad de la contraseña son similares a los que se definen en la directiva de seguridad local de Microsoft Windows.

La contraseña debe cumplir los siguientes criterios:

- Debe tener al menos seis caracteres de longitud
- No se debe contener el nombre de cuenta de usuario
- Debe contener caracteres de al menos tres de las siguientes cuatro categorías:
  - Caracteres en mayúsculas (De La A a la Z)
  - Caracteres en minúscula (de la a a la z)
  - Base de 10 dígitos (de 0 a 9)
  - Caracteres especiales:

~ ! @ # \$ % ^ & \* \_ - + = ' \ | ( ) [ ] ; : " < > , . ? /

**Información relacionada**

[Habilitar o deshabilitar la complejidad de contraseña necesaria para los usuarios locales de la SMB](#)

[Mostrar información acerca de la configuración de seguridad del servidor CIFS](#)

[Cambio de contraseñas de cuenta de usuario local](#)

**Grupos BUILTIN predefinidos y privilegios predeterminados**

Puede asignar la pertenencia de un usuario local o un usuario de dominio a un conjunto predefinido de grupos BUILTIN proporcionados por ONTAP. Los grupos predefinidos tienen privilegios predefinidos asignados.

En la siguiente tabla se describen los grupos predefinidos:

| Grupo BUILTIN predefinido                                                                                                                                                                                                                                                                                                                                                                      | Privilegios predeterminados                                                                                                                                                                         |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>BUILTIN\AdministratorsRID 544</p> <p>Cuando se crea por primera vez, el local Administrator La cuenta, CON UN RID de 500, se hace automáticamente miembro de este grupo. Cuando la máquina virtual de almacenamiento (SVM) se une a un dominio, el domain\Domain Admins el grupo se agrega al grupo. Si la SVM sale del dominio, el domain\Domain Admins el grupo se elimina del grupo.</p> | <ul style="list-style-type: none"><li>• SeBackupPrivilege</li><li>• SeRestorePrivilege</li><li>• SeSecurityPrivilege</li><li>• SeTakeOwnershipPrivilege</li><li>• SeChangeNotifyPrivilege</li></ul> |

| Grupo BUILTIN predefinido                                                                                                                                                                                                                                                                                                                                                           | Privilegios predeterminados                                                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| <p>BUILTIN\Power UsersRID 547</p> <p>Cuando se crea por primera vez, este grupo no tiene miembros. Los miembros de este grupo tienen las siguientes características:</p> <ul style="list-style-type: none"> <li>• Puede crear y administrar usuarios y grupos locales.</li> <li>• No se pueden agregar a sí mismos ni a ningún otro objeto BUILTIN\Administrators grupo.</li> </ul> | SeChangeNotifyPrivilege                                                                                                                |
| <p>BUILTIN\Backup OperatorsRID 551</p> <p>Cuando se crea por primera vez, este grupo no tiene miembros. Los miembros de este grupo pueden anular los permisos de lectura y escritura en archivos o carpetas si se abren con la intención de copia de seguridad.</p>                                                                                                                 | <ul style="list-style-type: none"> <li>• SeBackupPrivilege</li> <li>• SeRestorePrivilege</li> <li>• SeChangeNotifyPrivilege</li> </ul> |
| <p>BUILTIN\UsersRID 545</p> <p>Cuando se crea por primera vez, este grupo no tiene ningún miembro (además del implícito Authenticated Users grupo especial). Cuando la SVM se une a un dominio, el domain\Domain Users el grupo se agrega a este grupo. Si la SVM sale del dominio, el domain\Domain Users el grupo se elimina de este grupo.</p>                                   | SeChangeNotifyPrivilege                                                                                                                |
| <p>EveryoneSID S-1-1-0</p> <p>Este grupo incluye a todos los usuarios, incluidos invitados (pero no usuarios anónimos). Este es un grupo implícito con una membresía implícita.</p>                                                                                                                                                                                                 | SeChangeNotifyPrivilege                                                                                                                |

### Información relacionada

[Directrices para el uso de grupos BUILTIN y la cuenta de administrador local](#)

[Lista de privilegios compatibles](#)

[Configuración de la comprobación de recorrido de derivación](#)

**Habilite o deshabilite la funcionalidad de grupos y usuarios locales**

**Habilite o deshabilite la descripción general de la funcionalidad de los usuarios locales y los grupos**

Antes de poder utilizar usuarios y grupos locales para controlar el acceso a los datos del estilo de seguridad NTFS, se debe habilitar la funcionalidad de usuario local y grupo.

Además, si desea utilizar usuarios locales para la autenticación SMB, se debe habilitar la funcionalidad de autenticación de usuarios locales.

La funcionalidad de grupos y usuarios locales y la autenticación de usuarios locales están habilitadas de forma predeterminada. Si no están habilitadas, debe habilitarlas para poder configurar y utilizar usuarios y grupos locales. La funcionalidad de grupos y usuarios locales se puede deshabilitar en cualquier momento.

Además de deshabilitar explícitamente la funcionalidad de grupo y usuario local, ONTAP deshabilita la funcionalidad de grupo y usuario local si algún nodo del clúster se revierte a una versión de ONTAP que no admite la funcionalidad. La funcionalidad de usuario local y de grupo no está habilitada hasta que todos los nodos del clúster ejecuten una versión de ONTAP que la admita.

**Información relacionada**

[Modifique las cuentas de usuario local](#)

[Modificar grupos locales](#)

[Añada privilegios a usuarios o grupos locales o de dominio](#)

**Habilite o deshabilite usuarios y grupos locales**

Puede habilitar o deshabilitar usuarios y grupos locales para el acceso SMB en máquinas virtuales de almacenamiento (SVM). La funcionalidad de grupos y usuarios locales está activada de forma predeterminada.

**Acerca de esta tarea**

Puede usar usuarios y grupos locales al configurar los permisos de archivos NTFS y compartidos de SMB, y puede usar, opcionalmente, usuarios locales para la autenticación al crear una conexión SMB. Para usar usuarios locales para la autenticación, también debe habilitar la opción de autenticación de grupos y usuarios locales.

**Pasos**

- 1. Configure el nivel de privilegio en Advanced: `set -privilege advanced`
- 2. Ejecute una de las siguientes acciones:

| Si desea que los grupos y usuarios locales sean... | Introduzca el comando...                                                                                 |
|----------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| Activado                                           | <code>vserver cifs options modify -vserver vserver_name -is-local-users-and -groups-enabled true</code>  |
| Deshabilitado                                      | <code>vserver cifs options modify -vserver vserver_name -is-local-users-and -groups-enabled false</code> |

- 3. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

**Ejemplo**

El siguiente ejemplo habilita la funcionalidad de grupos y usuarios locales en SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vsserver cifs options modify -vsserver vs1 -is-local-users-and
-groups-enabled true

cluster1::*> set -privilege admin
```

## Información relacionada

[Habilite o deshabilite la autenticación de usuario local](#)

[Habilite o deshabilite cuentas de usuario locales](#)

## Habilite o deshabilite la autenticación de usuario local

Puede habilitar o deshabilitar la autenticación de usuario local para el acceso SMB en máquinas virtuales de almacenamiento (SVM). El valor predeterminado es permitir la autenticación de usuario local, que resulta útil cuando la SVM no puede ponerse en contacto con un controlador de dominio o si decide no utilizar controles de acceso a nivel de dominio.

### Antes de empezar

La funcionalidad de grupos y usuarios locales debe estar habilitada en el servidor CIFS.

### Acerca de esta tarea

Es posible habilitar o deshabilitar la autenticación de usuario local en cualquier momento. Si desea usar usuarios locales para la autenticación al crear una conexión SMB, también debe habilitar la opción de grupos y usuarios locales del servidor CIFS.

### Pasos

1. Configure el nivel de privilegio en Advanced: `set -privilege advanced`
2. Ejecute una de las siguientes acciones:

| Si desea que la autenticación local sea... | Introduzca el comando...                                                                       |
|--------------------------------------------|------------------------------------------------------------------------------------------------|
| Activado                                   | <code>vsserver cifs options modify -vsserver vsserver_name -is-local-auth-enabled true</code>  |
| Deshabilitado                              | <code>vsserver cifs options modify -vsserver vsserver_name -is-local-auth-enabled false</code> |

3. Vuelva al nivel de privilegio de administrador: `set -privilege admin`



Ejemplo

El siguiente ejemplo habilita la autenticación de usuario local en SVM vs1:

```
cluster1::>set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-auth
-enabled true

cluster1::*> set -privilege admin
```

Información relacionada

[Cómo funciona la autenticación de usuarios locales](#)

[Habilitar o deshabilitar usuarios y grupos locales](#)

Permite gestionar cuentas de usuario local

Modifique las cuentas de usuario local

Puede modificar una cuenta de usuario local si desea cambiar el nombre completo o la descripción de un usuario existente y si desea habilitar o deshabilitar la cuenta de usuario. También puede cambiar el nombre de una cuenta de usuario local si el nombre del usuario está en peligro o si se necesita un cambio de nombre con fines administrativos.

| Si desea...                                       | Introduzca el comando...                                                                                                                                                                                                   |
|---------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Modifique el nombre completo del usuario local    | <code>vserver cifs users-and-groups local-user modify -vserver <i>vserver_name</i> -user -name <i>user_name</i> -full-name <i>text</i></code> Si el nombre completo contiene un espacio, debe estar entre comillas dobles. |
| Modifique la descripción del usuario local        | <code>vserver cifs users-and-groups local-user modify -vserver <i>vserver_name</i> -user -name <i>user_name</i> -description <i>text</i></code> Si la descripción contiene un espacio, debe estar entre comillas dobles.   |
| Habilite o deshabilite la cuenta de usuario local | <code>`vserver cifs users-and-groups local-user modify -vserver <i>vserver_name</i> -user-name <i>user_name</i> -is -account-disabled {true</code>                                                                         |
| <code>false}`</code>                              | Cambie el nombre de la cuenta de usuario local                                                                                                                                                                             |

Ejemplo

En el siguiente ejemplo, se cambia el nombre del usuario local «'CIFS\_SERVER\sue'» a «'CIFS\_SERVER\sue\_new» en la máquina virtual de almacenamiento (SVM, antes conocida como Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups local-user rename -user-name CIFS_SERVER\sue -new-user-name CIFS_SERVER\sue_new -vserver vs1
```

Habilite o deshabilite cuentas de usuario locales

Es posible habilitar una cuenta de usuario local si desea que el usuario pueda acceder a los datos contenidos en la máquina virtual de almacenamiento (SVM) a través de una conexión de SMB. También puede deshabilitar una cuenta de usuario local si no desea que ese usuario acceda a los datos de SVM mediante SMB.

Acerca de esta tarea

Para habilitar un usuario local, debe modificar la cuenta de usuario.

Paso

- 1. Ejecute la acción adecuada:

| Si desea...                    | Introduzca el comando...                                                                                                            |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Habilite la cuenta de usuario  | <code>vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -is-account -disabled false</code> |
| Desactive la cuenta de usuario | <code>vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -is-account -disabled true</code>  |

Cambiar las contraseñas de la cuenta de usuario local

Es posible cambiar la contraseña de la cuenta de un usuario local. Esto puede ser útil si la contraseña del usuario está en peligro o si el usuario ha olvidado la contraseña.

Paso

- 1. Realice la acción correspondiente para cambiar la contraseña: `vserver cifs users-and-groups local-user set-password -vserver vserver_name -user-name user_name`

Ejemplo

En el siguiente ejemplo, se establece la contraseña del usuario local "CIFS\_SERVER\sue" asociada con la máquina virtual de almacenamiento (SVM, antes denominada Vserver) vs1:

```
cluster1::> vsriver cifs users-and-groups local-user set-password -user
-name CIFS_SERVER\sue -vsriver vs1
```

Enter the new password:

Confirm the new password:

## Información relacionada

[Habilitar o deshabilitar la complejidad de contraseña necesaria para los usuarios locales de la SMB](#)

[Mostrar información acerca de la configuración de seguridad del servidor CIFS](#)

## Muestra información acerca de los usuarios locales

Puede mostrar una lista de todos los usuarios locales en un formulario de resumen. Si desea determinar qué configuración de cuenta está configurada para un usuario específico, puede mostrar información detallada de la cuenta para ese usuario, así como la información de la cuenta para varios usuarios. Esta información puede ayudarle a determinar si necesita modificar la configuración de un usuario y también a resolver problemas de autenticación o acceso a archivos.

## Acerca de esta tarea

Nunca se muestra información sobre la contraseña de un usuario.

## Paso

1. Ejecute una de las siguientes acciones:

| Si desea...                                                                                | Introduzca el comando...                                                                                        |
|--------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Mostrar información sobre todos los usuarios de la máquina virtual de almacenamiento (SVM) | <code>vsriver cifs users-and-groups local-user show -vsriver vsriver_name</code>                                |
| Muestra información detallada de la cuenta de un usuario                                   | <code>vsriver cifs users-and-groups local-user show -instance -vsriver vsriver_name -user-name user_name</code> |

Hay otros parámetros opcionales que puede elegir cuando ejecuta el comando. Consulte la página del manual para obtener más información.

## Ejemplo

El siguiente ejemplo muestra información sobre todos los usuarios locales en la SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver User Name Full Name Description
----- -
vs1 CIFS_SERVER\Administrator James Smith Built-in administrator
account
vs1 CIFS_SERVER\sue Sue Jones
```

## Muestra información acerca de las pertenencias a grupos de usuarios locales

Puede mostrar información sobre los grupos locales a los que pertenece un usuario local. Puede utilizar esta información para determinar qué acceso debe tener el usuario a los archivos y carpetas. Esta información puede ser útil para determinar qué derechos de acceso debe tener el usuario a los archivos y carpetas o al solucionar problemas de acceso a archivos.

### Acerca de esta tarea

Puede personalizar el comando para que muestre solo la información que desea ver.

### Paso

1. Ejecute una de las siguientes acciones:

| Si desea...                                                                                                                                            | Introduzca el comando...                                                                                     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| Muestra información de pertenencia de usuario local para un usuario local específico                                                                   | <code>vserver cifs users-and-groups local-user show-membership -user-name <i>user_name</i></code>            |
| Mostrar información de pertenencia al usuario local para el grupo local del que forma parte este usuario local                                         | <code>vserver cifs users-and-groups local-user show-membership -membership <i>group_name</i></code>          |
| Mostrar información de pertenencia al usuario para los usuarios locales que están asociados a una máquina virtual de almacenamiento (SVM) especificada | <code>vserver cifs users-and-groups local-user show-membership -vserver <i>vserver_name</i></code>           |
| Mostrar información detallada para todos los usuarios locales en una SVM especificada                                                                  | <code>vserver cifs users-and-groups local-user show-membership -instance -vserver <i>vserver_name</i></code> |

### Ejemplo

En el siguiente ejemplo se muestra la información de pertenencia de todos los usuarios locales de SVM vs1; el usuario «CIFS\_SERVER\Administrator» es miembro del grupo «BUILTIN\Administrators» y «CIFS\_SERVER\sue» es miembro del grupo «CIFS\_SERVER\g1»:

```
cluster1::> vserver cifs users-and-groups local-user show-membership
-vserver vs1
```

| Vserver | User Name                 | Membership             |
|---------|---------------------------|------------------------|
| vs1     | CIFS_SERVER\Administrator | BUILTIN\Administrators |
|         | CIFS_SERVER\sue           | CIFS_SERVER\g1         |

## Eliminar cuentas de usuario locales

Es posible eliminar cuentas de usuario locales de la máquina virtual de almacenamiento (SVM) si ya no son necesarias para la autenticación local de SMB en el servidor CIFS o para determinar los derechos de acceso a los datos incluidos en la SVM.

### Acerca de esta tarea

Tenga en cuenta lo siguiente al eliminar usuarios locales:

- El sistema de archivos no se ha modificado.

Los descriptores de seguridad de Windows de los archivos y directorios que hacen referencia a este usuario no están ajustados.

- Todas las referencias a los usuarios locales se eliminan de las bases de datos de pertenencia y privilegios.
- No se pueden eliminar los usuarios estándar conocidos, como el Administrador.

### Pasos

1. Determine el nombre de la cuenta de usuario local que desea eliminar: `vserver cifs users-and-groups local-user show -vserver vserver_name`
2. Elimine el usuario local: `vserver cifs users-and-groups local-user delete -vserver vserver_name -user-name username_name`
3. Compruebe que la cuenta de usuario se ha eliminado: `vserver cifs users-and-groups local-user show -vserver vserver_name`

### Ejemplo

En el siguiente ejemplo se elimina el usuario local "CIFS\_SERVER\sue" asociado con SVM vs1:

```

cluster1::> vsriver cifs users-and-groups local-user show -vsriver vs1
Vserver User Name Full Name Description
----- -
vs1 CIFS_SERVER\Administrator James Smith Built-in administrator
account
vs1 CIFS_SERVER\sue Sue Jones

cluster1::> vsriver cifs users-and-groups local-user delete -vsriver vs1
-user-name CIFS_SERVER\sue

cluster1::> vsriver cifs users-and-groups local-user show -vsriver vs1
Vserver User Name Full Name Description
----- -
vs1 CIFS_SERVER\Administrator James Smith Built-in administrator
account

```

Administrar grupos locales

Modificar grupos locales

Puede modificar los grupos locales existentes cambiando la descripción de un grupo local existente o cambiando el nombre del grupo.

| Si desea...                              | Usar el comando...                                                                                                                                                                       |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Modifique la descripción del grupo local | vsriver cifs users-and-groups local-group modify -vsriver vsriver_name -group-name group_name -description text Si la descripción contiene un espacio, debe estar entre comillas dobles. |
| Cambie el nombre del grupo local         | vsriver cifs users-and-groups local-group rename -vsriver vsriver_name -group-name group_name -new-group-name new_group_name                                                             |

Ejemplos

En el ejemplo siguiente se cambia el nombre del grupo local "CIFS\_SERVER\engineering" a "CIFS\_SERVER\engineering\_new":

```

cluster1::> vsriver cifs users-and-groups local-group rename -vsriver vs1
-group-name CIFS_SERVER\engineering -new-group-name
CIFS_SERVER\engineering_new

```

En el siguiente ejemplo se modifica la descripción del grupo local "CIFS\_SERVER\engineering":

```
cluster1::> vsserver cifs users-and-groups local-group modify -vsserver vs1
-group-name CIFS_SERVER\engineering -description "New Description"
```

**Muestra información acerca de los grupos locales**

Es posible mostrar una lista de todos los grupos locales configurados en el clúster o en una máquina virtual de almacenamiento (SVM) específica. Esta información puede ser útil para solucionar problemas de acceso a los archivos en la SVM o problemas de derechos de usuario (privilegios) en la SVM.

**Paso**

- 1. Ejecute una de las siguientes acciones:

| Si desea información acerca de...    | Introduzca el comando...                                                             |
|--------------------------------------|--------------------------------------------------------------------------------------|
| Todos los grupos locales del clúster | <code>vsserver cifs users-and-groups local-group show</code>                         |
| Todos los grupos locales en la SVM   | <code>vsserver cifs users-and-groups local-group show -vsserver vsserver_name</code> |

Hay otros parámetros opcionales que puede elegir cuando ejecuta este comando. Consulte la página del manual para obtener más información.

**Ejemplo**

En el siguiente ejemplo, se muestra información sobre todos los grupos locales en la SVM vs1:

```
cluster1::> vsserver cifs users-and-groups local-group show -vsserver vs1
Vserver Group Name Description
----- -
vs1 BUILTIN\Administrators Built-in Administrators group
vs1 BUILTIN\Backup Operators Backup Operators group
vs1 BUILTIN\Power Users Restricted administrative privileges
vs1 BUILTIN\Users All users
vs1 CIFS_SERVER\engineering
vs1 CIFS_SERVER\sales
```

**Administrar la pertenencia a grupos locales**

Puede administrar la pertenencia a grupos locales agregando y eliminando usuarios locales o de dominio, o agregando y eliminando grupos de dominios. Esto resulta útil si desea controlar el acceso a los datos basándose en los controles de acceso colocados en el grupo o si desea que los usuarios tengan privilegios asociados a ese grupo.

**Acerca de esta tarea**

Directrices para agregar miembros a un grupo local:

- No puede agregar usuarios al grupo especial *Everyone*.
- El grupo local debe existir antes de poder añadir un usuario.
- El usuario debe existir antes de poder agregar el usuario a un grupo local.
- No puede agregar un grupo local a otro grupo local.
- Para agregar un usuario o grupo de dominio a un grupo local, Data ONTAP debe poder resolver el nombre a un SID.

Directrices para eliminar miembros de un grupo local:

- No puede eliminar miembros del grupo especial *Everyone*.
- El grupo del que desea quitar un miembro debe existir.
- ONTAP debe poder resolver los nombres de los miembros que desea quitar del grupo a un SID correspondiente.

**Paso**

1. Agregar o quitar un miembro de un grupo.

| Si desea...                   | A continuación, se usa el comando...                                                                                                                                                                                                                                                                              |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Agregar un miembro a un grupo | <pre>vserver cifs users-and-groups local-group add-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]</pre> <p>Puede especificar una lista delimitada por comas de usuarios locales, usuarios de dominio o grupos de dominio que desee agregar al grupo local especificado.</p>    |
| Quitar un miembro de un grupo | <pre>vserver cifs users-and-groups local-group remove-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]</pre> <p>Puede especificar una lista delimitada por comas de usuarios locales, usuarios de dominio o grupos de dominio que desee quitar del grupo local especificado.</p> |

En el siguiente ejemplo, se agrega un usuario local "MB\_SERVER\sue" y un grupo de dominios "AD\_DOM\dom\_eng" al grupo local "MB\_SERVER\engineering" en SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group add-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,AD_DOMAIN\dom_eng
```

En el siguiente ejemplo se eliminan los usuarios locales «MB\_SERVER\sue» y «MB\_SERVER\james» del



grupo local «MB\_SERVER\engineering» de SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

Información relacionada

[Mostrar información acerca de los miembros de los grupos locales](#)

Muestra información acerca de los miembros de los grupos locales

Es posible mostrar una lista de todos los miembros de grupos locales configurados en el clúster o en una máquina virtual de almacenamiento (SVM) especificada. Esta información puede ser útil para solucionar problemas de acceso a archivos o problemas de derechos de usuario (privilegios).

Paso

- 1. Ejecute una de las siguientes acciones:

| Si desea mostrar información acerca de...        | Introduzca el comando...                                                            |
|--------------------------------------------------|-------------------------------------------------------------------------------------|
| Miembros de todos los grupos locales del cluster | vserver cifs users-and-groups local-group show-members                              |
| Miembros de todos los grupos locales en la SVM   | vserver cifs users-and-groups local-group show-members -vserver <i>vserver_name</i> |

Ejemplo

En el siguiente ejemplo, se muestra información acerca de los miembros de todos los grupos locales en la SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group show-members
-vserver vs1
Vserver Group Name Members

vs1 BUILTIN\Administrators CIFS_SERVER\Administrator
 AD_DOMAIN\Domain Admins
 AD_DOMAIN\dom_grp1
 BUILTIN\Users AD_DOMAIN\Domain Users
 AD_DOMAIN\dom_usr1
 CIFS_SERVER\engineering CIFS_SERVER\james
```

## Eliminar un grupo local

Es posible eliminar un grupo local de la máquina virtual de almacenamiento (SVM) si ya no es necesario para determinar los derechos de acceso a los datos asociados con esa SVM o si ya no es necesario para asignar los derechos de usuario (privilegios) de SVM a los miembros del grupo.

### Acerca de esta tarea

Tenga en cuenta lo siguiente al eliminar grupos locales:

- El sistema de archivos no se ha modificado.

Los descriptores de seguridad de Windows de los archivos y directorios que hacen referencia a este grupo no se ajustan.

- Si el grupo no existe, se devuelve un error.
- El grupo especial *Everyone* no se puede eliminar.
- Los grupos integrados como *BUILTIN\Administrators* *BUILTIN\Users* no se pueden eliminar.

### Pasos

1. Determine el nombre del grupo local que desea eliminar mostrando la lista de grupos locales de la SVM:  
`vserver cifs users-and-groups local-group show -vserver vserver_name`
2. Elimine el grupo local: `vserver cifs users-and-groups local-group delete -vserver vserver_name -group-name group_name`
3. Compruebe que el grupo se ha eliminado: `vserver cifs users-and-groups local-user show -vserver vserver_name`

### Ejemplo

En el siguiente ejemplo se elimina el grupo local "CIFS\_SERVER\sales" asociado con SVM vs1:

```

cluster1::> vsserver cifs users-and-groups local-group show -vsserver vs1
Vserver Group Name Description

vs1 BUILTIN\Administrators Built-in Administrators group
vs1 BUILTIN\Backup Operators Backup Operators group
vs1 BUILTIN\Power Users Restricted administrative
privileges
vs1 BUILTIN\Users All users
vs1 CIFS_SERVER\engineering
vs1 CIFS_SERVER\sales

cluster1::> vsserver cifs users-and-groups local-group delete -vsserver vs1
-group-name CIFS_SERVER\sales

cluster1::> vsserver cifs users-and-groups local-group show -vsserver vs1
Vserver Group Name Description

vs1 BUILTIN\Administrators Built-in Administrators group
vs1 BUILTIN\Backup Operators Backup Operators group
vs1 BUILTIN\Power Users Restricted administrative
privileges
vs1 BUILTIN\Users All users
vs1 CIFS_SERVER\engineering

```

## Actualizar nombres de usuario y grupo de dominio en bases de datos locales

Puede agregar usuarios y grupos de dominio a los grupos locales de un servidor CIFS. Estos objetos de dominio se registran en bases de datos locales en el clúster. Si se cambia el nombre de un objeto de dominio, las bases de datos locales deben actualizarse manualmente.

### Acerca de esta tarea

Debe especificar el nombre de la máquina virtual de almacenamiento (SVM) en la que desea actualizar los nombres de dominio.

### Pasos

1. Configure el nivel de privilegio en Advanced: `set -privilege advanced`
2. Ejecute la acción adecuada:

| Si desea actualizar usuarios y grupos de dominio y...                                                       | Se usa este comando...                                                           |
|-------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| Muestra usuarios y grupos de dominio que se han actualizado correctamente y que no se han podido actualizar | <code>vsserver cifs users-and-groups update-names -vsserver vsserver_name</code> |

| Si desea actualizar usuarios y grupos de dominio y...                         | Se usa este comando...                                                                                    |
|-------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| Muestra los usuarios y grupos de dominio que se han actualizado correctamente | <code>vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only false</code> |
| Muestra sólo los usuarios y grupos de dominio que no se pueden actualizar     | <code>vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only true</code>  |
| Suprimir toda la información de estado acerca de las actualizaciones          | <code>vserver cifs users-and-groups update-names -vserver vserver_name -suppress -all-output true</code>  |

3. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

### Ejemplo

En el siguiente ejemplo se actualizan los nombres de los usuarios y grupos de dominio asociados con la máquina virtual de almacenamiento (SVM, antes denominada Vserver) vs1. Para la última actualización, hay una cadena de nombres dependiente que se debe actualizar:

```

cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vsserver cifs users-and-groups update-names -vsserver vs1

Vserver: vs1
SID: S-1-5-21-123456789-234565432-987654321-12345
Domain: EXAMPLE1
Out-of-date Name: dom_user1
Updated Name: dom_user2
Status: Successfully updated

Vserver: vs1
SID: S-1-5-21-123456789-234565432-987654322-23456
Domain: EXAMPLE2
Out-of-date Name: dom_user1
Updated Name: dom_user2
Status: Successfully updated

Vserver: vs1
SID: S-1-5-21-123456789-234565432-987654321-123456
Domain: EXAMPLE1
Out-of-date Name: dom_user3
Updated Name: dom_user4
Status: Successfully updated; also updated SID "S-1-5-21-
123456789-234565432-987654321-123457"
 to name "dom_user5"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123458"
 to name "dom_user6"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123459"
 to name "dom_user7"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123460"
 to name "dom_user8"

The command completed successfully. 7 Active Directory objects have been
updated.

cluster1::*> set -privilege admin

```

## Añada privilegios a usuarios o grupos locales o de dominio

Puede administrar los derechos de usuario para usuarios o grupos locales o de dominio mediante la adición de privilegios. Los privilegios agregados anulan los privilegios predeterminados asignados a cualquiera de estos objetos. Esto proporciona una seguridad mejorada al permitirle personalizar qué privilegios tiene un usuario o grupo.

### Antes de empezar

Debe haber ya el usuario o grupo local o de dominio al que se añadirán privilegios.

### Acerca de esta tarea

Al agregar un privilegio a un objeto se reemplazan los privilegios predeterminados para ese usuario o grupo. Al añadir un privilegio, no se quitan los privilegios añadidos anteriormente.

Debe tener en cuenta lo siguiente al agregar privilegios a usuarios o grupos locales o de dominio:

- Puede añadir uno o varios privilegios.
- Al agregar privilegios a un usuario o grupo de dominio, ONTAP puede validar el usuario o grupo de dominio poniéndose en contacto con el controlador de dominio.

Es posible que se produzca un error en el comando si ONTAP no puede comunicarse con la controladora de dominio.

### Pasos

1. Agregue uno o más privilegios a un usuario o grupo local o de dominio: `vserver cifs users-and-groups privilege add-privilege -vserver _vserver_name_ -user-or-group-name name -privileges _privilege_[,...]`
2. Compruebe que los privilegios deseados se aplican al objeto: `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

### Ejemplo

En el siguiente ejemplo, se añaden los privilegios «ShebPrivilege» y «SeeTakeOwnershipPrivilege» al usuario «CIFS\_SERVER\sue» en la máquina virtual de almacenamiento (SVM, antes denominada Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver User or Group Name Privileges

vs1 CIFS_SERVER\sue SeTcbPrivilege
 SeTakeOwnershipPrivilege
```

## Quitar privilegios de usuarios o grupos locales o de dominio

Puede administrar derechos de usuario para usuarios o grupos locales o de dominio eliminando privilegios. Esto proporciona una seguridad mejorada al permitirle

personalizar los privilegios máximos que tienen los usuarios y los grupos.

### Antes de empezar

Debe haber ya el usuario o grupo local o de dominio del que se eliminarán los privilegios.

### Acerca de esta tarea

Al quitar privilegios de usuarios o grupos locales o de dominio, debe tener en cuenta lo siguiente:

- Puede eliminar uno o varios privilegios.
- Al eliminar privilegios de un usuario o grupo de dominio, ONTAP puede validar el usuario o grupo de dominio poniéndose en contacto con el controlador de dominio.

Es posible que se produzca un error en el comando si ONTAP no puede comunicarse con la controladora de dominio.

### Pasos

1. Elimine uno o más privilegios de un usuario o grupo local o de dominio: `vserver cifs users-and-groups privilege remove-privilege -vserver _vserver_name_ -user-or-group-name _name_ -privileges _privilege_[,...]`
2. Compruebe que los privilegios deseados se han eliminado del objeto: `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

### Ejemplo

En el siguiente ejemplo se eliminan los privilegios «DeeTcbPrivilege» y «SeeTakeOwnershipPrivilege» del usuario «CIFS\_SERVER\sue» en la máquina virtual de almacenamiento (SVM, antes denominada Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver User or Group Name Privileges

vs1 CIFS_SERVER\sue SeTcbPrivilege
 SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver User or Group Name Privileges

vs1 CIFS_SERVER\sue -
```

### Restablecer privilegios para usuarios y grupos locales o de dominio

Es posible restablecer privilegios para los grupos y usuarios locales o de dominio. Esto puede ser útil si ha realizado modificaciones a los privilegios de un usuario o grupo local o de dominio y esas modificaciones ya no se desean ni se necesitan.

## Acerca de esta tarea

Al restablecer los privilegios de un usuario o grupo local o de dominio, se quitan todas las entradas de privilegios de ese objeto.

## Pasos

1. Restablecer los privilegios de un usuario o grupo local o de dominio: `vserver cifs users-and-groups privilege reset-privilege -vserver vserver_name -user-or-group-name name`
2. Compruebe que los privilegios se restablecen en el objeto: `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

## Ejemplos

En el siguiente ejemplo, se restablecen los privilegios para el usuario «'CIFS\_SERVER\sue'» en la máquina virtual de almacenamiento (SVM, anteriormente conocida como Vserver) vs1. De forma predeterminada, los usuarios normales no tienen privilegios asociados a sus cuentas:

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver User or Group Name Privileges

vs1 CIFS_SERVER\sue SeTcbPrivilege
 SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

En el ejemplo siguiente se restablecen los privilegios para el grupo "BUILTIN\Administrators", eliminando de forma efectiva la entrada de privilegios:

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver User or Group Name Privileges

vs1 BUILTIN\Administrators SeRestorePrivilege
 SeSecurityPrivilege
 SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name BUILTIN\Administrators

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```



Muestra información acerca de anulaciones de privilegios

Puede mostrar información acerca de los privilegios personalizados asignados a cuentas o grupos de usuarios locales o de dominio. Esta información le ayuda a determinar si se aplican los derechos de usuario deseados.

Paso

- 1. Ejecute una de las siguientes acciones:

| Si desea mostrar información acerca de...                                                                                      | Introduzca este comando...                                                                                       |
|--------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Privilegios personalizados para todos los grupos y usuarios locales y de dominio en la máquina virtual de almacenamiento (SVM) | <code>vserver cifs users-and-groups<br/>privilege show -vserver vserver_name</code>                              |
| Privilegios personalizados para un dominio o un grupo y usuario local específicos de la SVM                                    | <code>vserver cifs users-and-groups<br/>privilege show -vserver vserver_name<br/>-user-or-group-name name</code> |

Hay otros parámetros opcionales que puede elegir cuando ejecuta este comando. Consulte la página del manual para obtener más información.

Ejemplo

El siguiente comando muestra todos los privilegios asociados explícitamente con los usuarios y grupos locales o de dominio para SVM vs1:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver User or Group Name Privileges

vs1 BUILTIN\Administrators SeTakeOwnershipPrivilege
 SeRestorePrivilege
vs1 CIFS_SERVER\sue SeTcbPrivilege
 SeTakeOwnershipPrivilege
```

Configurar la comprobación de recorrido de derivación

Configurar el resumen de comprobación de recorrido de derivación

La comprobación de recorrido de omisión es un derecho de usuario (también conocido como *Privilege*) que determina si un usuario puede recorrer todos los directorios de la ruta de acceso a un archivo incluso si el usuario no tiene permisos en el directorio de recorrido. Debe comprender lo que sucede al permitir o dejar de permitir la comprobación de recorrido por omisión, y cómo configurar la comprobación de recorrido por omisión para los usuarios en máquinas virtuales de almacenamiento (SVM).

## Qué sucede cuando se permite o se despermite la comprobación de recorrido de derivación

- Si se permite, cuando un usuario intenta acceder a un archivo, ONTAP no comprueba el permiso Traverse para los directorios intermedios al determinar si se concede o deniega el acceso al archivo.
- Si no se permite, ONTAP comprueba el permiso recorrer (ejecutar) para todos los directorios de la ruta de acceso al archivo.

Si alguno de los directorios intermedios no tiene el "X" (permiso de desplazamiento), ONTAP niega el acceso al archivo.

## Configurar la comprobación de recorrido de derivación

Puede configurar la comprobación de recorrido de desvío mediante la interfaz de línea de comandos de ONTAP o mediante la configuración de directivas de grupo de Active Directory con este derecho de usuario.

La `SeChangeNotifyPrivilege` los privilegios controlan si se permite a los usuarios omitir la comprobación de recorrido.

- Si se la agrega a los usuarios o grupos SMB locales en la SVM o a usuarios o grupos de dominio, permite omitir el control transversal.
- Si lo elimina de usuarios o grupos SMB locales en la SVM o de usuarios o grupos de dominio, no permite omitir la comprobación cruzada.

De forma predeterminada, los siguientes grupos BUILTIN de la SVM tienen derecho a omitir la comprobación de recorrido:

- BUILTIN\Administrators
- BUILTIN\Power Users
- BUILTIN\Backup Operators
- BUILTIN\Users
- Everyone

Si no desea permitir a los miembros de uno de estos grupos omitir la comprobación de recorrido, debe quitar este privilegio del grupo.

Debe tener en cuenta lo siguiente al configurar la comprobación de derivación cruzada de usuarios y grupos de SMB locales en la SVM mediante la CLI:

- Si desea permitir a los miembros de un grupo de dominio o local personalizado omitir la comprobación de recorrido, debe agregar el `SeChangeNotifyPrivilege` privilegio para ese grupo.
- Si desea permitir que un usuario local o de dominio individual omita la comprobación de recorrido y que el usuario no sea miembro de un grupo con ese privilegio, puede agregar el `SeChangeNotifyPrivilege` privilegio para esa cuenta de usuario.
- Puede deshabilitar la comprobación de recorrido de omisión para usuarios o grupos locales o de dominio quitando el `SeChangeNotifyPrivilege` de privilegio en cualquier momento.



Para deshabilitar la comprobación de traversal de omisión para usuarios o grupos locales o de dominio especificados, también debe quitar el `SeChangeNotifyPrivilege` privilegio de la Everyone grupo.

## Información relacionada

[Permitir a los usuarios o grupos omitir la comprobación de recorrido del directorio](#)

[No permitir a los usuarios o grupos omitir la comprobación de recorrido del directorio](#)

[Configurar la asignación de caracteres para la traducción de nombres de archivo SMB en volúmenes](#)

[Cree listas de control de acceso a recursos compartidos de SMB](#)

[Acceso seguro a archivos mediante Storage-Level Access Guard](#)

[Lista de privilegios compatibles](#)

[Añada privilegios a usuarios o grupos locales o de dominio](#)

## Permitir a los usuarios o grupos omitir la comprobación de recorrido del directorio

Si desea que un usuario pueda recorrer todos los directorios de la ruta de acceso a un archivo incluso si el usuario no tiene permisos en un directorio atravesado, puede agregar el `SeChangeNotifyPrivilege` Privilegios para los usuarios o grupos de SMB locales en máquinas virtuales de almacenamiento (SVM). De forma predeterminada, los usuarios pueden omitir la comprobación de recorrido del directorio.

### Antes de empezar

- Debe haber un servidor SMB en la SVM.
- Debe habilitarse la opción del servidor SMB para los usuarios locales y los grupos.
- El usuario o el grupo local o de dominio al que se va `SeChangeNotifyPrivilege` el privilegio se añadirá debe existir.

### Acerca de esta tarea

Al agregar privilegios a un usuario o grupo de dominio, ONTAP puede validar el usuario o grupo de dominio poniéndose en contacto con el controlador de dominio. Es posible que se produzca un error en el comando si ONTAP no puede comunicarse con la controladora de dominio.

### Pasos

1. Active la comprobación de recorrido de derivación agregando el `SeChangeNotifyPrivilege` privilegio para un usuario o grupo local o de dominio: `vserver cifs users-and-groups privilege add-privilege -vserver vserver_name -user-or-group-name name -privileges SeChangeNotifyPrivilege`

El valor de `-user-or-group-name` parámetro es un usuario o grupo local, o un usuario o grupo de dominio.

2. Compruebe que el usuario o grupo especificado tiene activada la comprobación de recorrido de derivación: `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

### Ejemplo

El siguiente comando permite a los usuarios que pertenecen al grupo `"EXAMPLE\eng"` omitir la comprobación de recorrido del directorio agregando el `SeChangeNotifyPrivilege` privilegio para el grupo:

```
cluster1::> vsserver cifs users-and-groups privilege add-privilege -vsserver
vs1 -user-or-group-name EXAMPLE\eng -privileges SeChangeNotifyPrivilege

cluster1::> vsserver cifs users-and-groups privilege show -vsserver vs1
Vserver User or Group Name Privileges

vs1 EXAMPLE\eng SeChangeNotifyPrivilege
```

## Información relacionada

[No permitir que usuarios o grupos pasen por alto la comprobación de recorrido del directorio](#)

## No permitir a los usuarios o grupos omitir la comprobación de recorrido del directorio

Si no desea que un usuario atraviese todos los directorios de la ruta de acceso a un archivo porque el usuario no tiene permisos en el directorio atravesado, puede quitar el `SeChangeNotifyPrivilege` Privilegios de usuarios o grupos de SMB locales en máquinas virtuales de almacenamiento (SVM).

## Antes de empezar

Debe haber ya el usuario o grupo local o de dominio del que se eliminarán los privilegios.

## Acerca de esta tarea

Al eliminar privilegios de un usuario o grupo de dominio, ONTAP puede validar el usuario o grupo de dominio poniéndose en contacto con el controlador de dominio. Es posible que se produzca un error en el comando si ONTAP no puede comunicarse con la controladora de dominio.

## Pasos

1. Desactivar la comprobación de recorrido de derivación: `vsserver cifs users-and-groups privilege remove-privilege -vsserver vsserver_name -user-or-group-name name -privileges SeChangeNotifyPrivilege`

El comando quita el `SeChangeNotifyPrivilege` privilegio del usuario o grupo de dominio o local que especifique con el valor para `-user-or-group-name name` parámetro.

2. Compruebe que el usuario o grupo especificado tiene desactivada la comprobación de recorrido de derivación: `vsserver cifs users-and-groups privilege show -vsserver vsserver_name -user-or-group-name name`

## Ejemplo

El siguiente comando evita que los usuarios que pertenecen al grupo "EXAMPLE\eng" pasen por alto la comprobación de recorrido del directorio:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver User or Group Name Privileges

vs1 EXAMPLE\eng SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name EXAMPLE\eng -privileges
SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver User or Group Name Privileges

vs1 EXAMPLE\eng -
```

### Información relacionada

[Permitir a usuarios o grupos omitir la comprobación de recorrido del directorio](#)

### Muestra información acerca de las políticas de auditoría y seguridad de archivos

Muestra información general sobre la seguridad de archivos y las políticas de auditoría

Puede mostrar información sobre la seguridad de los archivos y directorios contenidos en volúmenes en máquinas virtuales de almacenamiento (SVM). Puede mostrar información sobre las políticas de auditoría en los volúmenes de FlexVol. Si se configura, se puede mostrar información acerca de las opciones de seguridad Protección del acceso a nivel de almacenamiento y Control de acceso dinámico en volúmenes de FlexVol.

### Mostrar información acerca de la seguridad de archivos

Puede visualizar la información sobre la seguridad de los archivos aplicada a los datos contenidos en volúmenes y qtrees (para volúmenes FlexVol) con los siguientes estilos de seguridad:

- NTFS
- UNIX
- Mixto

### Visualización de información acerca de las directivas de auditoría

Puede mostrar información sobre las políticas de auditoría para auditar eventos de acceso en los volúmenes FlexVol mediante los siguientes protocolos NAS:

- SMB (todas las versiones)
- NFSv4. X

## Mostrar información acerca de la seguridad de la protección de acceso a nivel de almacenamiento (SLAG)

La seguridad de protección de acceso a nivel de almacenamiento se puede aplicar en volúmenes de FlexVol y objetos de qtree con los siguientes estilos de seguridad:

- NTFS
- Mixto
- UNIX (si se configura un servidor CIFS en la SVM que contiene el volumen)

## Mostrar información acerca de la seguridad del control de acceso dinámico (DAC)

La seguridad de control de acceso dinámico se puede aplicar a un objeto dentro de un volumen FlexVol con los siguientes estilos de seguridad:

- NTFS
- Mixto (si el objeto tiene seguridad efectiva NTFS)

### Información relacionada

[Protección del acceso a archivos mediante Storage-Level Access Guard](#)

[Se muestra información acerca de Storage-Level Access Guard](#)

## Mostrar información acerca de la seguridad de archivos en volúmenes de estilo de seguridad NTFS

Puede mostrar información acerca de la seguridad de archivos y directorios en volúmenes de estilo de seguridad NTFS, incluidos el estilo de seguridad y los estilos de seguridad efectivos, los permisos que se aplican e información acerca de los atributos dos. Puede utilizar los resultados para validar la configuración de seguridad o solucionar problemas de acceso a archivos.

### Acerca de esta tarea

Debe proporcionar el nombre de la máquina virtual de almacenamiento (SVM) y la ruta a los datos cuya información de seguridad de archivo o carpeta desee mostrar. Puede mostrar el resultado en forma de resumen o como una lista detallada.

- Debido a que los volúmenes y qtrees de estilo de seguridad NTFS utilizan sólo permisos de archivo NTFS y usuarios y grupos de Windows al determinar los derechos de acceso a archivos, los campos de salida relacionados con UNIX contienen información de permisos de archivo UNIX de sólo visualización.
- Se muestra la salida de ACL para archivos y carpetas con seguridad NTFS.
- Como la seguridad de Access Guard a nivel de almacenamiento se puede configurar en el volumen raíz o en el qtree, la salida de un volumen o una ruta de qtree en la que se configure la protección de acceso a nivel de almacenamiento puede mostrar tanto ACL de archivos normales como ACL de Storage-Level Access Guard.
- El resultado también muestra información acerca de los ACE de control de acceso dinámico si el Control de acceso dinámico está configurado para la ruta de acceso de archivo o directorio indicada.

### Paso

1. Mostrar la configuración de seguridad de archivos y directorios con el nivel de detalle deseado:

| Si desea mostrar información... | Introduzca el siguiente comando...                                                                           |
|---------------------------------|--------------------------------------------------------------------------------------------------------------|
| En forma de resumen             | <code>vserver security file-directory show<br/>-vserver vserver_name -path path</code>                       |
| Con detalle ampliado            | <code>vserver security file-directory show<br/>-vserver vserver_name -path path<br/>-expand-mask true</code> |

## Ejemplos

En el ejemplo siguiente se muestra la información de seguridad acerca de la ruta `/vol4` En SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 -path /vol4
```

```

 Vserver: vs1
 File Path: /vol4
 File Inode Number: 64
 Security Style: ntfs
 Effective Style: ntfs
 DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
 Unix User Id: 0
 Unix Group Id: 0
 Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
 ACLs: NTFS Security Descriptor
 Control:0x8004
 Owner:BUILTIN\Administrators
 Group:BUILTIN\Administrators
 DACL - ACEs
 ALLOW-Everyone-0x1f01ff
 ALLOW-Everyone-0x10000000-
```

OI|CI|IO

En el ejemplo siguiente se muestra la información de seguridad con máscaras ampliadas acerca de la ruta `/data/engineering` En SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 -path -path
/data/engineering -expand-mask true
```

```

 Vserver: vs1
 File Path: /data/engineering
 File Inode Number: 5544
```

```

Security Style: ntfs
Effective Style: ntfs
DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
 ...0 = Offline
 0. = Sparse
 0... = Normal
 0. = Archive
 1 = Directory
 0.. = System
 0. = Hidden
 0 = Read Only
 Unix User Id: 0
 Unix Group Id: 0
 Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
 ACLs: NTFS Security Descriptor
 Control:0x8004

 1... = Self Relative
 .0.. = RM Control Valid
 ..0. = SACL Protected
 ...0 = DACL Protected
 0... = SACL Inherited
 0.. = DACL Inherited
 0. = SACL Inherit Required
 0 = DACL Inherit Required
 0. = SACL Defaulted
 0 = SACL Present
 0... = DACL Defaulted
 1.. = DACL Present
 0. = Group Defaulted
 0 = Owner Defaulted

Owner:BUILTIN\Administrators
Group:BUILTIN\Administrators
DACL - ACEs
 ALLOW-Everyone-0x1f01ff
 0... =
Generic Read
 .0.. =
Generic Write
 ..0. =
Generic Execute
 ...0 =

```



|                                    |             |   |
|------------------------------------|-------------|---|
| Generic All                        | .....0..... | = |
| System Security                    | .....1..... | = |
| Synchronize                        | .....1..... | = |
| Write Owner                        | .....1..... | = |
| Write DAC                          | .....1..... | = |
| Read Control                       | .....1..... | = |
| Delete                             | .....1..... | = |
| Write Attributes                   | .....1..... | = |
| Read Attributes                    | .....1..... | = |
| Delete Child                       | .....1..... | = |
| Execute                            | .....1..... | = |
| Write EA                           | .....1..... | = |
| Read EA                            | .....1..... | = |
| Append                             | .....1..... | = |
| Write                              | .....1..... | = |
| Read                               | .....1..... | = |
| ALLOW-Everyone-0x10000000-OI CI IO |             |   |
| Generic Read                       | 0.....      | = |
| Generic Write                      | .0.....     | = |
| Generic Execute                    | ..0.....    | = |
| Generic All                        | ...1.....   | = |
| System Security                    | .....0..... | = |
| Synchronize                        | .....0..... | = |

|                  |               |
|------------------|---------------|
| Write Owner      | .....0..... = |
| Write DAC        | .....0..... = |
| Read Control     | .....0..... = |
| Delete           | .....0..... = |
| Write Attributes | .....0..... = |
| Read Attributes  | .....0..... = |
| Delete Child     | .....0..... = |
| Execute          | .....0..... = |
| Write EA         | .....0..... = |
| Read EA          | .....0..... = |
| Append           | .....0..... = |
| Write            | .....0..... = |
| Read             | .....0..... = |

En el siguiente ejemplo, se muestra información de seguridad, incluida la información de seguridad de Storage-Level Access Guard, para el volumen con la ruta /datavol1 En SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1
```

```

 Vserver: vs1
 File Path: /datavol1
 File Inode Number: 77
 Security Style: ntfs
 Effective Style: ntfs
 DOS Attributes: 10
 DOS Attributes in Text: ----D---
 Expanded Dos Attributes: -
 Unix User Id: 0
 Unix Group Id: 0
 Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
 ACLs: NTFS Security Descriptor
 Control:0x8004
 Owner:BUILTIN\Administrators
 Group:BUILTIN\Administrators
 DACL - ACEs
 ALLOW-Everyone-0x1f01ff
 ALLOW-Everyone-0x10000000-OI|CI|IO

 Storage-Level Access Guard security
 SACL (Applies to Directories):
 AUDIT-EXAMPLE\Domain Users-0x120089-FA
 AUDIT-EXAMPLE\engineering-0x1f01ff-SA
 DACL (Applies to Directories):
 ALLOW-EXAMPLE\Domain Users-0x120089
 ALLOW-EXAMPLE\engineering-0x1f01ff
 ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
 SACL (Applies to Files):
 AUDIT-EXAMPLE\Domain Users-0x120089-FA
 AUDIT-EXAMPLE\engineering-0x1f01ff-SA
 DACL (Applies to Files):
 ALLOW-EXAMPLE\Domain Users-0x120089
 ALLOW-EXAMPLE\engineering-0x1f01ff
 ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

### Información relacionada

[Mostrar información sobre la seguridad de archivos en volúmenes mixtos de estilo de seguridad](#)

[Visualización de información acerca de la seguridad de archivos en volúmenes de estilo de seguridad de UNIX](#)

Puede mostrar información acerca de la seguridad de archivos y directorios en volúmenes mixtos de estilo de seguridad, incluidos el estilo de seguridad y los estilos de seguridad efectivos, los permisos que se aplican y la información acerca de los propietarios y grupos de UNIX. Puede utilizar los resultados para validar la configuración de seguridad o solucionar problemas de acceso a archivos.

**Acerca de esta tarea**

Debe proporcionar el nombre de la máquina virtual de almacenamiento (SVM) y la ruta a los datos cuya información de seguridad de archivo o carpeta desee mostrar. Puede mostrar el resultado en forma de resumen o como una lista detallada.

- Los volúmenes y qtrees de estilo de seguridad mixtos pueden contener archivos y carpetas que utilizan permisos de archivo de UNIX, bits de modo o ACL de NFSv4 y algunos archivos y directorios que utilizan permisos de archivo NTFS.
- El nivel superior de un volumen mixto de estilo de seguridad puede tener una seguridad efectiva de UNIX o NTFS.
- La salida de ACL se muestra solo para archivos y carpetas con seguridad NTFS o NFSv4.

Este campo está vacío para archivos y directorios que utilizan la seguridad de UNIX que solo tienen aplicados permisos de bit de modo (sin ACL de NFSv4).

- Los campos de salida de propietario y grupo de la salida ACL se aplican sólo en el caso de los descriptores de seguridad NTFS.
- Debido a que la seguridad de Access Guard a nivel de almacenamiento se puede configurar en un volumen o qtree de estilo de seguridad mixto incluso si el estilo de seguridad efectivo del volumen raíz o qtree es UNIX, La salida de un volumen o una ruta de qtree en la que se configure Storage-Level Access Guard podría mostrar tanto los permisos de archivos UNIX como las ACL de Storage-Level Access Guard.
- Si la ruta de acceso introducida en el comando es a datos con seguridad efectiva de NTFS, el resultado también muestra información acerca de ACE de Control de acceso dinámico si Control de acceso dinámico está configurado para el archivo o la ruta de acceso de directorio dada.

**Paso**

1. Mostrar la configuración de seguridad de archivos y directorios con el nivel de detalle deseado:

| Si desea mostrar información... | Introduzca el siguiente comando...                                                                           |
|---------------------------------|--------------------------------------------------------------------------------------------------------------|
| En forma de resumen             | <code>vserver security file-directory show<br/>-vserver vserver_name -path path</code>                       |
| Con detalle ampliado            | <code>vserver security file-directory show<br/>-vserver vserver_name -path path<br/>-expand-mask true</code> |

**Ejemplos**

En el ejemplo siguiente se muestra la información de seguridad acerca de la ruta /projects En SVM vs1 con una máscara expandida. Esta ruta mixta de estilo de seguridad tiene una seguridad efectiva de UNIX.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/projects -expand-mask true
```

```
 Vserver: vs1
 File Path: /projects
 File Inode Number: 78
 Security Style: mixed
 Effective Style: unix
 DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
 ...0 = Offline
 0. = Sparse
 0... = Normal
 0. = Archive
 1 = Directory
 0.. = System
 0. = Hidden
 0 = Read Only
 Unix User Id: 0
 Unix Group Id: 1
 Unix Mode Bits: 700
 Unix Mode Bits in Text: rwx-----
 ACLs: -
```

En el ejemplo siguiente se muestra la información de seguridad acerca de la ruta /data En SVM vs1. Esta ruta mixta de estilo de seguridad tiene una seguridad NTFS efectiva.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /data
```

```

 Vserver: vs1
 File Path: /data
 File Inode Number: 544
 Security Style: mixed
 Effective Style: ntfs
 DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
 Unix User Id: 0
 Unix Group Id: 0
 Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
 ACLs: NTFS Security Descriptor
 Control:0x8004
 Owner:BUILTIN\Administrators
 Group:BUILTIN\Administrators
 DACL - ACEs
 ALLOW-Everyone-0x1f01ff
 ALLOW-Everyone-0x10000000-
```

OI|CI|IO

En el siguiente ejemplo, se muestra la información de seguridad sobre el volumen en la ruta /datavol5 En SVM vs1. El nivel superior de este volumen mixto de estilo de seguridad ofrece una seguridad efectiva para UNIX. El volumen tiene seguridad de protección de acceso en el nivel de almacenamiento.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /datavol5
```

```
 Vserver: vs1
 File Path: /datavol5
File Inode Number: 3374
 Security Style: mixed
 Effective Style: unix
 DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
 Unix User Id: 0
 Unix Group Id: 0
 Unix Mode Bits: 755
Unix Mode Bits in Text: rwxr-xr-x
 ACLs: Storage-Level Access Guard security
 SACL (Applies to Directories):
 AUDIT-EXAMPLE\Domain Users-0x120089-FA
 AUDIT-EXAMPLE\engineering-0x1f01ff-SA
 AUDIT-EXAMPLE\market-0x1f01ff-SA
 DACL (Applies to Directories):
 ALLOW-BUILTIN\Administrators-0x1f01ff
 ALLOW-CREATOR OWNER-0x1f01ff
 ALLOW-EXAMPLE\Domain Users-0x120089
 ALLOW-EXAMPLE\engineering-0x1f01ff
 ALLOW-EXAMPLE\market-0x1f01ff
 SACL (Applies to Files):
 AUDIT-EXAMPLE\Domain Users-0x120089-FA
 AUDIT-EXAMPLE\engineering-0x1f01ff-SA
 AUDIT-EXAMPLE\market-0x1f01ff-SA
 DACL (Applies to Files):
 ALLOW-BUILTIN\Administrators-0x1f01ff
 ALLOW-CREATOR OWNER-0x1f01ff
 ALLOW-EXAMPLE\Domain Users-0x120089
 ALLOW-EXAMPLE\engineering-0x1f01ff
 ALLOW-EXAMPLE\market-0x1f01ff
```

### Información relacionada

[Mostrar información acerca de la seguridad de archivos en volúmenes de estilo de seguridad NTFS](#)

[Visualización de información acerca de la seguridad de archivos en volúmenes de estilo de seguridad de UNIX](#)

### Muestra información sobre la seguridad de archivos en volúmenes de estilo de seguridad UNIX

Puede mostrar información acerca de la seguridad de archivos y directorios en los volúmenes de estilo de seguridad de UNIX, incluidos los estilos de seguridad y los estilos de seguridad efectivos, los permisos que se aplican y la información acerca de los

propietarios y grupos de UNIX. Puede utilizar los resultados para validar la configuración de seguridad o solucionar problemas de acceso a archivos.

**Acerca de esta tarea**

Debe proporcionar el nombre de la máquina virtual de almacenamiento (SVM) y la ruta a los datos cuyo archivo o información de seguridad de directorio desee mostrar. Puede mostrar el resultado en forma de resumen o como una lista detallada.

- Los volúmenes y qtrees de estilo de seguridad de UNIX solo utilizan permisos de archivos UNIX, ya sea bits de modo o ACL de NFSv4 al determinar los derechos de acceso a los archivos.
- La salida de ACL se muestra solo para los archivos y las carpetas con seguridad de NFSv4.

Este campo está vacío para archivos y directorios que utilizan la seguridad de UNIX que solo tienen aplicados permisos de bit de modo (sin ACL de NFSv4).

- Los campos de salida de propietario y grupo de la salida de ACL no se aplican en el caso de los descriptores de seguridad de NFSv4.

Sólo son significativos para los descriptores de seguridad NTFS.

- Como la seguridad de Access Guard de nivel de almacenamiento es compatible en un volumen o qtree UNIX si se configura un servidor CIFS en la SVM, la salida puede contener información acerca de la seguridad Storage-Level Access Guard aplicada al volumen o al qtree especificado en el `-path` parámetro.

**Paso**

1. Mostrar la configuración de seguridad de archivos y directorios con el nivel de detalle deseado:

| Si desea mostrar información... | Introduzca el siguiente comando...                                                                   |
|---------------------------------|------------------------------------------------------------------------------------------------------|
| En forma de resumen             | <code>vserver security file-directory show -vserver vserver_name -path path</code>                   |
| Con detalle ampliado            | <code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code> |

**Ejemplos**

En el ejemplo siguiente se muestra la información de seguridad acerca de la ruta `/home` En SVM `vs1`:



```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
```

```

 Vserver: vs1
 File Path: /home
 File Inode Number: 9590
 Security Style: unix
 Effective Style: unix
 DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
 Unix User Id: 0
 Unix Group Id: 1
 Unix Mode Bits: 700
 Unix Mode Bits in Text: rwx-----
 ACLs: -
```

En el ejemplo siguiente se muestra la información de seguridad acerca de la ruta /home En SVM vs1 con una máscara expandida:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
-expand-mask true
```

```

 Vserver: vs1
 File Path: /home
 File Inode Number: 9590
 Security Style: unix
 Effective Style: unix
 DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
 ...0 = Offline
 0. = Sparse
 0... = Normal
 0. = Archive
 1 = Directory
 0.. = System
 0. = Hidden
 0 = Read Only
 Unix User Id: 0
 Unix Group Id: 1
 Unix Mode Bits: 700
 Unix Mode Bits in Text: rwx-----
 ACLs: -
```

## Información relacionada

[Mostrar información acerca de la seguridad de archivos en volúmenes de estilo de seguridad NTFS](#)

[Mostrar información sobre la seguridad de archivos en volúmenes mixtos de estilo de seguridad](#)

**Muestra información sobre las políticas de auditoría de NTFS en los volúmenes de FlexVol usando la interfaz de línea de comandos**

Puede mostrar información acerca de las directivas de auditoría NTFS en los volúmenes FlexVol, incluidos los estilos de seguridad y los estilos de seguridad efectivos, los permisos que se aplican e información acerca de las listas de control de acceso al sistema. Puede utilizar los resultados para validar la configuración de seguridad o para solucionar problemas de auditoría.

### Acerca de esta tarea

Debe proporcionar el nombre de la máquina virtual de almacenamiento (SVM) y la ruta a los archivos o carpetas cuya información de auditoría desee mostrar. Puede mostrar el resultado en forma de resumen o como una lista detallada.

- Los volúmenes y qtrees de estilo de seguridad NTFS sólo utilizan listas de control de acceso al sistema (SACL) NTFS para las directivas de auditoría.
- Los archivos y carpetas de un volumen mixto de estilo de seguridad con seguridad efectiva NTFS pueden tener directivas de auditoría NTFS aplicadas.

Los volúmenes y qtrees de estilo de seguridad mixtos pueden contener archivos y directorios que utilizan permisos de archivo de UNIX, bits de modo o ACL de NFSv4 y algunos archivos y directorios que utilizan permisos de archivo NTFS.

- El nivel superior de un volumen de estilo de seguridad mixto puede tener seguridad efectiva de UNIX o NTFS y puede que no contenga SACL NTFS.
- Debido a que la seguridad de Access Guard a nivel de almacenamiento se puede configurar en un volumen o qtree de estilo de seguridad mixto incluso si el estilo de seguridad efectivo del volumen raíz o qtree es UNIX, El resultado de una ruta de volumen o qtree en la que se configuró Storage-Level Access Guard puede mostrar tanto el archivo normal como la carpeta NFSv4 SACL y Storage-Level Access Guard NTFS SACL.
- Si la ruta de acceso que se introduce en el comando es para los datos con seguridad efectiva NTFS, la salida también muestra información sobre los ACE de control dinámico de acceso si el Control dinámico de acceso está configurado para la ruta de acceso del archivo o directorio dada.
- Cuando se muestra información de seguridad sobre archivos y carpetas con seguridad efectiva NTFS, los campos de salida relacionados con UNIX contienen información de permisos de archivo UNIX de sólo visualización.

Los archivos y carpetas de estilo de seguridad NTFS utilizan sólo permisos de archivo NTFS y usuarios y grupos de Windows al determinar los derechos de acceso a archivos.

- El resultado de ACL se muestra solo para los archivos y las carpetas con seguridad NTFS o NFSv4.

Este campo está vacío para archivos y carpetas que utilizan la seguridad de UNIX que solo tienen aplicados permisos de bit de modo (sin ACL de NFSv4).

- Los campos de salida de propietario y grupo de la salida ACL se aplican sólo en el caso de los descriptores de seguridad NTFS.

**Paso**

- 1. Mostrar la configuración de la directiva de auditoría de archivos y directorios con el nivel de detalle deseado:

| Si desea mostrar información... | Introduzca el siguiente comando...                                                                           |
|---------------------------------|--------------------------------------------------------------------------------------------------------------|
| En forma de resumen             | <code>vserver security file-directory show<br/>-vserver vserver_name -path path</code>                       |
| Como una lista detallada        | <code>vserver security file-directory show<br/>-vserver vserver_name -path path<br/>-expand-mask true</code> |

**Ejemplos**

En el ejemplo siguiente se muestra la información de la directiva de auditoría de la ruta de acceso /corp En SVM vs1. La ruta de acceso tiene seguridad efectiva NTFS. El descriptor de seguridad NTFS contiene UNA entrada SACL CORRECTA y UNA entrada SACL SUCCESS/FAIL.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
 Vserver: vs1
 File Path: /corp
 File Inode Number: 357
 Security Style: ntfs
 Effective Style: ntfs
 DOS Attributes: 10
 DOS Attributes in Text: ----D---
 Expanded Dos Attributes: -
 Unix User Id: 0
 Unix Group Id: 0
 Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
 ACLs: NTFS Security Descriptor
 Control:0x8014
 Owner:DOMAIN\Administrator
 Group:BUILTIN\Administrators
 SACL - ACEs
 ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
 SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
 DACL - ACEs
 ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
 ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
 ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
 ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

En el ejemplo siguiente se muestra la información de la directiva de auditoría de la ruta de acceso /datavol1 En SVM vs1. La ruta de acceso contiene tanto SACL de archivo normal como de carpeta y SACL de Storage-

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

 Vserver: vs1
 File Path: /datavol1
 File Inode Number: 77
 Security Style: ntfs
 Effective Style: ntfs
 DOS Attributes: 10
 DOS Attributes in Text: ----D---
 Expanded Dos Attributes: -
 Unix User Id: 0
 Unix Group Id: 0
 Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
 ACLs: NTFS Security Descriptor
 Control:0xaa14
 Owner:BUILTIN\Administrators
 Group:BUILTIN\Administrators
 SACL - ACEs
 AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
 DACL - ACEs
 ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
 ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

 Storage-Level Access Guard security
 SACL (Applies to Directories):
 AUDIT-EXAMPLE\Domain Users-0x120089-FA
 AUDIT-EXAMPLE\engineering-0x1f01ff-SA
 DACL (Applies to Directories):
 ALLOW-EXAMPLE\Domain Users-0x120089
 ALLOW-EXAMPLE\engineering-0x1f01ff
 ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
 SACL (Applies to Files):
 AUDIT-EXAMPLE\Domain Users-0x120089-FA
 AUDIT-EXAMPLE\engineering-0x1f01ff-SA
 DACL (Applies to Files):
 ALLOW-EXAMPLE\Domain Users-0x120089
 ALLOW-EXAMPLE\engineering-0x1f01ff
 ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Puede mostrar información sobre las políticas de auditoría de NFSv4 en volúmenes de FlexVol mediante la interfaz de línea de comandos de ONTAP, incluidos los estilos de seguridad y los estilos de seguridad efectivos, qué permisos se aplican e información sobre las listas de control de acceso del sistema (SACL). Puede utilizar los resultados para validar la configuración de seguridad o para solucionar problemas de auditoría.

**Acerca de esta tarea**

Debe proporcionar el nombre de la máquina virtual de almacenamiento (SVM) y la ruta a los archivos o directorios cuya información de auditoría desea mostrar. Puede mostrar el resultado en forma de resumen o como una lista detallada.

- Los volúmenes y qtrees de estilo de seguridad de UNIX solo utilizan NFSv4 SACL para las políticas de auditoría.
- Los archivos y directorios de un volumen de estilo de seguridad mixto que sea de estilo de seguridad UNIX pueden hacer que se les apliquen las políticas de auditoría de NFSv4.

Los volúmenes y qtrees de estilo de seguridad mixtos pueden contener archivos y directorios que utilizan permisos de archivo de UNIX, bits de modo o ACL de NFSv4 y algunos archivos y directorios que utilizan permisos de archivo NTFS.

- El nivel superior de un volumen con estilo de seguridad mixto puede tener seguridad efectiva de UNIX o NTFS y puede que contenga o no SACL de NFSv4.
- La salida de ACL se muestra solo para archivos y carpetas con seguridad NTFS o NFSv4.

Este campo está vacío para archivos y carpetas que utilizan la seguridad de UNIX que solo tienen aplicados permisos de bit de modo (sin ACL de NFSv4).

- Los campos de salida de propietario y grupo de la salida ACL se aplican sólo en el caso de los descriptores de seguridad NTFS.
- Debido a que la seguridad de Access Guard a nivel de almacenamiento se puede configurar en un volumen o qtree de estilo de seguridad mixto incluso si el estilo de seguridad efectivo del volumen raíz o qtree es UNIX, Los resultados de una ruta de volumen o qtree en la que se configuró Storage-Level Access Guard pueden mostrar tanto el archivo NFSv4 normal como las SACL de directorio y las SACL de Storage-Level Access Guard.
- Como la seguridad de Access Guard de nivel de almacenamiento es compatible en un volumen o qtree UNIX si se configura un servidor CIFS en la SVM, la salida puede contener información acerca de la seguridad Storage-Level Access Guard aplicada al volumen o al qtree especificado en el `-path` parámetro.

**Pasos**

1. Mostrar la configuración de seguridad de archivos y directorios con el nivel de detalle deseado:

| Si desea mostrar información... | Introduzca el siguiente comando...                                                 |
|---------------------------------|------------------------------------------------------------------------------------|
| En forma de resumen             | <code>vserver security file-directory show -vserver vserver_name -path path</code> |

| Si desea mostrar información... | Introduzca el siguiente comando...                                                                 |
|---------------------------------|----------------------------------------------------------------------------------------------------|
| Con detalle ampliado            | <pre>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</pre> |

## Ejemplos

En el ejemplo siguiente se muestra la información de seguridad acerca de la ruta /lab En SVM vs1. Esta ruta de seguridad de UNIX tiene un SACL de NFSv4.

```
cluster::> vserver security file-directory show -vserver vs1 -path /lab

 Vserver: vs1
 File Path: /lab
File Inode Number: 288
 Security Style: unix
Effective Style: unix
 DOS Attributes: 11
DOS Attributes in Text: ----D--R
Expanded Dos Attributes: -
 Unix User Id: 0
 Unix Group Id: 0
 Unix Mode Bits: 0
Unix Mode Bits in Text: -----
 ACLs: NFSV4 Security Descriptor
Control:0x8014
 SACL - ACEs
 SUCCESSFUL-S-1-520-0-0xf01ff-SA
 FAILED-S-1-520-0-0xf01ff-FA
 DACL - ACEs
 ALLOW-S-1-520-1-0xf01ff
```

## Formas de mostrar información acerca de las políticas de auditoría y seguridad de archivos

Puede utilizar el carácter comodín (\*) para mostrar información acerca de las directivas de auditoría y seguridad de archivos de todos los archivos y directorios de una ruta de acceso determinada o de un volumen raíz.

El carácter comodín () **se puede utilizar como último subcomponente de una ruta de directorio dada debajo de la cual se desea mostrar información de todos los archivos y directorios. Si desea mostrar información de un archivo o directorio concreto denominado «»», deberá proporcionar la ruta completa dentro de comillas dobles («»")**.

## Ejemplo

El siguiente comando con el carácter comodín muestra la información sobre todos los archivos y directorios debajo de la ruta de acceso /1/ De SVM vs1:

```

cluster::> vserver security file-directory show -vserver vs1 -path /1/*

 Vserver: vs1
 File Path: /1/1
 Security Style: mixed
 Effective Style: ntfs
 DOS Attributes: 10
 DOS Attributes in Text: ----D---
 Expanded Dos Attributes: -
 Unix User Id: 0
 Unix Group Id: 0
 Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
 ACLs: NTFS Security Descriptor
 Control:0x8514
 Owner: BUILTIN\Administrators
 Group: BUILTIN\Administrators
 DACL - ACEs
 ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)

 Vserver: vs1
 File Path: /1/1/abc
 Security Style: mixed
 Effective Style: ntfs
 DOS Attributes: 10
 DOS Attributes in Text: ----D---
 Expanded Dos Attributes: -
 Unix User Id: 0
 Unix Group Id: 0
 Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
 ACLs: NTFS Security Descriptor
 Control:0x8404
 Owner: BUILTIN\Administrators
 Group: BUILTIN\Administrators
 DACL - ACEs
 ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)

```

El siguiente comando muestra la información de un archivo denominado "" en la ruta de acceso /vol1/a De SVM vs1. La ruta está entre comillas dobles (" ").

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"
```

```
 Vserver: vs1
 File Path: "/vol1/a/*"
 Security Style: mixed
 Effective Style: unix
 DOS Attributes: 10
 DOS Attributes in Text: ----D---
 Expanded Dos Attributes: -
 Unix User Id: 1002
 Unix Group Id: 65533
 Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
 ACLs: NFSV4 Security Descriptor
 Control:0x8014
 SACL - ACEs
 AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
 DACL - ACEs
 ALLOW-EVERYONE@-0x1f00a9-FI|DI
 ALLOW-OWNER@-0x1f01ff-FI|DI
 ALLOW-GROUP@-0x1200a9-IG
```

## **Gestione la seguridad de archivos NTFS, políticas de auditoría NTFS y Storage-Level Access Guard mediante la CLI**

**Gestione la seguridad de archivos NTFS, políticas de auditoría NTFS y Storage-Level Access Guard mediante la información general de la CLI**

Puede gestionar la seguridad de archivos NTFS, políticas de auditoría de NTFS y Storage-Level Access Guard en máquinas virtuales de almacenamiento (SVM) mediante la interfaz de línea de comandos.

Puede gestionar las políticas de auditoría y seguridad de archivos NTFS desde clientes SMB o mediante la CLI. Sin embargo, al utilizar la interfaz de línea de comandos para configurar las políticas de seguridad de los archivos y de auditoría, no es necesario utilizar un cliente remoto para gestionar la seguridad de los archivos. El uso de la CLI puede reducir significativamente el tiempo que lleva aplicar la seguridad en muchos archivos y carpetas mediante un único comando.

Puede configurar la protección de acceso al nivel de almacenamiento, que es otra capa de seguridad aplicada por ONTAP a los volúmenes de SVM. Storage-Level Access Guard se aplica a los accesos desde todos los protocolos NAS al objeto de almacenamiento al que se aplica la protección de acceso a nivel de almacenamiento.

El protector de acceso a nivel de almacenamiento se puede configurar y gestionar solo desde la interfaz de línea de comandos de ONTAP. No se puede gestionar la configuración de Access Guard en el nivel de almacenamiento desde clientes SMB. Además, si ve la configuración de seguridad en un archivo o un directorio desde un cliente NFS o SMB, no verá la seguridad Storage-Level Access Guard. La seguridad de protección de acceso a nivel de almacenamiento no se puede revocar de un cliente, ni siquiera por un



administrador de sistema (Windows o UNIX). Por lo tanto, Storage-Level Access Guard ofrece una capa adicional de seguridad para el acceso a los datos que el administrador de almacenamiento establece y gestiona independientemente.



Aunque solo se admiten permisos de acceso NTFS para Storage-Level Access Guard, ONTAP puede realizar comprobaciones de seguridad para acceder a través de NFS a datos en volúmenes donde se aplica Storage-Level Access Guard si el usuario UNIX se asigna a un usuario de Windows en la SVM propietaria del volumen.

## Volúmenes de estilo de seguridad NTFS

Todos los archivos y carpetas contenidos en qtrees y volúmenes de estilo de seguridad NTFS tienen una seguridad efectiva de NTFS. Puede utilizar el `vserver security file-directory` Familia de comandos para implementar los siguientes tipos de seguridad en volúmenes de estilo de seguridad NTFS:

- Los permisos de archivo y las políticas de auditoría a los archivos y las carpetas que contiene el volumen
- Seguridad para proteger el acceso al nivel de almacenamiento en los volúmenes

## Volúmenes mixtos de estilo de seguridad

Los volúmenes y qtrees de estilo de seguridad mixtos pueden contener algunos archivos y carpetas con seguridad efectiva de UNIX y usar permisos de archivos de UNIX, bits de modo o ACL de NFSv4.x y políticas de auditoría de NFSv4.x, y algunos archivos y carpetas que tengan seguridad efectiva de NTFS y usen permisos de archivos NTFS y políticas de auditoría. Puede utilizar el `vserver security file-directory` familia de comandos para aplicar los siguientes tipos de seguridad a los datos mixtos de estilo de seguridad:

- Permisos de archivo y políticas de auditoría para archivos y carpetas con un estilo de seguridad NTFS efectivo en el volumen o qtree mixtos
- Protección del acceso a nivel de almacenamiento para volúmenes con seguridad efectiva de NTFS y UNIX

## Volúmenes de estilo de seguridad de UNIX

Los volúmenes y qtrees de estilo de seguridad de UNIX contienen archivos y carpetas que tienen una seguridad efectiva de UNIX (bits de modo o ACL de NFSv4.x). Si desea utilizar el, debe tener en cuenta los siguientes aspectos `vserver security file-directory` Familia de comandos para implementar la seguridad en volúmenes de estilo de seguridad UNIX:

- La `vserver security file-directory` No se puede utilizar la familia de comandos para gestionar las políticas de auditoría y seguridad de archivos UNIX en volúmenes y qtrees de estilo de seguridad de UNIX.
- Puede utilizar el `vserver security file-directory` Familia de comandos para configurar Storage-Level Access Guard en volúmenes de estilo de seguridad UNIX, siempre que la SVM con el volumen de destino contenga un servidor CIFS.

## Información relacionada

[Muestra información acerca de las políticas de auditoría y seguridad de archivos](#)

[Configurar y aplicar la seguridad de archivos en archivos y carpetas NTFS mediante la CLI](#)

[Configurar y aplicar directivas de auditoría a archivos y carpetas NTFS mediante la interfaz de línea de comandos](#)

### Utilice casos para utilizar la CLI para establecer la seguridad de archivos y carpetas

Dado que puede aplicar y administrar la seguridad de archivos y carpetas localmente sin la participación de un cliente remoto, puede reducir significativamente el tiempo que tarda en establecer la seguridad masiva en un gran número de archivos o carpetas.

Puede beneficiarse del uso de la CLI para establecer la seguridad de archivos y carpetas en los siguientes casos de uso:

- Almacenamiento de ficheros en entornos empresariales de gran tamaño, como el almacenamiento de ficheros en directorios iniciales
- Migración de datos
- Cambio de dominio de Windows
- Estandarización de las políticas de auditoría y seguridad de archivos en sistemas de archivos NTFS

### Limita el uso de la CLI para establecer la seguridad de archivos y carpetas

Debe estar al tanto de determinados límites cuando utilice la CLI para establecer la seguridad de archivos y carpetas.

- La `vserver security file-directory` La familia de comandos no admite la configuración de ACL de NFSv4.

Sólo puede aplicar descriptores de seguridad NTFS a archivos y carpetas NTFS.

### Cómo se utilizan los descriptores de seguridad para aplicar la seguridad de archivos y carpetas

Los descriptores de seguridad contienen las listas de control de acceso que determinan qué acciones puede realizar un usuario en archivos y carpetas, y qué se audita cuando un usuario accede a archivos y carpetas.

- **Permisos**

El propietario de un objeto permite o deniega los permisos y determina qué acciones puede realizar un objeto (usuarios, grupos u objetos de equipo) en archivos o carpetas especificados.

- **Descriptores de seguridad**

Los descriptores de seguridad son estructuras de datos que contienen información de seguridad que definen los permisos asociados a un archivo o carpeta.

- **Listas de control de acceso (ACL)**

Las listas de control de acceso son las listas contenidas en un descriptor de seguridad que contienen información sobre las acciones que los usuarios, grupos o objetos de equipo pueden realizar en el archivo o la carpeta a la que se aplica el descriptor de seguridad. El descriptor de seguridad puede contener los siguientes dos tipos de ACL:

- Listas de control de acceso discrecional (DACL)

- Listas de control de acceso del sistema (SACL)

- **Listas de control de acceso discrecional (DACL)**

Las DACL contienen la lista de SIDS para los usuarios, grupos y objetos de equipo a los que se permite o deniega el acceso para realizar acciones en archivos o carpetas. Las DACL contienen entradas de control de acceso cero o más (ACE).

- **Listas de control de acceso al sistema (SACL)**

SACL contiene la lista de SID para los usuarios, grupos y objetos de equipo para los que se registran eventos de auditoría correctos o fallidos. Las SACL contienen entradas de control de acceso cero o más (ACE).

- **Entradas de control de acceso (ACE)**

Las ACE son entradas individuales en DACL o SACL:

- Una entrada de control de acceso DACL especifica los derechos de acceso que se permiten o deniegan para determinados usuarios, grupos o objetos de equipo.
- Una entrada de control de acceso SACL especifica los eventos de éxito o de error que se deben registrar al auditar acciones especificadas realizadas por usuarios, grupos o objetos de equipo específicos.

- **Herencia de permisos**

La herencia de permisos describe cómo los permisos definidos en los descriptores de seguridad se propagan a un objeto de un objeto primario. Sólo los objetos secundarios heredan los permisos heredables. Al establecer permisos en el objeto primario, puede decidir si las carpetas, subcarpetas y archivos pueden heredarlos con "aplicar a. `this-folder`, `sub-folders`, y «`ficheros`».

## Información relacionada

["Seguimiento de seguridad y auditoría de SMB y NFS"](#)

[Configurar y aplicar directivas de auditoría a archivos y carpetas NTFS mediante la CLI](#)

### Directrices para aplicar políticas de directorio de archivos que utilizan usuarios o grupos locales en el destino de recuperación ante desastres de SVM

Hay ciertas directrices que debe tener en cuenta antes de aplicar políticas de directorio de archivos en el destino de recuperación ante desastres de la máquina virtual de almacenamiento (SVM) en una configuración de descarte de ID si la configuración de la política de directorio de archivos usa usuarios o grupos locales en el descriptor de seguridad, o en las entradas DACL o SACL.

Puede configurar una configuración de recuperación ante desastres para una SVM donde la SVM de origen en el clúster de origen replica los datos y la configuración desde la SVM de origen a una SVM de destino en un clúster de destino.

Puede configurar uno de los dos tipos de recuperación ante desastres de SVM:

- Se conserva la identidad

Con esta configuración se conserva la identidad de la SVM y el servidor CIFS.

- Identidad descartada

Con esta configuración, no se conserva la identidad de la SVM y el servidor CIFS. En esta situación, el nombre de la SVM y el servidor CIFS en la SVM de destino es diferente de la SVM y del nombre del servidor CIFS en la SVM de origen.

### Directrices para configuraciones de identidad descartadas

En una configuración de identidad descartada, en el caso de un origen de SVM que contenga configuraciones de usuarios locales, grupos y privilegios, se debe cambiar el nombre del dominio local (nombre del servidor CIFS local) para que coincida con el nombre del servidor CIFS en el destino de SVM. Por ejemplo, si el nombre de la SVM de origen es «'vs1'» y el nombre del servidor CIFS es «'CIFS1'» y el nombre de la SVM de destino es «'vs1\_dst'» y el nombre del servidor CIFS es «'CIFS1\_DST'», el nombre de dominio local de un usuario local denominado «'CIFS1\user1' se cambia automáticamente a «'CIFS1'» en el destino».

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1_dst
```

| Vserver               | User Name           | Full Name | Description |
|-----------------------|---------------------|-----------|-------------|
| vs1                   | CIFS1\Administrator |           | Built-in    |
| administrator account |                     |           |             |
| vs1                   | CIFS1\user1         | -         | -           |

```
cluster1dst::> vserver cifs users-and-groups local-user show -vserver vs1_dst
```

| Vserver               | User Name               | Full Name | Description |
|-----------------------|-------------------------|-----------|-------------|
| vs1_dst               | CIFS1_DST\Administrator |           | Built-in    |
| administrator account |                         |           |             |
| vs1_dst               | CIFS1_DST\user1         | -         | -           |

Aunque los nombres de usuario local y de grupo se cambian automáticamente en las bases de datos de usuario local y de grupo, los usuarios locales o los nombres de grupo no se cambian automáticamente en las configuraciones de políticas de directorio de archivos (las políticas configuradas en la CLI mediante el `vserver security file-directory` familia de comandos).

Por ejemplo, para "vs1", si ha configurado una entrada DACL en la `-account` El parámetro se establece en "CIFS1\user1", la configuración no se cambia automáticamente en la SVM de destino para reflejar el nombre del servidor CIFS del destino.

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1
```

```
Vserver: vs1
```

```
NTFS Security Descriptor Name: sdl
```

| Account Name | Access Type | Access Rights | Apply To    |
|--------------|-------------|---------------|-------------|
| -----        | -----       | -----         | -----       |
| CIFS1\user1  | allow       | full-control  | this-folder |

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1_dst
```

```
Vserver: vs1_dst
```

```
NTFS Security Descriptor Name: sdl
```

| Account Name    | Access Type | Access Rights | Apply To    |
|-----------------|-------------|---------------|-------------|
| -----           | -----       | -----         | -----       |
| **CIFS1**\user1 | allow       | full-control  | this-folder |

Debe utilizar el `vserver security file-directory modify` Comandos para cambiar manualmente el nombre del servidor CIFS en el nombre del servidor CIFS de destino.

## Componentes de configuración de directivas de directorio de archivos que contienen parámetros de cuenta

Existen tres componentes de configuración de directivas de directorio de archivos que pueden utilizar parámetros que pueden contener usuarios o grupos locales:

- Descriptor de seguridad

Opcionalmente, puede especificar el propietario del descriptor de seguridad y el grupo primario del propietario del descriptor de seguridad. Si el descriptor de seguridad utiliza un usuario o grupo local para las entradas del propietario y del grupo primario, debe modificar el descriptor de seguridad para utilizar la SVM de destino en el nombre de cuenta. Puede utilizar el `vserver security file-directory ntfs modify` para realizar los cambios necesarios en los nombres de cuentas.

- Entradas DACL

Cada entrada DACL debe estar asociada con una cuenta. Debe modificar todas las DACL que utilicen cuentas de usuario local o de grupo para usar el nombre de la SVM de destino. Debido a que no puede modificar el nombre de cuenta para las entradas DACL existentes, debe eliminar todas las entradas DACL con usuarios o grupos locales de los descriptores de seguridad, crear nuevas entradas DACL con los nombres de cuenta de destino corregidos y asociar estas entradas DACL nuevas con los descriptores de seguridad adecuados.

- Entradas de SACL

Cada entrada de SACL debe estar asociada a una cuenta. Debe modificar todas las SACL que utilicen

cuentas de usuario o de grupo local para utilizar el nombre de la SVM de destino. Debido a que no puede modificar el nombre de cuenta para las entradas SACL existentes, debe eliminar todas las entradas SACL con usuarios o grupos locales de los descriptores de seguridad, crear nuevas entradas SACL con los nombres de cuenta de destino corregidos y asociar estas nuevas entradas SACL con los descriptores de seguridad adecuados.

Debe realizar los cambios necesarios en los usuarios o grupos locales utilizados en la configuración de la directiva de directorio de archivos antes de aplicar la directiva; de lo contrario, el trabajo de aplicación fallará.

**Configurar y aplicar la seguridad de archivos en archivos y carpetas NTFS mediante la CLI**

**Cree un descriptor de seguridad NTFS**

Crear un descriptor de seguridad NTFS (política de seguridad de archivos) es el primer paso para configurar y aplicar listas de control de acceso NTFS (ACL) a archivos y carpetas que residen en máquinas virtuales de almacenamiento (SVM). Puede asociar el descriptor de seguridad a la ruta de archivo o carpeta en una tarea de directiva.

**Acerca de esta tarea**

Puede crear descriptores de seguridad NTFS para archivos y carpetas que residen dentro de volúmenes de estilo de seguridad NTFS o para archivos y carpetas que residen en volúmenes de estilo de seguridad mixtos.

De forma predeterminada, cuando se crea un descriptor de seguridad, se agregan cuatro entradas de control de acceso de lista de control de acceso discrecional (DACL) a ese descriptor de seguridad. Los cuatro ACE predeterminados son los siguientes:

| Objeto                  | Tipo de acceso | Derechos de acceso | Dónde aplicar los permisos          |
|-------------------------|----------------|--------------------|-------------------------------------|
| BUILTIN\Administrators  | Permita        | Control total      | esta carpeta, subcarpetas, archivos |
| BUILTIN\Users           | Permita        | Control total      | esta carpeta, subcarpetas, archivos |
| PROPIETARIO DEL CREADOR | Permita        | Control total      | esta carpeta, subcarpetas, archivos |
| NT AUTHORITY\SYSTEM     | Permita        | Control total      | esta carpeta, subcarpetas, archivos |

Es posible personalizar la configuración del descriptor de seguridad mediante los siguientes parámetros opcionales:

- Propietario del descriptor de seguridad
- Grupo principal del propietario
- Indicadores de control RAW

Se ignora el valor de cualquier parámetro opcional para Storage-Level Access Guard. Consulte las páginas de manual para obtener más información.

## Añada entradas de control de acceso DACL de NTFS al descriptor de seguridad de NTFS

La adición de entradas de control de acceso (ACE) de DACL (lista de control de acceso discrecional) al descriptor de seguridad de NTFS es el segundo paso para configurar y aplicar ACL de NTFS a un archivo o carpeta. Cada entrada identifica qué objeto tiene permiso o acceso denegado, y define lo que el objeto puede o no puede hacer con los archivos o carpetas definidos en ACE.

### Acerca de esta tarea

Puede añadir una o varias ACE a la DACL del descriptor de seguridad.

Si el descriptor de seguridad contiene una DACL que tiene ACE existentes, el comando agrega la nueva ACE a la DACL. Si el descriptor de seguridad no contiene una DACL, el comando crea la DACL y le agrega la nueva ACE.

Opcionalmente, puede personalizar las entradas DACL especificando los derechos que desea permitir o denegar para la cuenta especificada en `-account` parámetro. Hay tres métodos mutuamente exclusivos para especificar los derechos:

- Derechos
- Derechos avanzados
- Derechos RAW (privilegio avanzado)



Si no especifica derechos para la entrada DACL, el valor predeterminado es establecer los derechos `Full Control`.

Opcionalmente, puede personalizar las entradas DACL especificando cómo aplicar herencia.

Se ignora el valor de cualquier parámetro opcional para Storage-Level Access Guard. Consulte las páginas de manual para obtener más información.

### Pasos

1. Agregue una entrada DACL a un descriptor de seguridad: `vserver security file-directory ntfs dacl add -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SID optional_parameters`

```
vserver security file-directory ntfs dacl add -ntfs-sd sd1 -access-type deny
-account domain\joe -rights full-control -apply-to this-folder -vserver vs1
```

2. Compruebe que la entrada DACL es correcta: `vserver security file-directory ntfs dacl show -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SID`

```
vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
-access-type deny -account domain\joe
```

```
Vserver: vs1
Security Descriptor Name: sd1
 Allow or Deny: deny
 Account Name or SID: DOMAIN\joe
 Access Rights: full-control
Advanced Access Rights: -
 Apply To: this-folder
 Access Rights: full-control
```

## Cree políticas de seguridad

Crear una política de seguridad de archivos para SVM es el tercer paso a la hora de configurar y aplicar ACL a un archivo o carpeta. Una directiva actúa como contenedor para varias tareas, donde cada tarea es una entrada única que se puede aplicar a archivos o carpetas. Posteriormente, puede agregar tareas a la directiva de seguridad.

### Acerca de esta tarea

Las tareas que agrega a una directiva de seguridad contienen asociaciones entre el descriptor de seguridad NTFS y las rutas de acceso de archivos o carpetas. Por lo tanto, debe asociar la política de seguridad con cada SVM (que contenga volúmenes de estilo de seguridad NTFS o volúmenes mixtos de estilo de seguridad).

### Pasos

1. Cree una política de seguridad: `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

```
vserver security file-directory policy create -policy-name policy1 -vserver vs1
```

2. Compruebe la directiva de seguridad: `vserver security file-directory policy show`

```
vserver security file-directory policy show
Vserver Policy Name

vs1 policy1
```

## Agregar una tarea a la directiva de seguridad

Crear y añadir una tarea de política a una política de seguridad es el cuarto paso para configurar y aplicar ACL a archivos o carpetas en SVM. Al crear la tarea de directiva, asocie la tarea a una directiva de seguridad. Puede agregar una o más entradas de tareas a una directiva de seguridad.

### Acerca de esta tarea

La política de seguridad es un contenedor para una tarea. Una tarea hace referencia a una única operación



que puede realizar una directiva de seguridad para archivos o carpetas con seguridad NTFS o mixta (o a un objeto de volumen si se configura Storage-Level Access Guard).

Existen dos tipos de tareas:

- Tareas de archivo y directorio

Se utiliza para especificar tareas que aplican descriptores de seguridad a archivos y carpetas especificados. Las ACL aplicadas mediante tareas de archivo y directorio se pueden gestionar con clientes de SMB o con la interfaz de línea de comandos de ONTAP.

- Tareas de protección de acceso al nivel de almacenamiento

Se utiliza para especificar tareas que aplican descriptores de seguridad de Access Guard de nivel de almacenamiento a un volumen especificado. Las ACL aplicadas mediante tareas de protección de acceso al nivel de almacenamiento solo se pueden gestionar a través de la interfaz de línea de comandos de ONTAP.

Una tarea contiene definiciones para la configuración de seguridad de un archivo (o carpeta) o un conjunto de archivos (o carpetas). Cada tarea de una política se identifica de forma única por la ruta. Sólo puede haber una tarea por ruta dentro de una única política. Una directiva no puede tener entradas de tareas duplicadas.

Directrices para agregar una tarea a una directiva:

- Puede haber un máximo de 10,000 entradas de tareas por directiva.
- Una política puede contener una o más tareas.

Aunque una directiva puede contener más de una tarea, no puede configurar una directiva para que contenga tareas de directorio de archivos y de protección de acceso a nivel de almacenamiento. Una política debe contener todas las tareas de Storage-Level Access Guard o todas las tareas de directorio de archivos.

- Se utiliza Storage-Level Access Guard para restringir los permisos.

Nunca dará permisos de acceso adicionales.

Al agregar tareas a las directivas de seguridad, debe especificar los siguientes cuatro parámetros necesarios:

- Nombre de SVM
- Nombre de la política
- Ruta
- Descriptor de seguridad que se asociará a la ruta de acceso

Es posible personalizar la configuración del descriptor de seguridad mediante los siguientes parámetros opcionales:

- Tipo de seguridad
- Modo de propagación
- Posición de índice
- Tipo de control de acceso

Se ignora el valor de cualquier parámetro opcional para Storage-Level Access Guard. Consulte las páginas de manual para obtener más información.

**Pasos**

1. Añada una tarea con un descriptor de seguridad asociado a la directiva de seguridad: `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`
- `file-directory` es el valor predeterminado para `-access-control` parámetro. Es opcional especificar el tipo de control de acceso cuando se configuran las tareas de acceso a archivos y directorios.

```
vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2 -index-num 1 -access-control file-directory
```

2. Compruebe la configuración de la tarea de directiva: `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`
- ```
vserver security file-directory policy task show
```

Vserver: vs1
Policy: policy1

| Index | File/Folder | Access | Security | NTFS | NTFS |
|-----------------|-------------|----------------|----------|-----------|------|
| Security | Path | Control | Type | Mode | |
| Descriptor Name | | | | | |
| ----- | ----- | ----- | ----- | ----- | |
| ----- | | | | | |
| 1 | /home/dir1 | file-directory | ntfs | propagate | sd2 |

Aplicación de las políticas de seguridad

Aplicar una política de seguridad de archivos a las SVM es el último paso a la hora de crear y aplicar ACL de NTFS a archivos o carpetas.

Acerca de esta tarea

Puede aplicar la configuración de seguridad definida en la política de seguridad a archivos y carpetas NTFS que residen en volúmenes FlexVol (estilo de seguridad NTFS o mixto).



Cuando se aplican una directiva de auditoría y SACL asociadas, se sobrescriben todas las DACL existentes. Cuando se aplica una directiva de seguridad y sus DACL asociados, se sobrescriben todas las DACL existentes. Debe revisar las directivas de seguridad existentes antes de crear y aplicar otras nuevas.

Paso

1. Aplicar una política de seguridad: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

```
vserver security file-directory apply -vserver vs1 -policy-name policy1
```

El trabajo de aplicación de política está programado y se devuelve el ID de trabajo.

```
[Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id 53322" command to view the status of the operation
```

Supervise el trabajo de política de seguridad

Al aplicar la política de seguridad a máquinas virtuales de almacenamiento (SVM), puede supervisar el progreso de la tarea supervisando el trabajo de la política de seguridad. Esto es útil si desea comprobar que la aplicación de la política de seguridad ha sido satisfactoria. Esto también resulta útil si tiene un trabajo de larga ejecución en el que está aplicando seguridad masiva a un gran número de archivos y carpetas.

Acerca de esta tarea

Para mostrar información detallada sobre un trabajo de política de seguridad, debe usar `-instance` parámetro.

Paso

1. Supervise el trabajo de la política de seguridad: `vserver security file-directory job show -vserver vserver_name`

```
vserver security file-directory job show -vserver vs1
```

| Job ID | Name | Vserver | Node | State |
|--|-----------------|---------|-------|---------|
| 53322 | Fsecurity Apply | vs1 | node1 | Success |
| Description: File Directory Security Apply Job | | | | |

Compruebe la seguridad del archivo aplicado

Es posible verificar la configuración de seguridad de archivos para confirmar que los archivos o las carpetas de la máquina virtual de almacenamiento (SVM) a la que aplicó la política de seguridad tienen la configuración deseada.

Acerca de esta tarea

Debe suministrar el nombre de la SVM que contenga los datos y la ruta de acceso al archivo y las carpetas en los que desea verificar la configuración de seguridad. Puede usar el opcional `-expand-mask` parámetro para mostrar información detallada acerca de la configuración de seguridad.

Paso

1. Mostrar la configuración de seguridad de archivos y carpetas: `vserver security file-directory show -vserver vserver_name -path path [-expand-mask true]`

```
vserver security file-directory show -vserver vs1 -path /data/engineering
```

-expand-mask true

```
Vserver: vs1
      File Path: /data/engineering
File Inode Number: 5544
      Security Style: ntfs
      Effective Style: ntfs
      DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
    ...0 .... = Offline
    .... ..0. .... = Sparse
    .... .... 0... .... = Normal
    .... .... ..0. .... = Archive
    .... .... ...1 .... = Directory
    .... .... .... .0.. = System
    .... .... .... ..0. = Hidden
    .... .... .... ...0 = Read Only
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
      Control:0x8004

1... .... = Self Relative
.0.. .... = RM Control Valid
..0. .... = SACL Protected
...0 .... = DACL Protected
.... 0... = SACL Inherited
.... .0.. = DACL Inherited
.... ..0. = SACL Inherit Required
.... ...0 = DACL Inherit Required
.... .... ..0. = SACL Defaulted
.... .... ...0 = SACL Present
.... .... .... 0... = DACL Defaulted
.... .... .... .1.. = DACL Present
.... .... .... ..0. = Group Defaulted
.... .... .... ...0 = Owner Defaulted

Owner:BUILTIN\Administrators
Group:BUILTIN\Administrators
DACL - ACEs
      ALLOW-Everyone-0x1f01ff
      0... .... =

Generic Read
```

| | | |
|------------------------------------|---------------------------------|---|
| Generic Write | .0.. | = |
| Generic Execute | ..0. | = |
| Generic All | ...0 | = |
| System Security |0 | = |
| Synchronize |1 | = |
| Write Owner | 1.... | = |
| Write DAC |1.. | = |
| Read Control |1. | = |
| Delete |1 | = |
| Write Attributes |1 | = |
| Read Attributes | 1.... | = |
| Delete Child |1.. | = |
| Execute |1. | = |
| Write EA |1 | = |
| Read EA | 1.... | = |
| Append |1.. | = |
| Write |1. | = |
| Read |1 | = |
| ALLOW-Everyone-0x10000000-OI CI IO | | |
| Generic Read | 0... | = |
| Generic Write | .0.. | = |
| Generic Execute | ..0. | = |
| Generic All | ...1 | = |

| | | |
|------------------|-------------|---|
| |0..... | = |
| System Security | | |
| |0..... | = |
| Synchronize | | |
| |0..... | = |
| Write Owner | | |
| |0..... | = |
| Write DAC | | |
| |0..... | = |
| Read Control | | |
| |0..... | = |
| Delete | | |
| |0..... | = |
| Write Attributes | | |
| |0..... | = |
| Read Attributes | | |
| |0..... | = |
| Delete Child | | |
| |0..... | = |
| Execute | | |
| |0..... | = |
| Write EA | | |
| |0..... | = |
| Read EA | | |
| |0..... | = |
| Append | | |
| |0..... | = |
| Write | | |
| |0..... | = |
| Read | | |

Configure y aplique políticas de auditoría a archivos y carpetas NTFS usando la información general de la CLI

Hay varios pasos que debe realizar para aplicar políticas de auditoría a archivos y carpetas NTFS cuando use la CLI de ONTAP. En primer lugar, debe crear un descriptor de seguridad NTFS y agregar SACL al descriptor de seguridad. A continuación, cree una directiva de seguridad y agregue tareas de directiva. Luego, debe aplicar la política de seguridad a una SVM.

Acerca de esta tarea

Después de aplicar la directiva de seguridad, puede supervisar el trabajo de directiva de seguridad y, a continuación, verificar la configuración de la directiva de auditoría aplicada.



Quando se aplican una directiva de auditoría y SACL asociadas, se sobrescriben todas las DACL existentes. Debe revisar las directivas de seguridad existentes antes de crear y aplicar otras nuevas.

Información relacionada

[Protección del acceso a archivos mediante Storage-Level Access Guard](#)

[Limita el uso de la CLI para establecer la seguridad de archivos y carpetas](#)

[Cómo se utilizan los descriptores de seguridad para aplicar la seguridad de archivos y carpetas](#)

["Seguimiento de seguridad y auditoría de SMB y NFS"](#)

[Configurar y aplicar la seguridad de archivos en archivos y carpetas NTFS mediante la CLI](#)

Cree un descriptor de seguridad NTFS

Crear una política de auditoría de descriptor de seguridad NTFS es el primer paso para configurar y aplicar listas de control de acceso NTFS (ACL) a archivos y carpetas que residen en SVM. Asociará el descriptor de seguridad a la ruta de archivo o carpeta en una tarea de directiva.

Acerca de esta tarea

Puede crear descriptores de seguridad NTFS para archivos y carpetas que residen dentro de volúmenes de estilo de seguridad NTFS o para archivos y carpetas que residen en volúmenes de estilo de seguridad mixtos.

De forma predeterminada, cuando se crea un descriptor de seguridad, se agregan cuatro entradas de control de acceso de lista de control de acceso discrecional (DACL) a ese descriptor de seguridad. Los cuatro ACE predeterminados son los siguientes:

| Objeto | Tipo de acceso | Derechos de acceso | Dónde aplicar los permisos |
|-------------------------|----------------|--------------------|-------------------------------------|
| BUILTIN\Administrators | Permita | Control total | esta carpeta, subcarpetas, archivos |
| BUILTIN\Users | Permita | Control total | esta carpeta, subcarpetas, archivos |
| PROPIETARIO DEL CREADOR | Permita | Control total | esta carpeta, subcarpetas, archivos |
| NT AUTHORITY\SYSTEM | Permita | Control total | esta carpeta, subcarpetas, archivos |

Es posible personalizar la configuración del descriptor de seguridad mediante los siguientes parámetros opcionales:

- Propietario del descriptor de seguridad
- Grupo principal del propietario
- Indicadores de control RAW

Se ignora el valor de cualquier parámetro opcional para Storage-Level Access Guard. Consulte las páginas de manual para obtener más información.

Pasos

1. Si desea usar los parámetros avanzados, configure el nivel de privilegio en Advanced: `set -privilege advanced`
2. Cree un descriptor de seguridad: `vserver security file-directory ntfs create -vserver vserver_name -ntfs-sd SD_name optional_parameters`

```
vserver security file-directory ntfs create -ntfs-sd sd1 -vserver vs1 -owner DOMAIN\joe
```

3. Compruebe que la configuración del descriptor de seguridad sea correcta: `vserver security file-directory ntfs show -vserver vserver_name -ntfs-sd SD_name`

```
vserver security file-directory ntfs show -vserver vs1 -ntfs-sd sd1
```

```
Vserver: vs1
Security Descriptor Name: sd1
Owner of the Security Descriptor: DOMAIN\joe
```

4. Si se encuentra en el nivel de privilegio avanzado, regrese al nivel de privilegio de administrador: `set -privilege admin`

Añada entradas de control de acceso SACL a NTFS al descriptor de seguridad de NTFS

Añadir entradas de control de acceso (ACE) SACL (lista de control de acceso del sistema) al descriptor de seguridad NTFS es el segundo paso a la hora de crear directivas de auditoría NTFS para archivos o carpetas en SVM. Cada entrada identifica el usuario o grupo que desea auditar. La entrada SACL define si desea auditar los intentos de acceso fallidos o correctos.

Acerca de esta tarea

Puede agregar uno o varios ACE al SACL del descriptor de seguridad.

Si el descriptor de seguridad contiene un SACL que tiene ACE existentes, el comando agrega el nuevo ACE al SACL. Si el descriptor de seguridad no contiene un SACL, el comando crea el SACL y le agrega el nuevo ACE.

Puede configurar las entradas SACL especificando los derechos que desea auditar para los eventos de éxito o error de la cuenta especificada en `-account` parámetro. Hay tres métodos mutuamente exclusivos para especificar los derechos:

- Derechos
- Derechos avanzados
- Derechos RAW (privilegio avanzado)



Si no especifica derechos para la entrada SACL, la configuración predeterminada es `Full Control`.

Opcionalmente, puede personalizar las entradas SACL especificando cómo aplicar herencia con `apply to` parámetro. Si no especifica este parámetro, el valor predeterminado es aplicar esta entrada SACL a esta carpeta, subcarpetas y archivos.

Pasos

1. Añada una entrada SACL a un descriptor de seguridad: `vserver security file-directory ntfs sac1 add -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SIDOptional_parameters`

```
vserver security file-directory ntfs sac1 add -ntfs-sd sd1 -access-type failure -account domain\joe -rights full-control -apply-to this-folder -vserver vs1
```

2. Compruebe que la entrada de SACL es correcta: `vserver security file-directory ntfs sac1 show -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SID`

```
vserver security file-directory ntfs sac1 show -vserver vs1 -ntfs-sd sd1 -access-type deny -account domain\joe
```

```
Vserver: vs1
Security Descriptor Name: sd1
Access type for Specified Access Rights: failure
Account Name or SID: DOMAIN\joe
Access Rights: full-control
Advanced Access Rights: -
Apply To: this-folder
Access Rights: full-control
```

Cree políticas de seguridad

Crear una política de auditoría para máquinas virtuales de almacenamiento (SVM) es el tercer paso a la hora de configurar y aplicar ACL a un archivo o una carpeta. Una directiva actúa como contenedor para varias tareas, donde cada tarea es una entrada única que se puede aplicar a archivos o carpetas. Posteriormente, puede agregar tareas a la directiva de seguridad.

Acerca de esta tarea

Las tareas que agrega a una directiva de seguridad contienen asociaciones entre el descriptor de seguridad NTFS y las rutas de acceso de archivos o carpetas. Por lo tanto, debe asociar la política de seguridad con cada máquina virtual de almacenamiento (SVM) (que contenga volúmenes de estilo de seguridad NTFS o volúmenes mixtos de estilo de seguridad).

Pasos

1. Cree una política de seguridad: `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

```
vserver security file-directory policy create -policy-name policy1 -vserver
```

vs1

2. Compruebe la directiva de seguridad: `vserver security file-directory policy show`

```
vserver security file-directory policy show
Vserver          Policy Name
-----
vs1              policy1
```

Agregar una tarea a la directiva de seguridad

Crear y añadir una tarea de política a una política de seguridad es el cuarto paso para configurar y aplicar ACL a archivos o carpetas en SVM. Al crear la tarea de directiva, asocie la tarea a una directiva de seguridad. Puede agregar una o más entradas de tareas a una directiva de seguridad.

Acerca de esta tarea

La política de seguridad es un contenedor para una tarea. Una tarea hace referencia a una única operación que puede realizar una directiva de seguridad para archivos o carpetas con seguridad NTFS o mixta (o a un objeto de volumen si se configura Storage-Level Access Guard).

Existen dos tipos de tareas:

- Tareas de archivo y directorio

Se utiliza para especificar tareas que aplican descriptores de seguridad a archivos y carpetas especificados. Las ACL aplicadas mediante tareas de archivo y directorio se pueden gestionar con clientes de SMB o con la interfaz de línea de comandos de ONTAP.

- Tareas de protección de acceso al nivel de almacenamiento

Se utiliza para especificar tareas que aplican descriptores de seguridad de Access Guard de nivel de almacenamiento a un volumen especificado. Las ACL aplicadas mediante tareas de protección de acceso al nivel de almacenamiento solo se pueden gestionar a través de la interfaz de línea de comandos de ONTAP.

Una tarea contiene definiciones para la configuración de seguridad de un archivo (o carpeta) o un conjunto de archivos (o carpetas). Cada tarea de una política se identifica de forma única por la ruta. Sólo puede haber una tarea por ruta dentro de una única política. Una directiva no puede tener entradas de tareas duplicadas.

Directrices para agregar una tarea a una directiva:

- Puede haber un máximo de 10,000 entradas de tareas por directiva.
- Una política puede contener una o más tareas.

Aunque una directiva puede contener más de una tarea, no puede configurar una directiva para que contenga tareas de directorio de archivos y de protección de acceso a nivel de almacenamiento. Una política debe contener todas las tareas de Storage-Level Access Guard o todas las tareas de directorio de archivos.

- Se utiliza Storage-Level Access Guard para restringir los permisos.

Nunca dará permisos de acceso adicionales.

Es posible personalizar la configuración del descriptor de seguridad mediante los siguientes parámetros opcionales:

- Tipo de seguridad
- Modo de propagación
- Posición de índice
- Tipo de control de acceso

Se ignora el valor de cualquier parámetro opcional para Storage-Level Access Guard. Consulte las páginas de manual para obtener más información.

Pasos

1. Añada una tarea con un descriptor de seguridad asociado a la directiva de seguridad: `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

`file-directory` es el valor predeterminado para `-access-control` parámetro. Es opcional especificar el tipo de control de acceso cuando se configuran las tareas de acceso a archivos y directorios.

```
vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2 -index-num 1 -access-control file-directory
```

2. Compruebe la configuración de la tarea de directiva: `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

```
vserver security file-directory policy task show
```

```
Vserver: vs1
Policy: policy1
```

| Index | File/Folder | Access | Security | NTFS | NTFS |
|-----------------|-------------|----------------|----------|-----------|------|
| Security | Path | Control | Type | Mode | |
| Descriptor Name | | | | | |
| ----- | ----- | ----- | ----- | ----- | |
| ----- | | | | | |
| 1 | /home/dir1 | file-directory | ntfs | propagate | sd2 |

Aplicación de las políticas de seguridad

Aplicar una política de auditoría a las SVM es el último paso a la hora de crear y aplicar ACL de NTFS a archivos o carpetas.

Acerca de esta tarea

Puede aplicar la configuración de seguridad definida en la política de seguridad a archivos y carpetas NTFS que residen en volúmenes FlexVol (estilo de seguridad NTFS o mixto).



Cuando se aplican una directiva de auditoría y SACL asociadas, se sobrescriben todas las DACL existentes. Cuando se aplica una directiva de seguridad y sus DACL asociados, se sobrescriben todas las DACL existentes. Debe revisar las directivas de seguridad existentes antes de crear y aplicar otras nuevas.

Paso

- 1. Aplicar una política de seguridad: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

```
vserver security file-directory apply -vserver vs1 -policy-name policy1
```

El trabajo de aplicación de política está programado y se devuelve el ID de trabajo.

```
[Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id 53322" command to view the status of the operation
```

Supervise el trabajo de política de seguridad

Al aplicar la política de seguridad a máquinas virtuales de almacenamiento (SVM), puede supervisar el progreso de la tarea supervisando el trabajo de la política de seguridad. Esto es útil si desea comprobar que la aplicación de la política de seguridad ha sido satisfactoria. Esto también resulta útil si tiene un trabajo de larga ejecución en el que está aplicando seguridad masiva a un gran número de archivos y carpetas.

Acerca de esta tarea

Para mostrar información detallada sobre un trabajo de política de seguridad, debe usar `-instance` parámetro.

Paso

- 1. Supervise el trabajo de la política de seguridad: `vserver security file-directory job show -vserver vserver_name`

```
vserver security file-directory job show -vserver vs1
```

| Job | ID | Name | Vserver | Node | State |
|--|----|-----------------|---------|-------|---------|
| 53322 | | Fsecurity Apply | vs1 | node1 | Success |
| Description: File Directory Security Apply Job | | | | | |

Compruebe la política de auditoría aplicada

Puede verificar la política de auditoría para confirmar que los archivos o las carpetas de

la máquina virtual de almacenamiento (SVM) a la que aplicó la política de seguridad tienen la configuración de seguridad de auditoría deseada.

Acerca de esta tarea

Utilice la `vserver security file-directory show` comando para mostrar información de la política de auditoría. Debe proporcionar el nombre de la SVM que contiene los datos y la ruta a los datos cuyo archivo o carpeta de información de la política de auditoría que desea mostrar.

Paso

1. Mostrar la configuración de directivas de auditoría: `vserver security file-directory show -vserver vserver_name -path path`

Ejemplo

El siguiente comando muestra la información de la directiva de auditoría aplicada a la ruta `"/corp"` en SVM `vs1`. La ruta de acceso tiene aplicada UNA entrada SACL DE ÉXITO y DE FALLO:

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp

      Vserver: vs1
      File Path: /corp
      Security Style: ntfs
      Effective Style: ntfs
      DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0x8014
            Owner:DOMAIN\Administrator
            Group:BUILTIN\Administrators
            SACL - ACEs
              ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
              SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
            DACL - ACEs
              ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
              ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
              ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
              ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

Consideraciones que tener en cuenta al administrar trabajos de directiva de seguridad

Si existe un trabajo de política de seguridad, en determinadas circunstancias, no puede modificar dicha política de seguridad ni las tareas asignadas a dicha política. Debe entender en qué condiciones puede o no puede modificar las directivas de seguridad

para que cualquier intento que realice para modificar la directiva se realice correctamente. Las modificaciones de la directiva incluyen agregar, eliminar o modificar tareas asignadas a la directiva y eliminar o modificar la directiva.

No puede modificar una política de seguridad ni una tarea asignada a esa política si existe un trabajo para esa política y ese trabajo está en los estados siguientes:

- El trabajo está en ejecución o en curso.
- El trabajo está en pausa.
- El trabajo se reanuda y se encuentra en estado en ejecución.
- Si el trabajo está esperando a conmutar al respaldo a otro nodo.

En las siguientes circunstancias, si existe un trabajo para una política de seguridad, puede modificar correctamente dicha política de seguridad o una tarea asignada a dicha directiva:

- El trabajo de política se ha detenido.
- El trabajo de directiva ha finalizado correctamente.

Comandos para administrar descriptores de seguridad NTFS

Existen comandos ONTAP específicos para administrar descriptores de seguridad. Puede crear, modificar, eliminar y mostrar información acerca de los descriptores de seguridad.

| Si desea... | Se usa este comando... |
|---|--|
| Crear descriptores de seguridad NTFS | <code>vserver security file-directory ntfs create</code> |
| Modifique los descriptores de seguridad NTFS existentes | <code>vserver security file-directory ntfs modify</code> |
| Mostrar información acerca de los descriptores de seguridad NTFS existentes | <code>vserver security file-directory ntfs show</code> |
| Eliminar descriptores de seguridad NTFS | <code>vserver security file-directory ntfs delete</code> |

Vea las páginas de manual para el `vserver security file-directory ntfs` comandos para obtener más información.

Comandos para administrar entradas de control de acceso DACL de NTFS

Hay comandos ONTAP específicos para administrar entradas de control de acceso de DACL (ACE). Puede agregar ACE a DACL NTFS en cualquier momento. También puede administrar las DACL de NTFS existentes modificando, eliminando y mostrando información acerca de las ACE en las DACL.

| Si desea... | Se usa este comando... |
|---|---|
| Cree ACE y agréguelos a DACL NTFS | <code>vserver security file-directory ntfs dacl add</code> |
| Modifique los ACE existentes en las DACL NTFS | <code>vserver security file-directory ntfs dacl modify</code> |
| Mostrar información acerca de los ACE existentes en las DACL NTFS | <code>vserver security file-directory ntfs dacl show</code> |
| Elimine los ACE existentes de las DACL NTFS | <code>vserver security file-directory ntfs dacl remove</code> |

Vea las páginas de manual para el `vserver security file-directory ntfs dacl` comandos para obtener más información.

Comandos para gestionar entradas de control de acceso SACL de NTFS

Hay comandos ONTAP específicos para administrar entradas de control de acceso SACL (ACE). Puede agregar ACE a SACL NTFS en cualquier momento. También puede administrar SACL NTFS existentes modificando, eliminando y mostrando información acerca de ACE en SACL.

| Si desea... | Se usa este comando... |
|---|---|
| Cree ACE y agréguelos a SACL NTFS | <code>vserver security file-directory ntfs sacl add</code> |
| Modifique los ACE existentes en SACL NTFS | <code>vserver security file-directory ntfs sacl modify</code> |
| Muestra información acerca de los ACE existentes en SACL NTFS | <code>vserver security file-directory ntfs sacl show</code> |
| Elimine los ACE existentes de SACL NTFS | <code>vserver security file-directory ntfs sacl remove</code> |

Vea las páginas de manual para el `vserver security file-directory ntfs sacl` comandos para obtener más información.

Comandos para gestionar políticas de seguridad

Existen comandos ONTAP específicos para administrar las políticas de seguridad. Puede mostrar información acerca de las políticas y eliminarla. No puede modificar una política de seguridad.

| Si desea... | Se usa este comando... |
|---|--|
| Cree políticas de seguridad | <code>vserver security file-directory policy create</code> |
| Mostrar información acerca de las directivas de seguridad | <code>vserver security file-directory policy show</code> |
| Eliminar políticas de seguridad | <code>vserver security file-directory policy delete</code> |

Vea las páginas de manual para el `vserver security file-directory policy` comandos para obtener más información.

Comandos para administrar tareas de políticas de seguridad

Hay comandos de ONTAP para añadir, modificar, quitar y mostrar información acerca de tareas de políticas de seguridad.

| Si desea... | Se usa este comando... |
|--|---|
| Agregar tareas de directiva de seguridad | <code>vserver security file-directory policy task add</code> |
| Modifique las tareas de las políticas de seguridad | <code>vserver security file-directory policy task modify</code> |
| Muestra información acerca de las tareas de directiva de seguridad | <code>vserver security file-directory policy task show</code> |
| Quitar tareas de directiva de seguridad | <code>vserver security file-directory policy task remove</code> |

Vea las páginas de manual para el `vserver security file-directory policy task` comandos para obtener más información.

Comandos para gestionar trabajos de políticas de seguridad

Hay comandos de la ONTAP para pausar, reanudar, detener y mostrar información acerca de los trabajos de políticas de seguridad.

| Si desea... | Se usa este comando... |
|---|--|
| Pausar trabajos de directiva de seguridad | <code>vserver security file-directory job pause -vserver vserver_name -id integer</code> |

| Si desea... | Se usa este comando... |
|---|--|
| Reanudar trabajos de directiva de seguridad | <code>vserver security file-directory job resume -vserver vserver_name -id integer</code> |
| Mostrar información sobre trabajos de directivas de seguridad | <code>vserver security file-directory job show -vserver vserver_name</code> Es posible determinar el ID de trabajo de un trabajo con este comando. |
| Detener trabajos de directiva de seguridad | <code>vserver security file-directory job stop -vserver vserver_name -id integer</code> |

Vea las páginas de manual para el `vserver security file-directory job` comandos para obtener más información.

Configure la caché de metadatos para los recursos compartidos de SMB

Cómo funciona el almacenamiento en caché de metadatos de SMB

El almacenamiento en caché de metadatos permite almacenar en caché atributos de archivos en clientes SMB 1.0 para proporcionar un acceso más rápido a los atributos de archivos y carpetas. Puede habilitar o deshabilitar el almacenamiento en caché de atributos por recurso compartido. También puede configurar el tiempo de espera para las entradas en caché si está activado el almacenamiento en caché de metadatos. No es necesario configurar el almacenamiento en caché de metadatos si los clientes se conectan a recursos compartidos mediante SMB 2.x o SMB 3.0.

Cuando se habilita esta opción, la caché de metadatos del SMB almacena los datos de atributos de archivos y rutas por una cantidad limitada de tiempo. Esto puede mejorar el rendimiento de SMB para los clientes de SMB 1.0 con cargas de trabajo comunes.

En determinadas tareas, SMB crea una cantidad significativa de tráfico que puede incluir varias consultas idénticas para los metadatos de archivos y rutas. Puede reducir el número de consultas redundantes y mejorar el rendimiento de clientes de SMB 1.0 utilizando el almacenamiento en caché de metadatos del SMB para recuperar información de la caché.



Si bien es poco probable, es posible que la caché de metadatos proporcione información obsoleta a clientes SMB 1.0. Si su entorno no se puede permitir este riesgo, no debe habilitar esta función.

Habilite la caché de metadatos de SMB

Puede mejorar el rendimiento de SMB para los clientes de SMB 1.0 al habilitar la caché de metadatos de SMB. De manera predeterminada, el almacenamiento en caché de metadatos de SMB está deshabilitado.

Paso

1. Realice la acción deseada:

| Si desea... | Introduzca el comando... |
|--|---|
| Habilite el almacenamiento en caché de metadatos de SMB cuando crea un recurso compartido | <pre>vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties attributecache</pre> |
| Habilite el almacenamiento en caché de metadatos de SMB en un recurso compartido existente | <pre>vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties attributecache</pre> |

Información relacionada

[Configuración de la vida útil de las entradas de la caché de metadatos SMB](#)

[Agregar o quitar propiedades de recursos compartidos en un recurso compartido SMB existente](#)

Configure la vida útil de las entradas de la caché de metadatos del SMB

Puede configurar la vida útil de las entradas de la caché de metadatos SMB para optimizar el rendimiento de la caché de metadatos de SMB en su entorno. El valor predeterminado es 10 segundos.

Antes de empezar

Debe haber habilitado la función de caché de metadatos SMB. Si el almacenamiento en caché de metadatos de SMB no está habilitado, no se utiliza la configuración TTL de la caché de SMB.

Paso

1. Realice la acción deseada:

| Si desea configurar la vida útil de las entradas de la caché de metadatos SMB al... | Introduzca el comando... |
|---|---|
| Crear un recurso compartido | <pre>vserver cifs share -create -vserver vserver_name -share-name share_name -path path -attribute-cache-ttl [integerh][integerm][integers]</pre> |
| Modifique un recurso compartido existente | <pre>vserver cifs share -modify -vserver vserver_name -share-name share_name -attribute-cache-ttl [integerh][integerm][integers]</pre> |

Puede especificar propiedades y opciones de configuración de recursos compartidos adicionales al crear o modificar recursos compartidos. Consulte las páginas de manual para obtener más información.

Administrar bloqueos de archivos

Acerca del bloqueo de archivos entre protocolos

El bloqueo de archivos es un método que utilizan las aplicaciones cliente para evitar que un usuario acceda a un archivo abierto previamente por otro usuario. La forma en que ONTAP bloquea los archivos depende del protocolo del cliente.

Si el cliente es NFS, los bloqueos son consultivos; si el cliente es un cliente SMB, los bloqueos son obligatorios.

Debido a las diferencias entre los bloqueos de archivos NFS y SMB, es posible que un cliente NFS no pueda acceder a un archivo que abrió previamente una aplicación SMB.

Lo siguiente se produce cuando un cliente NFS intenta acceder a un archivo bloqueado por una aplicación SMB:

- En volúmenes mixtos o NTFS, operaciones de manipulación de archivos como `rm`, `rmdir`, y `mv`. Puede provocar un fallo en la aplicación NFS.
- Las operaciones de lectura y escritura de NFS se deniegan en los modos abiertos Deny-Read y Deny-write de SMB, respectivamente.
- Error en las operaciones de escritura de NFS cuando el rango escrito del archivo está bloqueado por un `bytelock` exclusivo de SMB.

- Desenlazar

- En el caso de los sistemas de archivos NTFS, se admiten las operaciones de eliminación de SMB y CIFS.

El archivo se eliminará después del último cierre.

- No se admiten las operaciones de desenlace de NFS.

No es compatible porque la semántica NTFS y SMB es necesaria, y la última operación `Delete-on-Close` no es compatible con NFS.

- Para los sistemas de archivos UNIX, se admite la operación de desvinculación.

Es compatible porque se necesitan semántica NFS y UNIX.

- Cambiar el nombre

- Para los sistemas de archivos NTFS, si el archivo de destino se abre desde SMB o CIFS, se puede cambiar el nombre del archivo de destino.

- No se admite el cambio de nombre de NFS.

No es compatible porque se requieren semánticas NTFS y SMB.

En los volúmenes de estilo de seguridad de UNIX, las operaciones de desenlace y cambio de nombre de NFS ignoran el estado de bloqueo de SMB y permiten el acceso al archivo. Todas las demás operaciones de NFS en volúmenes de estilo de seguridad de UNIX honran el estado de bloqueo de SMB.

El bit de sólo lectura se establece en base a archivo para reflejar si un archivo es grabable (deshabilitado) o de sólo lectura (habilitado).

Los clientes SMB que usan Windows pueden establecer un bit de solo lectura por archivo. Los clientes NFS no establecen un bit de solo lectura por archivo, ya que los clientes NFS no tienen ninguna operación de protocolo que utilice un bit de solo lectura por archivo.

ONTAP puede establecer un bit de solo lectura en un archivo cuando un cliente SMB que utiliza Windows crea ese archivo. ONTAP también puede establecer un bit de solo lectura cuando se comparte un archivo entre los clientes NFS y los clientes SMB. Parte del software, cuando lo utilizan los clientes NFS y clientes SMB, requiere que se habilite el bit de solo lectura.

Para que ONTAP mantenga los permisos de lectura y escritura adecuados en un archivo compartido entre clientes NFS y clientes SMB, trata el bit de solo lectura de acuerdo con las siguientes reglas:

- NFS trata cualquier archivo con el bit de solo lectura habilitado como si no tiene bits de permiso de escritura habilitados.
- Si un cliente NFS deshabilita todos los bits de permiso de escritura y al menos uno de esos bits se había habilitado anteriormente, ONTAP habilita el bit de solo lectura para ese archivo.
- Si un cliente NFS habilita algún bit de permiso de escritura, ONTAP deshabilita el bit de solo lectura para ese archivo.
- Si se habilita el bit de solo lectura de un archivo y un cliente NFS intenta detectar permisos para el archivo, los bits de permiso del archivo no se envían al cliente NFS; en su lugar, ONTAP envía los bits de permiso al cliente NFS con los bits de permiso de escritura enmascarados.
- Si se habilita el bit de solo lectura de un archivo y un cliente SMB deshabilita el bit de solo lectura, ONTAP habilita el bit de permiso de escritura del propietario para el archivo.
- Los archivos con el bit de sólo lectura activado sólo son grabables por raíz.



Los cambios en los permisos de archivo se aplican inmediatamente en los clientes SMB, pero es posible que no se apliquen de inmediato en los clientes NFS si el cliente NFS habilita el almacenamiento de atributos en caché.

Diferencias entre ONTAP y Windows al administrar bloqueos en los componentes de ruta de acceso compartida

A diferencia de Windows, ONTAP no bloquea cada componente de la ruta de acceso a un archivo abierto mientras el archivo está abierto. Este comportamiento también afecta a las rutas de recursos compartidos de SMB.

Como ONTAP no bloquea cada componente de la ruta, es posible cambiar el nombre de un componente de ruta por encima del archivo o el recurso compartido abierto, lo que puede provocar problemas en determinadas aplicaciones o hacer que la ruta del recurso compartido en la configuración del SMB no sea válida. Esto puede hacer que el recurso compartido sea inaccesible.

Para evitar problemas causados por el cambio de nombre de los componentes de la ruta de acceso, puede aplicar configuraciones de seguridad que impidan que los usuarios o aplicaciones cambien el nombre de los directorios críticos.

Mostrar información sobre bloqueos

Puede mostrar información acerca de los bloqueos de archivos actuales, incluidos los tipos de bloqueos que se conservan y el estado de bloqueo, detalles sobre bloqueos de rango de bytes, modos sharelock, bloqueos de delegación y bloqueos oportunistas, y si se abren bloqueos con identificadores duraderos o persistentes.

Acerca de esta tarea

No se puede mostrar la dirección IP del cliente para los bloqueos establecidos a través de NFSv4 o NFSv4.1.

De forma predeterminada, el comando muestra información sobre todos los bloqueos. Puede usar los parámetros del comando para mostrar información sobre los bloqueos de una máquina virtual de almacenamiento (SVM) específica o para filtrar el resultado del comando según otros criterios.

La `vserver locks show` el comando muestra información sobre cuatro tipos de bloqueos:

- Bloqueos de rango de bytes, que bloquean sólo una parte de un archivo.
- Bloqueos de uso compartido, que bloquean los archivos abiertos.
- Bloqueos oportunistas, que controlan el almacenamiento en caché en el cliente a través de SMB.
- Delegaciones, que controlan el almacenamiento en caché en el cliente a través de NFSv4.x.

Al especificar parámetros opcionales, puede determinar información importante sobre cada tipo de bloqueo. Consulte la página de manual del comando para obtener más información.

Paso

1. Muestra información sobre los bloqueos mediante `vserver locks show` comando.

Ejemplos

En el siguiente ejemplo, se muestra información de resumen para un bloqueo de NFSv4 en un archivo con la ruta `/vol1/file1`. El modo de acceso sharelock es `write-deny_none`, y el bloqueo se concedió mediante la delegación de escritura:

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path                LIF          Protocol  Lock Type  Client
-----
-----
vol1    /vol1/file1                    lif1         nfsv4     share-level -
                                     Sharelock Mode: write-deny_none
                                     delegation  -
                                     Delegation Type: write
```

En el siguiente ejemplo se muestra información detallada sobre oplock y sharelock acerca del bloqueo SMB en un archivo con la ruta de acceso `/data2/data2_2/intro.pptx`. Se concede un identificador duradero en el archivo con un modo de acceso de bloqueo compartido de `Write-Deny_none` a un cliente con una dirección IP de 10.3.1.3. Un plock de arrendamiento se concede con un nivel de plock por lotes:



```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx
```

```

    Vserver: vs1
      Volume: data2_2
    Logical Interface: lif2
      Object Path: /data2/data2_2/intro.pptx
      Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
      Lock Protocol: cifs
      Lock Type: share-level
    Node Holding Lock State: node3
      Lock State: granted
    Bytelock Starting Offset: -
      Number of Bytes Locked: -
      Bytelock is Mandatory: -
      Bytelock is Exclusive: -
      Bytelock is Superlock: -
      Bytelock is Soft: -
      Oplock Level: -
    Shared Lock Access Mode: write-deny_none
      Shared Lock is Soft: false
      Delegation Type: -
      Client Address: 10.3.1.3
      SMB Open Type: durable
      SMB Connect State: connected
    SMB Expiration Time (Secs): -
      SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

```

    Vserver: vs1
      Volume: data2_2
    Logical Interface: lif2
      Object Path: /data2/data2_2/test.pptx
      Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
      Lock Protocol: cifs
      Lock Type: op-lock
    Node Holding Lock State: node3
      Lock State: granted
    Bytelock Starting Offset: -
      Number of Bytes Locked: -
      Bytelock is Mandatory: -
      Bytelock is Exclusive: -
      Bytelock is Superlock: -
      Bytelock is Soft: -
      Oplock Level: batch
    Shared Lock Access Mode: -
      Shared Lock is Soft: -
```

```
Delegation Type: -
Client Address: 10.3.1.3
SMB Open Type: -
SMB Connect State: connected
SMB Expiration Time (Secs): -
SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

Bloqueos de rotura

Cuando los bloqueos de archivos impiden que los clientes accedan a los archivos, puede mostrar información sobre los bloqueos retenidos actualmente y romperán bloqueos específicos. Entre los ejemplos de escenarios en los que es posible que necesite romper los bloqueos se incluyen las aplicaciones de depuración.

Acerca de esta tarea

La `vserver locks break` el comando solo está disponible en el nivel de privilegios avanzado y superior. La página man del comando contiene información detallada.

Pasos

1. Para encontrar la información que necesita para romper un bloqueo, utilice `vserver locks show` comando.

La página man del comando contiene información detallada.

2. Configure el nivel de privilegio en Advanced: `set -privilege advanced`
3. Ejecute una de las siguientes acciones:

| Si desea romper un bloqueo especificando... | Introduzca el comando... |
|--|--|
| El nombre de SVM, el nombre del volumen, el nombre de LIF y la ruta de archivo | <code>vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif</code> |
| El ID del bloqueo | <code>vserver locks break -lockid UUID</code> |

4. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

Supervise la actividad del SMB

Muestra información de la sesión SMB

Puede mostrar información acerca de las sesiones SMB establecidas, incluidos la conexión SMB y el ID de sesión y la dirección IP de la estación de trabajo mediante la sesión. Es posible mostrar información sobre la versión del protocolo SMB de la sesión y el nivel de protección disponible continuamente, lo que ayuda a identificar si la sesión admite operaciones no disruptivas.

Acerca de esta tarea

Puede mostrar información de todas las sesiones de la SVM en formato de resumen. Sin embargo, en muchos casos, la cantidad de producción que se devuelve es grande. Puede personalizar la información que se muestra en el resultado especificando parámetros opcionales:

- Puede usar el opcional `-fields` parámetro para mostrar el resultado de los campos seleccionados.

Puede entrar `-fields ?` para determinar qué campos se pueden utilizar.

- Puede utilizar el `-instance` Parámetro para mostrar información detallada sobre las sesiones SMB establecidas.
- Puede utilizar el `-fields` o el `-instance` parámetro independiente o en combinación con otros parámetros opcionales.

Paso

1. Ejecute una de las siguientes acciones:

| Si desea mostrar información de la sesión SMB... | Introduzca el siguiente comando... |
|---|--|
| Para todas las sesiones del SVM en formato de resumen | <code>vserver cifs session show -vserver vserver_name</code> |
| En un ID de conexión especificado | <code>vserver cifs session show -vserver vserver_name -connection-id integer</code> |
| Desde una dirección IP de estación de trabajo especificada | <code>vserver cifs session show -vserver vserver_name -address workstation_IP_address</code> |
| En una dirección IP de LIF especificada | <code>vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address</code> |
| En un nodo especificado | <code>`vserver cifs session show -vserver vserver_name -node {node_name</code> |
| <code>local}`</code> | Desde un usuario de Windows especificado |
| <code>vserver cifs session show -vserver vserver_name -windows-user domain_name\\user_name</code> | Con un mecanismo de autenticación especificado |
| <code>`vserver cifs session show -vserver vserver_name -auth-mechanism {NTLMv1</code> | NTLMv2 |
| Kerberos | <code>Anonymous}`</code> |

| Si desea mostrar información de la sesión SMB... | Introduzca el siguiente comando... |
|---|---|
| Con una versión de protocolo especificada | <code>`vserver cifs session show -vserver vserver_name -protocol-version {SMB1</code> |
| SMB2 | SMB2_1 |
| SMB3 | SMB3_1} [NOTE] ==== Protección de disponibilidad continua y multicanal de SMB solo están disponibles en sesiones SMB 3.0 y posteriores. Para ver su estado en todas las sesiones de calificación, debe especificar este parámetro con el valor establecido en SMB3 o posterior. ===== |
| Con un nivel especificado de protección continua disponible | <code>`vserver cifs session show -vserver vserver_name -continuously-available {No</code> |
| Yes | Partial} [NOTE] ==== Si el estado continuamente disponible es <code>Partial</code> , esto significa que la sesión contiene al menos un archivo abierto continuamente disponible, pero la sesión tiene algunos archivos que no están abiertos con protección continua disponible. Puede utilizar el <code>vserver cifs sessions file show</code> comando para determinar qué archivos de la sesión establecida no están abiertos con protección continua disponible. ===== |
| Con un estado de sesión de firma SMB especificado | <code>`vserver cifs session show -vserver vserver_name -is-session-signed {true</code> |

Ejemplos

El siguiente comando muestra información de sesión para las sesiones en SVM vs1 establecidas desde una estación de trabajo con dirección IP 10.1.1.1:

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:      node1
Vserver:   vs1
Connection Session
ID          ID      Workstation      Windows User      Open      Idle
-----
3151272279,
3151272280,
3151272281  1          10.1.1.1          DOMAIN\joe        2          23s
```

El siguiente comando muestra información detallada de la sesión para las sesiones con protección continuamente disponible en SVM vs1. La conexión se realizó mediante la cuenta de dominio.

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

Node: node1
Vserver: vs1
Session ID: 1
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation IP address: 10.1.1.2
Authentication Mechanism: Kerberos
Windows User: DOMAIN\SERVER1$
UNIX User: pcuser
Open Shares: 1
Open Files: 1
Open Other: 0
Connected Time: 10m 43s
Idle Time: 1m 19s
Protocol Version: SMB3
Continuously Available: Yes
Is Session Signed: false
User Authenticated as: domain-user
NetBIOS Name: -
SMB Encryption Status: Unencrypted
```

El siguiente comando muestra información de sesión en una sesión mediante SMB 3.0 y SMB MultiChannel en SVM vs1. En el ejemplo, el usuario se conectó a este recurso compartido desde un cliente con capacidad para SMB 3.0 mediante la dirección IP de LIF; por lo tanto, el mecanismo de autenticación se estableció de forma predeterminada en NTLMv2. La conexión se debe realizar mediante la autenticación Kerberos para conectarse con la protección disponible continuamente.

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3
```

```
Node: node1
Vserver: vs1
Session ID: 1
**Connection IDs: 3151272607,31512726078,3151272609
Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
Workstation IP address: 10.1.1.3
Authentication Mechanism: NTLMv2
Windows User: DOMAIN\administrator
UNIX User: pcuser
Open Shares: 1
Open Files: 0
Open Other: 0
Connected Time: 6m 22s
Idle Time: 5m 42s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: false
User Authenticated as: domain-user
NetBIOS Name: -
SMB Encryption Status: Unencrypted
```

Información relacionada

[Mostrar información acerca de los archivos SMB abiertos](#)

Muestra información acerca de los archivos SMB abiertos

Es posible ver información sobre los archivos SMB abiertos, incluidos la conexión de SMB y el ID de sesión, el volumen de host, el nombre del recurso compartido y la ruta del recurso compartido. Es posible mostrar información acerca del nivel de protección disponible continuamente de un archivo, lo cual es útil para determinar si un archivo abierto está en un estado que admite operaciones no disruptivas.

Acerca de esta tarea

Puede ver información sobre los archivos abiertos en una sesión de SMB establecida. La información que se muestra es útil cuando necesita determinar la información de la sesión SMB para determinados archivos dentro de una sesión SMB.

Por ejemplo, si tiene una sesión SMB en la que algunos archivos abiertos están abiertos con protección continua disponible y algunos no están abiertos con protección continua disponible (el valor de la `-continuously-available` campo en `vserver cifs session show` el resultado del comando es `Partial`), puede determinar qué archivos no están disponibles continuamente mediante este comando.

Puede mostrar información de todos los archivos abiertos en sesiones SMB establecidas en máquinas virtuales de almacenamiento (SVM) de forma resumida mediante la `vserver cifs session file show`

comando sin ningún parámetro opcional.

Sin embargo, en muchos casos, la cantidad de producción devuelta es grande. Puede personalizar la información que se muestra en el resultado especificando parámetros opcionales. Esto puede resultar útil si desea ver información sólo de un pequeño subconjunto de archivos abiertos.

- Puede usar el opcional `-fields` parámetro para mostrar la salida en los campos que elija.

Es posible usar este parámetro de forma independiente o combinada con otros parámetros opcionales.

- Puede utilizar el `-instance` Parámetro para mostrar información detallada sobre los archivos SMB abiertos.

Es posible usar este parámetro de forma independiente o combinada con otros parámetros opcionales.

Paso

1. Ejecute una de las siguientes acciones:

| Si desea mostrar archivos SMB abiertos... | Introduzca el siguiente comando... |
|--|---|
| En la SVM de forma resumida | <code>vserver cifs session file show -vserver vserver_name</code> |
| En un nodo especificado | <code>`vserver cifs session file show -vserver vserver_name -node {node_name</code> |
| local}` | En un ID de archivo especificado |
| <code>vserver cifs session file show -vserver vserver_name -file-id integer</code> | En un ID de conexión de SMB especificado |
| <code>vserver cifs session file show -vserver vserver_name -connection-id integer</code> | En un ID de sesión de SMB especificado |
| <code>vserver cifs session file show -vserver vserver_name -session-id integer</code> | En el agregado de host especificado |
| <code>vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name</code> | En el volumen especificado |
| <code>vserver cifs session file show -vserver vserver_name -hosting-volume volume_name</code> | En el recurso compartido de SMB especificado |

| Si desea mostrar archivos SMB abiertos... | Introduzca el siguiente comando... |
|--|--|
| <code>vserver cifs session file show -vserver vserver_name -share share_name</code> | En la ruta del bloque de mensajes del servidor especificada |
| <code>vserver cifs session file show -vserver vserver_name -path path</code> | Con el nivel especificado de protección continua disponible |
| <code>`vserver cifs session file show -vserver vserver_name -continuously-available {No</code> | Yes} [NOTE] ==== Si el estado continuamente disponible es No, esto significa que estos archivos abiertos no son capaces de recuperarse de forma no disruptiva de la toma de control y la devolución. Tampoco pueden recuperarse de la reubicación general de agregados entre partners en una relación de alta disponibilidad. ==== |
| Con el estado reconectado especificado | <code>`vserver cifs session file show -vserver vserver_name -reconnected {No</code> |

Existen parámetros opcionales adicionales que se pueden utilizar para refinar los resultados de la salida. Consulte la página del manual para obtener más información.

Ejemplos

En el siguiente ejemplo, se muestra información sobre los archivos abiertos en la SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1
Node:      node1
Vserver:   vs1
Connection: 3151274158
Session:   1
File      File      Open Hosting      Continuously
ID        Type        Mode Volume      Share      Available
-----
41        Regular    r      data      data      Yes
Path: \mytest.rtf
```

En el siguiente ejemplo, se muestra información detallada sobre los archivos SMB abiertos con el ID de archivo 82 en la SVM vs1:

```
cluster1::> vsriver cifs session file show -vsriver vs1 -file-id 82
-instance
```

```
Node: node1
Vserver: vs1
File ID: 82
Connection ID: 104617
Session ID: 1
File Type: Regular
Open Mode: rw
Aggregate Hosting File: aggr1
Volume Hosting File: data1
CIFS Share: data1
Path from CIFS Share: windows\win8\test\test.txt
Share Mode: rw
Range Locks: 1
Continuously Available: Yes
Reconnected: No
```

Información relacionada

[Mostrar información de la sesión SMB](#)

Determine qué objetos de estadísticas y contadores están disponibles

Para poder obtener información acerca de las estadísticas de CIFS, SMB, auditoría y BranchCache hash, y supervisar el rendimiento, debe conocer los objetos y contadores disponibles desde los cuales puede obtener datos.

Pasos

1. Configure el nivel de privilegio en Advanced: `set -privilege advanced`
2. Ejecute una de las siguientes acciones:

| Si desea determinar... | Introduzca... |
|----------------------------------|---|
| Qué objetos están disponibles | <code>statistics catalog object show</code> |
| Objetos específicos disponibles | <code>statistics catalog object show object object_name</code> |
| Qué contadores están disponibles | <code>statistics catalog counter show object object_name</code> |

Consulte las páginas de manual para obtener más información acerca de los objetos y contadores disponibles.

3. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

Ejemplos

El siguiente comando muestra descripciones de los objetos de estadísticas seleccionados relacionados con CIFS y acceso SMB en el clúster tal y como se ve en el nivel de privilegio avanzado:

```
cluster1::> set -privilege advanced
```

Warning: These advanced commands are potentially dangerous; use them only when directed to do so by support personnel.

Do you want to continue? {y|n}: y

```
cluster1::*> statistics catalog object show -object audit
      audit_ng                CM object for exporting audit_ng
performance counters
```

```
cluster1::*> statistics catalog object show -object cifs
      cifs                    The CIFS object reports activity of the
                             Common Internet File System protocol
                             ...
```

```
cluster1::*> statistics catalog object show -object nblade_cifs
      nblade_cifs            The Common Internet File System (CIFS)
                             protocol is an implementation of the
Server
                             ...
```

```
cluster1::*> statistics catalog object show -object smb1
      smb1                   These counters report activity from the
SMB
                             revision of the protocol. For information
                             ...
```

```
cluster1::*> statistics catalog object show -object smb2
      smb2                   These counters report activity from the
                             SMB2/SMB3 revision of the protocol. For
                             ...
```

```
cluster1::*> statistics catalog object show -object hashd
      hashd                  The hashd object provides counters to
measure
                             the performance of the BranchCache hash
daemon.
```

```
cluster1::*> set -privilege admin
```

El siguiente comando muestra información acerca de algunos contadores de `cifs` objeto como se ve en el nivel de privilegio avanzado:



En este ejemplo no se muestran todos los contadores disponibles para el `cifs` objeto; la salida se truncará.

```
cluster1::> set -privilege advanced
```

Warning: These advanced commands are potentially dangerous; use them only when directed to do so by support personnel.

Do you want to continue? {y|n}: y

```
cluster1::*> statistics catalog counter show -object cifs
```

Object: cifs

| Counter | Description |
|----------------------|--|
| active_searches | Number of active searches over SMB and SMB2 |
| auth_reject_too_many | Authentication refused after too many requests were made in rapid succession |
| avg_directory_depth | Average number of directories crossed by SMB and SMB2 path-based commands |
| ... | ... |

```
cluster2::> statistics start -object client -sample-id
```

Object: client

| Counter | Value |
|----------------------|-------------------------|
| cifs_ops | 0 |
| cifs_read_ops | 0 |
| cifs_read_recv_ops | 0 |
| cifs_read_recv_size | 0B |
| cifs_read_size | 0B |
| cifs_write_ops | 0 |
| cifs_write_recv_ops | 0 |
| cifs_write_recv_size | 0B |
| cifs_write_size | 0B |
| instance_name | vserver_1:10.72.205.179 |
| instance_uuid | 2:10.72.205.179 |
| local_ops | 0 |
| mount_ops | 0 |

[...]

Información relacionada

[Mostrar estadísticas](#)

Mostrar estadísticas

Puede mostrar varias estadísticas, incluidas estadísticas sobre CIFS y SMB, auditoría y hash de BranchCache, para supervisar el rendimiento y diagnosticar problemas.

Antes de empezar

Debe haber recogido muestras de datos utilizando el `statistics start` y `statistics stop` comandos antes de mostrar información sobre los objetos.

Pasos

- 1. Configure el nivel de privilegio en Advanced: `set -privilege advanced`
- 2. Ejecute una de las siguientes acciones:

| Si desea mostrar estadísticas de... | Introduzca... |
|-------------------------------------|--|
| Todas las versiones de SMB | <code>statistics show -object cifs</code> |
| SMB 1,0 | <code>statistics show -object smb1</code> |
| SMB 2.x y SMB 3.0 | <code>statistics show -object smb2</code> |
| Subsistema CIFS del nodo | <code>statistics show -object nblade_cifs</code> |
| Auditoría multiprotocolo | <code>statistics show -object audit_ng</code> |
| Servicio hash de BranchCache | <code>statistics show -object hashd</code> |
| DNS dinámico | <code>statistics show -object ddns_update</code> |

Consulte la página de manual de cada comando para obtener más información.

- 3. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

Información relacionada

[Determinar qué objetos de estadísticas y contadores están disponibles](#)

[Supervisar estadísticas de sesión firmada por SMB](#)

[Mostrar las estadísticas de BranchCache](#)

[Uso de estadísticas para supervisar la actividad de referencia automática de los nodos](#)

["Configuración de SMB para Microsoft Hyper-V y SQL Server"](#)

["Configuración de supervisión del rendimiento"](#)

Ponga en marcha servicios basados en cliente de SMB

Utilice archivos sin conexión para permitir el almacenamiento en caché de archivos para su uso sin conexión

Utilizar archivos sin conexión para permitir el almacenamiento en caché de archivos para uso general sin conexión

ONTAP es compatible con la característica Archivos sin conexión de Microsoft, o con la función de almacenamiento en caché del cliente_, que permite almacenar los archivos en caché en el host local para su uso sin conexión. Los usuarios pueden utilizar la funcionalidad de archivos sin conexión para seguir trabajando en archivos incluso cuando están desconectados de la red.

Puede especificar si los documentos y programas de usuario de Windows se almacenan automáticamente en caché en un recurso compartido o si los archivos deben seleccionarse manualmente para almacenar en caché. El almacenamiento en caché manual está habilitado de forma predeterminada para nuevos recursos compartidos. Los archivos que están disponibles sin conexión se sincronizan con el disco local del cliente de Windows. La sincronización se produce cuando se restaura la conectividad de red a un recurso compartido de sistema de almacenamiento específico.

Puesto que los archivos y carpetas sin conexión conservan los mismos permisos de acceso que la versión de los archivos y carpetas guardados en el servidor CIFS, el usuario debe tener suficientes permisos en los archivos y carpetas guardados en el servidor CIFS para realizar acciones en los archivos y carpetas sin conexión.

Cuando el usuario y otra persona de la red realizan cambios en el mismo archivo, el usuario puede guardar la versión local del archivo en la red, conservar la otra versión o guardar ambas. Si el usuario conserva ambas versiones, se guarda localmente un nuevo archivo con los cambios del usuario local y el archivo almacenado en caché se sobrescribe con cambios de la versión del archivo guardado en el servidor CIFS.

Puede configurar archivos sin conexión de forma compartida mediante las opciones de configuración de recursos compartidos. Puede elegir una de las cuatro configuraciones de carpetas sin conexión al crear o modificar recursos compartidos:

- Sin almacenamiento en caché

Deshabilita el almacenamiento en caché en el cliente para el recurso compartido. Los archivos y carpetas no se almacenan automáticamente en caché local en clientes y los usuarios no pueden optar por almacenar en caché archivos o carpetas localmente.

- Almacenamiento en caché manual

Permite la selección manual de archivos para almacenar en caché en el recurso compartido. Esta es la configuración predeterminada. De forma predeterminada, no se almacenan en caché archivos ni carpetas en el cliente local. Los usuarios pueden elegir los archivos y carpetas que desean almacenar en caché localmente para utilizarlos sin conexión.

- Almacenamiento automático de documentos en caché

Permite que los documentos de usuario se almacenen automáticamente en caché en el recurso compartido. Sólo los archivos y carpetas a los que se tiene acceso se almacenan en caché localmente.

- Almacenamiento automático de programas en caché

Permite que los programas y los documentos de usuario se almacenen automáticamente en caché en el recurso compartido. Sólo los archivos, carpetas y programas a los que se tiene acceso se almacenan en caché localmente. Además, esta configuración permite al cliente ejecutar ejecutables almacenados localmente en caché incluso cuando se conecta a la red.

Para obtener más información acerca de la configuración de archivos sin conexión en servidores y clientes de Windows, consulte la biblioteca de Microsoft TechNet.

Información relacionada

[Uso de perfiles de itinerancia para almacenar perfiles de usuario de forma centralizada en un servidor CIFS asociado con la SVM](#)

[Uso de la redirección de carpetas para almacenar datos en un servidor CIFS](#)

[Uso de BranchCache para almacenar en caché contenido compartido de SMB en una sucursal](#)

["Biblioteca de Microsoft TechNet: \[technet.microsoft.com/en-us/library/\]\(http://technet.microsoft.com/en-us/library/\)"](#)

Requisitos para utilizar archivos sin conexión

Antes de poder utilizar la función Microsoft Offline Files con el servidor CIFS, debe conocer las versiones de ONTAP y SMB y los clientes Windows que admiten la función.

Requisitos de la versión de ONTAP

Las versiones ONTAP admiten archivos sin conexión.

Requisitos de la versión del protocolo SMB

Para las máquinas virtuales de almacenamiento (SVM), ONTAP admite archivos sin conexión en todas las versiones de SMB.

Requisitos del cliente Windows

El cliente Windows debe admitir los archivos sin conexión.

Para obtener la información más reciente sobre los clientes de Windows que admiten la función Archivos sin conexión, consulte la matriz de interoperabilidad.

["mysupport.netapp.com/matrix"](#)

Directrices para implementar archivos sin conexión

Hay algunas directrices importantes que debe entender al implementar archivos sin conexión en los recursos compartidos de directorios iniciales que tienen `showsnapshot` propiedad share establecida en directorios iniciales.

Si la `showsnapshot` La propiedad Share se establece en un recurso compartido de directorio principal que tiene configurados archivos sin conexión, los clientes de Windows almacenan en caché todas las copias Snapshot en la `~snapshot` en el directorio principal del usuario.

Los clientes de Windows almacenan en caché todas las copias Snapshot en el directorio inicial si se cumple alguna de las siguientes condiciones:

- El usuario hace que el directorio inicial esté disponible sin conexión desde el cliente.

El contenido del `~snapshot` la carpeta del directorio principal se incluye y se hace disponible sin conexión.

- El usuario configura la redirección de carpetas para redirigir una carpeta como, por ejemplo `My Documents` En la raíz de un directorio inicial que reside en el recurso compartido de servidor CIFS.

Es posible que algunos clientes de Windows hagan que la carpeta redirigida esté disponible sin conexión automáticamente. Si la carpeta se redirige a la raíz del directorio principal, el `~snapshot` la carpeta se incluye en el contenido sin conexión almacenado en caché.



Los archivos sin conexión se despliegan donde `~snapshot` la carpeta se incluye en los archivos sin conexión se debe evitar. Las copias Snapshot en la `~snapshot` La carpeta contiene todos los datos del volumen en el punto en que ONTAP creó la copia Snapshot. Por tanto, cree una copia sin conexión de `~snapshot` la carpeta consume una cantidad significativa de almacenamiento local en el cliente, consume ancho de banda de red durante la sincronización de archivos sin conexión y aumenta el tiempo necesario para sincronizar archivos sin conexión.

Configure la compatibilidad de archivos sin conexión en recursos compartidos SMB mediante la CLI

Puede configurar la compatibilidad de archivos sin conexión mediante la interfaz de línea de comandos de ONTAP especificando una de las cuatro archivos sin conexión al crear recursos compartidos de SMB o en cualquier momento modificando los recursos compartidos de SMB existentes. La compatibilidad con archivos manuales sin conexión es la configuración predeterminada.

Acerca de esta tarea

Al configurar el soporte de archivos sin conexión, puede elegir una de las siguientes cuatro opciones de archivos sin conexión:

| Ajuste | Descripción |
|------------------------|---|
| <code>none</code> | Despermite a los clientes de Windows almacenar en caché cualquier archivo en este recurso compartido. |
| <code>manual</code> | Permite a los usuarios de clientes de Windows seleccionar manualmente los archivos que se van a almacenar en caché. |
| <code>documents</code> | Permite a los clientes de Windows almacenar en caché los documentos de usuario utilizados por el usuario para el acceso sin conexión. |

| Ajuste | Descripción |
|----------|---|
| programs | Permite a los clientes de Windows almacenar en caché programas que utilizan el usuario para el acceso sin conexión. Los clientes pueden utilizar los archivos de programa almacenados en caché en modo sin conexión incluso si el recurso compartido está disponible. |

Sólo puede seleccionar una configuración de archivo sin conexión. Si modifica una configuración de archivos sin conexión en un recurso compartido SMB existente, la opción nuevos archivos sin conexión reemplaza la configuración original. Las demás opciones de configuración y propiedades de uso compartido de SMB existentes no se eliminan ni se reemplazan. Permanecen vigentes hasta que se eliminan o cambian explícitamente.

Pasos

1. Ejecute la acción adecuada:

| Si desea configurar archivos sin conexión en... | Introduzca el comando... |
|---|--|
| Un nuevo recurso compartido de SMB | <code>`vserver cifs share create -vserver vserver_name -share-name share_name -path path -offline-files {none</code> |
| manual | documents |
| programs}` | Un recurso compartido de SMB existente |
| <code>`vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files {none</code> | manual |
| documents | programs}` |

2. Compruebe que la configuración de recursos compartidos de SMB es correcta: `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

Ejemplo

El siguiente comando crea un recurso compartido SMB denominado «data1» con archivos sin conexión establecidos en `documents`:

```
cluster1::> vservice cifs share create -vservice vs1 -share-name data1 -path
/data1 -comment "Offline files" -offline-files documents

cluster1::> vservice cifs share show -vservice vs1 -share-name data1
-instance

                Vservice: vs1
                Share: data1
        CIFS Server NetBIOS Name: VS1
                Path: /data1
                Share Properties: oplocks
                                browsable
                                changenotify
                Symlink Properties: enable
                File Mode Creation Mask: -
        Directory Mode Creation Mask: -
                Share Comment: Offline files
                Share ACL: Everyone / Full Control
        File Attribute Cache Lifetime: -
                Volume Name: -
                Offline Files: documents
        Vscan File-Operations Profile: standard
        Maximum Tree Connections on Share: 4294967295
                UNIX Group for File Create: -
```

El siguiente comando modifica un recurso compartido SMB existente llamado «data1» cambiando la configuración de archivos sin conexión a. manual y agregando valores para la máscara de creación de modo de archivo y directorio:

```
cluster1::> vsserver cifs share modify -vsserver vs1 -share-name data1
-offline-files manual -file-umask 644 -dir-umask 777
```

```
cluster1::> vsserver cifs share show -vsserver vs1 -share-name data1
-instance
```

```

                Vserver: vs1
                Share: data1
CIFS Server NetBIOS Name: VS1
                Path: /data1
        Share Properties: oplocks
                        browsable
                        changenotify
        Symlink Properties: enable
        File Mode Creation Mask: 644
        Directory Mode Creation Mask: 777
                Share Comment: Offline files
                Share ACL: Everyone / Full Control
        File Attribute Cache Lifetime: -
                Volume Name: -
                Offline Files: manual
        Vscan File-Operations Profile: standard
        Maximum Tree Connections on Share: 4294967295
        UNIX Group for File Create: -
```

Información relacionada

[Agregar o quitar propiedades de recursos compartidos en un recurso compartido SMB existente](#)

Configure el soporte de archivos sin conexión en recursos compartidos SMB mediante la MMC de Administración de equipos

Si desea permitir a los usuarios almacenar en caché archivos localmente para su uso sin conexión, puede configurar la compatibilidad con archivos sin conexión mediante la MMC de Administración de equipos (Microsoft Management Console).

Pasos

1. Para abrir el MMC en el servidor de Windows, en el Explorador de Windows, haga clic con el botón secundario del mouse (ratón) en el icono del equipo local y, a continuación, seleccione **Administrar**.
2. En el panel izquierdo, seleccione **Administración de equipos**.
3. Seleccione **Acción > conectar a otro ordenador**.

Aparece el cuadro de diálogo Seleccionar equipo.

4. Escriba el nombre del servidor CIFS o haga clic en **examinar** para buscar el servidor CIFS.

Si el nombre del servidor CIFS es el mismo que el nombre de host de máquina virtual de almacenamiento (SVM), escriba el nombre de SVM. Si el nombre del servidor CIFS es diferente del nombre de host de la

SVM, escriba el nombre del servidor CIFS.

5. Haga clic en **Aceptar**.
6. En el árbol de la consola, haga clic en **Herramientas del sistema > carpetas compartidas**.
7. Haga clic en **comparticiones**.
8. En el panel de resultados, haga clic con el botón derecho en el recurso compartido.
9. Haga clic en **Propiedades**.

Se mostrarán las propiedades del recurso compartido seleccionado.

10. En la ficha **General**, haga clic en **Configuración sin conexión**.

Se muestra el cuadro de diálogo Configuración sin conexión.

11. Configure las opciones de disponibilidad sin conexión según corresponda.
12. Haga clic en **Aceptar**.

Use perfiles de itinerancia para almacenar perfiles de usuario de forma centralizada en un servidor SMB asociado con la SVM

Use perfiles de itinerancia para almacenar perfiles de usuario de forma centralizada en un servidor SMB asociado a la información general de SVM

ONTAP admite el almacenamiento de perfiles de itinerancia de Windows en un servidor CIFS asociado con la máquina virtual de almacenamiento (SVM). La configuración de perfiles de itinerancia de usuario ofrece ventajas al usuario, como la disponibilidad automática de recursos, independientemente de dónde inicie sesión el usuario. Los perfiles móviles también simplifican la administración y gestión de los perfiles de usuario.

Los perfiles de usuario móviles tienen las siguientes ventajas:

- Disponibilidad de recursos automática

El perfil único de un usuario está automáticamente disponible cuando ese usuario inicia sesión en cualquier equipo de la red que ejecuta Windows 8, Windows 7, Windows 2000 o Windows XP. Los usuarios no necesitan crear un perfil en cada equipo que utilizan en una red.

- Sustitución simplificada del ordenador

Dado que toda la información del perfil del usuario se mantiene por separado en la red, el perfil de un usuario se puede descargar fácilmente en un equipo nuevo y de repuesto. Cuando el usuario inicia sesión en el nuevo equipo por primera vez, la copia del servidor del perfil del usuario se copia en el nuevo equipo.

Información relacionada

[Uso de archivos sin conexión para permitir el almacenamiento en caché de archivos para su uso sin conexión](#)

[Uso de la redirección de carpetas para almacenar datos en un servidor CIFS](#)

Requisitos para utilizar perfiles de itinerancia

Antes de poder utilizar los perfiles de itinerancia de Microsoft en su servidor CIFS,

necesita saber qué versiones de ONTAP y SMB y qué clientes de Windows admiten esta función.

Requisitos de la versión de ONTAP

ONTAP admite perfiles de itinerancia.

Requisitos de la versión del protocolo SMB

En el caso de máquinas virtuales de almacenamiento (SVM), ONTAP admite perfiles de itinerancia en todas las versiones de SMB.

Requisitos del cliente Windows

Para que un usuario pueda utilizar los perfiles de itinerancia, el cliente de Windows debe admitir la función.

Para obtener la información más reciente acerca de los clientes de Windows que admiten perfiles de itinerancia, consulte matriz de interoperabilidad.

["Herramienta de matriz de interoperabilidad de NetApp"](#)

Configurar perfiles móviles

Si desea que el perfil de un usuario esté disponible automáticamente cuando ese usuario inicie sesión en cualquier equipo de la red, puede configurar perfiles de itinerancia mediante el complemento MMC usuarios y equipos de Active Directory. Si está configurando perfiles de itinerancia en Windows Server, puede utilizar el Centro de administración de Active Directory.

Pasos

1. En el servidor Windows, abra el MMC de Usuarios y equipos de Active Directory (o el Centro de administración de Active Directory en servidores Windows).
2. Busque el usuario para el que desea configurar un perfil de itinerancia.
3. Haga clic con el botón derecho del ratón en el usuario y haga clic en **Propiedades**.
4. En la ficha **Perfil**, introduzca la ruta del perfil en el recurso compartido en el que desea almacenar el perfil de itinerancia del usuario, seguido de %username%.

Por ejemplo, una ruta de acceso de perfil puede ser la siguiente:

\\vs1.example.com\profiles\%username%. La primera vez que un usuario inicia sesión, %username% se sustituye por el nombre del usuario.



En la ruta \\vs1.example.com\profiles\%username%, profiles Es el nombre compartido de un recurso compartido de una máquina virtual de almacenamiento (SVM) vs1 con derechos de control total para todos.

5. Haga clic en **Aceptar**.

Utilice la redirección de carpetas para almacenar datos en un servidor SMB

Utilice la redirección de carpetas para almacenar los datos en una introducción al servidor SMB

ONTAP admite la redirección de carpetas de Microsoft, lo que permite que los usuarios o administradores redirijan la ruta de una carpeta local a una ubicación en el servidor CIFS. Parece que si las carpetas redirigidas se almacenan en el cliente local de Windows, aunque los datos se almacenen en un recurso compartido de SMB.

La redirección de carpetas está destinada principalmente a las empresas que ya han implementado directorios iniciales y que desean mantener la compatibilidad con su entorno de directorio raíz existente.

- Documents, Desktop, y Start Menu son ejemplos de carpetas que puede redirigir.
- Los usuarios pueden redirigir carpetas desde su cliente Windows.
- Los administradores pueden configurar y administrar centralmente la redirección de carpetas configurando GPO en Active Directory.
- Si los administradores han configurado perfiles de itinerancia, la redirección de carpetas permite a los administradores dividir los datos de usuario de los datos de perfil.
- Los administradores pueden usar la redirección de carpetas y los archivos sin conexión juntos para redirigir el almacenamiento de datos de carpetas locales al servidor CIFS, permitiendo a los usuarios almacenar el contenido en la memoria caché localmente.

Información relacionada

[Uso de archivos sin conexión para permitir el almacenamiento en caché de archivos para su uso sin conexión](#)

[Uso de perfiles de itinerancia para almacenar perfiles de usuario de forma centralizada en un servidor CIFS asociado con la SVM](#)

Requisitos para utilizar la redirección de carpetas

Para poder utilizar la redirección de carpetas de Microsoft con el servidor CIFS, debe conocer las versiones de ONTAP y SMB y los clientes de Windows que admiten la función.

Requisitos de la versión de ONTAP

ONTAP admite redirección de carpetas de Microsoft.

Requisitos de la versión del protocolo SMB

Para la máquina virtual de almacenamiento (SVM), ONTAP admite el redireccionamiento de carpetas de Microsoft en todas las versiones de SMB.

Requisitos del cliente Windows

Para que un usuario pueda utilizar la redirección de carpetas de Microsoft, el cliente de Windows debe admitir la función.

Para obtener la información más reciente acerca de los clientes de Windows que admiten la redirección de carpetas, consulte la matriz de interoperabilidad.

["mysupport.netapp.com/matrix"](https://mysupport.netapp.com/matrix)

Configurar la redirección de carpetas

Puede configurar la redirección de carpetas mediante la ventana Propiedades de Windows. La ventaja de utilizar este método es que el usuario de Windows puede configurar la redirección de carpetas sin la ayuda del administrador de SVM.

Pasos

1. En el Explorador de Windows, haga clic con el botón secundario en la carpeta que desea redirigir a un recurso compartido de red.
2. Haga clic en **Propiedades**.

Se mostrarán las propiedades del recurso compartido seleccionado.

3. En la ficha **acceso directo**, haga clic en **destino** y especifique la ruta de acceso a la ubicación de red en la que desea redirigir la carpeta seleccionada.

Por ejemplo, si desea redirigir una carpeta al data carpeta de un directorio principal al que está asignado Q:\, especifique Q:\data como destino.

4. Haga clic en **Aceptar**.

Para obtener más información acerca de la configuración de carpetas sin conexión, consulte la Biblioteca de Microsoft TechNet.

Información relacionada

"Biblioteca de Microsoft TechNet: technet.microsoft.com/en-us/library/"

Acceda al directorio ~snapshot desde clientes de Windows mediante SMB 2.x.

El método que utiliza para acceder a ~snapshot el directorio de clientes de Windows que utilizan SMB 2.x difiere del método utilizado para SMB 1.0. Debe comprender cómo acceder al ~snapshot directorio al utilizar las conexiones SMB 2.x para acceder correctamente a los datos almacenados en copias Snapshot.

El administrador de SVM controla si los usuarios de clientes de Windows pueden ver y acceder a ~snapshot active o desactive el directorio en un recurso compartido showsnapshot comparta la propiedad mediante comandos de las familias de propiedades compartidas cifs del vserver.

Cuando la showsnapshot La propiedad Share está deshabilitada, un usuario de un cliente Windows que utilice SMB 2.x no puede ver la ~snapshot Y no puede acceder a las copias Snapshot dentro de la ~snapshot directorio, incluso cuando se introduce manualmente la ruta de acceso al ~snapshot directorio o a copias Snapshot específicas dentro del directorio.

Cuando la showsnapshot La propiedad Share está habilitada; un usuario de un cliente Windows que utilice SMB 2.x todavía no puede ver la ~snapshot directorio en la raíz del recurso compartido o dentro de cualquier unión o directorio debajo de la raíz del recurso compartido. Sin embargo, después de conectarse a un recurso compartido, el usuario puede acceder al oculto ~snapshot directorio anexando manualmente \~snapshot al final de la ruta de uso compartido. El oculto ~snapshot se puede acceder al directorio desde dos puntos de entrada:

- En la raíz del recurso compartido

- En cada punto de unión del espacio compartido

El oculto `~snapshot` no se puede acceder al directorio desde los subdirectorios que no son de unión dentro del recurso compartido.

Ejemplo

Con la configuración que se muestra en el ejemplo siguiente, un usuario de un cliente Windows con una conexión SMB 2.x al recurso compartido «eng» puede acceder al `~snapshot` directorio anexando manualmente `\~snapshot` a la ruta de uso compartido en la raíz del recurso compartido y en cada punto de unión del camino. El oculto `~snapshot` se puede acceder al directorio desde las tres rutas siguientes:

- `\\vs1\eng\~snapshot`
- `\\vs1\eng\projects1\~snapshot`
- `\\vs1\eng\projects2\~snapshot`

```
cluster1::> volume show -vserver vs1 -fields volume,junction-path
vserver volume          junction-path
-----
vs1      vs1_root        /
vs1      vs1_vol1        /eng
vs1      vs1_vol2        /eng/projects1
vs1      vs1_vol3        /eng/projects2

cluster1::> vsserver cifs share show
Vserver  Share  Path    Properties      Comment  ACL
-----
vs1      eng    /eng    oplocks         -        Everyone / Full Control
          chngenotify
          browsable
          showsnapshot
```

Recupere archivos y carpetas con versiones anteriores

Recupere archivos y carpetas usando la información general de versiones anteriores

La capacidad de usar las versiones anteriores de Microsoft es aplicable a los sistemas de archivos que admiten copias snapshot de algún modo y que las tengan habilitadas. La tecnología Snapshot forma parte de ONTAP. Los usuarios pueden recuperar archivos y carpetas de copias Snapshot de su cliente Windows mediante la función versiones anteriores de Microsoft.

La funcionalidad de versiones anteriores ofrece un método para que los usuarios navegen por las copias Snapshot o para restaurar datos de una copia Snapshot sin la intervención de un administrador de almacenamiento. Las versiones anteriores no se pueden configurar. Está siempre habilitada. Si el administrador de almacenamiento ha creado copias Snapshot en un recurso compartido, el usuario puede usar versiones anteriores para realizar las siguientes tareas:

- Recuperar archivos eliminados accidentalmente.
- Recuperación de la sobrescritura accidental de un archivo.
- Compare las versiones del archivo mientras está trabajando.

Los datos almacenados en las copias Snapshot son de solo lectura. Los usuarios deben guardar una copia de un archivo en otra ubicación para realizar cualquier cambio en el archivo. Las copias Snapshot se eliminan periódicamente y, por lo tanto, los usuarios deben crear copias de los archivos contenidos en las versiones anteriores si desean conservar de forma indefinida una versión anterior de un archivo.

Requisitos para usar versiones anteriores de Microsoft

Antes de poder utilizar las versiones anteriores con el servidor CIFS, debe conocer qué versiones de ONTAP y SMB, y qué clientes de Windows, admiten. También necesita saber acerca de los requisitos de configuración de la copia Snapshot.

Requisitos de la versión de ONTAP

Admite versiones anteriores.

Requisitos de la versión del protocolo SMB

Para las máquinas virtuales de almacenamiento (SVM), ONTAP admite las versiones anteriores de todas las versiones de SMB.

Requisitos del cliente Windows

Para que un usuario pueda utilizar versiones anteriores para acceder a los datos de las copias Snapshot, el cliente Windows debe admitir la función.

Para obtener la información más reciente sobre los clientes de Windows compatibles con versiones anteriores, consulte matriz de interoperabilidad.

["Herramienta de matriz de interoperabilidad de NetApp"](#)

Requisitos para la configuración de copias Snapshot

Para usar versiones anteriores y acceder a los datos de las copias Snapshot, se debe asociar una política de Snapshot habilitada al volumen que contiene los datos, los clientes deben poder acceder a los datos de Snapshot y deben existir copias Snapshot.

Utilice la pestaña versiones anteriores para ver y gestionar datos de copias snapshot

Los usuarios de equipos cliente Windows pueden usar la pestaña versiones anteriores de la ventana Propiedades de Windows para restaurar los datos almacenados en copias Snapshot sin necesidad de implicar al administrador de máquinas virtuales de almacenamiento (SVM).

Acerca de esta tarea

Solo puede usar la pestaña versiones anteriores para ver y gestionar los datos de las copias Snapshot de los datos almacenados en la SVM si el administrador ha habilitado copias Snapshot en el volumen que contiene el recurso compartido y si el administrador configura el recurso compartido para mostrar copias Snapshot.

Pasos

1. En el Explorador de Windows, muestre el contenido de la unidad asignada de los datos almacenados en el servidor CIFS.
2. Haga clic con el botón derecho del ratón en el archivo o carpeta de la unidad de red asignada cuyas copias Snapshot desee ver o administrar.
3. Haga clic en **Propiedades**.

Se muestran las propiedades del archivo o carpeta seleccionado.

4. Haga clic en la ficha **versiones anteriores**.

En el cuadro versiones de carpeta se muestra una lista de las copias Snapshot disponibles del archivo o carpeta seleccionados. Las copias Snapshot mostradas se identifican mediante el prefijo del nombre de la copia Snapshot y la Marca de hora de creación.

5. En el cuadro **versiones de carpeta**, haga clic con el botón secundario del mouse (ratón) en la copia del archivo o carpeta que desee administrar.
6. Ejecute la acción adecuada:

| Si desea... | Haga lo siguiente... |
|--|------------------------------|
| Vea los datos de esa copia Snapshot | Haga clic en Abrir . |
| Cree una copia de los datos a partir de esa copia Snapshot | Haga clic en Copiar . |

Los datos de las copias Snapshot son de solo lectura. Si desea realizar modificaciones en los archivos y carpetas enumerados en la ficha versiones anteriores, debe guardar una copia de los archivos y carpetas que desea modificar en una ubicación editable y realizar modificaciones en las copias.

7. Después de terminar de administrar los datos de instantánea, cierre el cuadro de diálogo **Propiedades** haciendo clic en **Aceptar**.

Para obtener más información acerca de cómo utilizar la ficha versiones anteriores para ver y administrar datos de instantánea, consulte la biblioteca de Microsoft TechNet.

Información relacionada

"Biblioteca de Microsoft TechNet: technet.microsoft.com/en-us/library/"

Determine si están disponibles copias Snapshot para versiones anteriores

Puede ver copias Snapshot en la pestaña versiones anteriores solo si se aplica una política de Snapshot habilitada al volumen que contiene el recurso compartido, y si la configuración del volumen permite acceder a copias Snapshot. Determinar la disponibilidad de copias Snapshot es útil cuando se ayuda a un usuario con acceso de versiones anteriores.

Pasos

1. Determine si el volumen en el que residen los datos compartidos tiene habilitadas las copias automáticas de Snapshot y si los clientes tienen acceso a los directorios de Snapshot: `volume show -vserver`

```
vserver-name -volume volume-name -fields vserver,volume,snapdir-  
access,snapshot-policy,snapshot-count
```

El resultado muestra qué política de Snapshot está asociada con el volumen, si el acceso al directorio Snapshot de cliente está habilitado y el número de copias Snapshot disponibles.

2. Determine si la política de Snapshot asociada está habilitada: `volume snapshot policy show -policy policy-name`
3. Enumere las copias Snapshot disponibles: `volume snapshot show -volume volume_name`

Para obtener más información sobre la configuración y gestión de políticas de Snapshot y programaciones de Snapshot, consulte ["Protección de datos"](#).

Ejemplo

En el siguiente ejemplo se muestra información sobre las políticas de Snapshot asociadas con el volumen denominado «data1», que contiene los datos compartidos y las copias Snapshot disponibles en «data1».

```
cluster1::> volume show -vserver vs1 -volume data1 -fields
vserver,volume,snapshot-policy,snapdir-access,snapshot-count
vserver  volume snapdir-access snapshot-policy snapshot-count
-----
vs1      data1  true                default                10

cluster1::> volume snapshot policy show -policy default
Vserver: cluster1

                Number of Is
Policy Name      Schedules Enabled Comment
-----
default          3 true      Default policy with hourly, daily &
weekly schedules.
  Schedule      Count      Prefix      SnapMirror Label
  -----
  hourly        6      hourly      -
  daily         2      daily       daily
  weekly        2      weekly      weekly

cluster1::> volume snapshot show -volume data1

                ---Blocks---
Vserver  Volume  Snapshot      State      Size  Total%  Used%
-----
vs1      data1
        weekly.2012-12-16_0015  valid      408KB    0%    1%
        daily.2012-12-22_0010  valid      420KB    0%    1%
        daily.2012-12-23_0010  valid      192KB    0%    0%
        weekly.2012-12-23_0015  valid      360KB    0%    1%
        hourly.2012-12-23_1405  valid      196KB    0%    0%
        hourly.2012-12-23_1505  valid      196KB    0%    0%
        hourly.2012-12-23_1605  valid      212KB    0%    0%
        hourly.2012-12-23_1705  valid      136KB    0%    0%
        hourly.2012-12-23_1805  valid      200KB    0%    0%
        hourly.2012-12-23_1905  valid      184KB    0%    0%
```

Información relacionada

[Crear una configuración de instantánea para permitir el acceso a versiones anteriores](#)

["Protección de datos"](#)

Cree una configuración de instantánea para habilitar el acceso a versiones anteriores

La funcionalidad de versiones anteriores está siempre disponible, siempre y cuando exista acceso de los clientes a las copias Snapshot. Si la configuración de su copia Snapshot no cumple estos requisitos, puede crear una configuración de copia Snapshot que sí lo haga.

Pasos

1. Si el volumen que contiene el recurso compartido al que desea permitir el acceso a versiones anteriores no tiene una política de Snapshot asociada, asocie una política de Snapshot al volumen y habilite esa política mediante el uso de `volume modify` comando.

Para obtener más información acerca del uso de `volume modify` consulte las páginas de manual.

2. Habilite el acceso a las copias de Snapshot mediante el `volume modify` para establecer el `-snap-dir` opción a `true`.

Para obtener más información acerca del uso de `volume modify` consulte las páginas de manual.

3. Compruebe que se han habilitado las políticas de Snapshot y que el acceso a los directorios de Snapshot se habilita mediante el `volume show y.. volume snapshot policy show` comandos.

Para obtener más información acerca del uso de `volume show y.. volume snapshot policy show` consulte las páginas de manual.

Para obtener más información sobre la configuración y gestión de políticas de Snapshot y programaciones de Snapshot, consulte ["Protección de datos"](#).

Información relacionada

["Protección de datos"](#)

Directrices para restaurar directorios que contienen uniones

Hay ciertas directrices que debe tener en cuenta al utilizar versiones anteriores para restaurar carpetas que contienen puntos de unión.

Cuando se usan versiones anteriores para restaurar carpetas que tienen carpetas secundarias que son puntos de unión, la restauración puede fallar con un `Access Denied` error.

Puede determinar si la carpeta que intenta restaurar contiene una unión mediante la `vol show` con el `-parent` opción. También puede utilizar el `vserver security trace` comandos para crear registros detallados sobre problemas de acceso a archivos y carpetas.

Información relacionada

[Crear y gestionar volúmenes de datos en espacios de nombres NAS](#)

Ponga en marcha servicios basados en servidor de SMB

Administrar directorios iniciales

Cómo habilita ONTAP los directorios iniciales dinámicos

Los directorios iniciales de ONTAP permiten configurar un recurso compartido de SMB que se asigna a directorios diferentes en función del usuario que se conecta a él y a un conjunto de variables. En lugar de crear recursos compartidos independientes para cada usuario, puede configurar un recurso compartido con algunos parámetros del directorio inicial para definir la relación de un usuario entre un punto de entrada (el recurso compartido) y el directorio inicial (un directorio en la SVM).

Un usuario que ha iniciado sesión como usuario invitado no tiene un directorio principal y no puede acceder a los directorios iniciales de otros usuarios. Existen cuatro variables que determinan cómo se asigna un usuario a un directorio:

- **Nombre del recurso compartido**

Éste es el nombre del recurso compartido que se crea al que se conecta el usuario. Debe establecer la propiedad del directorio principal para este recurso compartido.

El nombre del recurso compartido puede utilizar los siguientes nombres dinámicos:

- `%w` (Nombre de usuario de Windows del usuario)
- `%d` (Nombre de dominio de Windows del usuario)
- `%u` (Nombre de usuario UNIX asignado del usuario)

Para que el nombre del recurso compartido sea único en todos los directorios iniciales, el nombre del recurso compartido debe contener cualquiera de los dos `%w` o la `%u` variable. El nombre del recurso compartido puede contener ambos `%d` y la `%w` variable (por ejemplo, `%d/%w`), o el nombre del recurso compartido puede contener una parte estática y una parte variable (por ejemplo, `home_/%w`).

- **Compartir ruta**

Esta es la ruta relativa, que define el recurso compartido y, por lo tanto, está asociada con uno de los nombres de recurso compartido, que se anexa a cada ruta de búsqueda para generar toda la ruta de directorio inicial del usuario desde la raíz de la SVM. Puede ser estático (por ejemplo, `home`), dinámico (por ejemplo, `%w`), o una combinación de los dos (por ejemplo, `eng/%w`).

- **Rutas de búsqueda**

Este es el conjunto de rutas absolutas desde la raíz de la SVM que especifique que dirige la búsqueda ONTAP de directorios iniciales. Puede especificar una o varias rutas de búsqueda mediante el `vserver cifs home-directory search-path add` comando. Si especifica varias rutas de búsqueda, ONTAP las intenta en el orden especificado hasta que encuentre una ruta válida.

- **Directorio**

Éste es el directorio principal del usuario que se crea para el usuario. El nombre del directorio suele ser el nombre del usuario. Debe crear el directorio principal en uno de los directorios definidos por las rutas de búsqueda.

Por ejemplo, considere la siguiente configuración:

- Usuario: John Smith
- Dominio de usuario: acme
- Nombre de usuario: Jsmith
- Nombre de SVM: vs1
- Directorio principal nombre compartido #1: `home_ %w` - vía compartida: `%w`
- Nombre del recurso compartido del directorio inicial #2: `%w` - vía compartida: `%d/%w`
- Ruta de búsqueda #1: `/vol0home/home`
- Ruta de búsqueda #2: `/vol1home/home`

- Ruta de búsqueda #3: `/vol2home/home`
- Directorio inicial: `/vol1home/home/jsmith`

Escenario 1: El usuario se conecta a. `\\vs1\home_jsmith`. Esto coincide con el nombre del primer recurso compartido del directorio principal y genera la ruta de acceso relativa `jsmith`. ONTAP busca ahora un directorio llamado `jsmith` comprobando cada ruta de búsqueda en orden:

- `/vol0home/home/jsmith` no existe; pasar a la ruta de búsqueda #2.
- `/vol1home/home/jsmith` existe; por lo tanto, la ruta de búsqueda #3 no está activada; el usuario está conectado a su directorio principal.

Escenario 2: El usuario se conecta a. `\\vs1\jsmith`. Esto coincide con el segundo nombre del recurso compartido del directorio principal y genera la ruta de acceso relativa `acme/jsmith`. ONTAP busca ahora un directorio llamado `acme/jsmith` comprobando cada ruta de búsqueda en orden:

- `/vol0home/home/acme/jsmith` no existe; pasar a la ruta de búsqueda #2.
- `/vol1home/home/acme/jsmith` no existe; se pasa a la ruta de búsqueda #3.
- `/vol2home/home/acme/jsmith` no existe; el directorio principal no existe; por lo tanto, la conexión falla.

Recursos compartidos de directorios iniciales

Agregue un recurso compartido de directorio principal

Si desea utilizar la característica de directorio inicial SMB, debe agregar al menos un recurso compartido con la propiedad de directorio principal incluida en las propiedades de recurso compartido.

Acerca de esta tarea

Puede crear un recurso compartido de directorio principal en el momento de crear el recurso compartido mediante `vserver cifs share create` o puede cambiar un recurso compartido existente a un recurso compartido de directorio principal en cualquier momento mediante el `vserver cifs share modify` comando.

Para crear un recurso compartido de directorio principal, debe incluir `homedirectory` valor en la `-share-properties` opción al crear o modificar un recurso compartido. Puede especificar el nombre de recurso compartido y la ruta de acceso compartida mediante variables que se amplían dinámicamente cuando los usuarios se conectan a sus directorios iniciales. Las variables disponibles que puede utilizar en la ruta son `%w`, `%d`, y `%u`, Correspondiente al nombre de usuario, dominio y nombre de usuario UNIX asignado de Windows, respectivamente.

Pasos

1. Agregue un recurso compartido de directorio principal:

```
vserver cifs share create -vserver vserver_name -share-name share_name -path
path -share-properties homedirectory[,...]
```

`-vserver vserver` Especifica la máquina virtual de almacenamiento (SVM) habilitada para CIFS en la que se añadirá la ruta de búsqueda.

`-share-name share-name` especifica el nombre del recurso compartido del directorio principal.

Además de contener una de las variables necesarias, si el nombre del recurso compartido contiene una de las cadenas literales %w, %u, o. %d, Debe preceder a la cadena literal con un carácter de % (porcentaje) para evitar que ONTAP trate la cadena literal como una variable (por ejemplo, %%w).

- El nombre del recurso compartido debe contener a. %w o la %u variable.
- El nombre del recurso compartido también puede contener el %d variable (por ejemplo, %d/%w) o una parte estática en el nombre del recurso compartido (por ejemplo, home1_/%w).
- Si los administradores utilizan el recurso compartido para conectarse a los directorios principales de otros usuarios o para permitir que los usuarios se conecten a los directorios principales de otros usuarios, el patrón de nombre de recurso compartido dinámico debe ir precedido de una tilde (~).

La `vserver cifs home-directory modify` se utiliza para activar este acceso mediante la configuración de `-is-home-dirs-access-for-admin-enabled` opción a. `true`) o estableciendo la opción avanzada `-is-home-dirs-access-for-public-enabled` para `true`.

`-path path` especifica la ruta de acceso relativa al directorio principal.

`-share-properties homedirectory[,...]` especifica las propiedades de recurso compartido para ese recurso compartido. Debe especificar el `homedirectory` valor. Puede especificar propiedades de recursos compartidos adicionales mediante una lista delimitada por comas.

1. Compruebe que ha agregado correctamente el recurso compartido del directorio principal mediante el `vserver cifs share show` comando.

Ejemplo

El siguiente comando crea un recurso compartido de directorio principal denominado %w. La `oplocks`, `browsable`, y `changenotify` las propiedades de uso compartido se establecen además de establecer la `homedirectory` compartir propiedad.



Este ejemplo no muestra el resultado de todos los recursos compartidos de la SVM. La salida está truncada.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name %w -path %w
-share-properties oplocks,browsable,changenotify,homedirectory

vs1::> vserver cifs share show -vserver vs1
```

| Vserver | Share | Path | Properties | Comment | ACL |
|---------|-------|------|---------------|---------|-----------------|
| vs1 | %w | %w | oplocks | - | Everyone / Full |
| Control | | | browsable | | |
| | | | changenotify | | |
| | | | homedirectory | | |

Información relacionada

[Adición de una ruta de búsqueda de directorio raíz](#)

[Requisitos y directrices para el uso de referencias automáticas al nodo](#)

Los recursos compartidos del directorio inicial requieren nombres de usuario únicos

Tenga cuidado de asignar nombres de usuario únicos al crear recursos compartidos de directorio inicial mediante el %w (Nombre de usuario de Windows) o. %u (Nombre de usuario UNIX) variables para generar recursos compartidos de forma dinámica. El nombre del recurso compartido está asignado al nombre de usuario.

Pueden ocurrir dos problemas cuando el nombre de un recurso compartido estático y el nombre de un usuario son iguales:

- Cuando el usuario enumera los recursos compartidos en un clúster con el `net view` comando, se muestran dos recursos compartidos con el mismo nombre de usuario.
- Cuando el usuario se conecta a ese nombre de recurso compartido, el usuario siempre está conectado al recurso compartido estático y no puede acceder al recurso compartido del directorio principal con el mismo nombre.

Por ejemplo, hay un recurso compartido denominado «'Administrator'» y usted tiene un nombre de usuario «'Administrator'» de Windows. Si crea un recurso compartido de directorio principal y se conecta a dicho recurso compartido, se conecta a la unidad estática "'Administrator'", no a su directorio principal "'Administrator'".

Puede resolver el problema con nombres de recursos compartidos duplicados siguiendo cualquiera de estos pasos:

- Cambiar el nombre del recurso compartido estático para que deje de estar en conflicto con el recurso compartido del directorio principal del usuario.
- Dar al usuario un nuevo nombre de usuario para que no entre en conflicto con el nombre de recurso compartido estático.
- Creación de un recurso compartido de directorio raíz CIFS con un nombre estático como «'home'» en lugar de utilizar el %w parámetro para evitar conflictos con los nombres de recursos compartidos.

Qué sucede con los nombres de uso compartido de directorios iniciales estáticos después de actualizar

Los nombres de los recursos compartidos del directorio inicial deben contener cualquiera de los dos %w o la %u variable dinámica. Debe saber qué ocurre con los nombres de recursos compartidos de directorios iniciales estáticos existentes después de actualizar a una versión de ONTAP con el nuevo requisito.

Si la configuración del directorio raíz contiene nombres de recursos compartidos estáticos y se actualiza a ONTAP, los nombres de recursos compartidos de directorio raíz estáticos no se modifican y siguen siendo válidos. Sin embargo, no puede crear ningún recurso compartido de directorio principal nuevo que no contenga ninguno de los %w o. %u variable.

Al requerir que se incluya una de estas variables en el nombre del recurso compartido del directorio principal del usuario se garantiza que cada nombre de recurso compartido sea único en la configuración del directorio principal. Si lo desea, puede cambiar los nombres de los recursos compartidos del directorio principal estático por nombres que contengan cualquiera de los dos %w o. %u variable.

Agregue una ruta de búsqueda de directorio principal

Si desea utilizar directorios iniciales SMB de ONTAP, debe agregar al menos una ruta de búsqueda de directorio raíz.

Acerca de esta tarea

Puede agregar una ruta de búsqueda de directorio principal mediante la `vserver cifs home-directory search-path add` comando.

La `vserver cifs home-directory search-path add` el comando comprueba la ruta especificada en el `-path` durante la ejecución del comando. Si la ruta especificada no existe, el comando genera un mensaje solicitando si desea continuar. Usted elige `y` o `n`. Si lo desea `y` Para continuar, ONTAP crea la ruta de búsqueda. Sin embargo, debe crear la estructura de directorios para poder utilizar la ruta de búsqueda en la configuración del directorio principal. Si elige `n` no continuar, el comando falla; no se crea la ruta de búsqueda. A continuación, puede crear la estructura de directorio de la ruta de acceso y volver a ejecutar el `vserver cifs home-directory search-path add` comando.

Pasos

1. Agregar una ruta de búsqueda de directorio principal: `vserver cifs home-directory search-path add -vserver vserver -path path`
2. Compruebe que ha agregado correctamente la ruta de búsqueda mediante `vserver cifs home-directory search-path show` comando.

Ejemplo

En el ejemplo siguiente se agrega la ruta de acceso `/home1` A la configuración del directorio inicial en SVM `vs1`.

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path /home1

vs1::> vserver cifs home-directory search-path show
Vserver      Position Path
-----
vs1          1      /home1
```

En el ejemplo siguiente se intenta agregar la ruta `/home2` A la configuración del directorio inicial en SVM `vs1`. La ruta no existe. Se decide no continuar.

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path /home2
Warning: The specified path "/home2" does not exist in the namespace
        belonging to Vserver "vs1".
Do you want to continue? {y|n}: n
```

Información relacionada

[Adición de un recurso compartido de directorio raíz](#)

Cree una configuración de directorio principal utilizando las variables %w y %d.

Puede crear una configuración de directorio inicial mediante %w y.. %d variables. Los usuarios pueden conectarse a su propio recurso compartido mediante recursos compartidos creados dinámicamente.

Pasos

1. Cree un qtree para contener los directorios iniciales del usuario: `volume qtree create -vserver vserver_name -qtree-path qtree_path`

2. Compruebe que el qtree esté usando el estilo de seguridad correcto: `volume qtree show`

3. Si el qtree no está usando el estilo de seguridad deseado, cambie el estilo de seguridad mediante el `volume qtree security` comando.

4. Agregar un recurso compartido de directorio principal: `vserver cifs share create -vserver vserver -share-name %w -path %d/%w -share-properties homedirectory\[,...\]`

`-vserver vserver` Especifica la máquina virtual de almacenamiento (SVM) habilitada para CIFS en la que se añadirá la ruta de búsqueda.

`-share-name %w` especifica el nombre del recurso compartido del directorio principal. ONTAP crea dinámicamente el nombre del recurso compartido a medida que cada usuario se conecta a su directorio inicial. El nombre del recurso compartido tendrá el formato *Windows_USER_NAME*.

`-path %d/%w` especifica la ruta de acceso relativa al directorio principal. La ruta relativa se crea dinámicamente a medida que cada usuario se conecta a su directorio principal y tendrá el formato *domain/Windows_user_name*.

`-share-properties homedirectory\[,...\]` especifica las propiedades de recurso compartido para ese recurso compartido. Debe especificar el `homedirectory` valor. Puede especificar propiedades de recursos compartidos adicionales mediante una lista delimitada por comas.

5. Compruebe que el recurso compartido tenga la configuración deseada mediante el `vserver cifs share show` comando.

6. Agregar una ruta de búsqueda de directorio principal: `vserver cifs home-directory search-path add -vserver vserver -path path`

`-vserver vserver-name` Especifica la SVM habilitada para CIFS en la que se añade la ruta de búsqueda.

`-path path` especifica la ruta absoluta del directorio a la ruta de búsqueda.

7. Compruebe que ha agregado correctamente la ruta de búsqueda mediante `vserver cifs home-directory search-path show` comando.

8. Para los usuarios que dispongan de un directorio inicial, cree un directorio correspondiente en el qtree o en el volumen designado para que contengan directorios iniciales.

Por ejemplo, si creó un qtree con la ruta de `/vol/vol1/users` y el nombre de usuario cuyo directorio desea crear es `mydomain\user1`, debe crear un directorio con la siguiente ruta de acceso: `/vol/vol1/users/mydomain/user1`.

Si creó un volumen denominado «home1» montado en `/home1`, cree un directorio con la siguiente ruta

de acceso: /home1/mydomain/user1.

9. Compruebe que un usuario puede conectarse correctamente al recurso compartido principal mediante la asignación de una unidad o la conexión mediante la ruta UNC.

Por ejemplo, si el usuario mydomain\user1 desea conectarse al directorio creado en el paso 8 que se encuentra en SVM vs1, user1 se conectará mediante la ruta UNC \\vs1\user1.

Ejemplo

Los comandos del siguiente ejemplo crean una configuración de directorio inicial con los siguientes ajustes:

- El nombre del recurso compartido es %w.
- La ruta de acceso relativa al directorio principal es %d/%w.
- La ruta de búsqueda que se utiliza para contener los directorios principales, /home1, Es un volumen configurado con estilo de seguridad NTFS.
- La configuración se crea en SVM vs1.

Puede utilizar este tipo de configuración de directorio inicial cuando los usuarios acceden a sus directorios iniciales desde hosts de Windows. También puede utilizar este tipo de configuración cuando los usuarios acceden a sus directorios iniciales desde hosts Windows y UNIX y el administrador del sistema de archivos utiliza usuarios y grupos basados en Windows para controlar el acceso al sistema de archivos.


```

cluster::> vsriver cifs share create -vsriver vs1 -share-name %w -path
%d/%w -share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vsriver cifs share show -vsriver vs1 -share-name %w

                Vserver: vs1
                Share: %w
CIFS Server NetBIOS Name: VS1
                Path: %d/%w
                Share Properties: oplocks
                                browsable
                                changenotify
                                homedirectory
                Symlink Properties: enable
                File Mode Creation Mask: -
                Directory Mode Creation Mask: -
                Share Comment: -
                Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vsriver cifs home-directory search-path add -vsriver vs1 -path
/home1

cluster::> vsriver cifs home-directory search-path show
Vserver      Position Path
-----
vs1          1        /home1

```

Información relacionada

[Configuración de directorios principales mediante la variable %u](#)

[Configuraciones adicionales de directorio inicial](#)

[Mostrar información acerca de la ruta de acceso al directorio de inicio de un usuario SMB](#)

Configure directorios iniciales utilizando la variable %u

Puede crear una configuración de directorio inicial en la que designe el nombre del recurso compartido mediante %w variable pero se utiliza %u variable para designar la ruta relativa al recurso compartido del directorio principal. A continuación, los usuarios pueden conectarse a su recurso compartido doméstico mediante recursos compartidos dinámicamente creados con su nombre de usuario de Windows sin tener en cuenta el nombre real o la ruta de acceso del directorio principal.

Pasos

1. Cree un qtree para contener los directorios iniciales del usuario: `volume qtree create -vserver vsserver_name -qtree-path qtree_path`
2. Compruebe que el qtree esté usando el estilo de seguridad correcto: `volume qtree show`
3. Si el qtree no está usando el estilo de seguridad deseado, cambie el estilo de seguridad mediante el `volume qtree security` comando.
4. Agregar un recurso compartido de directorio principal: `vserver cifs share create -vserver vsserver -share-name %w -path %u -share-properties homedirectory ,...]`

`-vserver vsserver` Especifica la máquina virtual de almacenamiento (SVM) habilitada para CIFS en la que se añadirá la ruta de búsqueda.

`-share-name %w` especifica el nombre del recurso compartido del directorio principal. El nombre del recurso compartido se crea dinámicamente a medida que cada usuario se conecta a su directorio principal y tiene el formato *Windows_USER_NAME*.



También puede utilizar el `%u` variable para `-share-name` opción. Esto crea una ruta de acceso de recursos compartidos relativa que utiliza el nombre de usuario UNIX asignado.

`-path %u` especifica la ruta de acceso relativa al directorio principal. La ruta relativa se crea dinámicamente a medida que cada usuario se conecta a su directorio principal y tiene el formato *corated_UNIX_user_name*.



El valor de esta opción también puede contener elementos estáticos. Por ejemplo: `eng/%u`.

`-share-properties homedirectory\[,... \]` especifica las propiedades de recurso compartido para ese recurso compartido. Debe especificar el `homedirectory` valor. Puede especificar propiedades de recursos compartidos adicionales mediante una lista delimitada por comas.

5. Compruebe que el recurso compartido tenga la configuración deseada mediante el `vserver cifs share show` comando.
6. Agregar una ruta de búsqueda de directorio principal: `vserver cifs home-directory search-path add -vserver vsserver -path path`

`-vserver vsserver` Especifica la SVM habilitada para CIFS en la que se añade la ruta de búsqueda.

`-path path` especifica la ruta absoluta del directorio a la ruta de búsqueda.

7. Compruebe que ha agregado correctamente la ruta de búsqueda mediante `vserver cifs home-directory search-path show` comando.
8. Si el usuario UNIX no existe, cree el usuario UNIX utilizando `vserver services unix-user create` comando.



Debe existir el nombre de usuario UNIX al que se asigna el nombre de usuario de Windows antes de asignar el usuario.

9. Cree una asignación de nombres para el usuario de Windows al usuario UNIX mediante el siguiente comando: `vserver name-mapping create -vserver vsserver_name -direction win-unix`

`-priority integer -pattern windows_user_name -replacement unix_user_name`



Si ya existen asignaciones de nombres que asignan usuarios de Windows a usuarios UNIX, no es necesario realizar el paso de asignación.

El nombre de usuario de Windows está asignado al nombre de usuario UNIX correspondiente. Cuando el usuario de Windows se conecta a su recurso compartido de directorio principal, se conectan a un directorio raíz creado dinámicamente con un nombre de recurso compartido que corresponde a su nombre de usuario de Windows sin tener en cuenta que el nombre de directorio corresponde al nombre de usuario UNIX.

10. Para los usuarios que dispongan de un directorio inicial, cree un directorio correspondiente en el qtree o en el volumen designado para que contengan directorios iniciales.

Por ejemplo, si creó un qtree con la ruta de `/vol/vol1/users` Y el nombre de usuario UNIX asignado del usuario cuyo directorio desea crear es `"unixuser1"`, crearía un directorio con la siguiente ruta:
`/vol/vol1/users/unixuser1`.

Si creó un volumen denominado «home1» montado en `/home1`, cree un directorio con la siguiente ruta de acceso: `/home1/unixuser1`.

11. Compruebe que un usuario puede conectarse correctamente al recurso compartido principal mediante la asignación de una unidad o la conexión mediante la ruta UNC.

Por ejemplo, si el usuario `mydomain\user1` se asigna al usuario de UNIX `unixuser1` y desea conectarse al directorio creado en el paso 10 que se encuentra en SVM `vs1`, `user1` se conectará mediante la ruta UNC `\\vs1\user1`.

Ejemplo

Los comandos del siguiente ejemplo crean una configuración de directorio inicial con los siguientes ajustes:

- El nombre del recurso compartido es `%w`.
- La ruta de acceso relativa al directorio principal es `%u`.
- La ruta de búsqueda que se utiliza para contener los directorios principales, `/home1`, Es un volumen configurado con estilo de seguridad UNIX.
- La configuración se crea en SVM `vs1`.

Puede utilizar este tipo de configuración de directorio inicial cuando los usuarios acceden a sus directorios iniciales desde hosts Windows o hosts Windows y UNIX y el administrador del sistema de archivos utiliza usuarios y grupos basados en UNIX para controlar el acceso al sistema de archivos.

```
cluster::> vsriver cifs share create -vsriver vs1 -share-name %w -path %u
-share-properties oplocks,browsable,changenotify,homedirectory
```

```
cluster::> vsriver cifs share show -vsriver vs1 -share-name %u
```

```

                Vserver: vs1
                Share: %w
CIFS Server NetBIOS Name: VS1
                Path: %u
        Share Properties: oplocks
                        browsable
                        changenotify
                        homedirectory
        Symlink Properties: enable
        File Mode Creation Mask: -
        Directory Mode Creation Mask: -
                Share Comment: -
                Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

```
cluster::> vsriver cifs home-directory search-path add -vsriver vs1 -path
/home1
```

```
cluster::> vsriver cifs home-directory search-path show -vsriver vs1
```

```
Vserver      Position Path
-----
vs1           1      /home1
```

```
cluster::> vsriver name-mapping create -vsriver vs1 -direction win-unix
-position 5 -pattern user1 -replacement unixuser1
```

```
cluster::> vsriver name-mapping show -pattern user1
```

```
Vserver      Direction Position
-----
vs1           win-unix  5      Pattern: user1
                        Replacement: unixuser1
```

Información relacionada

[Creación de una configuración de directorio principal mediante las variables %w y %d.](#)

[Configuraciones adicionales de directorio inicial](#)

[Mostrar información acerca de la ruta de acceso al directorio de inicio de un usuario SMB](#)

Configuraciones adicionales de directorio inicial

Puede crear configuraciones adicionales del directorio principal mediante la %w, %d, y %u variables, que le permiten personalizar la configuración del directorio principal para satisfacer sus necesidades.

Puede crear una serie de configuraciones de directorios iniciales mediante una combinación de variables y cadenas estáticas en los nombres de recursos compartidos y las rutas de búsqueda. En la siguiente tabla se muestran algunos ejemplos que ilustran cómo crear distintas configuraciones de directorio principal:

| Rutas creadas cuando /vol1/user contiene directorios iniciales... | Compartir comando... |
|--|--|
| Para crear una ruta de acceso compartido \\vs1\~win_username esto dirige al usuario a. /vol1/user/win_username | <pre>vserver cifs share create -share-name ~%w -path %w -share-properties oplocks,browsable,changenotify,homedirectory</pre> |
| Para crear una ruta de acceso compartido \\vs1\win_username esto dirige al usuario a. /vol1/user/domain/win_username | <pre>vserver cifs share create -share-name %w -path %d/%w -share-properties oplocks,browsable,changenotify,homedirectory</pre> |
| Para crear una ruta de acceso compartido \\vs1\win_username esto dirige al usuario a. /vol1/user/unix_username | <pre>vserver cifs share create -share-name %w -path %u -share-properties oplocks,browsable,changenotify,homedirectory</pre> |
| Para crear una ruta de acceso compartido \\vs1\unix_username esto dirige al usuario a. /vol1/user/unix_username | <pre>vserver cifs share create -share-name %u -path %u -share-properties oplocks,browsable,changenotify,homedirectory</pre> |

Comandos para gestionar las rutas de búsqueda

Hay comandos ONTAP específicos para gestionar las rutas de búsqueda de las configuraciones de directorios iniciales de SMB. Por ejemplo, hay comandos para agregar, quitar y mostrar información acerca de las rutas de búsqueda. También hay un comando para cambiar el orden de la ruta de búsqueda.

| Si desea... | Se usa este comando... |
|------------------------------|---|
| Agregue una ruta de búsqueda | <pre>vserver cifs home-directory search-path add</pre> |
| Mostrar rutas de búsqueda | <pre>vserver cifs home-directory search-path show</pre> |

| Si desea... | Se usa este comando... |
|--|--|
| Cambie el orden de la ruta de búsqueda | <code>vserver cifs home-directory search-path reorder</code> |
| Quitar una ruta de búsqueda | <code>vserver cifs home-directory search-path remove</code> |

Consulte la página de manual de cada comando para obtener más información.

Muestra información acerca de la ruta de acceso al directorio principal de un usuario de SMB

Puede mostrar la ruta de directorio inicial de un usuario SMB en la máquina virtual de almacenamiento (SVM), que puede utilizarse si tiene varias rutas de directorio raíz CIFS configuradas y desea ver qué ruta contiene el directorio raíz del usuario.

Paso

1. Muestre la ruta del directorio principal mediante el `vserver cifs home-directory show-user` comando.

```
vserver cifs home-directory show-user -vserver vs1 -username user1
```

| Vserver | User | Home Dir Path |
|---------|-------|---------------|
| ----- | ----- | ----- |
| vs1 | user1 | /home/user1 |

Información relacionada

[Gestión de la accesibilidad a los directorios iniciales de los usuarios](#)

Gestionar la accesibilidad a los directorios iniciales de los usuarios

De forma predeterminada, sólo el usuario puede acceder al directorio principal de un usuario. Para los recursos compartidos donde el nombre dinámico del recurso compartido va precedido de una tilde (~), los administradores de Windows o cualquier otro usuario (acceso público) pueden habilitar o deshabilitar el acceso a los directorios principales de los usuarios.

Antes de empezar

Los recursos compartidos de directorio inicial en la máquina virtual de almacenamiento (SVM) deben configurarse con nombres de recursos compartidos dinámicos que van precedidos por una tilde (~). En los siguientes casos se ilustran los requisitos de nomenclatura de los recursos compartidos:

| Nombre del recurso compartido del directorio inicial | Ejemplo de comando para conectarse al recurso compartido |
|--|--|
| ~%d~%w | net use * \\IPAddress\~domain~user/u:credentials |
| ~%w | net use * \\IPAddress\~user/u:credentials |
| ~abc~%w | net use * \\IPAddress\abc~user/u:credentials |

Paso

1. Ejecute la acción adecuada:

| Si desea activar o desactivar el acceso a los directorios de inicio de los usuarios a... | Introduzca lo siguiente... |
|--|--|
| Administradores de Windows | vserver cifs home-directory modify -vserver vserver_name -is-home-dirs -access-for-admin-enabled {true false} El valor predeterminado es true. |
| Cualquier usuario (acceso público) | a. Establezca el nivel de privilegio en Advanced: set -privilege advanced b. Activar o desactivar el acceso: `vserver cifs home-directory modify -vserver vserver_name -is-home-dirs-access-for-public-enabled {true |

El ejemplo siguiente permite el acceso público a los directorios principales de los usuarios:

```
set -privilege advanced
vserver cifs home-directory modify -vserver vs1 -is-home-dirs-access-for-public
-enabled true
set -privilege admin
```

Información relacionada

[Mostrar información acerca de la ruta de acceso al directorio de inicio de un usuario SMB](#)

Configure el acceso del cliente SMB a los enlaces simbólicos de UNIX

Cómo ONTAP le permite proporcionar acceso de clientes SMB a enlaces simbólicos UNIX

Un enlace simbólico es un archivo creado en un entorno UNIX que contiene una referencia a otro archivo o directorio. Si un cliente accede a un enlace simbólico, se redirige al cliente al archivo o directorio de destino al que hace referencia el enlace simbólico. ONTAP soporta enlaces simbólicos relativos y absolutos, incluyendo enlaces de widelinks (enlaces absolutos con destinos fuera del sistema de archivos local).

ONTAP proporciona a los clientes SMB la capacidad de seguir enlaces simbólicos UNIX configurados en la SVM. Esta función es opcional y puede configurarla por recurso compartido mediante la `-symlink` `-properties` opción de `vserver cifs share create` comando, con una de las siguientes opciones de configuración:

- Habilitada con acceso de lectura/escritura
- Habilitado con acceso de solo lectura
- Desactivado mediante la ocultación de enlaces simbólicos de clientes SMB
- Deshabilitado sin acceso a enlaces simbólicos de clientes SMB

Si habilita enlaces simbólicos en un recurso compartido, los enlaces simbólicos relativos funcionan sin más configuración.

Si activa enlaces simbólicos en un recurso compartido, los enlaces simbólicos absolutos no funcionan de inmediato. Primero debe crear una asignación entre la ruta UNIX del enlace simbólico a la ruta SMB de destino. Al crear asignaciones de vínculos simbólicos absolutos, puede especificar si se trata de un enlace local o de un *widelink*; las *widelinks* pueden ser enlaces a sistemas de archivos en otros dispositivos de almacenamiento o vínculos a sistemas de archivos alojados en SVM independientes en el mismo sistema ONTAP. Al crear un *widelink*, debe incluir la información que debe seguir el cliente; es decir, cree un punto de reanálisis para que el cliente detecte el punto de unión del directorio. Si crea un vínculo simbólico absoluto a un archivo o directorio fuera del recurso compartido local pero establece la localidad en local, ONTAP no permite el acceso al destino.



Si un cliente intenta eliminar un enlace simbólico local (absoluto o relativo), sólo se eliminará el enlace simbólico, no el archivo o directorio de destino. Sin embargo, si un cliente intenta eliminar un *widelink*, podría eliminar el archivo de destino real o el directorio al que hace referencia el *widelink*. ONTAP no tiene control sobre esto, ya que el cliente puede abrir de forma explícita el archivo o directorio de destino fuera de la SVM y eliminarlo.

• Puntos de análisis y servicios del sistema de archivos ONTAP

Un *reanálisis point* es un objeto del sistema de archivos NTFS que se puede almacenar opcionalmente en volúmenes junto con un archivo. Los puntos de análisis proporcionan a los clientes SMB la capacidad de recibir servicios del sistema de archivos mejorados o ampliados al trabajar con volúmenes de estilo NTFS. Los puntos de reanálisis constan de etiquetas estándar que identifican el tipo de punto de reanálisis y el contenido del punto de reanálisis que pueden recuperar los clientes SMB para un procesamiento posterior por parte del cliente. De los tipos de objeto disponibles para la funcionalidad ampliada del sistema de archivos, ONTAP implementa la compatibilidad con enlaces simbólicos NTFS y puntos de unión de directorios mediante etiquetas de punto de reanálisis. Los clientes SMB que no pueden comprender el contenido de un punto de análisis simplemente lo ignoran y no proporcionan el servicio de sistema de archivos ampliado que podría habilitar el punto de análisis.

• Puntos de unión de directorios y soporte de ONTAP para enlaces simbólicos

Los puntos de unión de directorios son ubicaciones dentro de una estructura de directorios del sistema de archivos que pueden hacer referencia a ubicaciones alternativas en las que se almacenan los archivos, ya sea en una ruta de acceso diferente (enlaces simbólicos) o en un dispositivo de almacenamiento independiente (*widelinks*). Los servidores SMB de ONTAP exponen los puntos de unión de directorios a los clientes de Windows como puntos de análisis, lo que permite a los clientes con capacidad obtener contenidos de punto de análisis de ONTAP cuando se pasa un punto de unión de directorios. De este modo, pueden navegar y conectarse a diferentes rutas o dispositivos de almacenamiento, como si formaran parte del mismo sistema de archivos.

- **Activación de la compatibilidad con el uso de las opciones de punto de reanálisis**

La `-is-use-junctions-as-reparse-points-enabled` De forma predeterminada, la opción está habilitada en ONTAP 9. No todos los clientes de SMB admiten widelinks, por lo que la opción de activar la información se puede configurar de acuerdo con la versión del protocolo, lo que permite a los administradores acomodar clientes de SMB admitidos y no compatibles. En ONTAP 9.2 y versiones posteriores, debe habilitar la opción `-widelink-as-reparse-point-versions` Para cada protocolo de cliente que accede al recurso compartido mediante widelinks; el valor predeterminado es SMB1. En versiones anteriores, sólo se notificaron enlaces de cableado a los que se accedía mediante SMB1 predeterminado, y los sistemas que utilizaban SMB2 o SMB3 no podían acceder a los enlaces de cableado.

Para obtener más información, consulte la documentación NTFS de Microsoft.

["Documentación de Microsoft: Puntos de análisis"](#)

Límites al configurar enlaces simbólicos UNIX para el acceso a SMB

Debe estar al tanto de determinados límites al configurar los enlaces simbólicos UNIX para el acceso a SMB.

| Límite | Descripción |
|--------|--|
| 45 | <div>Longitud máxima del nombre del servidor CIFS que puede especificar al usar un FQDN para el nombre del servidor CIFS.</div> <div> También puede especificar el nombre del servidor CIFS como nombre NetBIOS, que está limitado a 15 caracteres.</div> |
| 80 | La longitud máxima del nombre del recurso compartido. |
| 256 | Longitud máxima de la ruta UNIX que se puede especificar al crear un enlace simbólico o al modificar la ruta UNIX de un enlace simbólico existente. La ruta UNIX debe empezar con una "/" (slash) and end with a "/". Las barras diagonales iniciales y finales cuentan como parte del límite de 256 caracteres. |
| 256 | Longitud máxima de la ruta CIFS que puede especificar al crear un enlace simbólico o al modificar la ruta CIFS de un enlace simbólico existente. La ruta CIFS debe empezar por «/» (slash) and end with a "/". Las barras diagonales iniciales y finales cuentan como parte del límite de 256 caracteres. |

Información relacionada

Controle los anuncios DFS automáticos en ONTAP con la opción de servidor CIFS

Una opción de servidor CIFS controla cómo se anuncian las funcionalidades DFS a los clientes SMB al conectarse a recursos compartidos. Dado que ONTAP utiliza referencias DFS cuando los clientes acceden a enlaces simbólicos a través de SMB, debe ser consciente del impacto que tiene al deshabilitar o habilitar esta opción.

Una opción de servidor CIFS determina si los servidores CIFS se anuncian automáticamente que son DFS capaz de clientes SMB. De forma predeterminada, esta opción está habilitada y el servidor CIFS siempre anuncia que es DFS capaz de los clientes SMB (incluso cuando se conecta a recursos compartidos donde el acceso a enlaces simbólicos está deshabilitado). Si desea que el servidor CIFS anuncie que es compatible con DFS sólo cuando se conectan a recursos compartidos donde está habilitado el acceso a enlaces simbólicos, puede deshabilitar esta opción.

Debe tener en cuenta lo que ocurre cuando se deshabilita esta opción:

- La configuración de uso compartido de los enlaces simbólicos no cambia.
- Si el parámetro share se establece para permitir el acceso de enlace simbólico (ya sea de lectura y escritura o de sólo lectura), el servidor CIFS DFS anuncia capacidades a clientes que se conectan a ese recurso compartido.

Las conexiones del cliente y el acceso a enlaces simbólicos se mantienen sin interrupción.

- Si el parámetro share se establece para no permitir el acceso de enlace simbólico (ya sea deshabilitando el acceso o si el valor del parámetro share es null), el servidor CIFS no anuncia capacidades DFS a clientes que se conectan a ese recurso compartido.

Como los clientes tienen información en caché que el servidor CIFS es compatible con DFS y ya no anuncia que es, es posible que los clientes conectados a recursos compartidos donde se deshabilita el acceso a enlaces simbólicos no puedan acceder a estos recursos compartidos una vez que se deshabilita la opción de servidor CIFS. Después de deshabilitar la opción, es posible que deba reiniciar los clientes conectados a estos recursos compartidos, borrando de esta forma la información almacenada en caché.

Estos cambios no se aplican a conexiones SMB 1.0.

Configurar la compatibilidad del enlace simbólico de UNIX en los recursos compartidos de SMB

Puede configurar la compatibilidad de vínculos simbólicos de UNIX en recursos compartidos de SMB especificando una configuración de propiedad de recurso compartido de vínculo simbólico al crear recursos compartidos de SMB o en cualquier momento mediante la modificación de recursos compartidos de SMB existentes. La compatibilidad con el enlace simbólico de UNIX está habilitada de forma predeterminada. También puede deshabilitar la compatibilidad con enlaces simbólicos de UNIX en un recurso compartido.

Acerca de esta tarea

Al configurar la compatibilidad de enlaces simbólicos de UNIX para recursos compartidos de SMB, puede elegir una de las siguientes opciones de configuración:

| Ajuste | Descripción |
|--|---|
| <code>enable</code> (EN DESUSO*) | Especifica que los enlaces simbólicos están habilitados para el acceso de lectura y escritura. |
| <code>read_only</code> (EN DESUSO*) | Especifica que los enlaces simbólicos están habilitados para el acceso de sólo lectura. Esta configuración no se aplica a las tintas widelinks. El acceso a Widelink siempre es de lectura y escritura. |
| <code>hide</code> (EN DESUSO*) | Especifica que los clientes SMB no pueden ver enlaces simbólicos. |
| <code>no-strict-security</code> | Especifica que los clientes siguen enlaces simbólicos fuera de los límites de recursos compartidos. |
| <code>symlinks</code> | Especifica que los enlaces simbólicos están habilitados localmente para el acceso de lectura y escritura. Los anuncios DFS no se generan aunque la opción CIFS sea <code>is-advertise-dfs-enabled</code> se establece en <code>true</code> . Esta es la configuración predeterminada. |
| <code>symlinks-and-widelinks</code> | Especifica que tanto los enlaces simbólicos locales como los widelinks para el acceso de lectura y escritura. Los anuncios DFS se generan tanto para symlink local como para widelinks aunque la opción CIFS <code>is-advertise-dfs-enabled</code> se establece en <code>false</code> . |
| <code>disable</code> | Especifica que los enlaces simbólicos y las tintas widelinks están desactivados. Los anuncios DFS no se generan aunque la opción CIFS sea <code>is-advertise-dfs-enabled</code> se establece en <code>true</code> . |
| <code>""</code> (nulo, no establecido) | Deshabilita los enlaces simbólicos en el recurso compartido. |
| <code>-</code> (no configurado) | Deshabilita los enlaces simbólicos en el recurso compartido. |



*Los parámetros *enable*, *ocultar* y *Read-only* están obsoletos y se pueden eliminar en una futura versión de ONTAP.

Pasos

1. Configure o deshabilite el soporte de enlaces simbólicos:

| Si es... | Introduzca... |
|---|---|
| Un nuevo recurso compartido de SMB | <code>`+vserver cifs share create -vserver vserver_name -share-name share_name -path path -symlink -properties {enable</code> |
| hide | read-only |
| "" | - |
| symlinks | symlinks-and-widelinks |
| disable},...]+` | Un recurso compartido de SMB existente |
| <code>`+vserver cifs share modify -vserver vserver_name -share-name share_name -symlink-properties {enable</code> | hide |
| read-only | "" |
| - | symlinks |
| symlinks-and-widelinks | disable},...]+` |

- Compruebe que la configuración de recursos compartidos de SMB es correcta: `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

Ejemplo

El siguiente comando crea un recurso compartido SMB denominado «data1» con la configuración de enlace simbólico de UNIX establecida a. `enable`:

```
cluster1::> vservers cifs share create -vsrvr vs1 -share-name data1 -path
/data1 -symlink-properties enable

cluster1::> vservers cifs share show -vsrvr vs1 -share-name data1
-instance

Vserver: vs1
Share: data1
CIFS Server NetBIOS Name: VS1
Path: /data1
Share Properties: oplocks
browsable
changenotify
Symlink Properties: enable
File Mode Creation Mask: -
Directory Mode Creation Mask: -
Share Comment: -
Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
Volume Name: -
Offline Files: manual
Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
UNIX Group for File Create: -
```

Información relacionada

[Creación de asignaciones de enlace simbólico para los recursos compartidos de SMB](#)

Crear asignaciones de enlace simbólico para los recursos compartidos de SMB

Puede crear asignaciones de enlaces simbólicos UNIX para los recursos compartidos de SMB. Puede crear un vínculo simbólico relativo, que hace referencia al archivo o la carpeta relativa a su carpeta principal, o bien puede crear un vínculo simbólico absoluto, que hace referencia al archivo o la carpeta utilizando una ruta absoluta.

Acerca de esta tarea

Los usuarios de Mac OS X no pueden acceder a Widelinks si utilizan SMB 2.x. Cuando un usuario intenta conectarse a un recurso compartido mediante widelinks desde un cliente Mac OS X, el intento falla. Sin embargo, puede utilizar widelinks con clientes Mac OS X si utiliza SMB 1.

Pasos

1. Para crear asignaciones de enlace simbólicas para los recursos compartidos de SMB: `vservers cifs symlink create -vsrvr virtual_server_name -unix-path path -share-name share_name -cifs-path path [-cifs-server server_name] [-locality {local|free|widelink}] [-home-directory {true|false}]`

`-vsrvr virtual_server_name` Especifica el nombre de la máquina virtual de almacenamiento

(SVM).

`-unix-path path` Especifica la ruta de acceso UNIX. La ruta UNIX debe comenzar con una barra (/) y debe terminar con una barra (/).

`-share-name share_name` Especifica el nombre del recurso compartido SMB que se va a asignar.

`-cifs-path path` Especifica la ruta CIFS. La ruta CIFS debe comenzar con una barra diagonal (/) y debe terminar con una barra (/).

`-cifs-server server_name` Especifica el nombre del servidor CIFS. El nombre del servidor CIFS puede especificarse como un nombre DNS (por ejemplo, mynetwork.cifs.server.com), una dirección IP o un nombre NetBIOS. El nombre NetBIOS se puede determinar mediante el `vserver cifs show` comando. Si no se especifica este parámetro opcional, el valor predeterminado es el nombre NetBIOS del servidor CIFS local.

`-locality local|free|widelink` especifica si se debe crear un vínculo local, un vínculo libre o un vínculo simbólico ancho. Un enlace simbólico local se asigna al recurso compartido local de SMB. Un enlace simbólico gratuito puede asignar en cualquier parte del servidor SMB local. Un amplio enlace simbólico se asigna a cualquier recurso compartido de SMB en la red. Si no se especifica este parámetro opcional, el valor predeterminado es `local`.

`-home-directory true false` especifica si el recurso compartido de destino es un directorio principal. Aunque este parámetro sea opcional, debe configurarse en `true` cuando el recurso compartido de destino está configurado como directorio principal. El valor predeterminado es `false`.

Ejemplo

El siguiente comando crea una asignación de enlaces simbólicos en la SVM llamada vs1. Tiene la ruta UNIX /src/, El nombre del recurso compartido SMB «SODURCE», la ruta CIFS /mycompany/source/, Y la dirección IP 123.123.123.123 del servidor CIFS, y es un widelink.

```
cluster1::> vserver cifs symlink create -vserver vs1 -unix-path /src/
-share-name SOURCE -cifs-path "/mycompany/source/" -cifs-server
123.123.123.123 -locality widelink
```

Información relacionada

[Configurar la compatibilidad de enlaces simbólicos UNIX en recursos compartidos de SMB](#)

Comandos para gestionar asignaciones de enlaces simbólicos

Hay comandos ONTAP específicos para gestionar las asignaciones de enlaces simbólicos.

| Si desea... | Se usa este comando... |
|--|--|
| Cree una asignación de vínculos simbólicos | <code>vserver cifs symlink create</code> |
| Mostrar información acerca de las asignaciones de enlaces simbólicos | <code>vserver cifs symlink show</code> |

| Si desea... | Se usa este comando... |
|---|--|
| Modificar una asignación de vínculos simbólicos | <code>vserver cifs symlink modify</code> |
| Eliminar una asignación de vínculos simbólicos | <code>vserver cifs symlink delete</code> |

Consulte la página de manual de cada comando para obtener más información.

Utilice BranchCache para almacenar en caché contenido compartido SMB en una sucursal

Use BranchCache para almacenar en caché contenido compartido SMB en una sucursal

BranchCache fue desarrollado por Microsoft para permitir el almacenamiento de contenido en la caché de los equipos locales de los clientes que lo soliciten. La implementación de BranchCache por parte de ONTAP puede reducir la utilización de la red de área amplia (WAN) y proporcionar un tiempo de respuesta de acceso mejorado cuando los usuarios de una sucursal acceden al contenido almacenado en máquinas virtuales de almacenamiento (SVM) mediante SMB.

Si configura BranchCache, los clientes de Windows BranchCache en primer lugar recuperan el contenido de la SVM y, a continuación, almacenan en caché el contenido de un equipo dentro de la sucursal. Si otro cliente con BranchCache habilitado en la sucursal solicita el mismo contenido, la SVM primero autentica y autoriza al usuario solicitante. A continuación, la SVM determina si el contenido en caché aún está actualizado y, si lo está, envía los metadatos del cliente sobre el contenido en caché. A continuación, el cliente utiliza los metadatos para recuperar contenido directamente desde la memoria caché basada en la ubicación local.

Información relacionada

[Uso de archivos sin conexión para permitir el almacenamiento en caché de archivos para su uso sin conexión](#)

Requisitos y directrices

Compatibilidad de versiones de BranchCache

Debe tener en cuenta qué versiones de BranchCache son compatibles con ONTAP.

ONTAP es compatible con BranchCache 1 y con BranchCache 2 mejorado:

- Cuando se configura BranchCache en el servidor SMB para la máquina virtual de almacenamiento (SVM), puede habilitar BranchCache 1, BranchCache 2 o todas las versiones.

De forma predeterminada, todas las versiones están habilitadas.

- Si solo habilita BranchCache 2, los equipos cliente Windows de oficina remota deben admitir BranchCache 2.

Solo los clientes SMB 3.0 o una versión posterior admiten BranchCache 2.

Para obtener más información sobre las versiones de BranchCache, consulte la biblioteca de Microsoft TechNet.

Información relacionada

Requisitos de compatibilidad de protocolos de red

Debe tener en cuenta los requisitos del protocolo de red para implementar BranchCache de ONTAP.

Puede implementar la función ONTAP BranchCache en redes IPv4 e IPv6 mediante SMB 2.1 o una versión posterior.

Todos los servidores CIFS y los equipos de oficinas remotas que participan en la implementación de BranchCache deben tener habilitado el protocolo SMB 2.1 o una versión posterior. SMB 2.1 tiene extensiones de protocolo que permiten que un cliente participe en un entorno de BranchCache. Esta es la versión mínima del protocolo SMB que ofrece compatibilidad con BranchCache. SMB 2.1 admite la versión de BranchCache, versión 1.

Si desea usar BranchCache versión 2, SMB 3.0 es la versión mínima admitida. Todos los servidores CIFS y los equipos de oficinas remotas que participan en una implementación de BranchCache 2 deben tener habilitado SMB 3.0 o una versión posterior.

Si tiene oficinas remotas en las que algunos clientes solo admiten SMB 2.1 y algunos de los clientes admiten SMB 3.0, puede implementar una configuración de BranchCache en el servidor CIFS que proporcione compatibilidad con el almacenamiento en caché tanto en BranchCache 1 como en BranchCache 2.



Aunque la función Microsoft BranchCache admite el uso de los protocolos HTTP/HTTPS y SMB como protocolos de acceso a archivos, ONTAP BranchCache solo admite el uso de SMB.

Requisitos de la versión para hosts de ONTAP y Windows

Los hosts de ONTAP y de oficina remota deben cumplir determinados requisitos de versión para poder configurar BranchCache.

Antes de configurar BranchCache, debe asegurarse de que la versión de ONTAP en el clúster y los clientes de la sucursal participantes sean compatibles con SMB 2.1 o una versión posterior y con la función de BranchCache. Si configura el modo de caché alojada, también debe asegurarse de que utiliza un host compatible para el servidor de caché.

BranchCache 1 es compatible con las siguientes versiones de ONTAP y hosts de Windows:

- Servidor de contenido: Máquina virtual de almacenamiento (SVM) con ONTAP
- Servidor de caché: Windows Server 2008 R2 o Windows Server 2012 o posterior
- Igual o cliente: Windows 7 Enterprise, Windows 7 Ultimate, Windows 8, Windows Server 2008 R2 o Windows Server 2012 o posterior

BranchCache 2 es compatible con las siguientes versiones de ONTAP y hosts de Windows:

- Servidor de contenido: SVM con ONTAP
- Servidor de caché: Windows Server 2012 o posterior
- Igual o cliente: Windows 8 o Windows Server 2012 o posterior

Razones por las que ONTAP invalida los hash de BranchCache

Comprender los motivos por los que ONTAP invalida los hash puede ser útil a la hora de planificar la configuración de BranchCache. Puede ayudarle a decidir el modo operativo que debe configurar y a elegir en qué recursos compartidos desea habilitar BranchCache.

ONTAP debe gestionar los hash de BranchCache para garantizar que sean válidos. Si un hash no es válido, ONTAP invalida el hash y calcula un nuevo hash la próxima vez que se solicite el contenido, suponiendo que BranchCache siga estando habilitado.

ONTAP invalida los hash por los siguientes motivos:

- Se modifica la clave de servidor.

Si se modifica la clave del servidor, ONTAP invalida todos los hash del almacén hash.

- Un hash se vacía de la caché porque se alcanzó el tamaño máximo del almacén hash de BranchCache.

Se trata de un parámetro ajustable y puede modificarse para satisfacer sus requisitos empresariales.

- Un archivo se modifica mediante un acceso SMB o NFS.
- Se restaura un archivo para el que hay valores hash calculados mediante el `snap restore` comando.
- Un volumen que contiene recursos compartidos SMB con la función BranchCache habilitada se restaura mediante el `snap restore` comando.

Directrices para elegir la ubicación del almacén hash

Al configurar BranchCache, elija dónde almacenar los hash y qué tamaño debe tener el almacén hash. Las directrices a la hora de elegir la ubicación y el tamaño del almacén hash pueden ayudarle a planificar la configuración de BranchCache en una SVM habilitada para CIFS.

- Debe localizar el almacén hash en un volumen en el que se permitan las actualizaciones de atime.

El tiempo de acceso de un archivo hash se utiliza para mantener los archivos a los que se accede con más frecuencia en el almacén hash. Si las actualizaciones de atime están deshabilitadas, se utiliza la hora de creación con este fin. Es preferible utilizar atime para realizar un seguimiento de los archivos utilizados con frecuencia.

- No puede almacenar hash en sistemas de archivos de solo lectura como los destinos de SnapMirror y los volúmenes SnapLock.
- Si se alcanza el tamaño máximo del almacén hash, los hash más antiguos se vacían para crear espacio para los hash nuevos.

Es posible aumentar el tamaño máximo del almacén hash para reducir la cantidad de hash que se vacía de la caché.

- Si el volumen en el que almacena hash no está disponible o lleno, o si hay un problema con la comunicación dentro del clúster donde el servicio BranchCache no puede recuperar información hash, los servicios de BranchCache no estarán disponibles.

El volumen puede no estar disponible porque está sin conexión o porque el administrador de almacenamiento especificó una nueva ubicación para el almacén de hash.

Esto no provoca problemas con el acceso a archivos. Si se ve afectado el acceso al almacén hash, ONTAP devolverá un error definido por Microsoft al cliente, que hace que el cliente solicite el archivo con la solicitud de lectura SMB normal.

Información relacionada

[Configure BranchCache en el servidor SMB](#)

[Modifique la configuración de BranchCache](#)

Recomendaciones de BranchCache

Antes de configurar BranchCache, hay ciertas recomendaciones que debe tener en cuenta a la hora de decidir qué recursos compartidos de SMB desea habilitar el almacenamiento en caché de BranchCache.

Debe tener en cuenta las siguientes recomendaciones a la hora de decidir qué modo operativo usar y en qué recursos compartidos de SMB para habilitar BranchCache:

- Las ventajas de BranchCache se reducen cuando los datos que se van a almacenar en caché de forma remota cambian con frecuencia.
- Los servicios de BranchCache son beneficiosos para los recursos compartidos que contienen contenido de archivos que se vuelve a utilizar por varios clientes de oficina remota o por contenido de archivo al que un único usuario remoto accede en repetidas ocasiones.
- Considere la posibilidad de habilitar el almacenamiento en caché para contenido de solo lectura, como los datos en copias Snapshot y los destinos de SnapMirror.

Configure BranchCache

Configure la información general de BranchCache

Puede configurar BranchCache en el servidor SMB con los comandos de la ONTAP. Para implementar BranchCache, también debe configurar los clientes y, opcionalmente, los servidores de caché alojados en las sucursales en las que desea almacenar en caché el contenido.

Si configura BranchCache para habilitar el almacenamiento en caché de recurso compartido por recurso, debe habilitar BranchCache en los recursos compartidos SMB para los que desea proporcionar servicios de almacenamiento en caché de BranchCache.

Requisitos para configurar BranchCache

Después de cumplir algunos requisitos previos, puede configurar BranchCache.

Debe cumplir los siguientes requisitos antes de configurar BranchCache en el servidor CIFS para la SVM:

- ONTAP debe instalarse en todos los nodos del clúster.
- CIFS debe tener una licencia y se debe configurar un servidor SMB. La licencia SMB se incluye con "ONTAP One". Si no tiene ONTAP One y la licencia no está instalada, póngase en contacto con su

representante de ventas.

- Se debe configurar la conectividad de red IPv4 o IPv6.
- Para BranchCache 1, se debe habilitar SMB 2.1 o una versión posterior.
- Para BranchCache 2, se debe habilitar SMB 3.0 y los clientes de Windows remotos deben admitir BranchCache 2.

Configure BranchCache en el servidor SMB

Puede configurar BranchCache para proporcionar servicios de BranchCache por recurso compartido. Como alternativa, puede configurar BranchCache para habilitar automáticamente el almacenamiento en caché en todos los recursos compartidos de SMB.

Acerca de esta tarea

Puede configurar BranchCache en las SVM.

- Puede crear una configuración de BranchCache para todos los recursos compartidos si desea ofrecer servicios de almacenamiento en caché para todo el contenido en todos los recursos compartidos SMB en el servidor CIFS.
- Puede crear una configuración de BranchCache por recurso compartido si desea ofrecer servicios de almacenamiento en caché para el contenido de ciertos recursos compartidos SMB en el servidor CIFS.

Debe especificar los siguientes parámetros al configurar BranchCache:

| Parámetros necesarios | Descripción |
|---------------------------|--|
| <i>SVM name</i> | BranchCache se configura por SVM. Debe especificar en qué SVM con la función CIFS habilitada desea configurar el servicio BranchCache. |
| <i>Path to hash store</i> | <p>Los hash de BranchCache se almacenan en archivos normales del volumen de SVM. Debe especificar la ruta a un directorio existente en el que desea que ONTAP almacene los datos de hash. la ruta hash de BranchCache debe ser de lectura y escritura. No se admiten rutas de solo lectura, como los directorios de Snapshot. Es posible almacenar datos de hash en un volumen que contiene otros datos o se puede crear un volumen independiente para almacenar datos hash.</p> <p>Si la SVM es un origen de recuperación ante desastres de SVM, la ruta de hash no puede estar en el volumen raíz. Esto se debe a que el volumen raíz no se replica en el destino de recuperación ante desastres.</p> <p>La ruta de hash puede contener espacios en blanco y cualquier carácter válido de nombre de archivo.</p> |

Opcionalmente, puede especificar los siguientes parámetros:

| Parámetros opcionales | Descripción |
|---------------------------------------|--|
| <i>Versiones compatibles</i> | ONTAP admite BranchCache 1 y 2. Puede habilitar la versión 1, la versión 2 o ambas versiones. El valor predeterminado es habilitar ambas versiones. |
| <i>Tamaño máximo del almacén hash</i> | Puede especificar el tamaño que se usará para el almacén de datos hash. Si los datos de hash superan este valor, ONTAP eliminará los hash más antiguos para hacer sitio a los más recientes. El tamaño predeterminado del almacén hash es 1 GB. BranchCache funciona de manera más eficiente si no se descartan los hash de una forma excesivamente agresiva. Si determina que los hash se descartan con frecuencia porque el almacén hash está lleno, puede aumentar el tamaño del almacén hash modificando la configuración de BranchCache. |
| <i>Clave de servidor</i> | Puede especificar una clave de servidor que el servicio de BranchCache utilice para evitar que los clientes suplanten el servidor de BranchCache. Si no se especifica una clave de servidor, se genera de forma aleatoria al crear la configuración de BranchCache. Puede establecer la clave de servidor como un valor específico, de modo que, si hay varios servidores que proporcionan datos de BranchCache para los mismos archivos, los clientes puedan usar hash de cualquier servidor que utilice la misma clave de servidor. Si la clave de servidor contiene espacios, debe escribirla entre comillas. |
| <i>Modo de funcionamiento</i> | El valor predeterminado es habilitar BranchCache por recurso compartido. <ul style="list-style-type: none"> • Para crear una configuración de BranchCache donde se habilita BranchCache por recurso compartido, no se puede especificar este parámetro opcional o bien se puede especificar <code>per-share</code>. • Para habilitar automáticamente BranchCache en todos los recursos compartidos, debe configurar el modo operativo en <code>all-shares</code>. |

Pasos

1. Habilite SMB 2.1 y 3.0 según sea necesario:
 - a. Configure el nivel de privilegio en Advanced: `set -privilege advanced`
 - b. Compruebe la configuración de SVM SMB configurada para determinar si todas las versiones necesarias de SMB están habilitadas: `vserver cifs options show -vserver vserver_name`
 - c. Si es necesario, habilite SMB 2.1: `vserver cifs options modify -vserver vserver_name -smb2-enabled true`

El comando habilita SMB 2.0 y SMB 2.1.

d. Si es necesario, habilite SMB 3.0: `vserver cifs options modify -vserver vserver_name -smb3-enabled true`

e. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

2. Configurar BranchCache: `vserver cifs branchcache create -vserver vserver_name -hash -store-path path [-hash-store-max-size {integer[KB|MB|GB|TB|PB]}] [-versions {v1-enable|v2-enable|enable-all}] [-server-key text] -operating-mode {per-share|all-shares}`

La ruta de almacenamiento hash especificada debe existir y debe residir en un volumen gestionado por la SVM. La ruta también debe ubicarse en un volumen de lectura y escritura. El comando falla si la ruta es de solo lectura o no existe.

Si desea usar la misma clave de servidor para configuraciones de BranchCache adicionales, registre el valor introducido para la clave de servidor. La clave de servidor no aparece cuando se muestra información sobre la configuración de BranchCache.

3. Compruebe que la configuración de BranchCache sea correcta: `vserver cifs branchcache show -vserver vserver_name`

Ejemplos

Los siguientes comandos verifican que tanto SMB 2.1 como 3.0 están habilitadas y configuran BranchCache para permitir automáticamente el almacenamiento en caché de todos los recursos compartidos de SMB en SVM vs1:

```

cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
-----
vs1      true      true

cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key" -operating-mode all-shares

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
        Supported BranchCache Versions: enable_all
                                Path to Hash Store: /hash_data
        Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: all_shares

```

Los siguientes comandos verifican que tanto SMB 2.1 como 3.0 están habilitadas, configure BranchCache para permitir el almacenamiento en caché de acuerdo con un recurso compartido en SVM vs1 y verifique la configuración de BranchCache:

```

cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vsserver cifs options show -vsserver vs1 -fields smb2-
enabled,smb3-enabled
vsserver smb2-enabled smb3-enabled
-----
vs1      true      true

cluster1::*> set -privilege admin

cluster1::> vsserver cifs branchcache create -vsserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key"

cluster1::> vsserver cifs branchcache show -vsserver vs1

                                Vserver: vs1
        Supported BranchCache Versions: enable_all
                                Path to Hash Store: /hash_data
        Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share

```

Información relacionada

[Requisitos y directrices: Compatibilidad con versiones de BranchCache](#)

[Dónde encontrar información sobre la configuración de BranchCache en la oficina remota](#)

[Cree un recurso compartido de SMB habilitado con BranchCache](#)

[Habilite BranchCache en un recurso compartido de SMB existente](#)

[Modifique la configuración de BranchCache](#)

[Deshabilite BranchCache en la información general de recursos compartidos SMB](#)

[Elimine la configuración de BranchCache en las SVM](#)

Dónde encontrar información sobre la configuración de BranchCache en la oficina remota

Después de configurar BranchCache en el servidor SMB, debe instalar y configurar BranchCache en los equipos cliente y, opcionalmente, en los servidores de almacenamiento en caché de la oficina remota. Microsoft proporciona instrucciones para la configuración de BranchCache en la oficina remota.

Las instrucciones para configurar clientes de sucursal y, de manera opcional, los servidores de almacenamiento en caché que usen BranchCache se encuentran en el sitio web de Microsoft BranchCache.

["Microsoft BranchCache Docs: Novedades"](#)

Configure los recursos compartidos SMB habilitados para BranchCache

Configure la información general de recursos compartidos SMB habilitados para BranchCache

Una vez que configura BranchCache en el servidor SMB y en la sucursal, puede habilitar BranchCache en recursos compartidos SMB que contienen contenido que desea permitir que los clientes de las sucursales se almacenen en caché.

El almacenamiento en caché de BranchCache puede habilitarse en todos los recursos compartidos de SMB en el servidor SMB o de recurso compartido por recurso.

- Si habilita BranchCache por recurso compartido, puede habilitar BranchCache a medida que crea el recurso compartido o modifica los recursos compartidos existentes.

Si habilita el almacenamiento en caché en un recurso compartido de SMB existente, ONTAP comienza a enviar hashes de computación y metadatos a clientes que soliciten contenido tan pronto como habilite BranchCache en ese recurso compartido.

- Todos los clientes que tengan una conexión SMB existente a un recurso compartido no obtienen compatibilidad con BranchCache si, a continuación, se habilita BranchCache en ese recurso compartido.

ONTAP anuncia el soporte de BranchCache para un recurso compartido en el momento de la configuración de la sesión del bloque de mensajes del servidor. Los clientes que ya han establecido sesiones cuando se habilita BranchCache deben desconectar y volver a conectarse para usar el contenido en caché para este recurso compartido.



Si BranchCache en un recurso compartido de SMB se encuentra deshabilitado posteriormente, ONTAP deja de enviar metadatos al cliente solicitante. Un cliente que necesita datos lo recupera directamente del servidor de contenido (servidor SMB).

Cree un recurso compartido de SMB habilitado con BranchCache

Puede habilitar BranchCache en un recurso compartido de SMB al crear el recurso compartido mediante la configuración del `branchcache` compartir propiedad.

Acerca de esta tarea

- Si se habilita BranchCache en el recurso compartido de SMB, el recurso compartido debe tener la configuración de los archivos sin conexión establecida en el almacenamiento manual en caché.

Esta es la configuración predeterminada cuando se crea un recurso compartido.

- También puede especificar parámetros de recurso compartido opcionales al crear el recurso compartido con BranchCache habilitado.
- Puede ajustar la `branchcache` Propiedad en un recurso compartido incluso si BranchCache no está configurado y habilitado en la máquina virtual de almacenamiento (SVM).

Sin embargo, si desea que el recurso compartido ofrezca contenido en caché, debe configurar y habilitar

BranchCache en la SVM.

- Puesto que no hay propiedades de recurso compartido predeterminadas aplicadas al recurso compartido cuando se utiliza `-share-properties` parámetro, debe especificar todas las demás propiedades de recursos compartidos que desea aplicar al recurso compartido además de `branchcache` compartir propiedad mediante una lista delimitada por comas.
- Para obtener más información, consulte la página de manual de `vserver cifs share create` comando.

Paso

1. Cree un recurso compartido SMB habilitado con BranchCache:
`vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties branchcache[,...]`
2. Compruebe que la propiedad share de BranchCache se establece en el recurso compartido de SMB mediante el `vserver cifs share show` comando.

Ejemplo

El siguiente comando crea un recurso compartido SMB habilitado con BranchCache denominado «data» con una ruta de `/data` En SVM vs1. De forma predeterminada, la opción Archivos sin conexión está establecida en manual:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data -path
/data -share-properties branchcache,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name data
      Vserver: vs1
      Share: data
CIFS Server NetBIOS Name: VS1
      Path: /data
      Share Properties: branchcache
                      oplocks
                      browsable
                      changenotify
      Symlink Properties: enable
      File Mode Creation Mask: -
      Directory Mode Creation Mask: -
      Share Comment: -
      Share ACL: Everyone / Full Control
      File Attribute Cache Lifetime: -
      Volume Name: data
      Offline Files: manual
      Vscan File-Operations Profile: standard
```

Información relacionada

[Deshabilitar BranchCache en un único recurso compartido de SMB](#)

Habilite BranchCache en un recurso compartido de SMB existente

Puede habilitar BranchCache en un recurso compartido de SMB existente agregando el `branchcache` compartir propiedad a la lista existente de propiedades de recursos compartidos.

Acerca de esta tarea

- Si se habilita BranchCache en el recurso compartido de SMB, el recurso compartido debe tener la configuración de los archivos sin conexión establecida en el almacenamiento manual en caché.

Si la opción de archivos sin conexión del recurso compartido existente no está establecida en almacenamiento en caché manual, debe configurarlo modificando el recurso compartido.

- Puede ajustar la `branchcache` Propiedad en un recurso compartido incluso si BranchCache no está configurado y habilitado en la máquina virtual de almacenamiento (SVM).

Sin embargo, si desea que el recurso compartido ofrezca contenido en caché, debe configurar y habilitar BranchCache en la SVM.

- Al agregar el `branchcache` se conserva la propiedad `share` (compartir) al recurso compartido, la configuración de recursos compartidos existente y las propiedades de recursos compartidos.

La propiedad `share` de BranchCache se agrega a la lista existente de propiedades compartidas. Para obtener más información acerca del uso de `vserver cifs share properties add` consulte las páginas de manual.

Pasos

1. Si es necesario, configure el parámetro de recursos compartidos de archivos sin conexión para el almacenamiento en caché manual:
 - a. Determine cuál es la configuración del recurso compartido de archivos sin conexión mediante `vserver cifs share show` comando.
 - b. Si la configuración del recurso compartido de archivos sin conexión no está establecida en manual, cámbiela al valor necesario: `vserver cifs share modify -vserver vserver_name -share -name share_name -offline-files manual`
2. Habilite BranchCache en un recurso compartido de SMB existente: `vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties branchcache`
3. Compruebe que la propiedad `share` de BranchCache se haya establecido en el recurso compartido de SMB: `vserver cifs share show -vserver vserver_name -share-name share_name`

Ejemplo

El siguiente comando habilita BranchCache en un recurso compartido SMB existente llamado «data2» con una ruta de `/data2` En SVM vs1:

```
cluster1::> vservice cifs share show -vservice vs1 -share-name data2
```

```

    Vservice: vs1
    Share: data2
    CIFS Server NetBIOS Name: VS1
    Path: /data2
    Share Properties: oplocks
                     browsable
                     changenotify
                     showsnapshot
    Symlink Properties: -
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
    Share Comment: -
    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
    Volume Name: -
    Offline Files: manual
Vscan File-Operations Profile: standard
```

```
cluster1::> vservice cifs share properties add -vservice vs1 -share-name
data2 -share-properties branchcache
```

```
cluster1::> vservice cifs share show -vservice vs1 -share-name data2
```

```

    Vservice: vs1
    Share: data2
    CIFS Server NetBIOS Name: VS1
    Path: /data2
    Share Properties: oplocks
                     browsable
                     showsnapshot
                     changenotify
                     branchcache
    Symlink Properties: -
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
    Share Comment: -
    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
    Volume Name: -
    Offline Files: manual
Vscan File-Operations Profile: standard
```

Información relacionada

Gestione y supervise la configuración de BranchCache

Modifique las configuraciones de BranchCache

Puede modificar la configuración del servicio BranchCache en las SVM, lo que incluye el cambio de la ruta de directorio del almacén hash, el tamaño máximo del directorio del almacén hash, el modo operativo y las versiones de BranchCache que son compatibles. También puede aumentar el tamaño del volumen que contiene el almacén hash.

Pasos

1. Ejecute la acción adecuada:

| Si desea... | Introduzca lo siguiente... |
|--|--|
| Modifique el tamaño del directorio del almacén hash | <code>`vserver cifs branchcache modify -vserver vserver_name -hash-store-max-size {integer[KB</code> |
| MB | GB |
| TB | PB]}` |
| Aumente el tamaño del volumen que contiene el almacén hash | <code>`volume size -vserver vserver_name -volume volume_name -new-size new_size[k</code> |
| m | g |
| tj` Si el volumen que contiene el almacén hash se llena, puede aumentar el tamaño del volumen. Puede especificar el nuevo tamaño del volumen como número, seguido de una designación de unidad. Más información acerca de " Gestión de volúmenes de FlexVol " | Modifique la ruta del directorio del almacén hash |

| Si desea... | Introduzca lo siguiente... |
|---|--|
| <code>`vserver cifs branchcache modify -vserver vserver_name -hash-store-path path -flush-hashes {true</code> | <p><code>false}`</code> Si la SVM es un origen de recuperación ante desastres de SVM, la ruta de hash no puede estar en el volumen raíz. Esto se debe a que el volumen raíz no se replica en el destino de recuperación ante desastres.</p> <p>La ruta de hash de BranchCache puede contener espacios en blanco y cualquier carácter válido de nombre de archivo.</p> <p>Si modifica la ruta de hash, <code>-flush-hashes</code> Es un parámetro obligatorio que especifica si desea que ONTAP vacíe los hash de la ubicación del almacén hash original. Puede definir los siguientes valores para <code>-flush-hashes</code> parámetro:</p> <p>Si especifica <code>true</code>, ONTAP elimina los hash de la ubicación original y crea nuevos hash en la nueva ubicación a medida que los clientes habilitados para BranchCache crean nuevas solicitudes.</p> <p>Si especifica <code>false</code>, los hashes no se ruboran.</p> <p>+</p> <p>En este caso, puede optar por reutilizar los hash existentes más adelante cambiando la ruta del almacén hash de vuelta a la ubicación original.</p> |
| Cambie el modo de funcionamiento | <code>`vserver cifs branchcache modify -vserver vserver_name -operating-mode {per-share</code> |
| all-shares | <p><code>disable}`</code></p> <p>Debe tener en cuenta lo siguiente al modificar el modo de funcionamiento:</p> <p>ONTAP anuncia el soporte de BranchCache para un recurso compartido cuando se configura la sesión SMB.</p> <p>Los clientes que ya han establecido sesiones cuando se habilita BranchCache deben desconectar y volver a conectarse para usar el contenido en caché para este recurso compartido.</p> |
| Cambie la compatibilidad de la versión de BranchCache | <code>`vserver cifs branchcache modify -vserver vserver_name -versions {v1-enable</code> |
| v2-enable | <code>enable-all}`</code> |

2. Compruebe los cambios de configuración mediante el `vserver cifs branchcache show` comando.

Muestra información acerca de las configuraciones de BranchCache

Puede mostrar información sobre las configuraciones de BranchCache en máquinas virtuales de almacenamiento (SVM), que se pueden utilizar al verificar una configuración o al determinar la configuración actual antes de modificar una configuración.

Paso

1. Ejecute una de las siguientes acciones:

| Si desea mostrar... | Introduzca este comando... |
|--|---|
| Información resumida sobre las configuraciones de BranchCache en todas las SVM | <code>vserver cifs branchcache show</code> |
| Información detallada sobre la configuración de una SVM específica | <code>vserver cifs branchcache show -vserver <i>vserver_name</i></code> |

Ejemplo

En el siguiente ejemplo, se muestra información sobre la configuración de BranchCache en la SVM vs1:

```
cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
        Supported BranchCache Versions: enable_all
                                Path to Hash Store: /hash_data
        Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Cambie la clave de servidor de BranchCache

Puede cambiar la clave de servidor de BranchCache mediante la modificación de la configuración de BranchCache en la máquina virtual de almacenamiento (SVM) y la especificación de una clave de servidor diferente.

Acerca de esta tarea

Puede establecer la clave de servidor como un valor específico, de modo que, si hay varios servidores que proporcionan datos de BranchCache para los mismos archivos, los clientes puedan usar hash de cualquier servidor que utilice la misma clave de servidor.

Cuando cambia la clave de servidor, también debe vaciar la caché hash. Después de vaciar los hash, ONTAP crea nuevos hash a medida que los clientes habilitados para BranchCache crean nuevas solicitudes.

Pasos

1. Cambie la clave de servidor con el siguiente comando: `vserver cifs branchcache modify -vserver vserver_name -server-key text -flush-hashes true`

Al configurar una clave de servidor nueva, también debe especificar `-flush-hashes` y establezca el valor en `true`.

2. Compruebe que la configuración de BranchCache sea correcta mediante el `vserver cifs branchcache show` comando.

Ejemplo

En el ejemplo siguiente se establece una nueva clave de servidor que contiene espacios y vacía la caché hash en la SVM vs1:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -server-key "new
vserver secret" -flush-hashes true

cluster1::> vserver cifs branchcache show -vserver vs1

                Vserver: vs1
Supported BranchCache Versions: enable_all
                Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
CIFS BranchCache Operating Modes: per_share
```

Información relacionada

[Razones por las que ONTAP invalida los hash de BranchCache](#)

Los hash de BranchCache previos a la computación en las rutas especificadas

Puede configurar el servicio BranchCache para que preajuste los valores hash de computación para un único archivo, para un directorio o para todos los archivos de una estructura de directorio. Esto puede resultar útil si desea calcular hash en datos de un recurso compartido habilitado con BranchCache durante las horas fuera de servicio y no en las horas punta.

Acerca de esta tarea

Si desea recoger una muestra de datos antes de mostrar las estadísticas de hash, debe usar la `statistics start` y opcional `statistics stop` comandos.

- Debe especificar la máquina virtual de almacenamiento (SVM) y la ruta en la que desea contar con los hash de tecnología previa.
- También debe especificar si desea calcular los valores hash de forma recursiva.
- Si desea calcular los hash de forma recursiva, el servicio BranchCache atraviesa todo el árbol de directorios bajo la ruta de acceso especificada y calcula los hash de cada objeto elegible.

Pasos

1. Hash de precomputación como desee:

| Si desea contar con hash de tecnología previa... | Introduzca el comando... |
|---|---|
| Un único archivo o directorio | <code>vserver cifs branchcache hash-create -vserver vserver_name -path path -recurse false</code> |
| Recursivamente en todos los archivos de una estructura de directorios | <code>vserver cifs branchcache hash-create -vserver vserver_name -path absolute_path -recurse true</code> |

2. Compruebe que los valores hash se están calculando utilizando `statistics` comando:

- a. Mostrar estadísticas de `hashd` Objeto de la instancia de SVM deseada: `statistics show
-object hashd -instance vserver_name`
- b. Compruebe que el número de hash creado aumenta repitiendo el comando.

Ejemplos

En el ejemplo siguiente se crean hash en la ruta de acceso `/data` Y en todos los archivos y subdirectorios contenidos en SVM vs1:


```
cluster1::> vserver cifs branchcache hash-create -vserver vs1 -path /data
-recurse true
```

```
cluster1::> statistics show -object hashd -instance vs1
```

Object: hashd

Instance: vs1

Start-time: 9/6/2012 19:09:54

End-time: 9/6/2012 19:11:15

Cluster: cluster1

| Counter | Value |
|---------------------------------|--------------------------------------|
| branchcache_hash_created | 85 |
| branchcache_hash_files_replaced | 0 |
| branchcache_hash_rejected | 0 |
| branchcache_hash_store_bytes | 0 |
| branchcache_hash_store_size | 0 |
| instance_name | vs1 |
| node_name | node1 |
| node_uuid | 11111111-1111-1111-1111-111111111111 |
| process_name | - |

```
cluster1::> statistics show -object hashd -instance vs1
```

Object: hashd

Instance: vs1

Start-time: 9/6/2012 19:09:54

End-time: 9/6/2012 19:11:15

Cluster: cluster1

| Counter | Value |
|---------------------------------|--------------------------------------|
| branchcache_hash_created | 92 |
| branchcache_hash_files_replaced | 0 |
| branchcache_hash_rejected | 0 |
| branchcache_hash_store_bytes | 0 |
| branchcache_hash_store_size | 0 |
| instance_name | vs1 |
| node_name | node1 |
| node_uuid | 11111111-1111-1111-1111-111111111111 |
| process_name | - |

Información relacionada

["Configuración de supervisión del rendimiento"](#)

Volcar los hash del almacén hash de BranchCache de SVM

Puede vaciar todos los hash almacenados en caché del almacén hash de BranchCache en la máquina virtual de almacenamiento (SVM). Esto puede ser útil si ha cambiado la configuración de BranchCache de la sucursal. Por ejemplo, si recientemente reconfiguró el modo de almacenamiento en caché desde el almacenamiento en caché distribuido al modo de almacenamiento en caché alojado, debería vaciar el almacén hash.

Acerca de esta tarea

Después de vaciar los hash, ONTAP crea nuevos hash a medida que los clientes habilitados para BranchCache crean nuevas solicitudes.

Paso

1. Vacíe los hash del almacén hash de BranchCache: `vserver cifs branchcache hash-flush`
`-vserver vserver_name`

`vserver cifs branchcache hash-flush -vserver vs1`

Muestra las estadísticas de BranchCache

Puede mostrar las estadísticas de BranchCache para, entre otras cosas, identificar el nivel de rendimiento del almacenamiento en caché, determinar si su configuración proporciona contenido en caché a los clientes y determinar si los archivos hash se eliminaron para dar cabida a los datos hash más recientes.

Acerca de esta tarea

La `hashd` El objeto de estadística contiene contadores que proporcionan información estadística sobre los hash de BranchCache. La `cifs` El objeto de estadística contiene contadores que proporcionan información estadística sobre la actividad relacionada con BranchCache. Puede recopilar y mostrar información acerca de estos objetos en el nivel de privilegio avanzado.

Pasos

1. Configure el nivel de privilegio en Advanced: `set -privilege advanced`

```
cluster1::> set -privilege advanced
```

```
Warning: These advanced commands are potentially dangerous; use them  
only when directed to do so by support personnel.  
Do you want to continue? {y|n}: y
```

2. Muestre los contadores relacionados con BranchCache mediante el `statistics catalog counter show` comando.

Para obtener más información acerca de los contadores de estadísticas, consulte la página man de este comando.

```
cluster1::*> statistics catalog counter show -object hashd
```

Object: hashd

| Counter | Description |
|---------------------------------|--|
| ----- | |
| ----- | |
| branchcache_hash_created | Number of times a request to generate BranchCache hash for a file succeeded. |
| branchcache_hash_files_replaced | Number of times a BranchCache hash file was deleted to make room for more recent hash data. This happens if the hash store size is exceeded. |
| branchcache_hash_rejected | Number of times a request to generate BranchCache hash data failed. |
| branchcache_hash_store_bytes | Total number of bytes used to store hash data. |
| branchcache_hash_store_size | Total space used to store BranchCache hash data for the Vserver. |
| instance_name | Instance Name |
| instance_uuid | Instance UUID |
| node_name | System node name |
| node_uuid | System node id |

9 entries were displayed.

cluster1::*> statistics catalog counter show -object cifs

Object: cifs

| Counter | Description |
|-----------------------------|--|
| ----- | |
| ----- | |
| active_searches | Number of active searches over SMB and SMB2 |
| auth_reject_too_many | Authentication refused after too many requests were made in rapid succession |
| avg_directory_depth | Average number of directories crossed by SMB and SMB2 path-based commands |
| avg_junction_depth | Average number of junctions crossed by SMB and SMB2 path-based commands |
| branchcache_hash_fetch_fail | Total number of times a request to fetch |

```

hash
data failed. These are failures when
attempting to read existing hash data.
It
does not include attempts to fetch hash
data
that has not yet been generated.
branchcache_hash_fetch_ok Total number of times a request to fetch
hash
data succeeded.
branchcache_hash_sent_bytes Total number of bytes sent to clients
requesting hashes.
branchcache_missing_hash_bytes
Total number of bytes of data that had
to be
read by the client because the hash for
that
content was not available on the server.
....Output truncated....

```

3. Recoja estadísticas relacionadas con BranchCache mediante el `statistics start` y `statistics stop` comandos.

```

cluster1::*> statistics start -object cifs -vserver vs1 -sample-id 11
Statistics collection is being started for Sample-id: 11

cluster1::*> statistics stop -sample-id 11
Statistics collection is being stopped for Sample-id: 11

```

4. Muestre las estadísticas de BranchCache recogidas mediante la `statistics show` comando.

```
cluster1::*> statistics show -object cifs -counter  
branchcache_hash_sent_bytes -sample-id 11
```

```
Object: cifs  
Instance: vs1  
Start-time: 12/26/2012 19:50:24  
End-time: 12/26/2012 19:51:01  
Cluster: cluster1
```

| Counter | Value |
|-----------------------------|-------|
| branchcache_hash_sent_bytes | 0 |
| branchcache_hash_sent_bytes | 0 |
| branchcache_hash_sent_bytes | 0 |
| branchcache_hash_sent_bytes | 0 |

```
cluster1::*> statistics show -object cifs -counter  
branchcache_missing_hash_bytes -sample-id 11
```

```
Object: cifs  
Instance: vs1  
Start-time: 12/26/2012 19:50:24  
End-time: 12/26/2012 19:51:01  
Cluster: cluster1
```

| Counter | Value |
|--------------------------------|-------|
| branchcache_missing_hash_bytes | 0 |
| branchcache_missing_hash_bytes | 0 |
| branchcache_missing_hash_bytes | 0 |
| branchcache_missing_hash_bytes | 0 |

5. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

```
cluster1::*> set -privilege admin
```

Información relacionada

[Mostrar estadísticas](#)

["Configuración de supervisión del rendimiento"](#)

Compatibilidad con objetos de política de grupo de BranchCache

BranchCache de ONTAP proporciona compatibilidad con objetos de directiva de grupo

(GPO) de BranchCache, los cuales permiten una gestión centralizada para ciertos parámetros de configuración de BranchCache. Hay dos GPO utilizados para BranchCache, la publicación Hash para el GPO de BranchCache y la compatibilidad con versiones Hash para el GPO de BranchCache.

- **Publicación Hash para BranchCache GPO**

La publicación Hash para BranchCache GPO corresponde a `-operating-mode` parámetro. Cuando se producen actualizaciones de GPO, este valor se aplica a los objetos de máquinas virtuales de almacenamiento (SVM) contenidos en la unidad organizativa (OU) a la que se aplica la directiva de grupo.

- **Compatibilidad con la versión Hash para el GPO de BranchCache**

La compatibilidad con la versión Hash para el GPO de BranchCache corresponde a `-versions` parámetro. Cuando se producen actualizaciones de GPO, este valor se aplica a los objetos SVM incluidos en la unidad organizativa a la que se aplica la directiva de grupo.

Información relacionada

[Aplicación de objetos de directiva de grupo a servidores CIFS](#)

Muestra información sobre los objetos de directiva de grupo de BranchCache

Puede mostrar información acerca de la configuración de objeto de directiva de grupo (GPO) del servidor CIFS para determinar si se definen GPO de BranchCache para el dominio al que pertenece el servidor CIFS y, si es así, ¿cuáles son las configuraciones permitidas? También puede determinar si la configuración de GPO de BranchCache se aplica al servidor CIFS.

Acerca de esta tarea

Aunque se ha definido una configuración de GPO en el dominio al que pertenece el servidor CIFS, no se aplica necesariamente a la unidad organizativa (OU) que contiene la máquina virtual de almacenamiento (SVM) habilitada para CIFS. La configuración de GPO aplicada es el subconjunto de todos los GPO definidos que se aplican a la SVM habilitada para CIFS. La configuración de BranchCache que se aplica a través de los GPO anula la configuración aplicada a través de la CLI.

Pasos

1. Muestre la configuración de GPO de BranchCache definida para el dominio de Active Directory mediante `vserver cifs group-policy show-defined` comando.



Este ejemplo no muestra todos los campos de resultado disponibles para el comando. La salida está truncada.

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1
```

```
Vserver: vs1
```

```
-----
```

```
    GPO Name: Default Domain Policy
```

```
    Level: Domain
```

```
    Status: enabled
```

```
Advanced Audit Settings:
```

```
    Object Access:
```

```
        Central Access Policy Staging: failure
```

```
Registry Settings:
```

```
    Refresh Time Interval: 22
```

```
    Refresh Random Offset: 8
```

```
    Hash Publication Mode for BranchCache: per-share
```

```
    Hash Version Support for BranchCache: version1
```

```
[...]
```

```
    GPO Name: Resultant Set of Policy
```

```
    Status: enabled
```

```
Advanced Audit Settings:
```

```
    Object Access:
```

```
        Central Access Policy Staging: failure
```

```
Registry Settings:
```

```
    Refresh Time Interval: 22
```

```
    Refresh Random Offset: 8
```

```
    Hash Publication for Mode BranchCache: per-share
```

```
    Hash Version Support for BranchCache: version1
```

```
[...]
```

2. Muestre la configuración de GPO de BranchCache que se aplica al servidor CIFS mediante `vserver cifs group-policy show-applied` comando. "



Este ejemplo no muestra todos los campos de resultado disponibles para el comando. La salida está truncada.

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1
```

```
Vserver: vs1
```

```
-----
```

```
    GPO Name: Default Domain Policy
```

```
        Level: Domain
```

```
        Status: enabled
```

```
Advanced Audit Settings:
```

```
    Object Access:
```

```
        Central Access Policy Staging: failure
```

```
Registry Settings:
```

```
    Refresh Time Interval: 22
```

```
    Refresh Random Offset: 8
```

```
    Hash Publication Mode for BranchCache: per-share
```

```
    Hash Version Support for BranchCache: version1
```

```
[...]
```

```
    GPO Name: Resultant Set of Policy
```

```
        Level: RSOP
```

```
Advanced Audit Settings:
```

```
    Object Access:
```

```
        Central Access Policy Staging: failure
```

```
Registry Settings:
```

```
    Refresh Time Interval: 22
```

```
    Refresh Random Offset: 8
```

```
    Hash Publication Mode for BranchCache: per-share
```

```
    Hash Version Support for BranchCache: version1
```

```
[...]
```

Información relacionada

[Habilitar o deshabilitar la compatibilidad de GPO en un servidor CIFS](#)

Deshabilite BranchCache en los recursos compartidos SMB

Deshabilite BranchCache en la información general de recursos compartidos SMB

Si no desea proporcionar servicios de almacenamiento en caché de BranchCache en ciertos recursos compartidos de SMB, pero quizás desee proporcionar servicios de almacenamiento en caché en esos recursos compartidos más tarde, puede deshabilitar BranchCache en función de su recurso compartido. Si tiene BranchCache configurado para ofrecer almacenamiento en caché en todos los recursos compartidos pero desea deshabilitar temporalmente todos los servicios de almacenamiento en caché, puede modificar la configuración de BranchCache para detener el almacenamiento en caché automático en todos los recursos compartidos.

Si BranchCache en un recurso compartido de SMB se deshabilita después de haber habilitado por primera vez, ONTAP deja de enviar metadatos al cliente que lo solicita. Un cliente que necesita datos los recupera directamente del servidor de contenido (servidor CIFS en la máquina virtual de almacenamiento (SVM)).

Información relacionada

[Configuración de recursos compartidos de SMB habilitados para BranchCache](#)

Deshabilite BranchCache en un único recurso compartido de SMB

Si no desea ofrecer servicios de almacenamiento en caché en determinados recursos compartidos que anteriormente ofrecían contenido en caché, puede deshabilitar BranchCache en un recurso compartido de SMB existente.

Paso

1. Introduzca el siguiente comando: `vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties branchcache`

Se elimina la propiedad compartida de BranchCache. Otras propiedades de recursos compartidos aplicadas permanecen en vigor.

Ejemplo

El siguiente comando deshabilita BranchCache en un recurso compartido de SMB existente llamado «data2»:

```
cluster1::> vservice cifs share show -vservice vs1 -share-name data2
```

```

        Vservice: vs1
        Share: data2
CIFS Server NetBIOS Name: VS1
        Path: /data2
    Share Properties: oplocks
                     browsable
                     changenotify
                     attributecache
                     branchcache
    Symlink Properties: -
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
        Share Comment: -
            Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
        Volume Name: -
        Offline Files: manual
Vscan File-Operations Profile: standard
```

```
cluster1::> vservice cifs share properties remove -vservice vs1 -share-name
data2 -share-properties branchcache
```

```
cluster1::> vservice cifs share show -vservice vs1 -share-name data2
```

```

        Vservice: vs1
        Share: data2
CIFS Server NetBIOS Name: VS1
        Path: /data2
    Share Properties: oplocks
                     browsable
                     changenotify
                     attributecache
    Symlink Properties: -
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
        Share Comment: -
            Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
        Volume Name: -
        Offline Files: manual
Vscan File-Operations Profile: standard
```

Detenga el almacenamiento en caché automático en todos los recursos compartidos de SMB

Si la configuración de BranchCache habilita automáticamente el almacenamiento en caché en todos los recursos compartidos SMB en cada máquina virtual de almacenamiento (SVM), puede modificar la configuración de BranchCache para detener el almacenamiento en caché automático de contenido para todos los recursos compartidos SMB.

Acerca de esta tarea

Para detener el almacenamiento en caché automático en todos los recursos compartidos SMB, debe cambiar el modo operativo de BranchCache a almacenamiento en caché por recurso compartido.

Pasos

1. Configure BranchCache para detener el almacenamiento en caché automático en todos los recursos compartidos de SMB: `vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share`
2. Compruebe que la configuración de BranchCache sea correcta: `vserver cifs branchcache show -vserver vserver_name`

Ejemplo

El siguiente comando cambia la configuración de BranchCache en una máquina virtual de almacenamiento (SVM, antes conocida como Vserver) vs1 para detener el almacenamiento en caché automático en todos los recursos compartidos SMB:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
per-share

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
        Supported BranchCache Versions: enable_all
                                Path to Hash Store: /hash_data
        Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Deshabilite o habilite BranchCache en la SVM

Qué sucede cuando se deshabilita o se vuelve a habilitar BranchCache en el servidor CIFS

Si anteriormente configuró BranchCache pero no desea que los clientes de la sucursal utilicen contenido almacenado en caché, puede deshabilitar el almacenamiento en caché en el servidor CIFS. Debe tener en cuenta lo que sucede al deshabilitar BranchCache.

Cuando deshabilita BranchCache, ONTAP ya no calcula los hash ni envía los metadatos al cliente solicitante. Sin embargo, no se interrumpe el acceso a los archivos. A partir de entonces, cuando los clientes habilitados para BranchCache solicitan información de metadatos sobre el contenido al que desean acceder, ONTAP responde con un error definido por Microsoft, lo que hace que el cliente envíe una segunda solicitud al


contenido real. En respuesta a la solicitud de contenido, el servidor CIFS envía el contenido real almacenado en la máquina virtual de almacenamiento (SVM).

Una vez que se deshabilita BranchCache en el servidor CIFS, los recursos compartidos de SMB no anuncian las funcionalidades de BranchCache. Para acceder a los datos de nuevas conexiones SMB, los clientes realizan solicitudes de lectura SMB normales.

Puede volver a habilitar BranchCache en el servidor CIFS en cualquier momento.

- Dado que el almacén hash no se elimina cuando deshabilita BranchCache, ONTAP puede usar los hash almacenados al responder a las solicitudes hash una vez que vuelva a habilitar BranchCache, siempre y cuando el hash solicitado siga siendo válido.
- Todos los clientes que hayan establecido conexiones SMB a recursos compartidos habilitados con BranchCache durante el momento en el que se deshabilitó BranchCache no obtienen compatibilidad con BranchCache si se vuelve a habilitar BranchCache después.

Esto se debe a que ONTAP anuncia el soporte de BranchCache para un recurso compartido en el momento de la configuración de la sesión del SMB. Los clientes que establecieron sesiones con recursos compartidos habilitados para BranchCache mientras BranchCache estaba deshabilitado necesitan desconectar y volver a conectarse para usar el contenido en caché para este recurso compartido.



Si no desea guardar el almacén hash después de deshabilitar BranchCache en un servidor CIFS, puede eliminarlo en forma manual. Si vuelve a habilitar BranchCache, debe asegurarse de que exista el directorio de almacén hash. Una vez que se vuelve a habilitar BranchCache, los recursos compartidos con BranchCache habilitados anuncian las funcionalidades de BranchCache. ONTAP crea nuevos hash a medida que las nuevas solicitudes las realizan los clientes habilitados para BranchCache.

Deshabilite o habilite BranchCache

Puede deshabilitar BranchCache en la máquina virtual de almacenamiento (SVM) cambiando el modo operativo de BranchCache a `disabled`. Puede habilitar BranchCache en cualquier momento cambiando el modo operativo para ofrecer servicios de BranchCache por recurso compartido o automáticamente para todos los recursos compartidos.

Pasos

1. Ejecute el comando apropiado:

| Si desea... | Introduzca lo siguiente... |
|---|--|
| Deshabilite BranchCache | <pre>vserver cifs branchcache modify -vserver vserver_name -operating-mode disable</pre> |
| Habilite BranchCache por recurso compartido | <pre>vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share</pre> |

| Si desea... | Introduzca lo siguiente... |
|--|---|
| Habilite BranchCache para todos los recursos compartidos | <code>vserver cifs branchcache modify -vserver vserver_name -operating-mode all-shares</code> |

2. Compruebe que el modo operativo de BranchCache esté configurado con la configuración deseada:

```
vserver cifs branchcache show -vserver vserver_name
```

Ejemplo

En el siguiente ejemplo, se deshabilita BranchCache en la SVM vs1:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode  
disable  
  
cluster1::> vserver cifs branchcache show -vserver vs1  
  
Vserver: vs1  
Supported BranchCache Versions: enable_all  
Path to Hash Store: /hash_data  
Maximum Size of the Hash Store: 20GB  
Encryption Key Used to Secure the Hashes: -  
CIFS BranchCache Operating Modes: disable
```

Elimine la configuración de BranchCache en las SVM

Qué sucede cuando se elimina la configuración de BranchCache

Si anteriormente configuró BranchCache, pero no desea que la máquina virtual de almacenamiento (SVM) continúe proporcionando contenido en caché, puede eliminar la configuración de BranchCache en el servidor CIFS. Debe saber lo que ocurre cuando se elimina la configuración.

Cuando se elimina la configuración, ONTAP quita la información de configuración de esa SVM del clúster y detiene el servicio BranchCache. Puede decidir si ONTAP debería eliminar el almacén hash de la SVM.

La eliminación de la configuración de BranchCache no interrumpe el acceso de los clientes habilitados para BranchCache. A partir de entonces, cuando los clientes habilitados para BranchCache solicitan información de metadatos sobre las conexiones SMB existentes para determinar el contenido que ya se ha almacenado en la caché, ONTAP responde con un error definido de Microsoft, lo que hace que el cliente envíe una segunda solicitud, solicitando el contenido real. En respuesta a la solicitud de contenido, el servidor CIFS envía el contenido real almacenado en la SVM.

Una vez que se elimina la configuración de BranchCache, los recursos compartidos de SMB no anuncian las funcionalidades de BranchCache. Para acceder a contenido que no se ha almacenado previamente en la caché mediante nuevas conexiones SMB, los clientes realizan solicitudes de SMB de lectura normales.

Elimine la configuración de BranchCache

El comando que se usa para eliminar el servicio BranchCache en la máquina virtual de almacenamiento (SVM) varía en función de si desea eliminar o conservar los hash existentes.

Paso

1. Ejecute el comando apropiado:

| Si desea... | Introduzca lo siguiente... |
|--|--|
| Elimine la configuración de BranchCache y elimine los hash existentes | <pre>vserver cifs branchcache delete -vserver vserver_name -flush-hashes true</pre> |
| Elimine la configuración de BranchCache, pero mantenga los hash existentes | <pre>vserver cifs branchcache delete -vserver vserver_name -flush-hashes false</pre> |

Ejemplo

En el siguiente ejemplo, se elimina la configuración de BranchCache en la SVM vs1 y se eliminan todos los hash existentes:

```
cluster1::> vserver cifs branchcache delete -vserver vs1 -flush-hashes  
true
```

Qué le sucede a BranchCache al revertir

Es importante comprender lo que sucede al revertir ONTAP a una versión que no admite BranchCache.

- Cuando revierte a una versión de ONTAP que no admite BranchCache, los recursos compartidos SMB no anuncian capacidades de BranchCache a los clientes habilitados para BranchCache; por lo tanto, los clientes no solicitan información hash.

En su lugar, solicitan el contenido real mediante las solicitudes de lectura SMB normales. En respuesta a la solicitud de contenido, el servidor SMB envía el contenido real almacenado en la máquina virtual de almacenamiento (SVM).

- Cuando un nodo que aloja un almacén hash se revierte a una versión que no admite BranchCache, el administrador de almacenamiento debe revertir manualmente la configuración de BranchCache mediante un comando que se imprime durante la reversión.

Este comando elimina la configuración y los hash de BranchCache.

Una vez finalizada la reversión, el administrador de almacenamiento puede eliminar manualmente el directorio que contenía el almacén hash, si lo desea.

Información relacionada

Mejorar el rendimiento de las copias remotas de Microsoft

Mejorar el rendimiento de las copias remotas de Microsoft

La transferencia de datos descargados (ODX) de Microsoft, también conocida como *copy flood*, permite transferir datos directamente dentro o entre dispositivos de almacenamiento compatibles sin transferir los datos a través del equipo host.

ONTAP admite ODX para los protocolos SMB Y SAN. El origen puede ser un servidor CIFS o una LUN; el destino puede ser un servidor CIFS o una LUN.

En las transferencias de archivos que no son ODX, los datos se leen del origen y se transfieren a través de la red al equipo cliente. El equipo cliente transfiere los datos a través de la red al destino. En resumen, el equipo cliente lee los datos del origen y los escribe en el destino. Con las transferencias de archivos ODX, los datos se copian directamente del origen al destino.

Dado que las copias descargados de ODX se realizan directamente entre el almacenamiento de origen y destino, se obtienen importantes ventajas en el rendimiento. Las ventajas en cuanto a rendimiento incluyen unos tiempos de copia más rápidos entre el origen y el destino, una menor utilización de recursos (CPU, memoria) en el cliente y una menor utilización de ancho de banda de I/O de la red.

En los entornos SMB, esta funcionalidad solo está disponible cuando el cliente y el servidor de almacenamiento admiten SMB 3.0 y la función ODX. En entornos SAN, esta funcionalidad solo está disponible cuando el cliente y el servidor de almacenamiento admiten la función ODX. Los equipos cliente compatibles con ODX y que tengan habilitada ODX automáticamente y de forma transparente utilizan la transferencia de archivos descargados cuando se mueven o copian archivos. ODX se utiliza independientemente de si arrastra y suelta archivos a través del Explorador de Windows, o si utiliza comandos de copia de archivos de la línea de comandos, o si una aplicación cliente inicia solicitudes de copia de archivos.

Información relacionada

[Mejorar el tiempo de respuesta del cliente al proporcionar referencias automáticas a nodos SMB con ubicación automática](#)

["Configuración de SMB para Microsoft Hyper-V y SQL Server"](#)

Cómo funciona ODX

La descarga de copias ODX utiliza un mecanismo basado en tokens para leer y escribir datos dentro o entre servidores CIFS habilitados para ODX. En lugar de enrutar los datos a través del host, el servidor CIFS envía al cliente un pequeño token que representa los datos. El cliente ODX presenta ese token al servidor de destino, que posteriormente puede transferir los datos que representa ese token del origen al destino.

Cuando un cliente ODX descubre que el servidor CIFS es compatible con ODX, abre el archivo de origen y solicita un token del servidor CIFS. Después de abrir el archivo de destino, el cliente utiliza el token para indicar al servidor que copie los datos directamente del origen al destino.



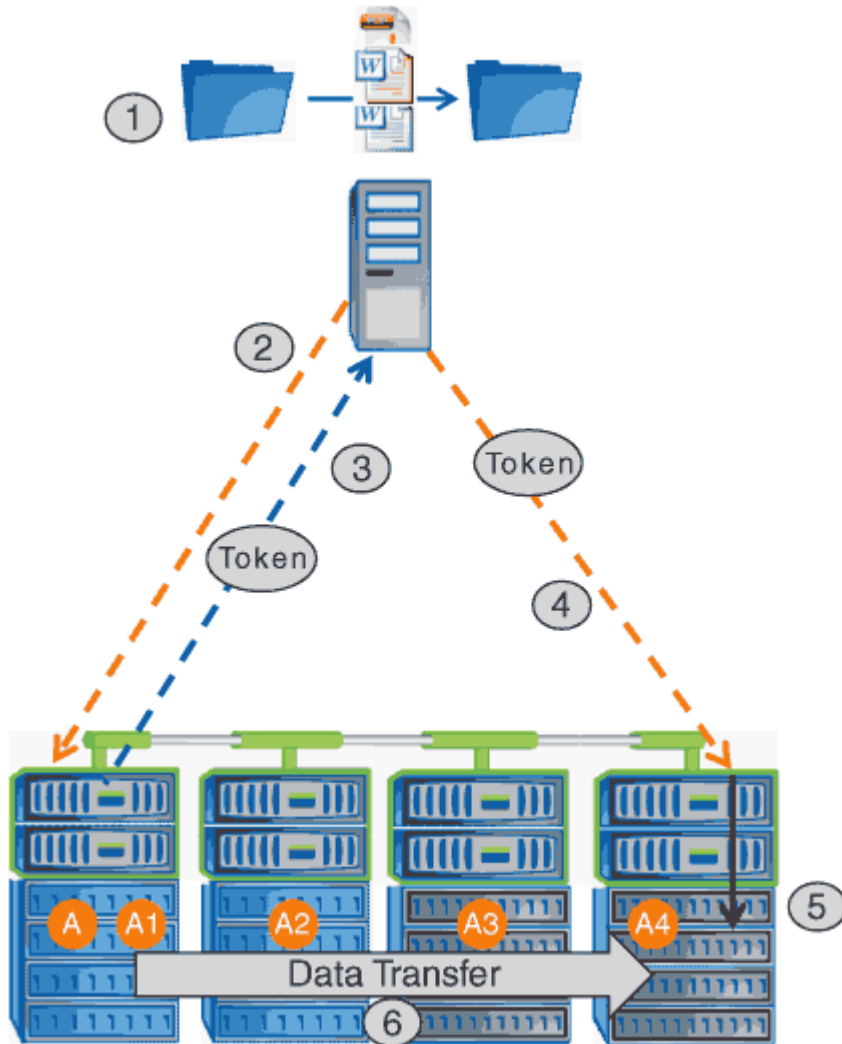
El origen y el destino pueden estar en la misma máquina virtual de almacenamiento (SVM) o en distintas SVM, según el alcance de la operación de copia.

El token sirve como representación puntual de los datos. Por ejemplo, cuando copia datos entre ubicaciones

de almacenamiento, se devuelve un token que representa un segmento de datos al cliente solicitante, que el cliente copia en el destino; de este modo, se elimina la necesidad de copiar los datos subyacentes a través del cliente.

ONTAP admite tokens que representan 8 MB de datos. Las copias ODX de más de 8 MB se realizan utilizando varios tokens, con cada token que representa 8 MB de datos.

En la siguiente figura, se explican los pasos involucrados en una operación de copia de ODX:



1. Un usuario copia o mueve un archivo mediante el Explorador de Windows, una interfaz de línea de comandos o como parte de la migración de un equipo virtual, o bien una aplicación inicia copias o traslados de archivos.
2. El cliente compatible con ODX convierte automáticamente esta solicitud de transferencia a una solicitud ODX.

La solicitud ODX que se envía al servidor CIFS contiene una solicitud de token.

3. Si se habilita ODX en el servidor CIFS y la conexión a través de SMB 3.0, el servidor CIFS genera un token, que es una representación lógica de los datos en el origen.
4. El cliente recibe un token que representa los datos y se envía con la solicitud de escritura al servidor CIFS de destino.

Se trata de los únicos datos que se copian a través de la red desde el origen al cliente y, después, desde

el cliente al destino.

5. El token se entrega al subsistema de almacenamiento.
6. La SVM realiza de forma interna la copia o el movimiento.

Si el archivo que se copia o se mueve es de más de 8 MB, se necesitan varios tokens para realizar la copia. Pasos 2 a 6 según se requiera para completar la copia.



Si se produce un error con la copia descargada de ODX, la operación de copia o movimiento se vuelve a leer y escribir tradicionales para la operación de copia o movimiento. Del mismo modo, si el servidor CIFS de destino no admite ODX ni ODX está deshabilitado, la operación de copia o movimiento se remonta a las lecturas y escrituras tradicionales para la operación de copia o movimiento.

Requisitos para usar ODX

Antes de poder usar ODX para llevar a cabo descargas de copias con la máquina virtual de almacenamiento (SVM), debe conocer ciertos requisitos.

Requisitos de la versión de ONTAP

ONTAP libera compatibilidad con ODX para realizar descargas de copias.

Requisitos de versión de SMB

- ONTAP es compatible con ODX mediante SMB 3.0 y versiones posteriores.
- Para poder habilitar ODX, es necesario habilitar SMB 3.0 en el servidor CIFS:
 - Si la función ODX no está habilitada, también habilita SMB 3.0.
 - Al deshabilitar SMB 3.0, también se deshabilita ODX.

Requisitos del servidor y del cliente de Windows

Antes de poder usar ODX para realizar descargas de copias, el cliente de Windows debe admitir la función.

La ["Matriz de interoperabilidad de NetApp"](#) contiene la información más reciente sobre los clientes de Windows compatibles.

Requisitos del volumen

- Los volúmenes de origen deben tener un mínimo de 1.25 GB.
- Si utiliza volúmenes comprimidos, el tipo de compresión debe ser adaptable y solo se admite el tamaño de grupo de compresión 8K.

No se admite el tipo de compresión secundaria.

Directrices para usar ODX

Antes de poder utilizar ODX para descarga de copias, debe conocer las directrices. Por ejemplo, debe saber en qué tipos de volúmenes se puede utilizar ODX y debe comprender las consideraciones dentro del clúster y entre clústeres de ODX.

Directrices de volumen

- No se puede usar ODX para descargar la copia con las siguientes configuraciones de volumen:
 - El tamaño del volumen de origen es inferior a 1.25 GB

El tamaño del volumen debe ser 1.25 GB o más para usar la función ODX.

- Volúmenes de solo lectura

ODX no se utiliza para archivos y carpetas que residen en reflejos de carga compartida o en volúmenes de destino de SnapMirror o SnapVault.

- Si el volumen de origen no está deduplicado
- Las copias ODX solo son compatibles con las copias dentro del clúster.

No se puede usar ODX para copiar archivos o carpetas en un volumen de otro clúster.

Otras directrices

- En los entornos SMB, para utilizar ODX para la descarga de copias, los archivos deben ser de 256 kb o más.

Los archivos más pequeños se transfieren mediante una operación de copia tradicional.

- La descarga de copias ODX utiliza la deduplicación como parte del proceso de copia.

Si no desea que la deduplicación se produzca en los volúmenes de SVM al copiar o mover datos, debe deshabilitar la descarga de la copia ODX en esa SVM.

- La aplicación que realiza la transferencia de datos debe escribirse para admitir ODX.

Las operaciones de aplicaciones compatibles con ODX incluyen lo siguiente:

- Las operaciones de gestión de Hyper-V, como la creación y conversión de discos duros virtuales (VHD), la gestión de copias Snapshot y la copia de archivos entre máquinas virtuales
- Operaciones del Explorador de Windows
- Comandos de copia de Windows PowerShell
- Comandos de copia en el símbolo del sistema de Windows

Robocopy en el símbolo del sistema de Windows admite ODX.



Las aplicaciones deben ejecutarse en servidores Windows o clientes que admitan ODX.

+

Para obtener más información acerca de las aplicaciones ODX admitidas en servidores y clientes Windows, consulte la biblioteca de Microsoft TechNet.

Información relacionada

"Biblioteca de Microsoft TechNet: technet.microsoft.com/en-us/library/"

Casos de uso para ODX

Debe conocer los casos de uso de ODX en SVM para poder determinar en qué circunstancias le proporciona ventajas en rendimiento.

Los servidores y los clientes de Windows que admiten ODX utilizan la descarga de copias como forma predeterminada de copiar datos en servidores remotos. Si el cliente o el servidor Windows no son compatibles con ODX o se produce un error en cualquier momento, la operación de copia o movimiento vuelve a las lecturas y escrituras tradicionales para la operación de copia o movimiento.

Los siguientes casos de uso admiten el uso de copias y movimientos ODX:

- Volumen interno

Los archivos o LUN de origen y destino están dentro del mismo volumen.

- Entre volúmenes, mismo nodo, misma SVM

Los archivos de origen y de destino o las LUN se encuentran en distintos volúmenes ubicados en el mismo nodo. Los datos son propiedad de la misma SVM.

- Entre volúmenes, distintos nodos, misma SVM

Los archivos de origen y de destino o las LUN se encuentran en volúmenes distintos que se encuentran en nodos diferentes. Los datos son propiedad de la misma SVM.

- Entre SVM, mismo nodo

El archivo de origen y los LUN de destino se encuentran en distintos volúmenes ubicados en el mismo nodo. Los datos son propiedad de diferentes SVM.

- Entre SVM, diferentes nodos

El archivo o las LUN de origen y destino se encuentran en distintos volúmenes ubicados en nodos diferentes. Los datos son propiedad de diferentes SVM.

- Entre clústeres

Las LUN de origen y de destino se encuentran en distintos volúmenes ubicados en distintos nodos en varios clústeres. Solo se admite para SAN y no funciona para CIFS.

Existen algunos casos de uso especiales adicionales:

- Con la implementación de ODX de ONTAP, se puede utilizar ODX para copiar archivos entre recursos compartidos de SMB y unidades virtuales asociadas a FC o iSCSI.

Puede utilizar el Explorador de Windows, la CLI de Windows o PowerShell, Hyper-V u otras aplicaciones que admiten ODX para copiar o mover archivos sin problemas mediante la descarga de la copia ODX entre recursos compartidos de SMB y LUN conectados, siempre y cuando los recursos compartidos y las LUN del SMB estén en el mismo clúster.

- Hyper-V proporciona algunos casos de uso adicionales para la descarga de copias ODX:

- Se puede utilizar la transferencia de la copia ODX mediante Hyper-V para copiar datos dentro o a través de archivos de disco duro virtual (VHD), o bien copiar datos entre recursos compartidos de SMB

asignados y LUN iSCSI conectados dentro del mismo clúster.

Esto permite que las copias de sistemas operativos invitados pasen al almacenamiento subyacente.

- Al crear discos duros virtuales de tamaño fijo, ODX se utiliza para inicializar el disco con ceros, empleando un token de cero conocido.
- La descarga de copias ODX se utiliza para la migración de almacenamiento de máquinas virtuales si el almacenamiento de origen y destino está en el mismo clúster.



Para aprovechar los casos de uso de un paso a través de la descarga de copias ODX mediante Hyper-V, el sistema operativo invitado debe ser compatible con ODX, mientras que los discos del sistema operativo invitado deben ser discos SCSI respaldados por almacenamiento (tanto SMB COMO SAN) que sean compatibles con ODX. Los discos IDE del sistema operativo invitado no admiten el paso a través de ODX.

Habilite o deshabilite ODX

Es posible habilitar o deshabilitar ODX en máquinas virtuales de almacenamiento (SVM). El valor predeterminado es habilitar la compatibilidad con la descarga de copias ODX si también se habilita SMB 3.0.

Antes de empezar

Se debe habilitar SMB 3.0.

Acerca de esta tarea

Si deshabilita SMB 3.0, ONTAP también deshabilita SMB ODX. Si vuelve a habilitar SMB 3.0, debe volver a habilitar manualmente SMB ODX.

Pasos

1. Configure el nivel de privilegio en Advanced: `set -privilege advanced`
2. Ejecute una de las siguientes acciones:

| Si desea que la descarga de copias de ODX sea... | Introduzca el comando... |
|--|--|
| Activado | <pre>vserver cifs options modify -vserver vserver_name -copy-offload-enabled true</pre> |
| Deshabilitado | <pre>vserver cifs options modify -vserver vserver_name -copy-offload-enabled false</pre> |

3. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

Ejemplo

En el ejemplo siguiente se habilita la descarga de copias ODX en SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster1::*> set -privilege admin
```

Información relacionada

Opciones disponibles del servidor SMB

Mejore el tiempo de respuesta del cliente al proporcionar referencias automáticas a nodos SMB con ubicación automática

Mejore el tiempo de respuesta del cliente al proporcionar referencias automáticas a nodos SMB con información general sobre la ubicación automática

Auto Location utiliza referencias de nodos automáticas de SMB para aumentar el rendimiento del cliente de SMB en máquinas virtuales de almacenamiento (SVM). Las referencias automáticas a nodos redirigen automáticamente el cliente solicitante a una LIF en la SVM de nodos que aloja el volumen en el que residen los datos, lo que puede mejorar los tiempos de respuesta del cliente.

Cuando un cliente SMB se conecta a un recurso compartido SMB alojado en la SVM, puede conectarse mediante una LIF que está en un nodo que no posee los datos solicitados. El nodo al que está conectado el cliente accede a los datos que pertenece a otro nodo mediante el uso de la red de clústeres. El cliente puede experimentar tiempos de respuesta más rápidos si la conexión SMB utiliza una LIF ubicada en el nodo que contiene los datos solicitados:

- ONTAP proporciona esta funcionalidad al utilizar referencias DFS de Microsoft para informar a los clientes SMB de que un archivo o carpeta solicitados en el espacio de nombres está alojado en otro lugar.

Un nodo hace una referencia cuando determina que hay una LIF ANSVM en el nodo que contiene los datos.

- Las referencias automáticas de nodos son compatibles con las direcciones IP de LIF IPv4 e IPv6.
- Las referencias se realizan en función de la ubicación de la raíz del recurso compartido a través del cual está conectado el cliente.
- La referencia se produce durante la negociación SMB.

La referencia se realiza antes de establecer la conexión. Una vez que ONTAP hace referencia al cliente SMB al nodo de destino, se establece la conexión y el cliente accede a los datos a través de la ruta LIF referida desde ese punto de encendido. Esto permite a los clientes acceder con más rapidez a los datos y evita la comunicación adicional del clúster.



Si un recurso compartido abarca varios puntos de unión y algunas uniones están en volúmenes contenidos en otros nodos, los datos del recurso compartido se distribuyen entre varios nodos. Dado que ONTAP proporciona las referencias que son locales a la raíz del recurso compartido, ONTAP debe usar la red de clúster para recuperar los datos contenidos en estos volúmenes no locales. Con este tipo de arquitectura de espacio de nombres, es posible que las referencias automáticas a nodos no ofrezcan importantes beneficios en el rendimiento.

Si el nodo que aloja los datos no tiene una LIF disponible, ONTAP establecerá la conexión mediante la LIF elegida por el cliente. Después de que un cliente SMB abre un archivo, éste continúa accediendo al archivo a través de la misma conexión referida.

Si, por algún motivo, el servidor CIFS no puede hacer una referencia, no se produce ninguna interrupción del servicio SMB. La conexión SMB se establece como si las referencias automáticas a nodos no estuvieran habilitadas.

Información relacionada

[Mejora del rendimiento de las copias remotas de Microsoft](#)

Requisitos y directrices para el uso de referencias automáticas al nodo

Antes de poder utilizar las referencias automáticas de nodos SMB, también conocido como *autoubicación*, debe tener en cuenta ciertos requisitos, como las versiones de ONTAP que admiten esta función. También debe saber acerca de las versiones del protocolo SMB compatibles y otras directrices especiales.

Requisitos de versión y licencia de ONTAP

- Todos los nodos del clúster deben ejecutar una versión de ONTAP que admita las referencias automáticas al nodo.
- Los widgets deben estar habilitados en un recurso compartido SMB para utilizar la autolocalización.
- CIFS debe tener una licencia y el servidor SMB debe existir en las SVM. La licencia SMB se incluye con "ONTAP One". Si no tiene ONTAP One y la licencia no está instalada, póngase en contacto con su representante de ventas.

Requisitos de la versión del protocolo SMB

- Para SVM, ONTAP admite referencias de nodos automáticas en todas las versiones de SMB.

Requisitos del cliente de SMB

Todos los clientes de Microsoft compatibles con ONTAP son compatibles con las referencias de nodo automáticas SMB.

La matriz de interoperabilidad contiene la información más reciente sobre los clientes Windows que admite ONTAP.

["Herramienta de matriz de interoperabilidad de NetApp"](#)

Requisitos de LIF de datos

Si desea utilizar una LIF de datos como referencia potencial para los clientes de SMB, debe crear LIF de datos con NFS y CIFS habilitados.

Las referencias automáticas de nodos pueden fallar si el nodo de destino contiene LIF de datos que están habilitadas solo para el protocolo NFS o solo para el protocolo SMB.

Si no se cumple este requisito, el acceso a los datos no se verá afectado. El cliente de SMB asigna el recurso compartido mediante la LIF original que utilizó el cliente para conectarse a la SVM.

Requisitos de autenticación NTLM al realizar una conexión SMB a la que se hace referencia

Se debe permitir la autenticación NTLM en el dominio que contiene el servidor CIFS y en los dominios que contienen clientes que desean utilizar referencias automáticas a nodos.

Al realizar una referencia, el servidor SMB hace referencia a una dirección IP al cliente Windows. Dado que la autenticación NTLM se utiliza al realizar una conexión mediante una dirección IP, la autenticación Kerberos no se realiza para conexiones a las que se hace referencia.

Esto sucede porque el cliente de Windows no puede diseñar el nombre principal de servicio utilizado por Kerberos (que es del formulario `service/NetBIOS name` y.. `service/FQDN`), lo que significa que el cliente no puede solicitar un billete Kerberos al servicio.

Instrucciones para el uso de referencias automáticas de nodos con la función de directorio inicial

Cuando los recursos compartidos se configuran con la propiedad del recurso compartido del directorio principal activada, puede haber una o varias rutas de búsqueda del directorio principal configuradas para una configuración de directorio principal. Las rutas de búsqueda pueden apuntar a los volúmenes contenidos en cada nodo que contiene volúmenes de SVM. Los clientes reciben una referencia y, si hay una LIF de datos local activa disponible, se conectan a través de una LIF de referencia que sea local al directorio raíz del usuario doméstico.

Existen directrices para que los clientes de SMB 1.0 accedan a directorios iniciales dinámicos con referencias de nodos automáticas habilitadas. Esto se debe a que los clientes de SMB 1.0 necesitan la referencia automática al nodo antes de que se hayan autenticado, lo que es antes de que el servidor SMB tenga el nombre del usuario. Sin embargo, el acceso al directorio raíz SMB funciona correctamente para los clientes SMB 1.0 si se cumplen las siguientes afirmaciones:

- Los directorios iniciales de SMB están configurados para usar nombres simples, como `""%w""` (nombre de usuario de Windows) o `""%u""` (nombre de usuario UNIX asignado), y no nombres de estilo de nombre de dominio, como `""%d\%w""` (nombre de dominio\nombre de usuario).
- Al crear recursos compartidos de directorios iniciales, los nombres de los recursos compartidos de directorios iniciales CIFS se configuran con variables (`""%w""` o `""%u""`), y no con nombres estáticos, como «HOME».

Para los clientes SMB 2.x y SMB 3.0, no hay directrices especiales al acceder a directorios iniciales con referencias automáticas a nodos.

Directrices para deshabilitar las referencias automáticas de nodos en servidores CIFS con conexiones existentes referidas

Si deshabilita las referencias automáticas a nodos después de habilitar la opción, los clientes que están actualmente conectados a una LIF conocida mantienen la conexión referida. Dado que ONTAP utiliza referencias DFS como mecanismo para las referencias automáticas de nodo SMB, los clientes pueden incluso

volver a conectarse a la LIF mencionada después de deshabilitar la opción hasta que se agote el tiempo de espera de la referencia de DFS en caché del cliente para la conexión mencionada. Esto es cierto incluso si se revierte a una versión de ONTAP que no admite referencias automáticas a los nodos. Los clientes continúan utilizando referencias hasta que se agote el tiempo de espera de la referencia DFS desde la memoria caché del cliente.

La ubicación automática utiliza las referencias de nodos automáticos de SMB para aumentar el rendimiento del cliente de SMB al remitir a los clientes a la LIF en el nodo propietario del volumen de datos de una SVM. Cuando un cliente SMB se conecta a un recurso compartido SMB alojado en una SVM, puede conectarse mediante una LIF en un nodo que no posea los datos solicitados y utilice una red de interconexión de clúster para recuperar los datos. El cliente puede experimentar tiempos de respuesta más rápidos si la conexión SMB utiliza una LIF ubicada en el nodo que contiene los datos solicitados.

ONTAP proporciona esta funcionalidad al utilizar referencias del sistema de archivos distribuidos (DFS) de Microsoft para informar a los clientes SMB de que un archivo o una carpeta solicitados en el espacio de nombres se alojan en otro lugar. Un nodo hace una referencia cuando determina que hay una LIF de SVM en el nodo que contiene los datos. Las referencias se realizan en función de la ubicación de la raíz del recurso compartido a través del cual está conectado el cliente.

La referencia se produce durante la negociación SMB. La referencia se realiza antes de establecer la conexión. Una vez que ONTAP hace referencia al cliente SMB al nodo de destino, se establece la conexión y el cliente accede a los datos a través de la ruta LIF referida desde ese punto de encendido. Esto permite a los clientes acceder con más rapidez a los datos y evita la comunicación adicional del clúster.

Instrucciones para el uso de referencias automáticas a nodos con clientes Mac OS

Los clientes de Mac OS X no admiten referencias automáticas de nodos SMB, aunque Mac OS sea compatible con Microsoft Distributed File System (DFS). Los clientes de Windows realizan una solicitud de referencia DFS antes de conectarse a un recurso compartido SMB. ONTAP proporciona una referencia a una LIF de datos que se encuentra en el mismo nodo que aloja los datos solicitados, lo cual mejora los tiempos de respuesta de los clientes. Aunque Mac OS admite DFS, los clientes de Mac OS no se comportan exactamente igual que los clientes de Windows en esta área.

Información relacionada

[Cómo habilita ONTAP los directorios iniciales dinámicos](#)

["Gestión de redes"](#)

["Herramienta de matriz de interoperabilidad de NetApp"](#)

Compatibilidad con referencias de nodos automáticas para SMB

Antes de habilitar las referencias automáticas al nodo SMB, tiene que tener en cuenta que ciertas funcionalidades de ONTAP no admiten referencias.

- Los siguientes tipos de volúmenes no son compatibles con las referencias de nodo automáticas del bloque de mensajes del servidor:
 - Miembros de solo lectura de un reflejo de carga compartida
 - Volumen de destino de un reflejo de protección de datos
- Las referencias de nodos no se mueven junto a un movimiento LIF.

Si un cliente utiliza una conexión a la que se hace referencia a través de una conexión SMB 2.x o SMB 3.0 y una LIF de datos se mueve de forma no disruptiva, el cliente sigue usando la misma conexión a la que

se hace referencia, aunque la LIF ya no sea local para los datos.

- Las referencias de los nodos no se mueven junto a un movimiento de volumen.

Si un cliente está usando una conexión a través de cualquier conexión SMB y se produce un movimiento de volúmenes, el cliente sigue utilizando la misma conexión conocida, aunque el volumen ya no esté ubicado en el mismo nodo que la LIF de datos.

Habilite o deshabilite las referencias de nodo automáticas para SMB

Puede habilitar las referencias de nodo automáticas para SMB para aumentar el rendimiento del acceso de los clientes SMB. Puede deshabilitar las referencias de nodo automáticas si no desea que ONTAP haga referencias a los clientes SMB.

Antes de empezar

Debe configurarse y ejecutarse un servidor CIFS en la máquina virtual de almacenamiento (SVM).

Acerca de esta tarea

La funcionalidad de referencias automáticas al nodo SMB está deshabilitada de manera predeterminada. Puede habilitar o deshabilitar esta funcionalidad en cada SVM, según sea necesario.

Esta opción está disponible en el nivel de privilegio avanzado.

Pasos

1. Configure el nivel de privilegio en Advanced: `set -privilege advanced`
2. Habilite o deshabilite las referencias de nodo automáticas para SMB según sea necesario:

| Si desea que las referencias automáticas de nodo de SMB sean... | Introduzca el siguiente comando... |
|---|---|
| Activado | <pre>vserver cifs options modify -vserver vserver_name -is-referral-enabled true</pre> |
| Deshabilitado | <pre>vserver cifs options modify -vserver vserver_name -is-referral-enabled false</pre> |

La configuración de la opción surte efecto para nuevas sesiones SMB. Los clientes con conexión existente solo pueden utilizar la referencia a nodos cuando finaliza el tiempo de espera de la caché existente.

3. Cambie al nivel de privilegio de administrador: `set -privilege admin`

Información relacionada

[Opciones disponibles del servidor SMB](#)

Utilice estadísticas para supervisar la actividad de referencia automática de nodos

Para determinar cuántas conexiones SMB se hacen referencia, puede supervisar la actividad de referencia automática de nodos mediante el `statistics` comando. Al supervisar las referencias puede determinar en qué medida las referencias automáticas

están ubicando conexiones en los nodos que alojan los recursos compartidos y si debe redistribuir sus LIF de datos para proporcionar un mejor acceso local a los recursos compartidos en el servidor CIFS.

Acerca de esta tarea

La `cifs` Object proporciona varios contadores en el nivel de privilegio avanzado que son útiles para supervisar referencias automáticas de nodos de SMB:

- `node_referral_issued`

Número de clientes a los que se ha emitido una referencia al nodo de la raíz compartida después de que el cliente se haya conectado mediante una LIF alojada por un nodo diferente al nodo de la raíz compartida.

- `node_referral_local`

Número de clientes que se conectan mediante una LIF alojada por el mismo nodo que aloja la raíz compartida. El acceso local generalmente proporciona un rendimiento óptimo.

- `node_referral_not_possible`

Número de clientes que no se han emitido una referencia al nodo que aloja el recurso compartido raíz tras la conexión mediante una LIF alojada por un nodo diferente al nodo raíz del recurso compartido. Esto se debe a que no se encontró una LIF de datos activa para el nodo raíz del recurso compartido.

- `node_referral_remote`

Número de clientes que se conectan mediante una LIF alojada por un nodo diferente al nodo que aloja la raíz compartida. El acceso remoto puede provocar una degradación del rendimiento.

Es posible supervisar las estadísticas de referencia automática de nodos en la máquina virtual de almacenamiento (SVM) mediante la recopilación y la visualización de datos de un período de tiempo específico (una muestra). Puede ver los datos de la muestra si no detiene la recopilación de datos. Al detener la recopilación de datos, se proporciona una muestra fija. No detener la recopilación de datos le ofrece la posibilidad de obtener datos actualizados que puede utilizar para compararlos con consultas anteriores. La comparativa puede ayudarle a identificar las tendencias de rendimiento.



Para evaluar y utilizar la información que recopila de `statistics` comando, debe comprender la distribución de clientes en sus entornos.

Pasos

1. Configure el nivel de privilegio en Advanced: `set -privilege advanced`
2. Para ver las estadísticas automáticas de referencia de nodos, utilice `statistics` comando.

En este ejemplo, se visualizan y recogen estadísticas de referencia automática de nodos:

- a. Inicie la colección: `statistics start -object cifs -instance vs1 -sample-id sample1`

```
Statistics collection is being started for Sample-id: sample1
```

- b. Espere a que transcurra el tiempo de recogida deseado.
- c. Detenga la colección: `statistics stop -sample-id sample1`

```
Statistics collection is being stopped for Sample-id: sample1
```

- d. Vea las estadísticas de referencia automática de nodos: `statistics show -sample-id sample1 -counter node`

```
Object: cifs
Instance: vs1
Start-time: 2/4/2013 19:27:02
End-time: 2/4/2013 19:30:11
Cluster: cluster1
```

| Counter | Value |
|----------------------------|-------|
| node_name | node1 |
| node_referral_issued | 0 |
| node_referral_local | 1 |
| node_referral_not_possible | 2 |
| node_referral_remote | 2 |
| ... | |
| node_name | node2 |
| node_referral_issued | 2 |
| node_referral_local | 1 |
| node_referral_not_possible | 0 |
| node_referral_remote | 2 |
| ... | |

La salida muestra los contadores de todos los nodos que participan en SVM vs1. Para mayor claridad, en el ejemplo solo se proporcionan los campos de salida relacionados con las estadísticas automáticas de referencia de nodos.

- 3. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

Información relacionada

[Mostrar estadísticas](#)

["Configuración de supervisión del rendimiento"](#)

Supervise la información de referencia automática de nodos SMB del lado del cliente mediante un cliente de Windows

Para determinar qué referencias se hacen desde la perspectiva del cliente, puede utilizar Windows `dfsutil.exe` utilidad.

El kit de herramientas de administración remota de servidores (RSAT) disponible con los clientes de Windows 7 y posteriores contiene el `dfsutil.exe` utilidad. Con esta utilidad, puede mostrar información acerca del contenido de la caché de referencias así como ver información acerca de cada referencia que esté utilizando actualmente el cliente. También puede utilizar la utilidad para borrar la memoria caché de referencia del cliente. Para obtener más información, consulte la biblioteca de Microsoft TechNet.

Información relacionada

"Biblioteca de Microsoft TechNet: technet.microsoft.com/en-us/library/"

Proporcione seguridad de carpetas en recursos compartidos con enumeración basada en acceso

Proporcione seguridad de carpetas en recursos compartidos con información general sobre enumeración basada en acceso

Cuando se habilita la enumeración basada en acceso (ABE) en un recurso compartido SMB, los usuarios que no tienen permiso para acceder a una carpeta o archivo contenido en el recurso compartido (ya sea mediante restricciones de permisos individuales o de grupo) no ven el recurso compartido que se muestra en su entorno, aunque el recurso compartido en sí sigue siendo visible.

Las propiedades de uso compartido convencionales permiten especificar qué usuarios (individualmente o en grupos) tienen permiso para ver o modificar archivos o carpetas contenidos en el recurso compartido. Sin embargo, no le permiten controlar si las carpetas o archivos dentro del recurso compartido son visibles para los usuarios que no tienen permiso para tener acceso a ellos. Esto podría plantear problemas si los nombres de estas carpetas o archivos del recurso compartido describen información confidencial, como los nombres de los clientes o los productos en desarrollo.

La enumeración basada en acceso (ABE) amplía las propiedades de recursos compartidos para incluir la enumeración de archivos y carpetas dentro del recurso compartido. POR tanto, ABE permite filtrar la visualización de archivos y carpetas dentro del recurso compartido en función de los derechos de acceso del usuario. Es decir, el recurso compartido en sí sería visible para todos los usuarios, pero los archivos y carpetas dentro del recurso compartido podrían mostrarse u ocultarse de los usuarios designados. Además de proteger la información confidencial en su lugar de trabajo, ABE le permite simplificar la presentación de grandes estructuras de directorio en beneficio de los usuarios que no necesitan acceso a su gama completa de contenido. Por ejemplo, el recurso compartido en sí sería visible para todos los usuarios, pero los archivos y carpetas dentro del recurso compartido podrían mostrarse u ocultarse.

Descubra "[Impacto sobre el rendimiento al utilizar la enumeración basada en SMB/CIFS Access](#)".

Habilite o deshabilite la enumeración basada en acceso en los recursos compartidos de SMB

Puede habilitar o deshabilitar la enumeración basada en acceso (ABE) en recursos compartidos SMB para permitir o impedir que los usuarios vean recursos compartidos a los que no tienen permiso para acceder.

Acerca de esta tarea

De forma predeterminada, ABE está deshabilitado.

Pasos

1. Ejecute una de las siguientes acciones:

| Si desea... | Introduzca el comando... |
|--|---|
| Habilite ABE en un nuevo recurso compartido | <code>vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties access-based-enumeration</code> Puede especificar configuraciones de recursos compartidos adicionales y propiedades de recursos compartidos adicionales al crear un recurso compartido SMB. Para obtener más información, consulte la página de manual de <code>vserver cifs share create</code> comando. |
| Habilite ABE en un recurso compartido existente | <code>vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties access-based-enumeration</code> Se conservan las propiedades de recursos compartidos existentes. La propiedad ABE share se agrega a la lista existente de propiedades compartidas. |
| Deshabilite ABE en un recurso compartido existente | <code>vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties access-based-enumeration</code> Se conservan otras propiedades compartidas. Sólo la propiedad compartida ABE se elimina de la lista de propiedades de recursos compartidos. |

2. Compruebe que la configuración de recurso compartido sea correcta mediante el `vserver cifs share show` comando.

Ejemplos

El siguiente ejemplo crea una unidad ABE SMB denominada «números» con una ruta de acceso `/sales` En SVM vs1. El recurso compartido se crea con `access-based-enumeration` como propiedad compartida:

```

cluster1::> vserver cifs share create -vserver vs1 -share-name sales -path
/sales -share-properties access-based-
enumeration,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name sales

          Vserver: vs1
          Share: sales
CIFS Server NetBIOS Name: VS1
          Path: /sales
    Share Properties: access-based-enumeration
                     oplocks
                     browsable
                     changenotify
    Symlink Properties: enable
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
          Share Comment: -
          Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
          Volume Name: -
          Offline Files: manual
Vscan File-Operations Profile: standard

```

En el siguiente ejemplo se agrega el access-based-enumeration Compartir propiedad a un recurso compartido SMB denominado «data2»:

```

cluster1::> vserver cifs share properties add -vserver vs1 -share-name
data2 -share-properties access-based-enumeration

cluster1::> vserver cifs share show -vserver vs1 -share-name data2 -fields
share-name,share-properties
server  share-name share-properties
-----
vs1     data2      oplocks,browsable,changenotify,access-based-enumeration

```

Información relacionada

[Agregar o quitar propiedades de recursos compartidos en un recurso compartido SMB existente](#)

Habilite o deshabilite la enumeración basada en acceso desde un cliente Windows

Puede habilitar o deshabilitar la enumeración basada en acceso (ABE) en recursos compartidos SMB desde un cliente Windows, que permite configurar esta configuración de recurso compartido sin tener que conectarse al servidor CIFS.



La abecmd La utilidad no está disponible en las nuevas versiones de los clientes de Windows Server y Windows. Se lanzó como parte de Windows Server 2008. El soporte finalizó para Windows Server 2008 el 14 de enero de 2020.

Pasos

1. Desde un cliente Windows compatible con ABE, introduzca el siguiente comando: `abecmd [/enable | /disable] [/server CIFS_server_name] {/all | share_name}`

Para obtener más información acerca de `abecmd` Consulte la documentación del cliente de Windows.

Dependencias de nomenclatura de archivos y directorios NFS y SMB

Información general sobre las dependencias de nomenclatura de archivos y directorios de NFS y SMB

Las convenciones de nomenclatura de archivos y directorios dependen tanto de los sistemas operativos de los clientes de red como de los protocolos de uso compartido de archivos, además de la configuración de idioma del clúster ONTAP y de los clientes.

El sistema operativo y los protocolos de uso compartido de archivos determinan lo siguiente:

- Caracteres que puede utilizar un nombre de archivo
- Distinción entre mayúsculas y minúsculas de un nombre de archivo

ONTAP admite caracteres de varios bytes en nombres de archivos, directorios y qtrees, según la versión de ONTAP.

Caracteres que puede utilizar un nombre de archivo o directorio

Si accede a un archivo o directorio desde clientes con sistemas operativos diferentes, debe utilizar caracteres válidos en ambos sistemas operativos.

Por ejemplo, si utiliza UNIX para crear un archivo o directorio, no utilice dos puntos (:) en el nombre porque no se permiten dos puntos en los nombres de archivos o directorios de MS-dos. Debido a que las restricciones de caracteres válidos varían de un sistema operativo a otro, consulte la documentación del sistema operativo cliente para obtener más información acerca de los caracteres prohibidos.

Distinción entre mayúsculas y minúsculas de nombres de archivos y directorios en un entorno multiprotocolo

Los nombres de archivo y directorio distinguen mayúsculas y minúsculas para los clientes NFS y no distinguen entre mayúsculas y minúsculas, pero sí lo hacen para los clientes SMB. Debe comprender las implicaciones que tiene en un entorno multiprotocolo y las acciones que podría tener que tomar al especificar la ruta al crear recursos compartidos de SMB y al acceder a datos dentro de los recursos compartidos.

Si un cliente SMB crea un directorio llamado `testdir`, Tanto los clientes SMB como NFS muestran el nombre de archivo como `testdir`. Sin embargo, si un usuario SMB posteriormente intenta crear un nombre de directorio `TESTDIR`, El nombre no está permitido porque, para el cliente SMB, ese nombre existe actualmente. Si un usuario NFS crea más adelante un directorio llamado `TESTDIR`, Los clientes NFS y SMB muestran el nombre del directorio de forma diferente, de la siguiente manera:

- En los clientes NFS, se ven los dos nombres de directorio tal como se crearon, por ejemplo `testdir` y `TESTDIR`, porque los nombres de directorio distinguen entre mayúsculas y minúsculas.
- Los clientes SMB utilizan los nombres 8.3 para distinguir entre los dos directorios. Un directorio tiene el nombre del archivo base. A directorios adicionales se les asigna un nombre de archivo 8.3.
 - En los clientes SMB, consulte `testdir` y `TESTDI~1`.
 - ONTAP creará el `TESTDI~1` nombre de directorio para diferenciar los dos directorios.

En este caso, debe usar el nombre 8.3 al especificar una ruta de recurso compartido mientras crea o modifica un recurso compartido en una máquina virtual de almacenamiento (SVM).

Del mismo modo para los archivos, si un cliente SMB crea `test.txt`, Tanto los clientes SMB como NFS muestran el nombre de archivo como `test.txt`. Sin embargo, si un usuario SMB posteriormente intenta crear `Test.txt`, El nombre no está permitido porque, para el cliente SMB, ese nombre existe actualmente. Si más adelante un usuario NFS crea un archivo llamado `Test.txt`, Los clientes NFS y SMB muestran el nombre del archivo de forma diferente, de la siguiente manera:

- En los clientes NFS, se ven los dos nombres de archivo tal como se crearon, `test.txt` y `Test.txt`, porque los nombres de archivo distinguen entre mayúsculas y minúsculas.
- Los clientes SMB utilizan los nombres 8.3 para distinguir entre los dos archivos. Un archivo tiene el nombre del archivo base. Se asigna un nombre de archivo 8.3 a archivos adicionales.
 - En los clientes SMB, consulte `test.txt` y `TEST~1.TXT`.
 - ONTAP creará el `TEST~1.TXT` nombre de archivo para diferenciar los dos archivos.



Si ha habilitado o modificado la asignación de caracteres mediante los comandos de asignación de caracteres CIFS del Vserver, una búsqueda de Windows normalmente no distingue mayúsculas y minúsculas se convierte en sensible a mayúsculas y minúsculas.

Cómo crea ONTAP nombres de archivos y directorios

ONTAP crea y mantiene dos nombres para archivos o directorios en cualquier directorio que tenga acceso desde un cliente SMB: El nombre largo original y un nombre en formato 8.3.

Para los nombres de archivos o directorios que excedan el nombre de ocho caracteres o el límite de extensión de tres caracteres (para archivos), ONTAP genera un nombre de formato de 8.3 de la siguiente manera:

- Trunca el nombre del archivo o directorio original a seis caracteres, si el nombre supera los seis.
- Agrega una tilde (~) y un número, de uno a cinco, a los nombres de archivo o directorio que ya no son únicos después de truncarse.

Si se queda sin números porque hay más de cinco nombres similares, crea un nombre único que no tiene relación con el nombre original.

- En el caso de los archivos, trunca la extensión del nombre de archivo a tres caracteres.

Por ejemplo, si un cliente NFS crea un archivo llamado `specifications.html`, El nombre de archivo de formato 8.3 creado por ONTAP es `specif~1.htm`. Si este nombre ya existe, ONTAP utiliza un número diferente al final del nombre de archivo. Por ejemplo, si un cliente NFS crea otro archivo llamado `specifications_new.html`, el formato 8.3 de `specifications_new.html` es `specif~2.htm`.

Cómo maneja ONTAP los nombres de archivos, directorios y qtrees de varios bytes

A partir de ONTAP 9.5, la compatibilidad con nombres codificados UTF-8 de 4 bytes permite la creación y visualización de nombres de archivos, directorios y árboles que incluyen caracteres complementarios Unicode fuera del plano multilingüe básico (BMP). En las versiones anteriores, estos caracteres complementarios no se mostraba correctamente en entornos multiprotocolo.

Para habilitar la compatibilidad con nombres codificados UTF-8 de 4 bytes, hay disponible un nuevo código de idioma *utf8mb4* para *vserver* y.. *volume* familias de comando.

Debe crear un nuevo volumen de una de las siguientes maneras:

- Configuración del volumen `-language` opción explícitamente: `volume create -language utf8mb4 {...}`
- Heredar el volumen `-language` Opción de una SVM que se ha creado con la opción o que se ha modificado para ella: `vserver [create|modify] -language utf8mb4 {...}``volume create {...}`
- En ONTAP 9,6 y versiones anteriores, no puede modificar los volúmenes existentes para la compatibilidad con *utf8mb4*. Debe crear un volumen listo para *utf8mb4* y después migrar los datos con las herramientas de copia basadas en cliente.

Puede actualizar las SVM para que admitan *utf8mb4*, pero los volúmenes existentes conservan sus códigos de idioma originales.

Si utiliza ONTAP 9.7P1 o una versión posterior, puede modificar los volúmenes existentes para *utf8mb4* con una solicitud de soporte. Para obtener más información, consulte "[¿Se puede cambiar el idioma del volumen después de crearlo en ONTAP?](#)".

- A partir de ONTAP 9,8, puede utilizar el `[-language <Language code>]` Parámetro para cambiar el idioma del volumen de *.*utf-8* a *utf8mb4*. Para cambiar el idioma de un volumen, póngase en contacto con "[Soporte de NetApp](#)".



Los nombres de las LUN con caracteres UTF-8 de 4 bytes no se admiten actualmente.

- Los datos de caracteres Unicode se suelen representar en aplicaciones de sistemas de archivos Windows que utilizan el formato de transformación Unicode de 16 bits (UTF-16) y en sistemas de archivos NFS que utilizan el formato de transformación Unicode de 8 bits (UTF-8).

En las versiones anteriores a ONTAP 9.5, los nombres incluidos los caracteres complementarios UTF-16 creados por los clientes de Windows se mostraban correctamente a otros clientes de Windows pero no se tradujeron correctamente a UTF-8 para los clientes NFS. Del mismo modo, los nombres con caracteres complementarios UTF-8 de los clientes NFS creados no se tradujeron correctamente a UTF-16 para los clientes Windows.

- Cuando se crean nombres de archivo en sistemas que ejecutan ONTAP 9.4 o una versión anterior que contienen caracteres complementarios válidos o no válidos, ONTAP rechaza el nombre de archivo y devuelve un error de nombre de archivo no válido.

Para evitar este problema, utilice sólo los caracteres BMP en los nombres de archivo y evite utilizar caracteres complementarios, o actualice a ONTAP 9.5 o posterior.

A partir de ONTAP 9, se permiten caracteres Unicode en nombres de qtree.

- Puede utilizar cualquiera de los dos `volume qtree` Familia de comandos o System Manager para establecer o modificar los nombres de qtree.
- Los nombres de qtree pueden incluir caracteres de varios bytes en formato Unicode, como los caracteres japoneses y chinos.
- En versiones anteriores a ONTAP 9.5, sólo se admiten los caracteres BMP (es decir, los que podrían representarse en 3 bytes).



En las versiones anteriores a ONTAP 9.5, la ruta de unión del volumen principal del qtree puede contener nombres de qtree y directorio con caracteres Unicode. La `volume show` El comando muestra estos nombres correctamente cuando el volumen primario tiene una configuración de idioma UTF-8. Sin embargo, si el idioma del volumen principal no es uno de los valores de idioma UTF-8, algunas partes de la ruta de unión se muestran utilizando un nombre NFS alternativo numérico.

- En las versiones 9.5 y posteriores, se admiten caracteres de 4 bytes en nombres de qtree, siempre y cuando el qtree se encuentre en un volumen habilitado para utf8mb4.

Configurar la asignación de caracteres para la traducción de nombres de archivo SMB en volúmenes

Los clientes NFS pueden crear nombres de archivo que contengan caracteres que no son válidos para los clientes SMB y ciertas aplicaciones Windows. Puede configurar la asignación de caracteres para la traducción de nombres de archivo en volúmenes para permitir que los clientes SMB accedan a archivos con nombres NFS que, de lo contrario, no serían válidos.

Acerca de esta tarea

Cuando los clientes SMB acceden a los archivos creados por los clientes NFS, ONTAP observa el nombre del archivo. Si el nombre no es un nombre de archivo SMB válido (por ejemplo, si tiene un carácter ":" incrustado en dos puntos), ONTAP devuelve el nombre de archivo 8.3 que se mantiene para cada archivo. Sin embargo, esto causa problemas para las aplicaciones que codifican información importante en nombres de archivos largos.

Por lo tanto, si comparte un archivo entre clientes en diferentes sistemas operativos, debe utilizar caracteres en los nombres de archivo válidos en ambos sistemas operativos.

Sin embargo, si tiene clientes NFS que crean nombres de archivo que contienen caracteres que no son nombres de archivo válidos para clientes SMB, puede definir un mapa que convierte los caracteres NFS no válidos en caracteres Unicode que tanto SMB como determinadas aplicaciones Windows aceptan. Por ejemplo, esta funcionalidad admite las aplicaciones CATIA MCAD y Mathematica, así como otras aplicaciones que tienen este requisito.

Puede configurar la asignación de caracteres de volumen a volumen.

Debe tener en cuenta lo siguiente al configurar la asignación de caracteres en un volumen:

- La asignación de caracteres no se aplica a través de puntos de unión.

Debe configurar explícitamente la asignación de caracteres para cada volumen de unión.

- Debe asegurarse de que los caracteres Unicode que se utilizan para representar caracteres no válidos o

ilegales son caracteres que normalmente no aparecen en los nombres de archivo; de lo contrario, se producen asignaciones no deseadas.

Por ejemplo, si intenta asignar dos puntos (:) a un guión (-) pero el guión (-) se utilizó correctamente en el nombre del archivo, un cliente de Windows que intente acceder a un archivo denominado «'a-b'» tendría su solicitud asignada al nombre NFS de «'a:b'» (no al resultado deseado).

- Después de aplicar la asignación de caracteres, si la asignación aún contiene un carácter de Windows no válido, ONTAP vuelve a los nombres de archivo de Windows 8.3.
- En las notificaciones de FPolicy, los registros de auditoría de NAS y los mensajes de seguimiento de seguridad, se muestran los nombres de archivos asignados.
- Cuando se crea una relación de SnapMirror del tipo DP, la asignación de caracteres del volumen de origen no se replica en el volumen de DP de destino.
- Distinción entre mayúsculas y minúsculas: Debido a que los nombres de Windows asignados se convierten en nombres NFS, la búsqueda de los nombres sigue a la semántica NFS. Esto incluye el hecho de que las búsquedas de NFS distinguen mayúsculas de minúsculas. Esto significa que las aplicaciones que acceden a recursos compartidos asignados no deben depender de un comportamiento que no distingue mayúsculas y minúsculas de Windows. Sin embargo, el nombre 8.3 está disponible y no distingue mayúsculas y minúsculas.
- Asignaciones parciales o no válidas: Tras asignar un nombre para devolver a los clientes que realizan enumeración de directorios ("dir"), se comprueba la validez de Windows en el nombre Unicode resultante. Si ese nombre sigue teniendo caracteres no válidos, o si no es válido para Windows (p. ej., finaliza en "" o en blanco) se devuelve el nombre 8.3 en lugar del nombre no válido.

Paso

1. Configurar asignación de caracteres: +

```
vserver cifs character-mapping create -vserver vserver_name -volume volume_name  
-mapping mapping_text, ... +
```

El mapeo consta de una lista de pares de caracteres fuente-objetivo separados por ":". Los caracteres son caracteres Unicode introducidos mediante dígitos hexadecimales. Por ejemplo: 3C:E03C. +

El primer valor de cada uno mapping_text El par separado por dos puntos es el valor hexadecimal del carácter NFS que desea traducir y el segundo valor es el valor Unicode que utiliza SMB. Las parejas de asignación deben ser únicas (debe existir una asignación uno a uno).

- Asignación de fuentes +

La siguiente tabla muestra el conjunto de caracteres Unicode permisible para la asignación de origen:

+

| Carácter Unicode | Carácter impreso | Descripción |
|------------------|------------------|--|
| 0x01-0x19 | No aplicable | Caracteres de control que no se imprimen |
| 0x5c | | Barra invertida |
| 0x3A | : | Dos puntos |

| Carácter Unicode | Carácter impreso | Descripción |
|------------------|------------------|------------------------|
| 0x2A | * | Asterisco |
| 0x3f | ? | Signo de interrogación |
| 0x22 | " | Entre comillas |
| 0x3C | < | Menor que |
| 0x3E | > | Mayor que |
| 0x7C | | |
| Línea vertical | 0xB1 | ± |

- Asignación de objetivos

Puede especificar caracteres de destino en el "Área de uso privado" de Unicode en el siguiente intervalo: U+E0000...U+F8FF.

Ejemplo

El siguiente comando crea una asignación de caracteres para un volumen denominado «data» en la máquina virtual de almacenamiento (SVM) vs1:

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show
```

| Vserver | Volume Name | Character Mapping |
|---------|-------------|---------------------------|
| vs1 | data | 3c:e17c, 3e:f17d, 2a:f745 |

Información relacionada

[Crear y gestionar volúmenes de datos en espacios de nombres NAS](#)

Comandos para administrar las asignaciones de caracteres para la traducción de nombres de archivo SMB

Puede gestionar la asignación de caracteres creando, modificando, mostrando información o eliminando asignaciones de caracteres de archivo utilizadas para la traducción del nombre del archivo SMB en volúmenes FlexVol.

| Si desea... | Se usa este comando... |
|---|--|
| Cree nuevas asignaciones de caracteres de archivo | <code>vserver cifs character-mapping create</code> |

| Si desea... | Se usa este comando... |
|---|--|
| Mostrar información acerca de las asignaciones de caracteres de archivo | <code>vserver cifs character-mapping show</code> |
| Modifique las asignaciones de caracteres de archivo existentes | <code>vserver cifs character-mapping modify</code> |
| Eliminar asignaciones de caracteres de archivo | <code>vserver cifs character-mapping delete</code> |

Para obtener más información, consulte la página de manual de cada comando.

Información relacionada

[Configuración de la asignación de caracteres para la traducción de nombres de archivo SMB en volúmenes](#)

Proporcione acceso del cliente S3 a los datos NAS

Información general sobre multiprotocolo de S3

A partir de ONTAP 9.12.1, puede permitir que los clientes que ejecutan el protocolo S3 accedan a los mismos datos que los clientes que utilizan los protocolos NFS y SMB sin necesidad de volver a formatear. Esta funcionalidad permite seguir proporcionando datos de NAS a los clientes NAS, a la vez que presenta datos de objetos a clientes S3 que ejecutan aplicaciones S3 (como la minería de datos y la inteligencia artificial).

La funcionalidad multiprotocolo de S3 aborda dos casos prácticos:

1. Acceso a los datos NAS existentes mediante clientes S3

Si sus datos existentes se crearon con clientes NAS tradicionales (NFS o SMB) y están ubicados en volúmenes NAS (volúmenes FlexVol o FlexGroup), ahora puede utilizar herramientas de análisis en clientes S3 para acceder a estos datos.

2. Almacenamiento back-end para clientes modernos capaces de realizar I/O mediante protocolos NAS y S3

Ahora puede proporcionar acceso integrado para aplicaciones como Spark y Kafka que pueden leer y escribir los mismos datos utilizando los protocolos NAS y S3.

Cómo funciona el protocolo de S3

El protocolo multiprotocolo de ONTAP le permite presentar el mismo conjunto de datos que una jerarquía de archivos o como objetos en un bloque. Para ello, ONTAP crea “bloques NAS de S3” que permiten a los clientes de S3 crear, leer, eliminar y enumerar archivos en un almacenamiento NAS usando solicitudes de objetos de S3. Esta asignación se ajusta a la configuración de seguridad NAS, observando los permisos de acceso a archivos y directorios, así como escribiendo en la pista de auditoría de seguridad según sea necesario.

Esta asignación se logra presentando una jerarquía de directorios NAS especificada como bloque de S3. Cada archivo de la jerarquía de directorio se representa como un objeto S3 cuyo nombre es relativo del directorio asignado hacia abajo, con límites de directorio representados por el carácter de barra diagonal ("/").

Los usuarios normales de S3 definidos por ONTAP pueden acceder a este almacenamiento, según lo establecido por las políticas de bloque definidas para el bloque que se asigna al directorio NAS. Para que esto sea posible, deben definirse las asignaciones entre los usuarios de S3 y los usuarios SMB/NFS. Las credenciales del usuario SMB/NFS se utilizarán para la comprobación de permisos NAS y se incluirán en los registros de auditoría resultantes de estos accesos.

Cuando los clientes SMB o NFS lo crean, un archivo se coloca inmediatamente en un directorio y, por lo tanto, es visible para los clientes antes de escribir ningún dato en él. Los clientes S3 esperan una semántica diferente, en la que el nuevo objeto no esté visible en el espacio de nombres hasta que todos sus datos se hayan escrito. Esta asignación de S3 a almacenamiento NAS crea archivos mediante la semántica de S3, y mantiene los archivos invisibles de forma externa hasta que finaliza el comando de creación de S3.

Protección de datos para bloques NAS de S3

Los “bloques” NAS de S3 son simplemente asignaciones de datos NAS para clientes de S3, no son bloques S3 estándar. Por lo tanto, no es necesario proteger los bloques NAS de S3 utilizando la funcionalidad SnapMirror de NetApp S3. En su lugar, puede proteger los volúmenes que contienen buckets NAS de S3 GB mediante la replicación de volúmenes de SnapMirror asíncrona. No se admite la recuperación ante desastres de SnapMirror Synchronous ni SVM.

A partir de la versión 9.14.1 de ONTAP, los buckets NAS de S3 se admiten en agregados reflejados y no reflejados para las configuraciones de MetroCluster IP y FC.

Descubra ["SnapMirror asíncrono"](#).

Auditoría de bloques NAS de S3

Dado que los bloques NAS de S3 no son bloques S3 convencionales, la auditoría de S3 no se puede configurar para auditar el acceso entre ellos. Más información acerca de ["Auditoría de S3"](#).

No obstante, los archivos y directorios NAS que se asignan en bloques NAS de S3 pueden auditarse para eventos de acceso mediante procedimientos de auditoría ONTAP convencionales. Por lo tanto, las operaciones de S3 pueden activar eventos de auditoría de NAS, con las siguientes excepciones:

- Si la configuración de la política de S3 (grupo o política de bloques) deniega el acceso del cliente S3, no se inicia la auditoría de NAS para el evento. Esto se debe a que se comprueban los permisos de S3 antes de poder realizar comprobaciones de auditoría de SVM.
- Si el archivo de destino de una solicitud Get de S3 tiene un tamaño 0, se devuelve 0 contenido a la solicitud Get y el acceso de lectura no se registra.
- Si el archivo de destino de una solicitud Get de S3 se encuentra en una carpeta para la que el usuario no tiene permisos de recorrido, el intento de acceso falla y el evento no se registra.

Descubra ["Auditoría de eventos NAS en SVM"](#).

Interoperabilidad con S3 y NAS

Los bloques NAS de ONTAP S3 admiten las funcionalidades estándar de NAS y S3, a excepción de las enumeradas aquí.

La funcionalidad NAS no es compatible actualmente con bloques NAS de S3

Nivel de capacidad de FabricPool

Los bloques NAS de S3 no pueden configurarse como nivel de capacidad para FabricPool.

La funcionalidad de S3 no admite actualmente bloques NAS de S3

Metadatos de usuario de AWS

- Los pares de clave-valor que se reciben como parte de los metadatos del usuario S3 no se almacenan en el disco junto con los datos de objetos en la versión actual.
- Se ignoran los encabezados de solicitud con el prefijo "x-amz-meta".

Etiquetas de AWS

- En las solicitudes PUT object and Multipart initiate, se ignoran los encabezados con el prefijo "x-amz-tagging".
- Las solicitudes de actualización de etiquetas en un archivo existente (es decir, solicitudes put, Get y Delete con la cadena de consulta de etiquetado) se rechazan con un error.

Creación de versiones

No es posible especificar el control de versiones en la configuración de asignación de bloques.

- Las solicitudes que incluyen especificaciones de versión no nulas (el ID de versión=cadena de consulta xyz) reciben respuestas de error.
- Las solicitudes que afectan al estado de control de versiones de un bloque se rechazan con errores.

Operaciones de varias piezas

No se admiten las siguientes operaciones:

- AbortMultipartUpload
- CompleteMultipartUpload
- CreateMultipartUpload
- ListMultipartUpload

Requisitos de datos NAS para el acceso de clientes S3

Es importante comprender que hay algunas incompatibilidades inherentes a la asignación de archivos y directorios NAS para el acceso S3. Puede que sea necesario ajustar las jerarquías de archivos NAS antes de servirles mediante bloques NAS de S3.

Un bloque NAS de S3 proporciona acceso de S3 a un directorio NAS al asignar ese directorio mediante la sintaxis de bloque de S3, y los archivos del árbol de directorios se consideran objetos. Los nombres de objeto son los nombres de ruta delimitados por barras de los archivos en relación con el directorio especificado en la configuración de bloque de S3.

Este mapa impone algunos requisitos cuando se sirven archivos y directorios mediante bloques NAS de S3:

- Los nombres de S3 están limitados a 1024 bytes, de modo que no se puede acceder a los archivos con nombres de ruta más largos mediante S3.
- Los nombres de archivo y directorio están limitados a 255 caracteres, por lo que el nombre de objeto no puede tener más de 255 caracteres consecutivos que no sean de barra ("b/")
- En su lugar, un nombre de ruta SMB delimitado por caracteres de barra diagonal inversa ('\') aparecerá en s3 como nombre de objeto que contiene caracteres de barra diagonal ('/').
- Algunas parejas de nombres de objeto S3 legales no pueden coexistir en el árbol de directorios NAS asignados. Por ejemplo, los nombres de objetos legales S3 "part1/part2" y "part1/part2/part3" se asignan a

archivos que no pueden existir simultáneamente en el árbol de directorios NAS, ya que “part1/part2” es un archivo en el nombre y un directorio en el otro.

- Si “part1/part2” es un archivo existente, una creación S3 de “part1/part2/part3” fallará.
- Si “part1/part2/part3” es un archivo existente, se producirá un error en la creación o eliminación de S3 de “part1/part2”.
- Una creación de objetos S3 que se ajuste al nombre de un objeto existente sustituye al objeto preexistente (en bloques sin versiones), que se conserva en NAS pero requiere una coincidencia exacta. Los ejemplos anteriores no provocarán la eliminación del objeto existente porque mientras los nombres chocan, no coinciden.

Mientras que un almacén de objetos está diseñado para admitir un número muy grande de nombres arbitrarios, una estructura de directorio NAS puede experimentar problemas de rendimiento si se coloca un número muy grande de nombres en un directorio. En particular, los nombres sin caracteres de barra diagonal (“pies/”) se colocarán en el directorio raíz de la asignación NAS. Las aplicaciones que hacen un uso extensivo de nombres que no son “fáciles de usar para NAS” se hospedarían mejor en un cubo de almacén de objetos real en lugar de en un mapeo NAS.

Habilite el acceso de protocolo S3 a los datos NAS

Habilitar el acceso al protocolo S3 consiste en garantizar que una SVM habilitada para NAS cumpla los mismos requisitos que un servidor habilitado para S3, incluyendo la adición de un servidor de almacén de objetos y la verificación de los requisitos de red y autenticación.

Para nuevas instalaciones de ONTAP, es recomendable habilitar el acceso del protocolo S3 a una SVM después de configurarlo para que sirva datos NAS a los clientes. Para obtener más información sobre la configuración del protocolo NAS, consulte:

- ["Configuración de NFS"](#)
- ["Configuración de SMB"](#)

Antes de empezar

Debe configurarse lo siguiente antes de habilitar el protocolo S3:

- Se obtiene una licencia para el protocolo S3 y los protocolos NAS deseados, NFS, SMB o ambos.
- Una SVM está configurada para los protocolos NAS deseados.
- Existen servidores NFS y/o SMB.
- DNS y cualquier otro servicio requerido están configurados.
- Los datos NAS se exportan o comparten a sistemas cliente.

Acerca de esta tarea

Se requiere un certificado de la entidad de certificación (CA) para habilitar el tráfico HTTPS desde clientes S3 a la SVM habilitada para S3. Se pueden utilizar certificados DE CA de tres orígenes:


- Un nuevo certificado autofirmado de ONTAP en la SVM.
- Un certificado autofirmado existente de ONTAP en la SVM.
- Un certificado de terceros.

Puede usar las mismas LIF de datos para el bloque de S3/NAS que utilizará para servir datos NAS. Si se

requieren direcciones IP específicas, consulte ["Cree LIF de datos"](#). Es necesario aplicar una política de datos de servicio de S3 para habilitar el tráfico de datos S3 en las LIF; puede modificar la política de servicio existente de la SVM para incluir S3.

Cuando crea el servidor de objetos S3, debe estar preparado para introducir el nombre del servidor S3 como un nombre de dominio completo (FQDN), que los clientes utilizarán para el acceso S3. El FQDN del servidor S3 no debe comenzar por un nombre de bloque.

System Manager

1. Active S3 en una máquina virtual de almacenamiento con protocolos NAS configurados.
 - a. Haga clic en **almacenamiento > Storage VMs**, seleccione una VM de almacenamiento preparada para NAS, haga clic en Configuración y, a continuación, haga clic en  En S3.
 - b. Seleccione el tipo de certificado. Tanto si selecciona un certificado generado por el sistema como uno propio, será necesario para el acceso de los clientes.
 - c. Introduzca las interfaces de red.
2. Si seleccionó el certificado generado por el sistema, la información del certificado se muestra cuando se confirma la creación de la máquina virtual de almacenamiento nueva. Haga clic en **Descargar** y guárdelo para acceder a los clientes.
 - La clave secreta no se volverá a mostrar.
 - Si necesita de nuevo la información del certificado: Haga clic en **almacenamiento > Storage VMs**, seleccione la VM de almacenamiento y haga clic en **Configuración**.

CLI

1. Compruebe que el protocolo S3 esté permitido en la SVM:
`vserver show -fields allowed-protocols`
2. Registre el certificado de clave pública de esta SVM.
Si se necesita un certificado autofirmado ONTAP nuevo, consulte ["Cree e instale un certificado de CA en la SVM"](#).
3. Actualizar la política de datos de servicio
 - a. Mostrar la política de datos de servicio para la SVM
`network interface service-policy show -vserver svm_name`
 - b. Añada el data-core y.. data-s3-server services si no están presentes.
`network interface service-policy add-service -vserver svm_name -policy policy_name -services data-core,data-s3-server`
4. Compruebe que las LIF de datos de la SVM cumplen con sus requisitos:
`network interface show -vserver svm_name`
5. Cree el servidor S3:
`vserver object-store-server create -vserver svm_name -object-store-server s3_server_fqdn -certificate-name ca_cert_name -comment text [additional_options]`

Puede especificar opciones adicionales al crear el servidor S3 o en cualquier momento posterior.

- De forma predeterminada, HTTPS está habilitado en el puerto 443. Puede cambiar el número de puerto con la opción `-secure-listener-Port`.
Cuando HTTPS está habilitado, se requieren certificados de CA para una integración correcta con SSL/TLS.
- HTTP está desactivado de forma predeterminada; cuando está habilitado, el servidor escucha en el puerto 80. Puede activarlo con la opción `-is-http-enabled` o cambiar el número de puerto con la opción `-listener-Port`.
Cuando HTTP está activado, todas las solicitudes y respuestas se envían a través de la red en texto no cifrado.
 1. Compruebe que S3 esté configurado como se desee:

```
vserver object-store-server show
```

Ejemplo

El siguiente comando verifica los valores de configuración de todos los servidores de almacenamiento de objetos:

```
cluster1::> vserver object-store-server show
```

```
Vserver: vs1
```

```
Object Store Server Name: s3.example.com
Administrative State: up
Listener Port For HTTP: 80
Secure Listener Port For HTTPS: 443
HTTP Enabled: false
HTTPS Enabled: true
Certificate for HTTPS Connections: svml_ca
Comment: Server comment
```

Crear bloque NAS de S3

Un bloque NAS de S3 es una asignación entre un nombre de bloque de S3 y una ruta NAS. Los bloques NAS de S3 le permiten proporcionar acceso S3 a cualquier parte de un espacio de nombres de SVM que tenga volúmenes y estructura de directorio existentes.

Antes de empezar

- Un servidor de objetos S3 está configurado en una SVM que contiene datos NAS.
- Los datos NAS se ajustan a la ["Requisitos para el acceso de clientes S3"](#).

Acerca de esta tarea

Puede configurar cubos NAS de S3 para especificar cualquier conjunto de archivos y directorios dentro del directorio raíz de la SVM.

También puede establecer políticas de bloques que permitan o in permitan el acceso a datos NAS en función de cualquier combinación de estos parámetros:

- Archivos y directorios
- Permisos de usuario y grupo
- Operaciones de S3

Por ejemplo, es posible que desee aplicar políticas de bloque independientes que concedan acceso de solo lectura a un gran grupo de usuarios y otro que permita que un grupo limitado realice operaciones en un subconjunto de dichos datos.

Como los "bloques" NAS de S3 son asignaciones y no bloques de S3, las siguientes propiedades de los bloques estándar de S3 no se aplican a los bloques NAS de S3.

- **aggr-list \ aggr-list-multiplier \ storage-service-level \ volume \ size \ exclude-aggr-list \ qos-policy-group**
No se crean volúmenes o qtree al configurar buckets NAS de S3.
- **el rol \ está -protegido \ es -protected-on-ontap \ es -protected-on-cloud**
Los buckets NAS de S3 no se protegen ni duplican con SnapMirror de S3 TB, sino que se utilizarán protección SnapMirror normal disponible con granularidad de volumen.
- **versioning-state**
Los volúmenes NAS suelen tener tecnología Snapshot para guardar diferentes versiones. Sin embargo, el control de versiones no está disponible actualmente en bloques NAS de S3.
- **lógico-usado \ object-count**
Existen estadísticas equivalentes disponibles para los volúmenes NAS mediante los comandos de volumen.

System Manager

Añada un nuevo bloque NAS de S3 en una máquina virtual de almacenamiento compatible con NAS.

1. Haga clic en **almacenamiento > Cuchos** y, a continuación, haga clic en **Agregar**.
2. Introduzca un nombre para el bloque NAS de S3 y seleccione la máquina virtual de almacenamiento, no introduzca un tamaño y, a continuación, haga clic en **más opciones**.
3. Introduzca un nombre de ruta válido o haga clic en examinar para seleccionar de una lista de nombres de ruta válidos.
Al introducir un nombre de ruta válido, se ocultan las opciones que no son relevantes para la configuración de S3 NAS.
4. Si ya ha asignado usuarios S3 a usuarios NAS y ha creado grupos, puede configurar sus permisos y, a continuación, hacer clic en **Guardar**.
Debe haber asignado usuarios de S3 a usuarios NAS antes de configurar permisos en este paso.

De lo contrario, haga clic en **Guardar** para completar la configuración de bloque NAS S3.

CLI

Cree un bloque NAS S3 en una SVM que contenga sistemas de archivos NAS.

```
vserver object-store-server bucket create -vserver svm_name -bucket
bucket_name -type nas -nas-path junction_path [-comment text]
```

Ejemplo:

```
cluster1::> vserver object-store-server bucket create -bucket testbucket -type
nas -path /vol1
```

Habilite los usuarios de cliente S3

Para permitir que los usuarios del cliente S3 accedan a datos NAS, debe asignar nombres de usuario S3 a los usuarios NAS correspondientes y conceder permiso para acceder a los datos de NAS mediante políticas de servicio de bucket.

Antes de empezar

Los nombres de usuario para el acceso de clientes: Usuarios de clientes LINUX/UNIX, Windows y S3 ya deben existir.

Acerca de esta tarea

La asignación de un nombre de usuario de S3 a un usuario de LINUX/UNIX o Windows correspondiente permite que las comprobaciones de autorización de los archivos NAS se honren cuando los clientes de S3 accedan a ellos. Las asignaciones de S3 a NAS se especifican proporcionando un nombre de usuario de S3 *Pattern*, que puede expresarse como un único nombre o una expresión regular POSIX, y un nombre de usuario de LINUX/UNIX o Windows *Replacement*.

En caso de que no exista ninguna asignación de nombres, se utilizará la asignación de nombres predeterminada, donde se utilizará el propio nombre de usuario de S3 como nombre de usuario UNIX y nombre de usuario de Windows. Puede modificar las asignaciones de nombres de usuario predeterminados de UNIX y Windows con el `vserver object-store-server modify` comando.

Solo se admite la configuración de asignación de nombres local; no se admite LDAP.

Después de asignar usuarios de S3 a usuarios NAS, puede conceder permisos a los usuarios especificando los recursos (directorios y archivos) a los que tienen acceso y las acciones a las que se les permiten o no ejecutar allí.

System Manager

1. Cree asignaciones de nombres locales para clientes UNIX o Windows (o ambos).
 - a. Haga clic en **almacenamiento > Cuchos** y seleccione la VM de almacenamiento habilitada para S3/NAS.
 - b. Seleccione **Configuración** y, a continuación, haga clic en → En **asignación de nombres** (en **usuarios y grupos de host**).
 - c. En los mosaicos de **S3 a Windows** o **S3 a UNIX** (o ambos), haga clic en **Agregar** y, a continuación, introduzca los nombres de usuario de **patrón** (S3) y **reemplazo** (NAS) que desee.
2. Cree una política de bloques para proporcionar acceso de cliente.
 - a. Haga clic en **almacenamiento > Cuchos**, haga clic en ⓘ Junto al bloque S3 deseado, haga clic en **Editar**.
 - b. Haga clic en **Agregar** y proporcione los valores deseados.
 - **Principal:** Proporcione nombres de usuario S3 o utilice los valores predeterminados (todos los usuarios).
 - **Efecto:** Seleccione **permitir** o **Denegar**.
 - **Acciones:** Introduzca acciones para estos usuarios y recursos. El conjunto de operaciones de recursos que el servidor de almacén de objetos admite actualmente para los cubos NAS de S3 es: `GetObject`, `PutObject`, `DeleteObject`, `ListBucket`, `GetBucketAcl`, `GetObjectAcl`, `GetObjectTagging`, `PutObjectTagging`, `DeleteObjectTagging`, `GetBucketLocation`, `GetBucketVersioning`, `PutBucketVersioning` y `ListBucketVersions`. Se aceptan caracteres comodín para este parámetro.
 - **Recursos:** Introduzca las rutas de acceso a carpetas o archivos en las que se permiten o deniegan las acciones, o utilice los valores predeterminados (directorio raíz del bloque).

CLI

1. Cree asignaciones de nombres locales para clientes UNIX o Windows (o ambos).

```
vserver name-mapping create -vserver svm_name> -direction {s3-win|s3-unix}  
-position integer -pattern s3_user_name -replacement nas_user_name
```

 - `-position` - número de prioridad para la evaluación de mapas; escriba 1 o 2.
 - `-pattern` - Un nombre de usuario S3 o una expresión regular
 - `-replacement` - un nombre de usuario de windows o unix

Ejemplos

```
vserver name-mapping create -direction s3-win -position 1 -pattern s3_user_1  
-replacement win_user_1  
vserver name-mapping create -direction s3-unix -position 2 -pattern s3_user_1  
-replacement unix_user_1
```

1. Cree una política de bloques para proporcionar acceso de cliente.

```
vserver object-store-server bucket policy add-statement -vserver svm_name  
-bucket bucket_name -effect {deny|allow} -action list_of_actions -principal  
list_of_users_or_groups -resource [-sid alphanumeric_text]
```

 - `-effect {deny|allow}` - especifica si se permite o deniega el acceso cuando un usuario solicita una acción.

- `-action <Action>, ...` - especifica las operaciones de recursos que se permiten o se deniegan. El conjunto de operaciones de recursos que el servidor de almacén de objetos admite actualmente para los cubos NAS de S3 es: `GetObject`, `PutObject`, `DeleteObject`, `ListBucket`, `GetBucketAcl`, `GetObjectAcl`, `GetObjectTagging`, `PutObjectTagging`, `DeleteObjectTagging`, `GetBucketLocation`, `GetBucketVersioning`, `PutBucketVersioning` y `ListBucketVersions`. Se aceptan caracteres comodín para este parámetro.
- `-principal <Objectstore Principal>, ...` - valida el usuario que solicita acceso a los usuarios o grupos del servidor del almacén de objetos especificados en este parámetro.
 - Un grupo de servidores de almacenes de objetos se especifica agregando un grupo de prefijos/ al nombre del grupo.
 - `-principal -` (el carácter de guión) concede acceso a todos los usuarios.
- `-resource <text>, ...` - especifica el bloque, carpeta u objeto para el que se han establecido permisos permitir/denegar. Se aceptan caracteres comodín para este parámetro.
- `[-sid <SID>]` - especifica un comentario de texto opcional para la sentencia de política de bloque de servidor del almacén de objetos.

Ejemplos

```
cluster1::> vsriver object-store-server bucket policy add-statement -bucket
testbucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,
GetBucketLocation,GetBucketPolicy,PutBucketPolicy,DeleteBucketPolicy
-principal user1 -resource testbucket,testbucket/* sid "FullAccessForUser1"

cluster1::> vsriver object-store-server bucket policy statement create
-vsriver vs1 -bucket bucket1 -effect allow -action GetObject -principal -
-resource bucket1/readme/* -sid "ReadAccessToReadmeForAllUsers"
```

Configuración de SMB para Microsoft Hyper-V y SQL Server

Información general de la configuración de SMB para Microsoft Hyper-V y SQL Server

Las funciones de ONTAP le permiten habilitar las operaciones no disruptivas para dos aplicaciones de Microsoft a través del protocolo SMB: Microsoft Hyper-V y Microsoft SQL Server.

Debe utilizar estos procedimientos si desea implementar operaciones no disruptivas de SMB en las siguientes circunstancias:

- Se configuró el acceso básico a archivos del protocolo SMB.
- Quiere habilitar los recursos compartidos de archivos de SMB 3.0 o posteriores que residen en SVM para almacenar los siguientes objetos:
 - Archivos de equipos virtuales Hyper-V.
 - Bases de datos del sistema SQL Server

Información relacionada

Para obtener información adicional sobre la tecnología de ONTAP e interacción con servicios externos,

consulte estos informes técnicos (TR):

"Informe técnico de NetApp 4172: Prácticas recomendadas de Microsoft Hyper-V mediante SMB 3.0 con ONTAP"

"Informe técnico de NetApp 4369: Prácticas recomendadas para Microsoft SQL Server y SnapManager 7.2 para SQL Server con Clustered Data ONTAP"

Configurar ONTAP para soluciones Microsoft Hyper-V y SQL Server sobre SMB

Puede utilizar los recursos compartidos de archivos de SMB 3.0 y versiones posteriores disponibles de forma continua para almacenar archivos de máquinas virtuales de Hyper-V o bases de datos de sistemas de SQL Server y bases de datos de usuario en volúmenes que residen en SVM, al tiempo que ofrece operaciones no disruptivas (NDO) tanto para eventos planificados como no planificados.

Microsoft Hyper-V mediante SMB

Para crear una solución Hyper-V mediante SMB, primero debe configurar ONTAP para proporcionar servicios de almacenamiento para servidores de Microsoft Hyper-V. Además, también debe configurar clústeres de Microsoft (si se utiliza una configuración en clúster), servidores Hyper-V, conexiones SMB 3.0 disponibles de forma continua a los recursos compartidos alojados en el servidor CIFS y, opcionalmente, servicios de backup para proteger los archivos de máquina virtual almacenados en volúmenes de SVM.



Los servidores de Hyper-V deben estar configurados en Windows 2012 Server o una versión posterior. Se admiten tanto configuraciones independientes como de servidores de Hyper-V en cluster.

- Para obtener información sobre cómo crear clústeres de Microsoft y servidores Hyper-V, consulte el sitio web de Microsoft.
- SnapManager para Hyper-V es una aplicación basada en host que facilita los servicios de backup rápidos basados en copias de Snapshot, diseñados para integrarse con configuraciones de Hyper-V mediante SMB.

Para obtener información acerca del uso de SnapManager con configuraciones de Hyper-V mediante SMB, consulte *SnapManager para Hyper-V Guía de instalación y administración*.

Microsoft SQL Server sobre SMB

Para crear una solución SQL Server con SMB, primero debe configurar ONTAP para proporcionar servicios de almacenamiento para la aplicación Microsoft SQL Server. Además, también debe configurar clústeres de Microsoft (si se utiliza una configuración en clúster). A continuación, debe instalar y configurar SQL Server en los servidores Windows y crear conexiones SMB 3.0 disponibles de forma continua con los recursos compartidos alojados en el servidor CIFS. De manera opcional, es posible configurar los servicios de backup para proteger los archivos de base de datos que están almacenados en volúmenes de SVM.



SQL Server debe estar instalado y configurado en Windows 2012 Server o posterior. Se admiten tanto configuraciones independientes como en cluster.

- Para obtener información acerca de cómo crear clústeres de Microsoft e instalar y configurar SQL Server, consulte el sitio Web de Microsoft.
- El plugin de SnapCenter para Microsoft SQL Server es una aplicación basada en host que facilita los servicios de backup rápidos basados en copias de Snapshot, diseñados para integrarse con

configuraciones de SQL Server en SMB.

Para obtener información sobre cómo utilizar el plugin de SnapCenter para Microsoft SQL Server, consulte ["Plugin de SnapCenter para Microsoft SQL Server"](#) documentar.

Operaciones no disruptivas para Hyper-V y SQL Server sobre SMB

¿Qué significan las operaciones no disruptivas para Hyper-V y SQL Server sobre SMB

Las operaciones no disruptivas para Hyper-V y SQL Server en SMB se refieren a la combinación de funcionalidades que permiten que los servidores de aplicaciones y las máquinas virtuales o bases de datos contenidos permanezcan en línea y proporcionen una disponibilidad continua durante muchas tareas administrativas. Esto incluye tanto los tiempos de inactividad previstos como imprevistos de la infraestructura de almacenamiento.

Las operaciones no disruptivas compatibles con servidores de aplicaciones en SMB incluyen lo siguiente:

- Toma de control y retorno al nodo primario planificados
- Respaldo no planificado
- Renovar
- Reubicación planificada de agregados (ARL)
- Migración LIF y recuperación tras fallos
- Movimiento de volumen planificado

Protocolos que permiten las operaciones no disruptivas en SMB

Junto con el lanzamiento de SMB 3.0, Microsoft ha lanzado nuevos protocolos para proporcionar las funcionalidades necesarias para admitir operaciones no disruptivas para Hyper-V y SQL Server sobre SMB.

ONTAP usa estos protocolos cuando proporciona operaciones no disruptivas a los servidores de aplicaciones a través de SMB:

- SMB 3,0
- Testigo

Conceptos clave sobre las operaciones no disruptivas de Hyper-V y SQL Server sobre SMB

Hay ciertos conceptos sobre las operaciones no disruptivas (NDO) que debe comprender antes de configurar la solución Hyper-V o SQL Server sobre SMB.

- **Cuota continuamente disponible**

Un recurso compartido SMB 3.0 que tiene establecida la propiedad de recurso compartido disponible de forma continua. Los clientes que se conectan mediante recursos compartidos constantemente disponibles pueden sobrevivir a eventos disruptivos como la toma de control, la devolución y la reubicación de agregados.

- **Nodo**

Una única controladora que forma parte de un clúster. Para distinguir entre los dos nodos de un par SFO, un nodo se denomina a veces el *local node* y el otro nodo se denomina a veces el *Partner node* o *remote node*. El propietario principal del almacenamiento es el nodo local. El propietario secundario, que toma el control del almacenamiento cuando falla el propietario principal, es el nodo del partner. Cada nodo es el propietario principal de su almacenamiento y el propietario secundario para el almacenamiento de su partner.

- **Reubicación no disruptiva de agregados**

La capacidad de mover un agregado entre nodos de partner dentro de un par SFO en un clúster sin interrumpir las aplicaciones del cliente.

- **Recuperación tras fallos no disruptiva**

Consulte *takeover*.

- **Migración LIF no disruptiva**

La capacidad de realizar una migración LIF sin interrumpir las aplicaciones cliente que están conectadas al clúster a través de esa LIF. En el caso de las conexiones SMB, esto solo es posible para clientes que se conectan mediante SMB 2.0 o una versión posterior.

- **Operaciones no disruptivas**

La capacidad de realizar importantes operaciones de gestión y actualización de ONTAP, así como de resistir fallos de nodos sin interrumpir las aplicaciones cliente. Este término hace referencia a la colección de funciones de toma de control no disruptivas, actualización no disruptiva y migración en conjunto.

- **Actualización no disruptiva**

Posibilidad de actualizar el hardware o el software de los nodos sin interrumpir las aplicaciones.

- **Movimiento de volumen no disruptivo**

La capacidad de mover un volumen libremente por el clúster sin interrumpir las aplicaciones que estén utilizando el volumen. En el caso de las conexiones SMB, todas las versiones de SMB admiten movimientos de volúmenes no disruptivos.

- **Asas persistentes**

Propiedad de SMB 3.0 que permite la conexión disponible de forma continua para volver a conectarse con total transparencia al servidor CIFS en caso de desconexión. Al igual que sucede con las asas duraderas, el servidor CIFS mantiene las asas persistentes durante un período de tiempo tras la pérdida de la comunicación con el cliente conectado. Sin embargo, las asas persistentes tienen más resiliencia que las asas duraderas. Además de dar al cliente la posibilidad de recuperar el controlador en una ventana de 60 segundos después de volver a conectarse, el servidor CIFS niega el acceso a los demás clientes que soliciten acceso al archivo durante esa ventana de 60 segundos.

La información sobre las asas persistentes se refleja en el almacenamiento persistente del partner SFO, el cual permite a los clientes con asas persistentes desconectadas recuperar las asas duraderas tras un evento en el que el partner de SFO asume la propiedad del almacenamiento del nodo. Además de proporcionar operaciones no disruptivas en caso de movimiento de LIF (que gestiona mantenimiento duradero), las direcciones persistentes proporcionan operaciones no disruptivas para la toma de control, la

devolución y la reubicación de agregados.

- **Retorno SFO**

Devolver agregados a sus ubicaciones principales al recuperarse de un evento de toma de control.

- **Par SFO**

Un par de nodos cuyas controladoras están configuradas para suministrar datos entre sí si uno de los dos nodos deja de funcionar. Según el modelo del sistema, ambas controladoras pueden estar en un solo chasis o las controladoras pueden estar en chasis separados. Conocido como par de alta disponibilidad en un clúster de dos nodos.

- **Adquisición**

Proceso por el que el partner toma el control del almacenamiento cuando falla el propietario principal de ese almacenamiento. En el contexto de la OFS, la conmutación por error y la toma de control son sinónimos.

Cómo la funcionalidad SMB 3.0 admite operaciones no disruptivas en recursos compartidos de SMB

SMB 3.0 proporciona una funcionalidad crucial que permite admitir operaciones no disruptivas para Hyper-V y SQL Server en recursos compartidos SMB. Esto incluye la `continuously-available` Propiedad Share y un tipo de manejador de archivo conocido como *persistent handle* que permite a los clientes SMB reclamar el estado de apertura de archivo y restablecer de forma transparente las conexiones SMB.

Los identificadores persistentes se pueden otorgar a clientes compatibles con SMB 3.0 que se conectan a un recurso compartido con el conjunto de propiedades compartidas disponibles continuamente. Si la sesión SMB está desconectada, el servidor CIFS conserva información sobre el estado de gestión persistente. El servidor CIFS bloquea las solicitudes de otros clientes durante el periodo de 60 segundos en el que se permite al cliente reconectar, permitiendo al cliente con la gestión persistente recuperar el controlador tras una desconexión de red. Los clientes con controladores persistentes pueden volver a conectarse utilizando uno de los LIF de datos de la máquina virtual de almacenamiento (SVM), ya sea reconectando a través del mismo LIF o a través de un LIF diferente.

La reubicación, la toma de control y el retorno al nodo primario de los agregados se producen entre los pares de SFO. Para gestionar sin problemas la desconexión y reconexión de sesiones con archivos que tienen controladores persistentes, el nodo del partner mantiene una copia de toda la información del bloqueo del controlador persistente. Tanto si el evento está planificado como no planificado, el partner de SFO puede gestionar de forma no disruptiva el reconecta del controlador persistente. Con esta nueva funcionalidad, las conexiones SMB 3.0 al servidor CIFS pueden conmutar por error de forma transparente y sin interrupciones a otra LIF de datos asignada a la SVM en lo que tradicionalmente ha sido un evento disruptivo.

Aunque el uso de identificadores persistentes permite al servidor CIFS conmutar al respaldo de forma transparente en las conexiones de SMB 3.0, si un fallo provoca que la aplicación de Hyper-V conmute a otro nodo del clúster de Windows Server, el cliente no tiene forma de recuperar los controladores de archivos de estos controladores desconectados. En esta situación, los controladores de archivos en estado desconectado pueden bloquear potencialmente el acceso de la aplicación Hyper-V si se reinicia en un nodo diferente. "clúster de conmutación por error" es una parte de SMB 3.0 que aborda este escenario proporcionando un mecanismo para invalidar controladores obsoletos y en conflicto. Con este mecanismo, un clúster de Hyper-V se puede recuperar rápidamente cuando fallan los nodos del clúster de Hyper-V.

Lo que hace el protocolo de testigos para mejorar una conmutación por error transparente

El protocolo Witness proporciona funcionalidades mejoradas de recuperación tras fallos de clientes para recursos compartidos de SMB 3.0 continuamente disponibles (recursos compartidos de CA). Witness facilita una conmutación al nodo de respaldo más rápida porque evita el período de recuperación tras fallos de LIF. Notifica a los servidores de aplicaciones cuando un nodo no está disponible sin tener que esperar a que se agote el tiempo de espera de la conexión SMB 3.0.

La conmutación por error es fluida, con aplicaciones que se ejecutan en el cliente no siendo consciente de que se ha producido una conmutación por error. Si no se dispone de un testigo, las operaciones de conmutación por error siguen teniendo éxito, pero la conmutación por error sin un testigo es menos eficiente.

Es posible realizar una conmutación por error mejorada con los siguientes requisitos:

- Solo se puede utilizar con servidores CIFS compatibles con SMB 3.0 que tengan habilitada SMB 3.0.
- Los recursos compartidos deben utilizar SMB 3.0 con la propiedad compartida de disponibilidad continua establecida.
- El partner SFO del nodo al que están conectados los servidores de aplicaciones debe tener al menos una LIF de datos operativos asignada a la máquina virtual de almacenamiento (SVM) que aloja datos de los servidores de aplicaciones.



El protocolo de testigos funciona entre pares de SFO. Dado que las LIF pueden migrar a cualquier nodo del clúster, es posible que cualquier nodo deba ser el testigo de su partner SFO. El protocolo de observación no puede proporcionar una rápida conmutación por error de las conexiones SMB en un nodo determinado si la SVM que aloja datos de los servidores de aplicaciones no tiene una LIF de datos activa en el nodo del partner. Por lo tanto, cada nodo del clúster debe tener al menos una LIF de datos para cada SVM que aloje una de estas configuraciones.

- Los servidores de aplicación deben conectarse al servidor CIFS mediante el nombre del servidor CIFS que se almacena en DNS en lugar de utilizar direcciones IP de LIF individuales.

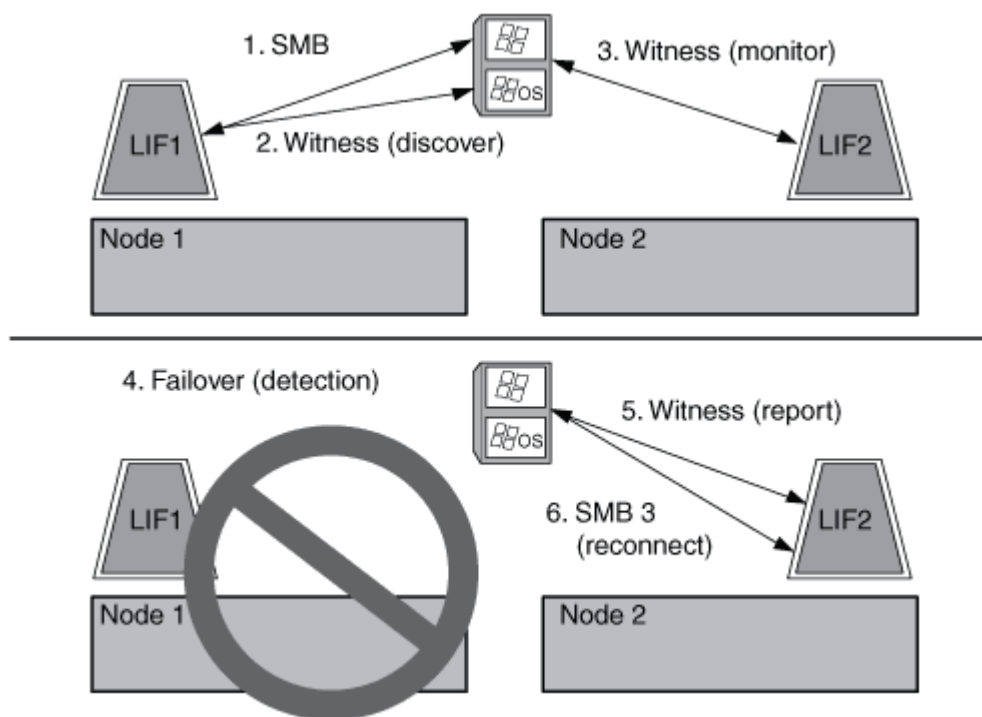
Cómo funciona el protocolo de testigos

ONTAP implementa el protocolo Witness mediante el uso del partner SFO de un nodo como testigo. En caso de fallo, el partner detecta rápidamente el fallo y notifica al cliente SMB.

El protocolo Witness proporciona una recuperación tras fallos mejorada mediante el siguiente proceso:

1. Cuando el servidor de aplicaciones establece una conexión SMB de disponibilidad continua a Node1, el servidor CIFS informa al servidor de aplicaciones que el testigo está disponible.
2. El servidor de aplicaciones solicita las direcciones IP del servidor testigo de Node1 y recibe una lista de direcciones IP de LIF de datos Node2 (el partner SFO) asignadas a la máquina virtual de almacenamiento (SVM).
3. El servidor de aplicaciones elige una de las direcciones IP, crea una conexión de testigo a Node2 y se registra para recibir una notificación si la conexión disponible continuamente en Node1 se debe mover.
4. Si se produce un evento de conmutación por error en Node1, el testigo facilita los eventos de conmutación por error, pero no se ve involucrado en la devolución.

5. Witness detecta el evento de conmutación por error y notifica al servidor de aplicaciones a través de la conexión de testigos que la conexión SMB debe moverse a Node2.
6. El servidor de aplicaciones mueve la sesión SMB a Node2 y recupera la conexión sin interrupción del acceso del cliente.



Backups basados en recursos compartidos con VSS remoto

Información general sobre backups basados en recursos compartidos con VSS remoto

Puede utilizar VSS remoto para realizar backups basados en recursos compartidos de los archivos de máquinas virtuales Hyper-V almacenados en un servidor CIFS.

Microsoft Remote VSS (Volume Shadow Copy Services) es una extensión de la infraestructura de Microsoft VSS existente. Con VSS remoto, Microsoft ha ampliado la infraestructura VSS para dar soporte a las copias en la sombra de los recursos compartidos de SMB. Además, las aplicaciones de servidor como Hyper-V pueden almacenar archivos VHD en recursos compartidos de archivos SMB. Con estas extensiones, es posible tomar copias redundantes coherentes con las aplicaciones para máquinas virtuales que almacenan datos y archivos de configuración en recursos compartidos.

Conceptos de VSS remoto

Debe conocer ciertos conceptos que se requieren para comprender cómo los servicios de backup utilizan VSS remoto (Volume Shadow Copy Service, Servicio de instantáneas de volumen) con las configuraciones de Hyper-V en SMB.

- **VSS (Volume Shadow Copy Service, Servicio de instantáneas de volumen)**

Tecnología de Microsoft que se usa para realizar copias de backup o copias Snapshot de datos en un volumen específico en un momento específico. VSS se coordina entre servidores de datos, aplicaciones de backup y software de gestión del almacenamiento para dar soporte a la creación y gestión de backups coherentes.

- **VSS remoto (Servicio de instantáneas de volumen remoto)**

Tecnología de Microsoft que se utiliza para realizar copias de backup basadas en recursos compartidos de datos que están en un estado consistente con los datos en un momento específico en el que se accede a los datos a través de recursos compartidos SMB 3.0. También se conoce como *Volume Shadow Copy Service*.

- **Copia de sombra**

Un conjunto de datos duplicado que contiene el recurso compartido en un instante bien definido. Las copias de sombra se utilizan para crear backups coherentes de un momento específico de los datos, lo que permite al sistema o aplicaciones seguir actualizando los datos en los volúmenes originales.

- **Sistema de instantáneas**

Colección de una o más instantáneas, con cada copia de sombra correspondiente a un recurso compartido. Las instantáneas de un conjunto de instantáneas representan todos los recursos compartidos de los que se debe realizar una copia de seguridad en la misma operación. El cliente VSS de la aplicación habilitada para VSS identifica las instantáneas que se incluirán en el conjunto.

- **Recuperación automática de conjuntos de instantáneas**

La parte del proceso de backup de las aplicaciones de backup habilitadas para VSS remotas en las que el directorio de réplica que contiene las instantáneas es coherente en un momento específico. Al inicio del backup, el cliente VSS de la aplicación activa la aplicación para llevar a cabo puntos de control de software en los datos programados para la copia de seguridad (los ficheros de la máquina virtual en el caso de Hyper-V). A continuación, el cliente VSS permite que las aplicaciones continúen. Una vez creado el conjunto de instantáneas, VSS remoto hace que el conjunto de instantáneas sea modificable y expone la copia modificable a las aplicaciones. La aplicación prepara el conjunto de instantáneas para la copia de seguridad realizando una recuperación automática con el punto de control del software tomado anteriormente. La recuperación automática hace que las instantáneas se encuentren en un estado coherente, desenrolando los cambios realizados en los archivos y directorios desde que se creó el punto de comprobación. La recuperación automática es un paso opcional para los backups con VSS habilitado.

- **Id. De copia de sombra**

GUID que identifica de forma exclusiva una copia oculta.

- **Id. De conjunto de copia de sombra**

GUID que identifica de forma exclusiva una colección de Id. De copia oculta en el mismo servidor.

- **SnapManager para Hyper-V**

El software que automatiza y simplifica las operaciones de backup y restauración para Microsoft Windows Server 2012 Hyper-V. SnapManager para Hyper-V utiliza VSS remoto con recuperación automática para realizar backups de archivos de Hyper-V en recursos compartidos SMB.

Información relacionada

[Conceptos clave sobre las operaciones no disruptivas de Hyper-V y SQL Server sobre SMB](#)

[Backups basados en recursos compartidos con VSS remoto](#)

Ejemplo de estructura de directorio utilizada por VSS remoto

VSS remoto atraviesa la estructura de directorios que almacena archivos de máquina virtual Hyper-V a medida que crea instantáneas. Es importante entender qué es una estructura de directorio adecuada, para que pueda crear copias de seguridad de archivos de equipos virtuales con éxito.

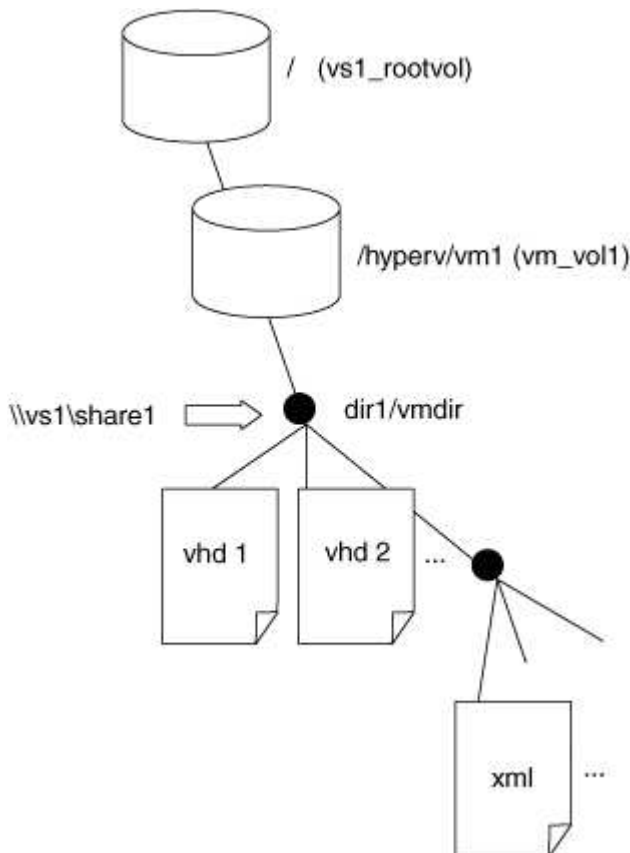
Una estructura de directorio compatible para la creación correcta de instantáneas cumple los siguientes requisitos:

- Sólo los directorios y los archivos normales están presentes en la estructura de directorios que se utiliza para almacenar archivos de máquinas virtuales.

La estructura de directorios no contiene uniones, vínculos ni archivos no regulares.

- Todos los archivos de una máquina virtual residen dentro de un único recurso compartido.
- La estructura de directorio que se utiliza para almacenar archivos de equipos virtuales no excede la profundidad configurada del directorio de instantáneas.
- El directorio raíz del recurso compartido sólo contiene directorios o archivos de la máquina virtual.

En la siguiente ilustración, el volumen llamado `vm_vol1` se crea con un punto de unión en `/hyperv/vm1`. En la máquina virtual de almacenamiento (SVM) `vs1`. Se crean subdirectorios para contener los archivos de la máquina virtual en el punto de unión. A los archivos de la máquina virtual del servidor de Hyper-V se accede a lo largo de `compartia1` que tiene la ruta de acceso `/hyperv/vm1/dir1/vmdir`. El servicio de instantáneas crea instantáneas de todos los archivos de la máquina virtual contenidos en la estructura de directorios bajo `share1` (hasta la profundidad configurada del directorio de instantáneas).



Cómo gestiona SnapManager para Hyper-V los backups basados en VSS remotos para Hyper-V en SMB

Puede utilizar SnapManager para Hyper-V para gestionar los servicios de backup basados en VSS remoto. El servicio de backup gestionado de SnapManager para Hyper-V ofrece ventajas con el fin de crear conjuntos de backup que utilizan el espacio de forma eficiente.

Entre las optimizaciones de SnapManager para backups gestionados por Hyper-V se incluyen las siguientes:

- La integración de SnapDrive con ONTAP ofrece optimización del rendimiento al detectar la ubicación de los recursos compartidos de SMB.

ONTAP proporciona a SnapDrive el nombre del volumen en el que reside el recurso compartido.

- SnapManager para Hyper-V especifica la lista de archivos de máquinas virtuales de los recursos compartidos de SMB que el servicio de copia en sombra necesita copiar.

Al proporcionar una lista de destino de archivos de máquinas virtuales, el servicio de instantáneas no necesita crear instantáneas de todos los archivos del recurso compartido.

- La máquina virtual de almacenamiento (SVM) conserva las copias de Snapshot para SnapManager para Hyper-V y así poder utilizarlas para las restauraciones.

No hay ninguna fase de backup. El backup es la copia Snapshot con una gestión eficiente del espacio.

SnapManager para Hyper-V proporciona funcionalidades de backup y restauración para HyperV mediante SMB mediante el siguiente proceso:

1. Preparación para la operación de copia oculta

El cliente VSS de la aplicación SnapManager para Hyper-V configura el conjunto de copias redundantes. El cliente VSS recopila información sobre los recursos compartidos que se incluirán en el conjunto de copias redundantes y proporciona esta información a ONTAP. Un conjunto puede contener una o más instantáneas y una copia de sombra corresponde a un recurso compartido.

2. Creación del conjunto de instantáneas (si se utiliza la recuperación automática)

Por cada recurso compartido incluido en el conjunto de instantáneas, ONTAP crea una copia de sombra y hace que la copia de sombra sea editable.

3. Exponiendo el conjunto de instantáneas

Una vez que ONTAP crea las copias instantáneas, éstas se exponen a SnapManager para Hyper-V para que los escritores de VSS de la aplicación puedan realizar una recuperación automática.

4. Recuperación automática del conjunto de instantáneas

Durante la creación de conjuntos de instantáneas, hay un período de tiempo en el que se producen cambios activos en los archivos incluidos en el conjunto de copias de seguridad. Los escritores de VSS de la aplicación deben actualizar las instantáneas para asegurarse de que están en un estado completamente coherente antes de realizar la copia de seguridad.



La forma en que se realiza la recuperación automática es específica para cada aplicación. La fase de VSS remota no participa en esta.

5. Completar y limpiar el conjunto de instantáneas

El cliente VSS notifica a ONTAP una vez que finaliza la recuperación automática. El conjunto de instantáneas es de sólo lectura y, a continuación, está listo para la copia de seguridad. Al usar SnapManager para Hyper-V para realizar un backup, los archivos de una copia snapshot se convierten en el backup. Por lo tanto, en la fase de backup se crea una copia snapshot para cada volumen que contenga recursos compartidos en el conjunto de backup. Una vez finalizada la copia de seguridad, el conjunto de instantáneas se elimina del servidor CIFS.

Cómo se utiliza la descarga de copias ODX con Hyper-V y SQL Server en recursos compartidos SMB

La transferencia de datos descargados (ODX), también conocida como *copy flood*, permite transferir datos directamente dentro o entre dispositivos de almacenamiento compatibles sin transferir los datos a través del equipo host. La descarga de copias ODX de ONTAP le ofrece ventajas en rendimiento al realizar operaciones de copia en su servidor de aplicaciones a través de la instalación de SMB.

En las transferencias de archivos que no son ODX, los datos se leen del servidor CIFS de origen y se transfieren a través de la red al equipo cliente. El equipo cliente transfiere los datos a través de la red al servidor CIFS de destino. En resumen, el equipo cliente lee los datos del origen y los escribe en el destino. Con las transferencias de archivos ODX, los datos se copian directamente del origen al destino.

Dado que las copias descargados de ODX se realizan directamente entre el almacenamiento de origen y destino, se obtienen importantes ventajas en el rendimiento. Las ventajas en cuanto a rendimiento incluyen unos tiempos de copia más rápidos entre el origen y el destino, una menor utilización de recursos (CPU, memoria) en el cliente y una menor utilización de ancho de banda de I/O de la red.

ONTAP ODX copy offload is supported on both SAN LUNs and SMB 3.0 continuously available connections.
Los siguientes casos de uso admiten el uso de copias y movimientos ODX:

- Volumen interno

Los archivos o LUN de origen y destino están dentro del mismo volumen.

- Entre volúmenes, mismo nodo, misma máquina virtual de almacenamiento (SVM)

Los archivos de origen y de destino o las LUN se encuentran en distintos volúmenes ubicados en el mismo nodo. Los datos son propiedad de la misma SVM.

- Entre volúmenes, distintos nodos, misma SVM

Los archivos de origen y de destino o las LUN se encuentran en volúmenes distintos que se encuentran en nodos diferentes. Los datos son propiedad de la misma SVM.

- Entre SVM, mismo nodo

El archivo de origen y los LUN de destino se encuentran en distintos volúmenes ubicados en el mismo nodo. Los datos son propiedad de diferentes SVM.

- Entre SVM, diferentes nodos

El archivo o las LUN de origen y destino se encuentran en distintos volúmenes ubicados en nodos diferentes. Los datos son propiedad de diferentes SVM.

Algunos casos de uso específicos para la descarga de copias de ODX con soluciones Hyper-V son los siguientes:

- Se puede utilizar la transferencia de la copia ODX mediante Hyper-V para copiar datos dentro o a través de archivos de disco duro virtual (VHD), o bien copiar datos entre recursos compartidos de SMB asignados y LUN iSCSI conectados dentro del mismo clúster.

Esto permite que las copias de sistemas operativos invitados pasen al almacenamiento subyacente.

- Al crear discos duros virtuales de tamaño fijo, ODX se utiliza para inicializar el disco con ceros, empleando un token de cero conocido.
- La descarga de copias ODX se utiliza para la migración de almacenamiento de máquinas virtuales si el almacenamiento de origen y destino está en el mismo clúster.



Para aprovechar los casos de uso de un paso a través de la descarga de copias ODX mediante Hyper-V, el sistema operativo invitado debe ser compatible con ODX, mientras que los discos del sistema operativo invitado deben ser discos SCSI respaldados por almacenamiento (tanto SMB COMO SAN) que sean compatibles con ODX. Los discos IDE del sistema operativo invitado no admiten el paso a través de ODX.

Los casos de uso específicos para la descarga de copias ODX mediante soluciones SQL Server son los siguientes:

- Puede utilizar la descarga de copias de ODX para exportar e importar bases de datos de SQL Server entre recursos compartidos de SMB asignados o entre recursos compartidos de SMB y LUN iSCSI conectados dentro del mismo clúster.
- La descarga de copias ODX se utiliza para exportar e importar bases de datos si el almacenamiento de origen y destino se encuentran en el mismo clúster.

Requisitos y consideraciones de configuración

Requisitos de licencia y ONTAP

Debe estar al tanto de determinados requisitos de ONTAP y licencia cuando cree soluciones de SQL Server o Hyper-V mediante SMB para realizar operaciones no disruptivas en SVM.

Requisitos de la versión de ONTAP

- Hyper-V mediante SMB

ONTAP admite operaciones no disruptivas en recursos compartidos SMB para Hyper-V que se ejecutan en Windows 2012 o posterior.

- SQL Server sobre SMB

ONTAP admite operaciones no disruptivas en recursos compartidos SMB para SQL Server 2012 o posterior que se ejecutan en Windows 2012 o posterior.

Para obtener la información más reciente sobre las versiones compatibles de ONTAP, Windows Server y SQL Server para realizar operaciones no disruptivas mediante recursos compartidos SMB, consulte la matriz de interoperabilidad.

["Herramienta de matriz de interoperabilidad de NetApp"](#)

Requisitos de licencia

Se requieren las siguientes licencias:

- CIFS
- FlexClone (solo para Hyper-V mediante SMB)

Esta licencia es necesaria si se usa VSS remoto para los backups. El servicio de copia de respaldo utiliza FlexClone para crear copias de un momento específico de los archivos que se usarán a la hora de crear un backup.

Una licencia de FlexClone es opcional si se utiliza un método de backup que no utiliza Remote VSS.

La licencia de FlexClone se incluye en ["ONTAP One"](#). Si no tiene ONTAP One, debe hacerlo ["verifique que las licencias necesarias estén instaladas"](#), y, si es necesario, ["instálelos"](#).

Requisitos de LIF de datos y red

Debe estar al tanto de determinados requisitos de la red y de la LIF de datos al crear configuraciones de SQL Server o Hyper-V mediante SMB para lograr operaciones no disruptivas).

Requisitos de protocolos de red

- Las redes IPv4 e IPv6 son compatibles.
- Se requiere SMB 3.0 o una versión posterior.

SMB 3.0 proporciona la funcionalidad necesaria para crear las conexiones SMB continuamente disponibles para ofrecer operaciones no disruptivas.

- Los servidores DNS deben contener entradas que asignan el nombre del servidor CIFS a las direcciones IP asignadas a las LIF de datos de la máquina virtual de almacenamiento (SVM).

Los servidores de aplicaciones de Hyper-V o SQL Server suelen realizar varias conexiones a través de varias LIF de datos al acceder a archivos de equipos virtuales o bases de datos. Para obtener una funcionalidad adecuada, los servidores de aplicaciones deben efectuar estas varias conexiones SMB mediante el nombre del servidor CIFS en lugar de realizar varias conexiones a varias direcciones IP únicas.

Para ello, también es necesario utilizar el nombre DNS del servidor CIFS en lugar de las direcciones IP de LIF individuales.

A partir de ONTAP 9.4, puede mejorar el rendimiento y la tolerancia a fallos del servidor Hyper-V y SQL en configuraciones de SMB al habilitar multicanal de SMB. Para ello, debe tener varias NIC de 1 G, 10 G o más grandes implementadas en el clúster y los clientes.

Requisitos de LIF de datos

- La SVM que aloja la solución de servidor de aplicaciones a través de SMB debe tener al menos una LIF de datos operativos en cada nodo del clúster.

Los LIF de datos de SVM pueden conmutar por error a otros puertos de datos del clúster, incluidos los nodos que actualmente no alojan datos a los que acceden los servidores de aplicaciones. Además, dado que el nodo testigo siempre es el partner SFO de un nodo al que está conectado el servidor de aplicaciones, cada nodo del clúster es un nodo testigo potencial.

- Los LIF de datos no deben configurarse para que la reversión se restaure automáticamente.

Tras un evento de toma de control o devolución, debe revertir manualmente las LIF de datos a sus puertos principales.

- Todas las direcciones IP de LIF de datos deben tener una entrada en DNS y todas las entradas se deben resolver en el nombre del servidor CIFS.

Los servidores de aplicaciones deben conectarse a recursos compartidos SMB mediante el nombre del servidor CIFS. No debe configurar los servidores de aplicaciones para realizar conexiones mediante las direcciones IP de LIF.

- Si el nombre del servidor CIFS es diferente del nombre de la SVM, las entradas DNS se deben resolver en el nombre del servidor CIFS.

Requisitos de volumen y servidor de SMB para Hyper-V mediante SMB

Debe estar al tanto de determinados requisitos de volumen y servidor de SMB al crear configuraciones de Hyper-V mediante SMB para proporcionar operaciones no disruptivas.

Requisitos del servidor SMB

- Se debe habilitar SMB 3.0.

Esta opción está habilitada de forma predeterminada.

- La opción de servidor CIFS del usuario UNIX predeterminado debe estar configurada con una cuenta de usuario UNIX válida.

Los servidores de aplicaciones utilizan la cuenta del equipo al crear una conexión SMB. Dado que todos los accesos del bloque de mensajes del servidor requieren que el usuario de Windows se asigne correctamente a una cuenta de usuario de UNIX o a la cuenta de usuario de UNIX predeterminada, ONTAP debe poder asignar la cuenta de equipo del servidor de aplicaciones a la cuenta de usuario UNIX predeterminada.

- Las referencias automáticas al nodo deben estar deshabilitadas (esta funcionalidad está deshabilitada de forma predeterminada).

Si desea utilizar referencias de nodo automáticas para acceder a datos que no sean archivos de máquina

de Hyper-V, debe crear una SVM independiente para esos datos.

- Se debe permitir tanto la autenticación Kerberos como NTLM en el dominio al que pertenece el servidor SMB.

ONTAP no anuncia el servicio Kerberos para VSS remoto; por lo tanto, el dominio debe configurarse para permitir NTLM.

- La función de copia de sombra debe estar activada.

Esta funcionalidad está habilitada de forma predeterminada.

- La cuenta de dominio de Windows que utiliza el servicio de copia de sombra al crear instantáneas debe ser miembro del grupo local BUILTIN\Administrators o BUILTIN\Backup Operators del servidor SMB.

Requisitos del volumen

- Los volúmenes utilizados para almacenar archivos de máquinas virtuales se deben crear como volúmenes de estilo de seguridad NTFS.

Para proporcionar NDOS a los servidores de aplicaciones mediante conexiones SMB disponibles de forma continua, el volumen que contiene el recurso compartido debe ser un volumen NTFS. Además, siempre debe haber sido un volumen NTFS. No se puede cambiar un volumen de estilo de seguridad mixto o un volumen de estilo de seguridad UNIX por un volumen de estilo de seguridad NTFS y utilizarlo directamente para NDOS en recursos compartidos SMB. Si cambia un volumen de estilo de seguridad mixto por un volumen de estilo de seguridad NTFS y piensa usarlo para NDO en recursos compartidos SMB, debe colocar manualmente una ACL en la parte superior del volumen y propagar esa ACL a todos los archivos y carpetas incluidos. De lo contrario, las migraciones de máquinas virtuales o exportaciones de archivos de base de datos e importaciones donde se mueven archivos a otro volumen pueden fallar si los volúmenes de origen o de destino se crearon inicialmente como volúmenes mixtos o de estilo de seguridad UNIX y posteriormente se cambiaron al estilo de seguridad NTFS.

- Para que las operaciones de copia de sombra se realicen correctamente, debe tener suficiente espacio disponible en el volumen.

El espacio disponible debe ser al menos tan grande como el espacio combinado utilizado por todos los archivos, directorios y subdirectorios contenidos en los recursos compartidos incluidos en el conjunto de copia de seguridad de instantánea. Este requisito solo se aplica a copias instantáneas con recuperación automática.

Información relacionada

"Biblioteca de Microsoft TechNet: technet.microsoft.com/en-us/library/"

Requisitos de volumen y servidor de SMB para SQL Server sobre SMB

Debe estar al tanto de determinados requisitos de volumen y servidor SMB al crear SQL Server en configuraciones de SMB para proporcionar operaciones no disruptivas.

Requisitos del servidor SMB

- Se debe habilitar SMB 3.0.

Esta opción está habilitada de forma predeterminada.

- La opción de servidor CIFS del usuario UNIX predeterminado debe estar configurada con una cuenta de usuario UNIX válida.

Los servidores de aplicaciones utilizan la cuenta del equipo al crear una conexión SMB. Dado que todos los accesos del bloque de mensajes del servidor requieren que el usuario de Windows se asigne correctamente a una cuenta de usuario de UNIX o a la cuenta de usuario de UNIX predeterminada, ONTAP debe poder asignar la cuenta de equipo del servidor de aplicaciones a la cuenta de usuario UNIX predeterminada.

Además, SQL Server utiliza un usuario de dominio como cuenta de servicio de SQL Server. La cuenta de servicio también debe tener asignado el usuario UNIX predeterminado.

- Las referencias automáticas al nodo deben estar deshabilitadas (esta funcionalidad está deshabilitada de forma predeterminada).

Si desea utilizar referencias de nodo automáticas para acceder a datos que no sean archivos de base de datos de SQL Server, debe crear una SVM independiente para esos datos.

- La cuenta de usuario de Windows utilizada para instalar SQL Server en ONTAP debe tener asignado el privilegio SeSecurityPrivilege.

Este privilegio se asigna al grupo BUILTINAdministrators local del servidor SMB.

Requisitos del volumen

- Los volúmenes utilizados para almacenar archivos de máquinas virtuales se deben crear como volúmenes de estilo de seguridad NTFS.

Para proporcionar NDOS a los servidores de aplicaciones mediante conexiones SMB disponibles de forma continua, el volumen que contiene el recurso compartido debe ser un volumen NTFS. Además, siempre debe haber sido un volumen NTFS. No se puede cambiar un volumen de estilo de seguridad mixto o un volumen de estilo de seguridad UNIX por un volumen de estilo de seguridad NTFS y utilizarlo directamente para NDOS en recursos compartidos SMB. Si cambia un volumen de estilo de seguridad mixto por un volumen de estilo de seguridad NTFS y piensa usarlo para NDO en recursos compartidos SMB, debe colocar manualmente una ACL en la parte superior del volumen y propagar esa ACL a todos los archivos y carpetas incluidos. De lo contrario, las migraciones de máquinas virtuales o exportaciones de archivos de base de datos e importaciones donde se mueven archivos a otro volumen pueden fallar si los volúmenes de origen o de destino se crearon inicialmente como volúmenes mixtos o de estilo de seguridad UNIX y posteriormente se cambiaron al estilo de seguridad NTFS.

- Aunque el volumen que contiene los archivos de la base de datos puede contener uniones, SQL Server no cruza las uniones al crear la estructura de directorio de la base de datos.
- Para que las operaciones de backup del plugin de SnapCenter para Microsoft SQL Server se realicen correctamente, es necesario contar con espacio disponible suficiente en el volumen.

El volumen en el que residen los archivos de base de datos de SQL Server debe ser lo suficientemente grande como para contener la estructura de directorio de la base de datos y todos los archivos contenidos que residen en el recurso compartido.

Información relacionada

"Biblioteca de Microsoft TechNet: technet.microsoft.com/en-us/library/"

Disponibilidad continua de los requisitos de recursos compartidos y consideraciones para Hyper-V en SMB

Debe tener en cuenta ciertos requisitos y consideraciones a la hora de configurar recursos compartidos disponibles de forma continua para configuraciones de Hyper-V en SMB que admiten operaciones no disruptivas.

Comparta los requisitos

- Los recursos compartidos utilizados por los servidores de aplicaciones deben configurarse con el conjunto de propiedades continuamente disponibles.

Los servidores de aplicaciones que se conectan a recursos compartidos disponibles de forma continua reciben controladores persistentes que les permiten volver a conectarse de forma no disruptiva a recursos compartidos de SMB y reclamar bloqueos de archivos tras eventos disruptivos como la toma de control, el retorno al nodo primario y la reubicación de agregados.

- Si desea utilizar los servicios de backup habilitados para VSS remoto, no podrá colocar los archivos Hyper-V en los recursos compartidos que contienen uniones.

En el caso de recuperación automática, se produce un error en la creación de instantáneas si se encuentra una unión mientras se pasa por el recurso compartido. En el caso no de recuperación automática, la creación de copias redundantes no falla, pero la unión no apunta a nada.

- Si desea utilizar servicios de backup habilitados para VSS remoto con recuperación automática, no puede colocar los archivos de Hyper-V en recursos compartidos que contengan lo siguiente:

- Enlaces simbólicos, enlaces duros o enlaces con cables
- Archivos no regulares

La creación de instantáneas falla si hay vínculos o archivos no regulares en el recurso compartido a instantáneas. Este requisito solo se aplica a copias instantáneas con recuperación automática.

- Para que las operaciones de copia oculta se realicen correctamente, debe tener suficiente espacio disponible en el volumen (solo para Hyper-V en SMB).

El espacio disponible debe ser al menos tan grande como el espacio combinado utilizado por todos los archivos, directorios y subdirectorios contenidos en los recursos compartidos incluidos en el conjunto de copia de seguridad de instantánea. Este requisito solo se aplica a copias instantáneas con recuperación automática.

- Las siguientes propiedades compartidas no deben definirse en recursos compartidos disponibles continuamente que utilizan los servidores de aplicaciones:

- Directorio inicial
- Almacenamiento de atributos en caché
- BranchCache

Consideraciones

- Las cuotas están soportadas por recursos compartidos constantemente disponibles.
- La siguiente funcionalidad no es compatible con las configuraciones de Hyper-V mediante SMB:
 - Auditoría

- FPolicy

- La detección de virus no se realiza en recursos compartidos de SMB con el `continuously-availability` parámetro establecido en `Yes`.

Requisitos de recursos compartidos y consideraciones continuamente disponibles para SQL Server en SMB

Debe tener en cuenta ciertos requisitos y consideraciones a la hora de configurar recursos compartidos disponibles de forma continua para configuraciones de SQL Server en SMB que admiten operaciones no disruptivas.

Comparta los requisitos

- Los volúmenes utilizados para almacenar archivos de máquinas virtuales se deben crear como volúmenes de estilo de seguridad NTFS.

Para proporcionar operaciones no disruptivas para servidores de aplicaciones mediante conexiones SMB disponibles de forma continua, el volumen que contiene el recurso compartido debe ser un volumen NTFS. Además, siempre debe haber sido un volumen NTFS. No se puede cambiar un volumen de estilo de seguridad mixto o un volumen de estilo de seguridad UNIX por un volumen de estilo de seguridad NTFS y usarlo directamente para operaciones no disruptivas sobre recursos compartidos SMB. Si cambia un volumen de estilo de seguridad mixto por un volumen de estilo de seguridad NTFS y piensa usarlo para operaciones no disruptivas en recursos compartidos de SMB, debe colocar manualmente una ACL en la parte superior del volumen y propagar esa ACL a todos los archivos y carpetas incluidos. De lo contrario, las migraciones de máquinas virtuales o exportaciones de archivos de base de datos e importaciones donde se mueven archivos a otro volumen pueden fallar si los volúmenes de origen o de destino se crearon inicialmente como volúmenes mixtos o de estilo de seguridad UNIX y posteriormente se cambiaron al estilo de seguridad NTFS.

- Los recursos compartidos utilizados por los servidores de aplicaciones deben configurarse con el conjunto de propiedades continuamente disponibles.

Los servidores de aplicaciones que se conectan a recursos compartidos disponibles de forma continua reciben controladores persistentes que les permiten volver a conectarse de forma no disruptiva a recursos compartidos de SMB y reclamar bloqueos de archivos tras eventos disruptivos como la toma de control, el retorno al nodo primario y la reubicación de agregados.

- Aunque el volumen que contiene los archivos de la base de datos puede contener uniones, SQL Server no cruza las uniones al crear la estructura de directorio de la base de datos.
- Para que las operaciones del plugin de SnapCenter para Microsoft SQL Server se realicen correctamente, es necesario contar con espacio disponible suficiente en el volumen.

El volumen en el que residen los archivos de base de datos de SQL Server debe ser lo suficientemente grande como para contener la estructura de directorio de la base de datos y todos los archivos contenidos que residen en el recurso compartido.

- Las siguientes propiedades compartidas no deben definirse en recursos compartidos disponibles continuamente que utilizan los servidores de aplicaciones:
 - Directorio inicial
 - Almacenamiento de atributos en caché
 - BranchCache

Comparta consideraciones

- Las cuotas están soportadas por recursos compartidos constantemente disponibles.
- La siguiente funcionalidad no es compatible con configuraciones de SQL Server en SMB:
 - Auditoría
 - FPolicy
- La detección de virus no se realiza en recursos compartidos de SMB con el `continuously-availability` propiedad compartida establecida.

Consideraciones de VSS remotas para configuraciones de Hyper-V mediante SMB

Al utilizar soluciones de backup habilitadas para VSS remoto para configuraciones de Hyper-V en SMB, debe tener en cuenta determinadas consideraciones.

Consideraciones generales sobre VSS remoto

- Se puede configurar un máximo de 64 recursos compartidos por servidor de aplicaciones de Microsoft.

La operación de copia de sombra falla si hay más de 64 recursos compartidos en un conjunto de instantáneas. Este es un requisito de Microsoft.

- Solo se permite un conjunto de copias redundantes por servidor CIFS.

Se producirá un error en las operaciones de copia de sombra si hay una operación de copia de sombra en curso en el mismo servidor CIFS. Este es un requisito de Microsoft.

- No se permiten uniones dentro de la estructura de directorios en la que VSS remoto crea una copia oculta.
 - En el caso de recuperación automática, se producirá un error en la creación de instantáneas si se encuentra una unión mientras se recorre el recurso compartido.
 - En el caso de recuperación no automática, la creación de instantáneas no falla, pero la unión no apunta a nada.

Consideraciones de VSS remotas que sólo son aplicables a las instantáneas con recuperación automática

Ciertos límites solo se aplican a las instantáneas con recuperación automática.

- Se permite una profundidad máxima de directorio de cinco subdirectorios para la creación de instantáneas.

Esta es la profundidad de directorio sobre la que el servicio de instantáneas crea un conjunto de copia de seguridad de instantánea. La creación de instantáneas falla si los directorios que contienen archivos de máquina virtual están anidados más de cinco niveles. Con esto se pretende limitar el cruce de directorios al clonar el recurso compartido. La profundidad máxima de directorio puede cambiarse con una opción de servidor CIFS.

- La cantidad de espacio disponible en el volumen debe ser adecuada.

El espacio disponible debe ser al menos tan grande como el espacio combinado utilizado por todos los archivos, directorios y subdirectorios contenidos en los recursos compartidos incluidos en el conjunto de copia de seguridad de instantánea.

- No se permiten vínculos ni archivos no regulares dentro de la estructura de directorios en la que Remote

VSS crea una copia de sombra.

La creación de instantáneas falla si hay vínculos o archivos no regulares en el recurso compartido a la instantánea. El proceso de clonación no es compatible con ellos.

- No se permiten ACL de NFSv4 en directorios.

Aunque la creación de copias redundantes mantiene las ACL de NFSv4 en los archivos, se pierden las ACL de NFSv4 en los directorios.

- Se permite un máximo de 60 segundos para crear un conjunto de instantáneas.

Las especificaciones de Microsoft permiten un máximo de 60 segundos para crear el conjunto de instantáneas. Si el cliente VSS no puede crear el conjunto de instantáneas en este momento, la operación de copia oculta falla; por lo tanto, esto limita el número de archivos en un conjunto de instantáneas. El número real de archivos o máquinas virtuales que se pueden incluir en un conjunto de backups varía. Este número depende de muchos factores y se debe determinar en cada entorno del cliente.

Requisitos de copia ODX para SQL Server y Hyper-V mediante SMB

La descarga de copias de ODX debe habilitarse si desea migrar archivos de máquinas virtuales o exportar e importar archivos de base de datos directamente desde la ubicación de almacenamiento de origen a la de destino sin enviar datos a través de los servidores de aplicaciones. Hay ciertos requisitos que debe comprender sobre el uso de la descarga de copias ODX mediante soluciones de SQL Server y Hyper-V mediante SMB.

El uso de la descarga de copias ODX ofrece una importante ventaja en cuanto al rendimiento. Esta opción del servidor CIFS está habilitada de forma predeterminada.

- Debe habilitarse SMB 3.0 para utilizar la descarga de copias ODX.
- Los volúmenes de origen deben tener un mínimo de 1.25 GB.
- La deduplicación debe estar activada en los volúmenes utilizados para la descarga de copias.
- Si utiliza volúmenes comprimidos, el tipo de compresión debe ser adaptable y solo se admite el tamaño de grupo de compresión 8K.

No se admite el tipo de compresión secundaria

- Para utilizar la descarga de copias ODX para migrar «guest» de Hyper-V dentro y entre discos, los servidores Hyper-V deben configurarse para usar discos SCSI.

El valor predeterminado es configurar discos IDE, pero la descarga de copias ODX no funciona cuando se migran invitados si los discos se crean mediante discos IDE.

Recomendaciones para configuraciones de SQL Server y Hyper-V mediante SMB

Para estar seguro de que sus configuraciones de SQL Server y Hyper-V mediante SMB son sólidas y operativas, debe estar familiarizado con las mejores prácticas recomendadas al configurar las soluciones.

Recomendaciones generales

- Separe los archivos del servidor de aplicaciones de los datos generales del usuario.

Si es posible, dedique una máquina virtual de almacenamiento (SVM) completa y su almacenamiento a los datos del servidor de aplicaciones.

- Para obtener el mejor rendimiento, no habilite la firma SMB en las SVM que se utilizan para almacenar los datos del servidor de aplicaciones.
- Para obtener el mejor rendimiento y una mejor tolerancia a fallos, permite que SMB MultiChannel proporcione múltiples conexiones entre ONTAP y clientes en una única sesión SMB.
- No cree recursos compartidos disponibles continuamente en ningún recurso compartido distinto a los que se utilizan en la configuración de Hyper-V o SQL Server sobre SMB.
- Deshabilite las notificaciones de cambio en los recursos compartidos utilizados para una disponibilidad continua.
- No mueva el volumen al mismo tiempo que la reubicación de agregados (ARL) porque la ARL tiene fases que pausan algunas operaciones.
- Para las soluciones Hyper-V en SMB, utilice unidades iSCSI de invitado al crear máquinas virtuales en clúster. Compartido .VHDX No se admiten archivos para Hyper-V sobre SMB en los recursos compartidos de SMB de ONTAP.

Planifique la configuración de Hyper-V o SQL Server con SMB

Complete la hoja de datos de configuración de volumen

La hoja de trabajo proporciona una forma sencilla de registrar los valores que necesita al crear volúmenes para configuraciones de SQL Server y Hyper-V en SMB.

Para cada volumen, debe especificar la siguiente información:

- El nombre de la máquina virtual de almacenamiento (SVM)

El nombre de SVM es el mismo para todos los volúmenes.

- Nombre del volumen
- Nombre del agregado

Puede crear volúmenes en agregados ubicados en cualquier nodo del clúster.

- Tamaño
- Ruta de unión

Debe tener en cuenta lo siguiente al crear volúmenes que se utilizan para almacenar datos del servidor de aplicaciones:

- Si el volumen raíz no tiene estilo de seguridad NTFS, se debe especificar el estilo de seguridad como NTFS al crear el volumen.

De forma predeterminada, los volúmenes heredan el estilo de seguridad del volumen raíz de la SVM.

- Los volúmenes se deben configurar con la garantía de espacio de volumen predeterminada.

- Opcionalmente, puede configurar la opción de gestión de espacio de autosize.
- Debe establecer la opción que determina la reserva de espacio de la copia Snapshot 0.
- Debe deshabilitarse la política de Snapshot aplicada al volumen.

Si está deshabilitada la política de Snapshot de SVM, no es necesario especificar una política de Snapshot para los volúmenes. Los volúmenes heredan la política de Snapshot para la SVM. Si la política de Snapshot para la SVM no está deshabilitada y se configura para crear copias de Snapshot, debe especificar una política de Snapshot en el nivel de volumen y esa política debe deshabilitarse. Los backups habilitados para el servicio de copia de sombra y los backups de SQL Server gestionan la creación y eliminación de copias de Snapshot.

- No se pueden configurar los reflejos con uso compartido de carga para los volúmenes.

Las rutas de unión en las que tiene previsto crear recursos compartidos que utilicen los servidores de aplicaciones deben seleccionarse de forma que no haya volúmenes con conexiones por debajo del punto de entrada de recurso compartido.

Por ejemplo, si desea almacenar archivos de máquinas virtuales en cuatro volúmenes denominados «'vol1'», «'vol2'», «'vol3'» y «'vol4'», puede crear el espacio de nombres que se muestra en el ejemplo. A continuación, puede crear recursos compartidos para los servidores de aplicaciones en las rutas siguientes: /data1/vol1, /data1/vol2, /data2/vol3, y. /data2/vol4.

| Vserver | Volume | Junction | | Junction Path Source |
|---------|--------|----------|---------------|----------------------|
| | | Active | Junction Path | |
| vs1 | data1 | true | /data1 | RW_volume |
| vs1 | vol1 | true | /data1/vol1 | RW_volume |
| vs1 | vol2 | true | /data1/vol2 | RW_volume |
| vs1 | data2 | true | /data2 | RW_volume |
| vs1 | vol3 | true | /data2/vol3 | RW_volume |
| vs1 | vol4 | true | /data2/vol4 | RW_volume |

| Tipos de información | Valores |
|--|---------|
| <i>Volume 1: Nombre del volumen, agregado, tamaño, ruta de unión</i> | |
| <i>Volume 2: Nombre del volumen, agregado, tamaño, ruta de unión</i> | |
| <i>Volume 3: Nombre del volumen, agregado, tamaño, ruta de unión</i> | |
| <i>Volume 4: Nombre del volumen, agregado, tamaño, ruta de unión</i> | |
| <i>Volume 5: Nombre del volumen, agregado, tamaño, ruta de unión</i> | |

| Tipos de información | Valores |
|---|---------|
| <i>Volume 6: Nombre del volumen, agregado, tamaño, ruta de unión</i> | |
| <i>Volúmenes adicionales: Nombre del volumen, agregado, tamaño, ruta de unión</i> | |

Complete la hoja de datos de configuración de recursos compartidos de SMB

Utilice esta hoja de datos para registrar los valores necesarios cuando cree recursos compartidos SMB disponibles de forma continua para configuraciones de SQL Server y Hyper-V en SMB.

Información acerca de las propiedades de los recursos compartidos de SMB y las opciones de configuración

Debe especificar la siguiente información para cada recurso compartido:

- El nombre de la máquina virtual de almacenamiento (SVM)

El nombre de SVM es el mismo para todos los recursos compartidos

- Nombre del recurso compartido
- Ruta
- Comparta propiedades

Debe configurar las siguientes dos propiedades compartidas:

- `oplocks`
- `continuously-available`

No deben configurarse las siguientes propiedades compartidas:

- `homedirectory attributecache`
- `branchcache`
- `access-based-enumeration`
 - Los enlaces simbólicos deben estar desactivados (el valor de `-symlink-properties` el parámetro debe ser nulo [""]).

Información sobre las rutas de recursos compartidos

Si utiliza VSS remoto para realizar backups de archivos de Hyper-V, la opción de rutas de uso compartido a la hora de realizar conexiones SMB desde los servidores de Hyper-V a las ubicaciones de almacenamiento en las que están almacenados los archivos de la máquina virtual es importante. Aunque los recursos compartidos se pueden crear en cualquier punto del espacio de nombres, las rutas de los recursos compartidos que utilizan los servidores de Hyper-V no deben contener volúmenes que se han Unido. No se pueden realizar operaciones de copia de sombra en rutas de uso compartido que contienen puntos de unión.

SQL Server no puede cruzar uniones al crear la estructura de directorio de la base de datos. No debe crear

rutas de acceso compartidas para SQL Server que contengan puntos de unión.

Por ejemplo, en el espacio de nombres que se muestra, si desea almacenar archivos de máquina virtual o archivos de base de datos en los volúmenes «'vol1'», «'vol2'», «'vol3'» y «'vol4'», deberá crear recursos compartidos para los servidores de aplicaciones en las rutas siguientes: /data1/vol1, /data1/vol2, /data2/vol3, y. /data2/vol4.

| Vserver | Volume | Junction | | Junction |
|---------|--------|----------|---------------|-------------|
| | | Active | Junction Path | Path Source |
| vs1 | data1 | true | /data1 | RW_volume |
| vs1 | vol1 | true | /data1/vol1 | RW_volume |
| vs1 | vol2 | true | /data1/vol2 | RW_volume |
| vs1 | data2 | true | /data2 | RW_volume |
| vs1 | vol3 | true | /data2/vol3 | RW_volume |
| vs1 | vol4 | true | /data2/vol4 | RW_volume |



Aunque puede crear recursos compartidos en la /data1 y.. /data2 rutas de acceso para la administración administrativa, no debe configurar los servidores de aplicaciones para que utilicen esos recursos compartidos para almacenar datos.

Hoja de trabajo de planificación

| Tipos de información | Valores |
|--|---------|
| Volume 1: Nombre y ruta del recurso compartido del SMB | |
| Volume 2: Nombre compartido SMB y ruta | |
| Volume 3: Nombre compartido SMB y ruta | |
| Volume 4: Nombre compartido SMB y ruta | |
| Volume 5: Nombre compartido SMB y ruta | |
| Volume 6: Nombre compartido SMB y ruta | |
| Volume 7: Nombre compartido SMB y ruta | |
| Volúmenes adicionales: Nombres de recursos compartidos SMB y rutas | |

Cree configuraciones de ONTAP para proporcionar operaciones no disruptivas con Hyper-V y SQL Server sobre SMB

Cree configuraciones de ONTAP para proporcionar operaciones no disruptivas con Hyper-V y SQL Server sobre SMB

Hay varios pasos de configuración de ONTAP que debe realizar para preparar las instalaciones de Hyper-V y SQL Server que proporcionan operaciones no disruptivas a través de SMB.

Antes de crear la configuración de ONTAP para operaciones no disruptivas con Hyper-V y SQL Server sobre SMB, deben completarse las siguientes tareas:

- Los servicios de hora deben configurarse en el clúster.
- Las redes deben configurarse para la SVM.
- Se debe crear la SVM.
- Las interfaces de LIF de datos deben configurarse en la SVM.
- DNS debe haberse configurado en la SVM.
- Los servicios de nombres deseados deben configurarse para la SVM.
- Debe crearse el servidor SMB.

Información relacionada

[Planifique la configuración de Hyper-V o SQL Server con SMB](#)

[Requisitos y consideraciones de configuración](#)

Verificar que la autenticación Kerberos y NTLMv2 están permitidas (Hyper-V en recursos compartidos SMB)

Las operaciones no disruptivas para Hyper-V a través de SMB requieren que el servidor CIFS en una SVM de datos y el servidor Hyper-V permita la autenticación Kerberos y NTLMv2. Debe verificar la configuración en el servidor CIFS y los servidores Hyper-V que controlan los métodos de autenticación permitidos.

Acerca de esta tarea

La autenticación Kerberos es necesaria cuando se hace una conexión compartida disponible continuamente. Parte del proceso de VSS remoto utiliza la autenticación NTLMv2. Por lo tanto, debe ser compatible con las conexiones que utilizan ambos métodos de autenticación en las configuraciones de Hyper-V mediante SMB.

Debe configurarse la siguiente configuración para permitir la autenticación Kerberos y NTLMv2:

- Debe deshabilitarse la política de exportación de SMB en la máquina virtual de almacenamiento (SVM).

La autenticación Kerberos y NTLMv2 siempre están habilitadas en las SVM, pero se pueden utilizar políticas de exportación para restringir el acceso en función del método de autenticación.

Las políticas de exportación de SMB son opcionales y están deshabilitadas de forma predeterminada. Si las directivas de exportación están deshabilitadas, la autenticación Kerberos y NTLMv2 se permite de forma predeterminada en un servidor CIFS.

- El dominio al que pertenecen el servidor CIFS y los servidores Hyper-V debe permitir la autenticación Kerberos y NTLMv2.

La autenticación Kerberos está habilitada de forma predeterminada en dominios de Active Directory. Sin embargo, la autenticación NTLMv2 puede estar permitida, ya sea mediante la configuración de la directiva de seguridad o las directivas de grupo.

Pasos

1. Realice lo siguiente para verificar que las políticas de exportación están deshabilitadas en la SVM:

- a. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

- b. Compruebe que el `-is-exportpolicy-enabled` La opción del servidor CIFS se establece en `false`:

```
vserver cifs options show -vserver vserver_name -fields vserver,is-exportpolicy-enabled
```

- c. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

2. Si no se deshabilitan las políticas de exportación de SMB, inhabilite estas opciones:

```
vserver cifs options modify -vserver vserver_name -is-exportpolicy-enabled false
```

3. Compruebe que tanto NTLMv2 como Kerberos están permitidos en el dominio.

Para obtener información acerca de cómo determinar qué métodos de autenticación se permiten en el dominio, consulte la biblioteca de Microsoft TechNet.

4. Si el dominio no permite la autenticación NTLMv2, habilite la autenticación NTLMv2 utilizando uno de los métodos descritos en la documentación de Microsoft.

Ejemplo

Los siguientes comandos verifican que las políticas de exportación de SMB se han deshabilitado en la SVM vs1:


```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vservers cifs options show -vservers vs1 -fields vservers,is-
exportpolicy-enabled

vservers  is-exportpolicy-enabled
-----  -----
vs1       false

cluster1::*> set -privilege admin
```

Compruebe que las cuentas de dominio se asignan al usuario UNIX predeterminado

Hyper-V y SQL Server utilizan cuentas de dominio para crear conexiones SMB a recursos compartidos constantemente disponibles. Para crear correctamente la conexión, la cuenta de equipo debe asignar correctamente a un usuario de UNIX. La forma más cómoda de lograrlo es asignar la cuenta de equipo al usuario UNIX predeterminado.

Acerca de esta tarea

Hyper-V y SQL Server utilizan las cuentas de equipo de dominio para crear conexiones SMB. Además, SQL Server utiliza una cuenta de usuario de dominio como cuenta de servicio que también realiza conexiones SMB.

Cuando se crea una máquina virtual de almacenamiento (SVM), ONTAP crea automáticamente el usuario predeterminado llamado "pcuser" (con un UID de 65534) Y el grupo denominado «'pcuser'» (con una GID de 65534), y agrega el usuario predeterminado al grupo «'pcuser'». Si configura una solución de Hyper-V mediante SMB en una SVM que existía antes de actualizar el clúster a Data ONTAP 8.2, es posible que el usuario y el grupo predeterminados no existan. Si no lo hacen, debe crearlos antes de configurar el usuario UNIX predeterminado del servidor CIFS.

Pasos

1. Determine si hay un usuario UNIX predeterminado:

```
vservers cifs options show -vservers vservers_name
```

2. Si la opción de usuario predeterminada no está establecida, determine si hay un usuario UNIX que se puede designar como usuario UNIX predeterminado:

```
vservers services unix-user show -vservers vservers_name
```

3. Si la opción de usuario predeterminada no está establecida y no hay ningún usuario UNIX que pueda designarse como usuario UNIX predeterminado, cree el usuario UNIX predeterminado y el grupo predeterminado y agregue el usuario predeterminado al grupo.

Por lo general, al usuario predeterminado se le asigna el nombre de usuario «'pcuser'» y debe asignarse el

UID de 65534. Por lo general, al grupo por defecto se le da el nombre de grupo «'pcuser'». El GID asignado al grupo debe ser 65534.

- a. Cree el grupo predeterminado:

```
vserver services unix-group create -vserver vserver_name -name pcuser -id 65534
```

- b. Cree el usuario predeterminado y agregue el usuario predeterminado al grupo predeterminado:

```
vserver services unix-user create -vserver vserver_name -user pcuser -id 65534 -primary-gid 65534
```

- c. Compruebe que el usuario predeterminado y el grupo predeterminado están configurados correctamente:

```
vserver services unix-user show -vserver vserver_name
```

```
vserver services unix-group show -vserver vserver_name -members
```

4. Si el usuario predeterminado del servidor CIFS no está configurado, realice lo siguiente:

- a. Configure el usuario predeterminado:

```
vserver cifs options modify -vserver *vserver_name -default-unix-user pcuser*
```

- b. Compruebe que el usuario UNIX predeterminado está configurado correctamente:

```
vserver cifs options show -vserver vserver_name
```

5. Para comprobar que la cuenta de equipo del servidor de aplicaciones se asigna correctamente al usuario predeterminado, asigne una unidad a un recurso compartido que reside en la SVM y confirme la asignación de usuario de Windows a UNIX mediante el `vserver cifs session show` comando.

Para obtener más información acerca de cómo utilizar este comando, consulte las páginas man.

Ejemplo

Los siguientes comandos determinan que el usuario predeterminado del servidor CIFS no está establecido, pero determinan que existen el usuario «'pcaduser'» y el grupo «'pcaduser'». Al usuario «'pcuser'» se le asigna como usuario predeterminado del servidor CIFS en la SVM vs1.

```
cluster1::> vserver cifs options show
```

```
Vserver: vs1
```

```
Client Session Timeout : 900
Default Unix Group      : -
Default Unix User       : -
Guest Unix User         : -
Read Grants Exec        : disabled
Read Only Delete        : disabled
```

```
WINS Servers : -
```

```
cluster1::> vservice unix-user show
```

| Vserver | User Name | User ID | Group ID | Full Name |
|---------|-----------|---------|----------|-----------|
| vs1 | nobody | 65535 | 65535 | - |
| vs1 | pcuser | 65534 | 65534 | - |
| vs1 | root | 0 | 1 | - |

```
cluster1::> vservice unix-group show -members
```

| Vserver | Name | ID |
|---------|----------|-------|
| vs1 | daemon | 1 |
| | Users: - | |
| vs1 | nobody | 65535 |
| | Users: - | |
| vs1 | pcuser | 65534 |
| | Users: - | |
| vs1 | root | 0 |
| | Users: - | |

```
cluster1::> vservice cifs options modify -vserver vs1 -default-unix-user pcuser
```

```
cluster1::> vservice cifs options show
```

```
Vserver: vs1
```

```
Client Session Timeout : 900
Default Unix Group      : -
Default Unix User       : pcuser
Guest Unix User         : -
Read Grants Exec        : disabled
Read Only Delete        : disabled
WINS Servers            : -
```

Compruebe que el estilo de seguridad del volumen raíz de SVM se haya establecido en NTFS

Para garantizar que las operaciones no disruptivas de Hyper-V y SQL Server sobre SMB se realicen correctamente, los volúmenes se deben crear con un estilo de seguridad NTFS. Dado que el estilo de seguridad del volumen raíz se aplica de manera predeterminada a los volúmenes creados en la máquina virtual de almacenamiento (SVM), el estilo de seguridad del volumen raíz se debe establecer en NTFS.

Acerca de esta tarea

- Puede especificar el estilo de seguridad del volumen raíz en el momento de crear la SVM.
- Si la SVM no se crea con el volumen raíz establecido en estilo de seguridad NTFS, puede cambiar el estilo de seguridad más adelante mediante el `volume modify` comando.

Pasos

1. Determine el estilo de seguridad actual del volumen raíz de la SVM:

```
volume show -vserver vs1 -fields vs1,volume,security-style
```

2. Si el volumen raíz no es un volumen con estilo de seguridad NTFS, cambie el estilo de seguridad a NTFS:

```
volume modify -vserver vs1 -volume vs1_root -security-style ntfs
```

3. Compruebe que el volumen raíz de la SVM esté establecido en el estilo de seguridad NTFS:

```
volume show -vserver vs1 -fields vs1,volume,security-style
```

Ejemplo

Los siguientes comandos verifican que el estilo de seguridad del volumen raíz es NTFS en la SVM vs1:

```
cluster1::> volume show -vserver vs1 -fields vs1,volume,security-style
vs1      volume      security-style
-----
vs1      vs1_root     unix

cluster1::> volume modify -vserver vs1 -volume vs1_root -security-style ntfs

cluster1::> volume show -vserver vs1 -fields vs1,volume,security-style
vs1      volume      security-style
-----
vs1      vs1_root     ntfs
```

Comprobar que se han configurado las opciones necesarias del servidor CIFS

Debe verificar que las opciones del servidor CIFS necesarias se encuentran habilitadas y configuradas según los requisitos para las operaciones no disruptivas de Hyper-V y SQL Server sobre SMB.

Acerca de esta tarea

- Se deben habilitar SMB 2.x y SMB 3.0.
- La descarga de copias ODX debe estar habilitada para utilizar el rendimiento, lo que mejora la descarga de copias.
- Se deben habilitar los servicios de copia de volúmenes redundantes de VSS si la solución Hyper-V mediante SMB utiliza servicios de backup habilitados con VSS remoto (solo Hyper-V).

Pasos

1. Compruebe que las opciones necesarias del servidor CIFS estén habilitadas en la máquina virtual de almacenamiento (SVM):
 - a. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

- b. Introduzca el siguiente comando:

```
vserver cifs options show -vserver vserver_name
```

Las siguientes opciones deben configurarse en `true`:

- `-smb2-enabled`
- `-smb3-enabled`
- `-copy-offload-enabled`
- `-shadowcopy-enabled` (Solo Hyper-V)

2. Si alguna de las opciones no se ha establecido en `true`, lleve a cabo lo siguiente:
 - a. Configúrelas como `true` mediante el uso de `vserver cifs options modify` comando.
 - b. Compruebe que las opciones están definidas en `true` mediante el uso de `vserver cifs options show` comando.
3. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

Ejemplo

Los siguientes comandos verifican que las opciones necesarias para la configuración de Hyper-V sobre SMB están habilitadas en SVM vs1. En el ejemplo, es necesario habilitar la descarga de copias ODX para satisfacer los requisitos de opciones.

```

cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled,copy-offload-enabled,shadowcopy-enabled
vserver smb2-enabled smb3-enabled copy-offload-enabled shadowcopy-enabled
-----
vs1      true          true          false          true

cluster-1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster-1::*> vserver cifs options show -vserver vs1 -fields copy-offload-
enabled
vserver  copy-offload-enabled
-----
vs1      true

cluster1::*> set -privilege admin

```

Configure multicanal de SMB para un mayor rendimiento y redundancia

A partir de ONTAP 9.4, puede configurar SMB MultiChannel para proporcionar varias conexiones entre ONTAP y clientes en una sola sesión SMB. Al hacerlo, mejora el rendimiento y la tolerancia a fallos para Hyper-V y SQL Server en configuraciones SMB.

Lo que necesitará

Solo se puede utilizar la funcionalidad multicanal de SMB cuando los clientes negocian en SMB 3.0 o versiones posteriores. De forma predeterminada, SMB 3.0 y las versiones posteriores se encuentran habilitadas en el servidor SMB de ONTAP.

Acerca de esta tarea

Los clientes de SMB detectan y utilizan automáticamente varias conexiones de red si se identifica una configuración adecuada en el clúster de ONTAP.

El número de conexiones simultáneas en una sesión SMB depende de las NIC que haya implementado:

- **1G NIC en el cluster ONTAP y cliente**

El cliente establece una conexión por NIC y enlaza la sesión a todas las conexiones.

- **NIC 10G y mayor capacidad en cluster ONTAP y cliente**

El cliente establece hasta cuatro conexiones por NIC y enlaza la sesión a todas las conexiones. El cliente puede establecer conexiones en varias NIC de 10 G y de mayor capacidad.

También puede modificar los siguientes parámetros (privilegios avanzados):

- **-max-connections-per-session**

El número máximo de conexiones permitidas por sesión multicanal. El valor predeterminado es 32 conexiones.

Si desea habilitar más conexiones que las predeterminadas, debe realizar ajustes comparables a la configuración del cliente, que también tiene un valor predeterminado de 32 conexiones.

- **-max-lifs-per-session**

Número máximo de interfaces de red anunciadas por sesión multicanal. El valor predeterminado es 256 interfaces de red.

Pasos

1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Habilite multicanal de SMB en el servidor SMB:

```
vserver cifs options modify -vserver vserver_name -is-multichannel-enabled true
```

3. Compruebe que ONTAP informa de sesiones multicanal de SMB:

```
vserver cifs session options show
```

4. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

Ejemplo

En el siguiente ejemplo, se muestra información sobre todas las sesiones SMB, donde se muestran varias conexiones para una sola sesión:

```
cluster1::> vserver cifs session show
Node:      node1
Vserver:   vs1
Connection Session                               Open
Idle
IDs        ID      Workstation      Windows User      Files
Time
-----
-----
138683,
138684,
138685      1      10.1.1.1      DOMAIN\
4s
Administrator
```

En el siguiente ejemplo, se muestra información detallada sobre una sesión SMB con el ID de sesión 1:

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1
Node: node1
Session ID: 1
Connection IDs: 138683,138684,138685
Connection Count: 3
Incoming Data LIF IP Address: 192.1.1.1
Workstation IP Address: 10.1.1.1
Authentication Mechanism: NTLMv1
User Authenticated as: domain-user
Windows User: DOMAIN\administrator
UNIX User: root
Open Shares: 2
Open Files: 5
Open Other: 0
Connected Time: 5s
Idle Time: 5s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: false
NetBIOS Name: -
```

Crear volúmenes de datos NTFS

Debe crear volúmenes de datos NTFS en la máquina virtual de almacenamiento (SVM) antes de poder configurar recursos compartidos disponibles de forma continua para

usarlos con Hyper-V o SQL Server en servidores de aplicaciones SMB. Use la hoja de cálculo de configuración de volúmenes para crear los volúmenes de datos.

Acerca de esta tarea

Existen parámetros opcionales que se pueden usar para personalizar un volumen de datos. Para obtener más información acerca de cómo personalizar volúmenes, consulte [xref:./smb-hyper-v-sql/"Gestión de almacenamiento lógico"](#).

A medida que cree los volúmenes de datos, no debe crear puntos de unión en un volumen que contenga los siguientes:

- Archivos de Hyper-V para los que ONTAP realiza instantáneas
- Archivos de base de datos de SQL Server de los que se realiza un backup mediante SQL Server



Si crea de forma accidental un volumen que utiliza un estilo de seguridad mixto o UNIX, no se puede cambiar el volumen a un volumen de estilo de seguridad NTFS y, a continuación, usarlo directamente para crear recursos compartidos disponibles de forma continua para operaciones no disruptivas. Las operaciones no disruptivas para Hyper-V y SQL Server sobre SMB no funcionan correctamente a menos que los volúmenes utilizados en la configuración se creen como volúmenes de estilo de seguridad NTFS. Debe eliminar el volumen y volver a crear el volumen con estilo de seguridad NTFS. También es posible asignar el volumen en un host de Windows y aplicar una ACL en la parte superior del volumen y propagar la ACL a todos los archivos y carpetas del volumen.

Pasos

1. Cree el volumen de datos introduciendo el comando correspondiente:

| Si desea crear un volumen en una SVM donde el estilo de seguridad del volumen raíz es... | Introduzca el comando... |
|--|--|
| NTFS | <code>volume create -vserver vservice_name -volume volume_name -aggregate aggregate_name -size integer[KB MB GB TB PB] -junction-path path</code> |
| No NTFS | <code>volume create -vserver vservice_name -volume volume_name -aggregate aggregate_name -size integer[KB MB GB TB PB] -security-style ntfs -junction-path path</code> |

2. Compruebe que la configuración del volumen sea correcta:

```
volume show -vserver vservice_name -volume volume_name
```

Crear recursos compartidos de SMB disponibles de forma continua

Después de crear los volúmenes de datos, puede crear los recursos compartidos disponibles de forma continua que los servidores de aplicaciones utilizan para acceder a

los archivos de configuración y de la máquina virtual Hyper-V y los archivos de la base de datos de SQL Server. Debe utilizar la hoja de datos de configuración del recurso compartido a medida que crea los recursos compartidos de SMB.

Pasos

1. Muestre información sobre los volúmenes de datos existentes y sus rutas de unión:

```
volume show -vserver vs1 -junction
```

2. Crear un recurso compartido de SMB disponible de forma continua:

```
vserver cifs share create -vserver vs1 -share-name share_name -path  
path -share-properties oplocks,continuously-available -symlink "" [-comment  
text]
```

- Opcionalmente, puede añadir un comentario a la configuración del recurso compartido.
 - De forma predeterminada, la propiedad de recurso compartido de archivos sin conexión está configurada en el recurso compartido y se establece en `manual`.
 - ONTAP crea el recurso compartido con el permiso de recurso compartido predeterminado de Windows `Everyone / Full Control`.
3. Repita el paso anterior para todos los recursos compartidos de la hoja de datos de configuración del recurso compartido.
 4. Compruebe que la configuración es correcta mediante el `vserver cifs share show` comando.
 5. Configure los permisos de archivo NTFS en los recursos compartidos disponibles continuamente asignando una unidad a cada recurso compartido y configurando los permisos de archivo mediante la ventana **Propiedades de Windows**.

Ejemplo

Los siguientes comandos crean un recurso compartido disponible de forma continua llamado «data2» en la máquina virtual de almacenamiento (SVM, antes denominada Vserver) vs1. Los enlaces simbólicos se desactivan mediante la configuración de `-symlink` parámetro a `""`:

```

cluster1::> volume show -vserver vs1 -junction

```

| Vserver | Volume | Active | Junction Path | Junction Path Source |
|---------|----------|--------|---------------|----------------------|
| vs1 | data | true | /data | RW_volume |
| vs1 | data1 | true | /data/data1 | RW_volume |
| vs1 | data2 | true | /data/data2 | RW_volume |
| vs1 | vs1_root | - | / | - |

```

cluster1::> vserver cifs share create -vserver vs1 -share-name data2 -path
/data/data2 -share-properties oplocks,continuously-available -symlink ""

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

```

```

Vserver: vs1
Share: data2
CIFS Server NetBIOS Name: VS1
Path: /data/data2
Share Properties: oplocks
continuously-available
Symlink Properties: -
File Mode Creation Mask: -
Directory Mode Creation Mask: -
Share Comment: -
Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
Volume Name: -
Offline Files: manual
Vscan File-Operations Profile: standard

```

Agregue el privilegio SeSecurityPrivilege a la cuenta de usuario (para recursos compartidos SMB de SQL Server).

La cuenta de usuario de dominio utilizada para instalar el servidor SQL debe tener asignado el privilegio "SeSecurityPrivilege" para realizar determinadas acciones en el servidor CIFS que requieren privilegios no asignados de forma predeterminada a los usuarios de dominio.

Lo que necesitará

La cuenta de dominio utilizada para instalar SQL Server ya debe existir.

Acerca de esta tarea

Al agregar el privilegio a la cuenta del instalador de SQL Server, ONTAP podría validar la cuenta poniéndose en contacto con el controlador de dominio. Es posible que se produzca un error en el comando si ONTAP no puede comunicarse con la controladora de dominio.

Pasos

1. Añada el privilegio "SeSecurityPrivilege":

```
vserver cifs users-and-groups privilege add-privilege -vserver vserver_name  
-user-or-group-name account_name -privileges SeSecurityPrivilege
```

El valor de `-user-or-group-name` Parámetro es el nombre de la cuenta de usuario de dominio utilizada para instalar SQL Server.

2. Compruebe que el privilegio se aplica a la cuenta:

```
vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-  
group-name account_name
```

Ejemplo

El siguiente comando agrega el privilegio "SeSecurityPrivilege" a la cuenta del instalador de SQL Server en el dominio DE EJEMPLO de la máquina virtual de almacenamiento (SVM) vs1:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver  
vs1 -user-or-group-name EXAMPLE\SQLInstaller -privileges  
SeSecurityPrivilege  
  
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1  
Vserver      User or Group Name          Privileges  
-----  
vs1          EXAMPLE\SQLInstaller        SeSecurityPrivilege
```

Configurar la profundidad del directorio de copia de sombra de VSS (para Hyper-V mediante recursos compartidos de SMB)

Opcionalmente, puede configurar la profundidad máxima de directorios dentro de recursos compartidos SMB en los que crear copias de sombra. Este parámetro resulta útil si desea controlar manualmente el nivel máximo de subdirectorios en los que ONTAP debe crear instantáneas.

Lo que necesitará

La función de copia de sombra VSS debe estar activada.

Acerca de esta tarea

El valor predeterminado es crear instantáneas para un máximo de cinco subdirectorios. Si el valor se establece en 0, ONTAP crea instantáneas para todos los subdirectorios.



Aunque puede especificar que la profundidad del directorio del conjunto de instantáneas incluya más de cinco subdirectorios o todos los subdirectorios, existe el requisito de Microsoft de que la creación del conjunto de instantáneas se lleve a cabo en 60 segundos. La creación del conjunto de instantáneas falla si no se puede completar en este momento. La profundidad del directorio de instantáneas que elija no debe hacer que el tiempo de creación supere el límite de tiempo.

Pasos

1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Establezca la profundidad del directorio de copia de sombra VSS en el nivel deseado:

```
vserver cifs options modify -vserver vserver_name -shadowcopy-dir-depth  
integer
```

```
vserver cifs options modify -vserver vs1 -shadowcopy-dir-depth 6
```

3. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

Gestione Hyper-V y SQL Server con las configuraciones de SMB

Configure los recursos compartidos existentes para una disponibilidad continua

Puede modificar los recursos compartidos existentes para que estén siempre disponibles y que los servidores de aplicaciones de Hyper-V y SQL Server utilicen para acceder de forma no disruptiva a los archivos de configuración y de máquinas virtuales de Hyper-V, así como a los archivos de bases de datos de SQL Server.

Acerca de esta tarea

No puede utilizar un recurso compartido existente como un recurso compartido disponible de forma continua para las operaciones no disruptivas con servidores de aplicaciones a través de SMB si el recurso compartido tiene las siguientes características:

- Si la `homedirectory` la propiedad share se establece en ese recurso compartido
- Si el recurso compartido contiene enlaces simbólicos activados o enlaces con cables
- Si el recurso compartido contiene volúmenes juntados por debajo de la raíz del recurso compartido

Debe verificar que los dos parámetros de recursos compartidos siguientes estén configurados correctamente:

- La `-offline-files` el parámetro está establecido en cualquiera de los dos `manual` (el valor predeterminado) o `none`.
- Los enlaces simbólicos deben estar desactivados.

Deben configurarse las siguientes propiedades compartidas:

- `continuously-available`
- `oplocks`

No se deben establecer las siguientes propiedades compartidas. Si están presentes en la lista de propiedades de recursos compartidos actuales, deben eliminarse del recurso compartido continuamente disponible:

- `attributecache`
- `branchcache`

Pasos

1. Mostrar la configuración actual de los parámetros de recursos compartidos y la lista actual de propiedades de recursos compartidos configuradas:

```
vserver cifs share show -vserver vserver_name -share-name share_name
```

2. Si es necesario, modifique los parámetros del recurso compartido para desactivar los enlaces simbólicos y establezca los archivos offline en manual mediante el `vserver cifs share properties modify` comando.

Puede deshabilitar los enlaces simbólicos estableciendo el valor de `-symlink` parámetro a `""`.

- Puede deshabilitar los enlaces simbólicos estableciendo el valor de `-symlink` parámetro a `""`.

- Puede ajustar la `-offline-files` especifique el parámetro en el ajuste correcto manual.

3. Añada el `continuously-available` compartir la propiedad y, si es necesario, la `oplocks` compartir propiedad:

```
vserver cifs share properties add -vserver vserver_name -share-name share_name  
-share-properties continuously-available[,oplock]
```

Si la `oplocks` la propiedad share no está establecida, debe añadirla junto con la `continuously-available` compartir propiedad.

4. Quite todas las propiedades de recursos compartidos que no sean compatibles con recursos compartidos disponibles de forma continua:

```
vserver cifs share properties remove -vserver vserver_name -share-name  
share_name -share-properties properties[,...]
```

Puede quitar una o varias propiedades de recursos compartidos si especifica las propiedades de recursos compartidos con una lista delimitada por comas.

5. Compruebe que el `-symlink` y.. `-offline-files` los parámetros se ajustan correctamente:

```
vserver cifs share show -vserver vserver_name -share-name share_name -fields  
symlink-properties,offline-files
```

6. Compruebe que la lista de propiedades de recursos compartidos configuradas es correcta:

```
vserver cifs shares properties show -vserver vserver_name -share-name  
share_name
```

Ejemplos

El siguiente ejemplo muestra cómo configurar un recurso compartido existente llamado «shara1» en la máquina virtual de almacenamiento (SVM) vs1 para NDOS con un servidor de aplicaciones en SMB:

- Los enlaces simbólicos se desactivan en el recurso compartido estableciendo la `-symlink` parámetro a `""`.
- La `-offline-file` el parámetro se modifica y se establece en manual.
- La `continuously-available` la propiedad share se agrega al recurso compartido.

- La `oplocks` la propiedad `share` ya está en la lista de propiedades de recurso compartido; por lo tanto, no es necesario añadirla.
- La `attributecache` la propiedad `share` se quita del recurso compartido.
- La `browsable` La propiedad `Share` es opcional para un recurso compartido disponible continuamente que se utiliza para NDOS con servidores de aplicaciones en SMB y se conserva como una de las propiedades compartidas.

```
cluster1::> vsserver cifs share show -vsserver vs1 -share-name share1
```

```

        Vserver: vs1
        Share: share1
CIFS Server NetBIOS Name: vs1
        Path: /data
    Share Properties: oplocks
                     browsable
                     attributecache
    Symlink Properties: enable
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
        Share Comment: -
        Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
        Volume Name: data
        Offline Files: documents
Vscan File-Operations Profile: standard
```

```
cluster1::> vsserver cifs share modify -vsserver vs1 -share-name share1
-offline-file manual -symlink ""
```

```
cluster1::> vsserver cifs share properties add -vsserver vs1 -share-name
share1 -share-properties continuously-available
```

```
cluster1::> vsserver cifs share properties remove -vsserver vs1 -share-name
share1 -share-properties attributecache
```

```
cluster1::> vsserver cifs share show -vsserver vs1 -share-name share1
-fields symlink-properties,offline-files
vsserver  share-name symlink-properties offline-files
```

```
-----
vs1      share1      -                      manual
```

```
cluster1::> vsserver cifs share properties show -vsserver vs1 -share-name
share1
```

```

        Vserver: vs1
        Share: share1
Share Properties: oplocks
                 browsable
                 continuously-available
```


Habilite o deshabilite las copias de sombra de VSS para backups de Hyper-V mediante SMB

Si utiliza una aplicación de backup compatible con VSS para realizar backups de los archivos de máquina virtual de Hyper-V almacenados en recursos compartidos SMB, debe habilitarse la copia de sombra de VSS. Puede deshabilitar la copia de sombra de VSS si no utiliza aplicaciones de backup compatibles con VSS. El valor predeterminado es activar la copia de sombra VSS.

Acerca de esta tarea

Puede activar o desactivar las instantáneas VSS en cualquier momento.

Pasos

- 1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

- 2. Ejecute una de las siguientes acciones:

| Si desea que las copias redundantes de VSS sean... | Introduzca el comando... |
|--|--|
| Activado | <code>vserver cifs options modify -vserver vserver_name -shadowcopy-enabled true</code> |
| Deshabilitado | <code>vserver cifs options modify -vserver vserver_name -shadowcopy-enabled false</code> |

- 3. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

Ejemplo

Los siguientes comandos habilitan las copias de sombra de VSS en la SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -shadowcopy-enabled
true

cluster1::*> set -privilege admin
```

Utilice estadísticas para supervisar la actividad de Hyper-V y SQL Server mediante SMB

Determine qué objetos de estadísticas y contadores están disponibles

Para poder obtener información acerca de las estadísticas de CIFS, SMB, auditoría y BranchCache hash, y supervisar el rendimiento, debe conocer los objetos y contadores disponibles desde los cuales puede obtener datos.

Pasos

1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Ejecute una de las siguientes acciones:

| Si desea determinar... | Introduzca... |
|----------------------------------|--|
| Qué objetos están disponibles | <code>statistics catalog object show</code> |
| Objetos específicos disponibles | <code>statistics catalog object show object <i>object_name</i></code> |
| Qué contadores están disponibles | <code>statistics catalog counter show object <i>object_name</i></code> |

Consulte las páginas de manual para obtener más información acerca de los objetos y contadores disponibles.

3. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

Ejemplos

El siguiente comando muestra descripciones de los objetos de estadísticas seleccionados relacionados con CIFS y acceso SMB en el clúster tal y como se ve en el nivel de privilegio avanzado:

```
cluster1::> set -privilege advanced
```

Warning: These advanced commands are potentially dangerous; use them only when directed to do so by support personnel.

Do you want to continue? {y|n}: y

```
cluster1::*> statistics catalog object show -object audit
      audit_ng          CM object for exporting audit_ng
performance counters
```

```
cluster1::*> statistics catalog object show -object cifs
      cifs              The CIFS object reports activity of the
                        Common Internet File System protocol
                        ...
```

```
cluster1::*> statistics catalog object show -object nblade_cifs
      nblade_cifs       The Common Internet File System (CIFS)
                        protocol is an implementation of the
Server
                        ...
```

```
cluster1::*> statistics catalog object show -object smb1
      smb1              These counters report activity from the
SMB
                        revision of the protocol. For information
                        ...
```

```
cluster1::*> statistics catalog object show -object smb2
      smb2              These counters report activity from the
                        SMB2/SMB3 revision of the protocol. For
                        ...
```

```
cluster1::*> statistics catalog object show -object hashd
      hashd             The hashd object provides counters to
measure
                        the performance of the BranchCache hash
daemon.
```

```
cluster1::*> set -privilege admin
```

El siguiente comando muestra información acerca de algunos contadores de `cifs` objeto como se ve en el nivel de privilegio avanzado:



En este ejemplo no se muestran todos los contadores disponibles para el `cifs` objeto; la salida se truncará.

```
cluster1::> set -privilege advanced
```

Warning: These advanced commands are potentially dangerous; use them only when directed to do so by support personnel.

Do you want to continue? {y|n}: y

```
cluster1::*> statistics catalog counter show -object cifs
```

Object: cifs

| Counter | Description |
|----------------------|--|
| active_searches | Number of active searches over SMB and SMB2 |
| auth_reject_too_many | Authentication refused after too many requests were made in rapid succession |
| avg_directory_depth | Average number of directories crossed by SMB and SMB2 path-based commands |
| ... | ... |

```
cluster2::> statistics start -object client -sample-id
```

Object: client

| Counter | Value |
|----------------------|-------------------------|
| cifs_ops | 0 |
| cifs_read_ops | 0 |
| cifs_read_recv_ops | 0 |
| cifs_read_recv_size | 0B |
| cifs_read_size | 0B |
| cifs_write_ops | 0 |
| cifs_write_recv_ops | 0 |
| cifs_write_recv_size | 0B |
| cifs_write_size | 0B |
| instance_name | vserver_1:10.72.205.179 |
| instance_uuid | 2:10.72.205.179 |
| local_ops | 0 |
| mount_ops | 0 |

[...]

Mostrar estadísticas de SMB

Puede mostrar varias estadísticas de SMB para supervisar el rendimiento y diagnosticar

problemas.

Pasos

1. Utilice la `statistics start` y opcional `statistics stop` comandos para recoger una muestra de datos.
2. Ejecute una de las siguientes acciones:

| Si desea mostrar estadísticas de... | Introduzca el siguiente comando... |
|-------------------------------------|--|
| Todas las versiones de SMB | <code>statistics show -object cifs</code> |
| SMB 1,0 | <code>statistics show -object smb1</code> |
| SMB 2.x y SMB 3.0 | <code>statistics show -object smb2</code> |
| Subsistema SMB del nodo | <code>statistics show -object nblade_cifs</code> |

Obtenga más información sobre la `statistics` comandos:

- ["se muestran las estadísticas"](#)
- ["inicio de las estadísticas"](#)
- ["se detienen las estadísticas"](#)

Compruebe que la configuración admite operaciones no disruptivas

Utilice la supervisión del estado para determinar si el estado de las operaciones no disruptivas es correcto

La supervisión del estado proporciona información sobre el estado del sistema en todo el clúster. El monitor de estado supervisa la configuración de Hyper-V y SQL Server en SMB para garantizar las operaciones no disruptivas (NDO) de los servidores de aplicaciones. Si el estado es degradado, puede ver detalles del problema, incluidas la causa probable y las acciones de recuperación recomendadas.

Hay varios monitores de estado. ONTAP supervisa el estado general del sistema y el de los monitores de estado individuales. El monitor de estado de conectividad del nodo contiene el subsistema CIFS-NDO. El monitor tiene un conjunto de políticas de estado que activan alertas si ciertas condiciones físicas pueden producir interrupciones y, si se produce una condición disruptiva, genera alertas y proporciona información sobre acciones correctivas. Para OPERACIONES NO DISRUPTIVAS en configuraciones de SMB, se generan alertas de las dos condiciones siguientes:

| ID de alerta | Gravedad | Condición |
|----------------------------------|------------|--|
| HaNotReadyCifsNdo_Alert | Importante | Se han abierto uno o varios archivos alojados por un volumen de un agregado del nodo a través de un recurso compartido de SMB disponible de forma continua con la promesa de persistencia en caso de fallo; sin embargo, la relación de alta disponibilidad con el partner no está configurada o no es correcta. |
| NoStandbyLifCifsNdo_Alert | Menor | La máquina virtual de almacenamiento (SVM) está sirviendo datos activamente en SMB a través de un nodo. Además, hay archivos SMB abiertos de forma persistente en recursos compartidos disponibles de forma continua; sin embargo, su nodo de partner no está exponiendo ningún LIF de datos activo para la SVM. |

Muestre el estado de funcionamiento no disruptivo mediante la supervisión del estado del sistema

Puede utilizar el `system health` Comandos para mostrar información sobre el estado general del sistema del clúster y el estado del subsistema CIFS-NDO, para responder a las alertas, configurar alertas futuras y mostrar información sobre cómo se configura la supervisión del estado.

Pasos

1. Supervise el estado realizando la acción correspondiente:

| Si desea mostrar... | Introduzca el comando... |
|--|--|
| El estado del sistema, que refleja el estado general de los monitores de estado individuales | <code>system health status show</code> |
| Información sobre el estado del subsistema CIFS-NDO | <code>system health subsystem show -subsystem CIFS-NDO -instance</code> |

2. Muestre información acerca de cómo se configura la supervisión de alertas CIFS-NDO mediante las acciones adecuadas:

| Si desea mostrar información acerca de... | Introduzca el comando... |
|--|---|
| La configuración y el estado del monitor de estado del subsistema CIFS-NDO, como nodos supervisados, estado de inicialización y estado | <code>system health config show -subsystem CIFS-NDO</code> |

| Si desea mostrar información acerca de... | Introduzca el comando... |
|---|---|
| Las alertas CIFS-NDO que un monitor de estado puede generar potencialmente | system health alert definition show -subsystem CIFS-NDO |
| Las políticas de supervisión del estado de CIFS-NDO, que determinan cuándo se generan las alertas | system health policy definition show -monitor node-connect |



Utilice la `-instance` parámetro para mostrar información detallada.

Ejemplos

En el siguiente resultado se muestra información acerca del estado general del clúster y del subsistema CIFS-NDO:

```
cluster1::> system health status show
Status
-----
ok

cluster1::> system health subsystem show -instance -subsystem CIFS-NDO

                Subsystem: CIFS-NDO
                Health: ok
        Initialization State: initialized
Number of Outstanding Alerts: 0
Number of Suppressed Alerts: 0
                Node: node2
Subsystem Refresh Interval: 5m
```

En el siguiente resultado, se muestra información detallada sobre la configuración y el estado del monitor de estado del subsistema CIFS-NDO:

```

cluster1::> system health config show -subsystem CIFS-NDO -instance

Node: node1
Monitor: node-connect
Subsystem: SAS-connect, HA-health, CIFS-NDO
Health: ok
Monitor Version: 2.0
Policy File Version: 1.0
Context: node_context
Aggregator: system-connect
Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0

Node: node2
Monitor: node-connect
Subsystem: SAS-connect, HA-health, CIFS-NDO
Health: ok
Monitor Version: 2.0
Policy File Version: 1.0
Context: node_context
Aggregator: system-connect
Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0

```

Compruebe la configuración de recursos compartidos de SMB continuamente disponible

Para admitir operaciones no disruptivas, los recursos compartidos de Hyper-V y SQL Server SMB deben configurarse como recursos compartidos constantemente disponibles. Además, hay otros ajustes de recursos compartidos que debe comprobar. Debe verificar que los recursos compartidos están correctamente configurados para proporcionar operaciones sin interrupciones para los servidores de aplicaciones, en caso de que se produzcan eventos de interrupción planificados o no planificados.

Acerca de esta tarea

Debe verificar que los dos parámetros de recursos compartidos siguientes estén configurados correctamente:

- La `-offline-files` el parámetro está establecido en cualquiera de los dos `manual` (el valor predeterminado) o. `none`.
- Los enlaces simbólicos deben estar desactivados.

Para que las operaciones sean correctas no disruptivas, debe configurarse las siguientes propiedades compartidas:

- `continuously-available`
- `oplocks`

No deben configurarse las siguientes propiedades compartidas:

- `homedirectory`
- `attributecache`
- `branchcache`
- `access-based-enumeration`

Pasos

1. Compruebe que los archivos sin conexión están establecidos en `manual` o. `disabled` y que los enlaces simbólicos están desactivados:

```
vserver cifs shares show -vserver vserver_name
```

2. Compruebe que los recursos compartidos de SMB están configurados para una disponibilidad continua:

```
vserver cifs shares properties show -vserver vserver_name
```

Ejemplos

En el siguiente ejemplo, se muestra la configuración de recurso compartido para un recurso compartido llamado «shara1» en la máquina virtual de almacenamiento (SVM, antes denominada Vserver) `vs1`. Los archivos sin conexión se establecen en `manual` y los enlaces simbólicos están desactivados (designados por un guión en el `Symlink Properties` salida de campo):

```

cluster1::> vserver cifs share show -vserver vs1 -share-name share1
                Vserver: vs1
                Share: share1
    CIFS Server NetBIOS Name: VS1
                Path: /data/share1
    Share Properties: oplocks
                    continuously-available
    Symlink Properties: -
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
    Share Comment: -
    Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
    Volume Name: -
    Offline Files: manual
    Vscan File-Operations Profile: standard

```

En el siguiente ejemplo, se muestran las propiedades de uso compartido de un recurso compartido denominado «shara1» en la SVM vs1:

```

cluster1::> vserver cifs share properties show -vserver vs1 -share-name
share1
Vserver      Share      Properties
-----      -
vs1          share1    oplocks
                    continuously-available

```

Comprobar el estado de la LIF

Aunque configure máquinas virtuales de almacenamiento (SVM) con Hyper-V y SQL Server en configuraciones de SMB para tener LIF en cada nodo de un clúster, durante las operaciones diarias, algunas LIF se pueden mover a puertos de otro nodo. Debe verificar el estado de LIF y realizar las acciones correctivas que sean necesarias.

Acerca de esta tarea

Para proporcionar soporte de operaciones no disruptivas y fluido, cada nodo de un clúster debe tener al menos un LIF para la SVM y todos los LIF deben estar asociados a un puerto de inicio. Si algunos de los LIF configurados actualmente no están asociados a su puerto de inicio, debe solucionar cualquier problema de los puertos y, a continuación, revertir los LIF a su puerto de inicio.

Pasos

1. Muestra información acerca de las LIF configuradas para la SVM:

```
network interface show -vserver vserver_name
```

En este ejemplo, "lif1" no se encuentra en el puerto de origen.

```
network interface show -vserver vs1
```

| Vserver | Logical Interface | Status Admin/Oper | Network Address/Mask | Current Node | Current Is Port |
|---------|-------------------|-------------------|----------------------|--------------|-----------------|
| Home | | | | | |
| ----- | ----- | ----- | ----- | ----- | ----- |
| vs1 | lif1 | up/up | 10.0.0.128/24 | node2 | e0d |
| false | lif2 | up/up | 10.0.0.129/24 | node2 | e0d |
| true | | | | | |

2. Si algunas de las LIF no están en sus puertos raíz, realice los pasos siguientes:

a. Para cada LIF, determine en qué puerto de inicio de la LIF se encuentra:

```
network interface show -vserver vserver_name -lif lif_name -fields home-node,home-port
```

```
network interface show -vserver vs1 -lif lif1 -fields home-node,home-port
```

| vserver | lif | home-node | home-port |
|---------|------|-----------|-----------|
| ----- | ---- | ----- | ----- |
| vs1 | lif1 | node1 | e0d |

b. Para cada LIF, determine si el puerto de inicio del LIF está activo:

```
network port show -node node_name -port port -fields port,link
```

```
network port show -node node1 -port e0d -fields port,link
```

| node | port | link |
|-------|------|------|
| ----- | ---- | ---- |
| node1 | e0d | up |

+

En este ejemplo, «lif1» debería ser trasladado de vuelta a su puerto de origen, node1:e0d.

- Si alguna de las interfaces de red del puerto de inicio a las que se deberían asociar las LIF no está en la up state, resuelva el problema para que estas interfaces estén en funcionamiento.
- Si es necesario, revierte las LIF a sus puertos de inicio:

```
network interface revert -vserver vserver_name -lif lif_name
```

```
network interface revert -vserver vs1 -lif lif1
```

5. Compruebe que cada nodo del clúster tiene un LIF activo para la SVM:

```
network interface show -vserver vserver_name
```

```
network interface show -vserver vs1
```

| Vserver | Logical Interface | Status Admin/Oper | Network Address/Mask | Current Node | Current Port | Is |
|---------|-------------------|-------------------|----------------------|--------------|--------------|-------|
| Home | | | | | | |
| ----- | ----- | ----- | ----- | ----- | ----- | ----- |
| ---- | | | | | | |
| vs1 | | | | | | |
| | lif1 | up/up | 10.0.0.128/24 | node1 | e0d | |
| true | | | | | | |
| | lif2 | up/up | 10.0.0.129/24 | node2 | e0d | |
| true | | | | | | |

Determinar si las sesiones SMB están disponibles continuamente

Muestra información de la sesión SMB

Puede mostrar información acerca de las sesiones SMB establecidas, incluidos la conexión SMB y el ID de sesión y la dirección IP de la estación de trabajo mediante la sesión. Es posible mostrar información sobre la versión del protocolo SMB de la sesión y el nivel de protección disponible continuamente, lo que ayuda a identificar si la sesión admite operaciones no disruptivas.

Acerca de esta tarea

Puede mostrar información de todas las sesiones de la SVM en formato de resumen. Sin embargo, en muchos casos, la cantidad de producción que se devuelve es grande. Puede personalizar la información que se muestra en el resultado especificando parámetros opcionales:

- Puede usar el opcional `-fields` parámetro para mostrar el resultado de los campos seleccionados.

Puede entrar `-fields ?` para determinar qué campos se pueden utilizar.

- Puede utilizar el `-instance` Parámetro para mostrar información detallada sobre las sesiones SMB establecidas.
- Puede utilizar el `-fields` o el `-instance` parámetro independiente o en combinación con otros parámetros opcionales.

Pasos

1. Ejecute una de las siguientes acciones:

| | |
|--|--|
| Si desea mostrar información de la sesión SMB... | Introduzca el siguiente comando... |
| Para todas las sesiones del SVM en formato de resumen | vserver cifs session show -vserver <i>vserver_name</i> |
| En un ID de conexión especificado | vserver cifs session show -vserver <i>vserver_name</i> -connection-id integer |
| Desde una dirección IP de estación de trabajo especificada | vserver cifs session show -vserver <i>vserver_name</i> -address <i>workstation_IP_address</i> |
| En una dirección IP de LIF especificada | vserver cifs session show -vserver <i>vserver_name</i> -lif -address <i>LIF_IP_address</i> |
| En un nodo especificado | <i>**vserver cifs session show -vserver vserver_name -node {node_name</i> |
| <i>local}**</i> | Desde un usuario de Windows especificado |
| vserver cifs session show -vserver <i>vserver_name</i> -windows-user <i>user_name</i> El formato para <i>user_name</i> es [domain]\user. | Con un mecanismo de autenticación especificado |

| | |
|--|---|
| Si desea mostrar información de la sesión SMB... | Introduzca el siguiente comando... |
| <pre> vserver cifs session show -vserver vserver_name -auth -mechanism authentication_mec hanism </pre> <p>Valor para -auth -mechanism puede ser uno de los siguientes:</p> <ul style="list-style-type: none"> • NTLMv1 • NTLMv2 • Kerberos • Anonymous | Con una versión de protocolo especificada |

Si desea mostrar información de la sesión SMB...

Introduzca el siguiente comando...

```
vserver cifs  
session show  
-vserver  
vserver_name  
-protocol-version  
protocol_version
```

Valor para -protocol
-version puede ser
uno de los siguientes:

- SMB1
- SMB2
- SMB2_1
- SMB3
- SMB3_1

Con un nivel especificado de protección continua disponible

| | |
|--|---|
| Si desea mostrar información de la sesión SMB... | Introduzca el siguiente comando... |
| <pre> vserver cifs session show -vserver vserver_name -continuously -available continuously_avail able_protection_le vel </pre> <p>Valor para -continuously -available puede ser uno de los siguientes:</p> <ul style="list-style-type: none"> • No • Yes • Partial | Con un estado de sesión de firma SMB especificado |

Ejemplos

El siguiente comando muestra información de sesión para las sesiones en SVM vs1 establecidas desde una estación de trabajo con dirección IP 10.1.1.1:

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:      node1
Vserver:   vs1
Connection Session
ID          ID          Workstation      Windows User      Open      Idle
-----
3151272279,
3151272280,
3151272281  1          10.1.1.1        DOMAIN\joe        2         23s
```

El siguiente comando muestra información detallada de la sesión para las sesiones con protección continuamente disponible en SVM vs1. La conexión se realizó mediante la cuenta de dominio.

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

Node: node1
Vserver: vs1
Session ID: 1
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation IP address: 10.1.1.2
Authentication Mechanism: Kerberos
Windows User: DOMAIN\SERVER1$
UNIX User: pcuser
Open Shares: 1
Open Files: 1
Open Other: 0
Connected Time: 10m 43s
Idle Time: 1m 19s
Protocol Version: SMB3
Continuously Available: Yes
Is Session Signed: false
User Authenticated as: domain-user
NetBIOS Name: -
SMB Encryption Status: Unencrypted
```

El siguiente comando muestra información de sesión en una sesión mediante SMB 3.0 y SMB MultiChannel en SVM vs1. En el ejemplo, el usuario se conectó a este recurso compartido desde un cliente con capacidad para SMB 3.0 mediante la dirección IP de LIF; por lo tanto, el mecanismo de autenticación se estableció de forma predeterminada en NTLMv2. La conexión se debe realizar mediante la autenticación Kerberos para

conectarse con la protección disponible continuamente.

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

Node: node1
Vserver: vs1
Session ID: 1
**Connection IDs: 3151272607,31512726078,3151272609
Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
Workstation IP address: 10.1.1.3
Authentication Mechanism: NTLMv2
Windows User: DOMAIN\administrator
UNIX User: pcuser
Open Shares: 1
Open Files: 0
Open Other: 0
Connected Time: 6m 22s
Idle Time: 5m 42s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: false
User Authenticated as: domain-user
NetBIOS Name: -
SMB Encryption Status: Unencrypted
```

Muestra información acerca de los archivos SMB abiertos

Es posible ver información sobre los archivos SMB abiertos, incluidos la conexión de SMB y el ID de sesión, el volumen de host, el nombre del recurso compartido y la ruta del recurso compartido. También es posible ver información acerca del nivel de protección continuamente disponible de un archivo, lo cual es útil para determinar si un archivo abierto está en un estado que admite operaciones no disruptivas.

Acerca de esta tarea

Puede ver información sobre los archivos abiertos en una sesión de SMB establecida. La información que se muestra es útil cuando necesita determinar la información de la sesión SMB para determinados archivos dentro de una sesión SMB.

Por ejemplo, si tiene una sesión SMB en la que algunos archivos abiertos están abiertos con protección continua disponible y algunos no están abiertos con protección continua disponible (el valor de la `-continuously-available` campo en `vserver cifs session show` el resultado del comando es `Partial`), puede determinar qué archivos no están disponibles continuamente mediante este comando.

Puede mostrar información de todos los archivos abiertos en sesiones SMB establecidas en máquinas virtuales de almacenamiento (SVM) de forma resumida mediante la `vserver cifs session file show` comando sin ningún parámetro opcional.

Sin embargo, en muchos casos, la cantidad de producción devuelta es grande. Puede personalizar la información que se muestra en el resultado especificando parámetros opcionales. Esto puede resultar útil si desea ver información sólo de un pequeño subconjunto de archivos abiertos.

- Puede usar el opcional `-fields` parámetro para mostrar la salida en los campos que elija.

Es posible usar este parámetro de forma independiente o combinada con otros parámetros opcionales.


- Puede utilizar el `-instance` Parámetro para mostrar información detallada sobre los archivos SMB abiertos.

Es posible usar este parámetro de forma independiente o combinada con otros parámetros opcionales.

Pasos

1. Ejecute una de las siguientes acciones:

| Si desea mostrar archivos SMB abiertos... | Introduzca el siguiente comando... |
|---|--|
| En la SVM de forma resumida | <code>vserver cifs session file show -vserver vserver_name</code> |
| En un nodo especificado | <code>`*vserver cifs session file show -vserver vserver_name -node {node_name</code> |
| <code>local}*`</code> | En un ID de archivo especificado |
| <code>vserver cifs session file show -vserver vserver_name -file-id integer</code> | En un ID de conexión de SMB especificado |
| <code>vserver cifs session file show -vserver vserver_name -connection-id integer</code> | En un ID de sesión de SMB especificado |
| <code>vserver cifs session file show -vserver vserver_name -session-id integer</code> | En el agregado de host especificado |
| <code>vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name</code> | En el volumen especificado |
| <code>vserver cifs session file show -vserver vserver_name -hosting-volume volume_name</code> | En el recurso compartido de SMB especificado |
| <code>vserver cifs session file show -vserver vserver_name -share share_name</code> | En la ruta del bloque de mensajes del servidor especificada |

| Si desea mostrar archivos SMB abiertos... | Introduzca el siguiente comando... |
|--|---|
| vserver cifs session file show -vserver <i>vserver_name</i> -path <i>path</i> | Con el nivel especificado de protección continua disponible |
| vserver cifs session file show -vserver <i>vserver_name</i> -continuously -available <i>continuously_available_status</i> Valor para <code>-continuously-available</code> puede ser uno de los siguientes: <ul style="list-style-type: none"> • No • Yes <div style="display: flex; align-items: center; margin-top: 20px;">  <p>Si el estado continuamente disponible es <code>No</code>, esto significa que estos archivos abiertos no son capaces de recuperarse de forma no disruptiva de la toma de control y la devolución. Tampoco pueden recuperarse de la reubicación general de agregados entre partners en una relación de alta disponibilidad.</p> </div> | Con el estado reconectado especificado |

Existen parámetros opcionales adicionales que se pueden utilizar para refinar los resultados de la salida. Consulte la página del manual para obtener más información.

Ejemplos

En el siguiente ejemplo, se muestra información sobre los archivos abiertos en la SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1
Node:      node1
Vserver:   vs1
Connection: 3151274158
Session:   1
File      File      Open Hosting      Continuously
ID        Type       Mode Volume      Share      Available
-----
41        Regular    r    data          data      Yes
Path: \mytest.rtf
```

En el siguiente ejemplo, se muestra información detallada sobre los archivos SMB abiertos con el ID de archivo 82 en la SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82  
-instance
```

```
        Node: node1  
        Vserver: vs1  
        File ID: 82  
    Connection ID: 104617  
        Session ID: 1  
        File Type: Regular  
        Open Mode: rw  
Aggregate Hosting File: aggr1  
    Volume Hosting File: data1  
        CIFS Share: data1  
    Path from CIFS Share: windows\win8\test\test.txt  
        Share Mode: rw  
        Range Locks: 1  
Continuously Available: Yes  
        Reconnected: No
```

Gestión del almacenamiento san

Conceptos de SAN

Aprovisionamiento SAN con iSCSI

En entornos SAN, los sistemas de almacenamiento son destinos que tienen dispositivos de almacenamiento objetivo. Para iSCSI y FC, los dispositivos de almacenamiento de destino se denominan LUN (unidades lógicas). Para la memoria no volátil rápida (NVMe) sobre Fibre Channel, los dispositivos de destino de almacenamiento se denominan espacios de nombres.

El almacenamiento se configura mediante la creación de LUN para iSCSI y FC, o bien mediante la creación de espacios de nombres para NVMe. Posteriormente, se accede a los LUN o espacios de nombres en hosts con redes de protocolos de interfaz de sistemas pequeños de Internet (iSCSI) o Fibre Channel (FC).

Para conectarse a redes iSCSI, los hosts pueden utilizar adaptadores de red Ethernet (NIC) estándar, tarjetas TOE (motor de descarga TCP) con iniciadores de software, adaptadores de red convergente (CNA) o adaptadores de bus de host (HBA) iSCSI dedicados.

Para conectarse a redes FC, los hosts requieren HBA o CNA FC.

Los protocolos FC compatibles incluyen:

- FC
- FCoE
- NVMe

Nombres y conexiones de red del nodo de destino iSCSI

Los nodos de destino iSCSI pueden conectarse a la red de varias maneras:

- Mediante interfaces Ethernet, que utilizan software integrado en ONTAP.
- En múltiples interfaces del sistema, con una interfaz usada para iSCSI que también puede transmitir tráfico para otros protocolos, como SMB y NFS.
- Mediante un adaptador de objetivo unificado (UTA) o un adaptador de red convergente (CNA).

Cada nodo iSCSI debe tener un nombre de nodo.

Los dos formatos, o designadores de tipo, para los nombres de nodo iSCSI son *IQN* y *eui*. El destino iSCSI de SVM siempre usa el indicador de tipo IQN. El iniciador puede usar el tipo IQN o el indicador de tipo eui.

Nombre del nodo del sistema de almacenamiento

Cada SVM que ejecuta iSCSI tiene un nombre de nodo predeterminado basado en un nombre de dominio inverso y un número de codificación único.

El nombre del nodo se muestra en el formato siguiente:

`iqn.1992-08.com.netapp:sn.unique-encoding-number`

En el ejemplo siguiente se muestra el nombre de nodo predeterminado para un sistema de almacenamiento con un número de codificación único:

```
iqn.1992-08.com.netapp:sn.812921059e6c11e097b3123478563412:vs.6
```

Puerto TCP para iSCSI

El protocolo iSCSI está configurado en ONTAP para utilizar el puerto TCP con el número 3260.

ONTAP no admite cambiar el número de puerto para iSCSI. El número de puerto 3260 se registra como parte de la especificación iSCSI y no puede utilizarlo ninguna otra aplicación o servicio.

Información relacionada

["Documentación de NetApp: Configuración de host SAN de ONTAP"](#)

Gestión de servicios iSCSI

Gestión de servicios iSCSI

Puede gestionar la disponibilidad del servicio iSCSI en las interfaces lógicas iSCSI de la máquina virtual de almacenamiento (SVM) mediante el `vserver iscsi interface enable 0`. `vserver iscsi interface disable` comandos.

De forma predeterminada, el servicio iSCSI está habilitado en todas las interfaces lógicas iSCSI.

Cómo se implementa iSCSI en el host

iSCSI se puede implementar en el host mediante hardware o software.

Es posible implementar iSCSI de una de las siguientes maneras:

- Utiliza el software Initiator que utiliza las interfaces Ethernet estándar del host.
- A través de un adaptador de bus de host (HBA) iSCSI: Un HBA iSCSI aparece al sistema operativo host como un adaptador de disco SCSI con discos locales.
- Con un adaptador DE motor de descarga TCP (TOE) que libera el procesamiento TCP/IP.

El procesamiento del protocolo iSCSI se sigue realizando mediante el software del host.

Cómo funciona la autenticación iSCSI

Durante la fase inicial de una sesión iSCSI, el iniciador envía una solicitud de inicio de sesión al sistema de almacenamiento para iniciar una sesión iSCSI. A continuación, el sistema de almacenamiento permite o rechaza la solicitud de inicio de sesión o determina que no es necesario iniciar sesión.

Los métodos de autenticación iSCSI son los siguientes:

- Primero: Protocolo de autenticación por desafío mutuo (CHAP): El iniciador inicia sesión con un nombre de usuario y una contraseña CHAP.

Es posible especificar una contraseña CHAP o generar una contraseña secreta hexadecimal. Existen dos tipos de nombres de usuario y contraseñas CHAP:

- Entrante: El sistema de almacenamiento autentica el iniciador.

Es necesario configurar de entrada si se utiliza la autenticación CHAP.

- Saliente: Esta es una opción para permitir que el iniciador autentique el sistema de almacenamiento.

Es posible utilizar la configuración saliente únicamente si se define un nombre de usuario y una contraseña entrantes en el sistema de almacenamiento.

- Denegar: El iniciador no tiene acceso al sistema de almacenamiento.
- Ninguno: El sistema de almacenamiento no requiere autenticación para el iniciador.

Puede definir la lista de iniciadores y sus métodos de autenticación. También puede definir un método de autenticación predeterminado que se aplique a los iniciadores que no aparecen en esta lista.

Información relacionada

["Opciones de múltiples rutas de Windows con Data ONTAP: Fibre Channel e iSCSI"](#)

Gestión de seguridad del iniciador iSCSI

ONTAP ofrece una serie de funciones para gestionar la seguridad de los iniciadores de iSCSI. Puede definir una lista de iniciadores iSCSI y el método de autenticación predeterminado para cada uno, mostrar los iniciadores y los métodos de autenticación asociados en la lista de autenticación, añadir y quitar iniciadores de la lista de autenticación, y definir el método de autenticación del iniciador iSCSI predeterminado para los iniciadores que no están en la lista.

Aislamiento de extremos iSCSI

A partir de la versión 9.1 de ONTAP se mejoraron los comandos de seguridad iSCSI existentes para aceptar un rango de direcciones IP o varias direcciones IP.

Todos los iniciadores de iSCSI deben proporcionar direcciones IP de origen al establecer una sesión o conexión con un destino. Esta nueva funcionalidad evita que un iniciador inicie sesión en el clúster si la dirección IP de origen no es compatible o desconocida, lo cual proporciona un esquema de identificación único. Los iniciadores originados por una dirección IP no compatible o desconocida serán rechazados su inicio de sesión en la capa de sesión iSCSI, lo que impide que el iniciador acceda a cualquier LUN o volumen del clúster.

Implemente esta nueva funcionalidad con dos comandos nuevos para ayudar a gestionar entradas preexistentes.

Añada un rango de direcciones del iniciador

Mejore la gestión de seguridad del iniciador de iSCSI añadiendo un rango de direcciones IP o varias direcciones IP con el `vserver iscsi security add-initiator-address-range` comando.

```
cluster1::> vserver iscsi security add-initiator-address-range
```


Quite el rango de direcciones del iniciador

Quite un rango de direcciones IP o varias direcciones IP con el `vserver iscsi security remove-initiator-address-range` comando.

```
cluster1::> vserver iscsi security remove-initiator-address-range
```

Qué es la autenticación CHAP

El protocolo de autenticación por desafío mutuo (CHAP) permite la comunicación autenticada entre iniciadores y destinos iSCSI. Cuando se utiliza la autenticación CHAP, se definen los nombres de usuario y las contraseñas CHAP tanto en el iniciador como en el sistema de almacenamiento.

Durante la fase inicial de una sesión iSCSI, el iniciador envía una solicitud de inicio de sesión al sistema de almacenamiento para iniciar la sesión. La solicitud de inicio de sesión incluye el nombre de usuario CHAP del iniciador y el algoritmo CHAP. El sistema de almacenamiento responde con un desafío CHAP. El iniciador proporciona una respuesta CHAP. El sistema de almacenamiento verifica la respuesta y autentica el iniciador. La contraseña CHAP se utiliza para calcular la respuesta.

Directrices para usar la autenticación CHAP

Debe seguir ciertas directrices al utilizar la autenticación CHAP.

- Si define un nombre de usuario y una contraseña entrantes en el sistema de almacenamiento, debe usar el mismo nombre de usuario y contraseña para la configuración de CHAP saliente en el iniciador. Si también define un nombre de usuario y una contraseña de salida en el sistema de almacenamiento para habilitar la autenticación bidireccional, debe usar el mismo nombre de usuario y la misma contraseña para la configuración de CHAP entrante en el iniciador.
- No es posible usar el mismo nombre de usuario y contraseña para la configuración de entrada y salida en el sistema de almacenamiento.
- Los nombres de usuario CHAP pueden tener entre 1 y 128 bytes.

No se permite un nombre de usuario nulo.

- Las contraseñas CHAP (secretos) pueden tener entre 1 y 512 bytes.

Las contraseñas pueden ser cadenas o valores hexadecimales. Para valores hexadecimales, debe introducir el valor con un prefijo "0x" o "0X". No se permite una contraseña nula.

ONTAP permite el uso de caracteres especiales, letras no inglesas, números y espacios para las contraseñas de CHAP (secretos). Sin embargo, esto está sujeto a restricciones de host. Si un host específico no permite alguno de estos, no se pueden usar.



Por ejemplo, el iniciador de software iSCSI de Microsoft requiere que las contraseñas CHAP de iniciador y destino tengan al menos 12 bytes si no se está utilizando el cifrado IPsec. La longitud máxima de la contraseña es de 16 bytes independientemente de si se usa IPsec.

Para ver más restricciones, debería consultar la documentación del iniciador.

La forma en que se utilizan las listas de acceso de interfaz iSCSI para limitar las interfaces de iniciador puede aumentar el rendimiento y la seguridad

Las listas DE acceso de interfaz iSCSI se pueden usar para limitar el número de LIF en una SVM a la que puede acceder un iniciador, con lo que aumenta el rendimiento y la seguridad.

Cuando un iniciador inicia una sesión de detección con un iSCSI `SendTargets` Comando, recibe las direcciones IP asociadas con la LIF (interfaz de red) que está en la lista de acceso. De forma predeterminada, todos los iniciadores tienen acceso a todas las LIF iSCSI de la SVM. Puede utilizar la lista de acceso para restringir el número de LIF en una SVM a la que tiene acceso un iniciador.

Servicio de nombres de almacenamiento de Internet (iSNS)

El servicio de nombres de almacenamiento de Internet (iSNS) es un protocolo que permite la detección y gestión automatizadas de dispositivos iSCSI en una red de almacenamiento TCP/IP. Un servidor iSNS mantiene información sobre dispositivos iSCSI activos en la red, incluidas sus direcciones IP, los nombres de nodos iSCSI IQN y los grupos de portales.

Puede obtener un servidor iSNS de un proveedor tercero. Si posee un servidor iSNS en la red configurado y habilitado para su uso por parte del iniciador y el destino, puede usar la LIF de gestión para una máquina virtual de almacenamiento (SVM) para registrar todos los LIF iSCSI para esa SVM en el servidor iSNS. Una vez completado el registro, el iniciador de iSCSI puede consultar el servidor iSNS para detectar todas las LIF de esa SVM en particular.

Si decide utilizar un servicio iSNS, debe asegurarse de que las máquinas virtuales de almacenamiento (SVM) estén registradas correctamente en un servidor de servicio de nombres de almacenamiento de Internet (iSNS).

Si no tiene un servidor iSNS en la red, debe configurar manualmente cada objetivo para que sea visible para el host.

Lo que hace un servidor iSNS

Un servidor iSNS utiliza el protocolo de servicio de nombres de almacenamiento de Internet (iSNS) para mantener información sobre los dispositivos iSCSI activos en la red, incluidas sus direcciones IP, nombres de nodos iSCSI (IQN) y grupos de portales.

El protocolo iSNS permite la detección y gestión automatizadas de dispositivos iSCSI en una red de almacenamiento IP. Un iniciador de iSCSI puede consultar el servidor iSNS para detectar dispositivos de destino iSCSI.

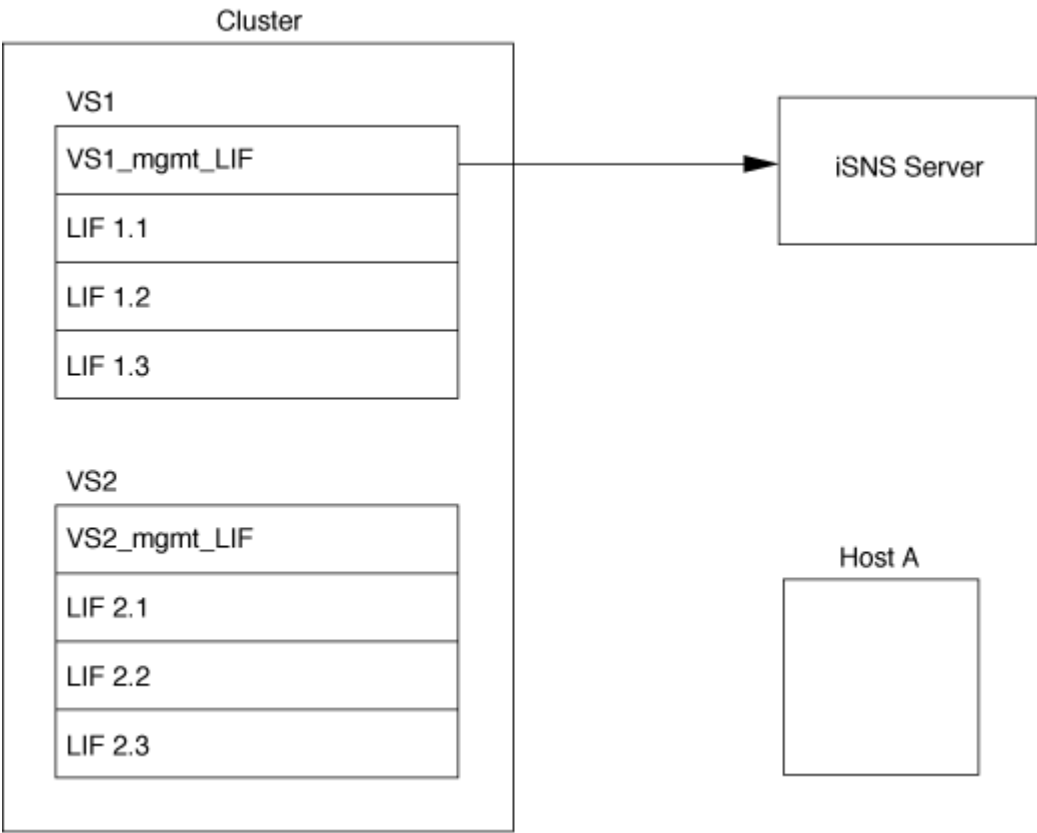
NetApp no suministra ni distribuye servidores iSNS. Puede obtener estos servidores de un proveedor con soporte de NetApp.

Cómo interactúan las SVM con un servidor iSNS

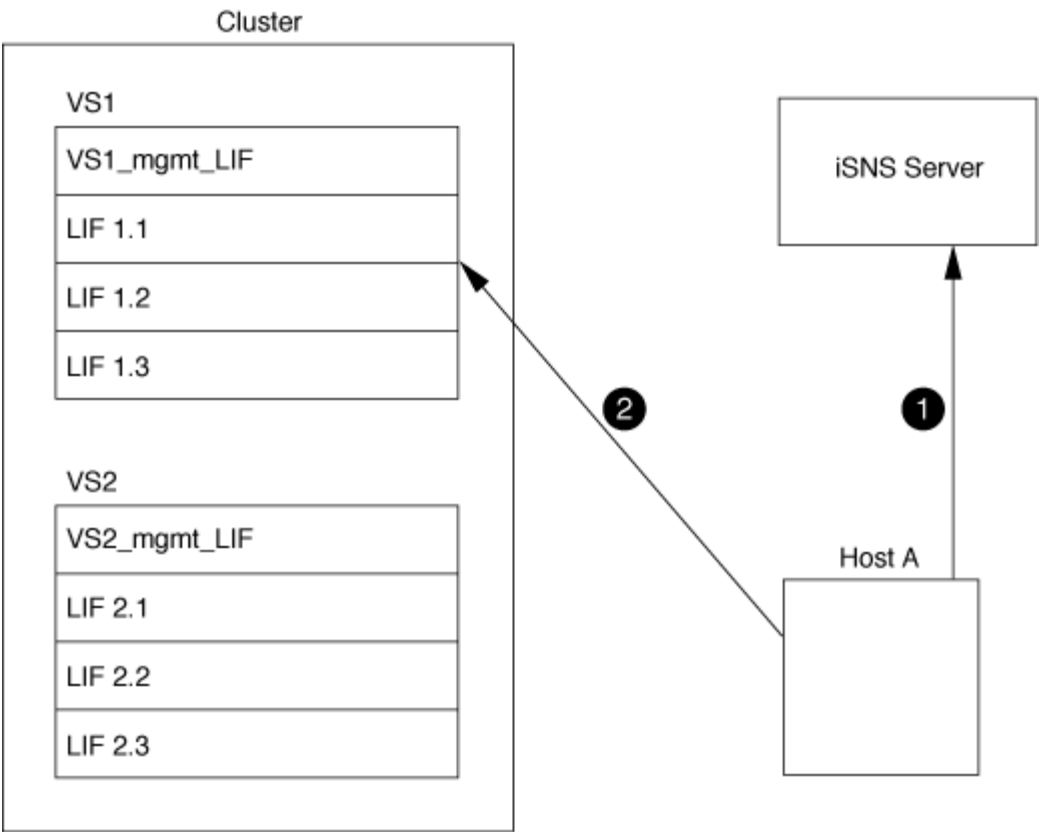
El servidor iSNS se comunica con cada máquina virtual de almacenamiento (SVM) a través de la LIF de gestión de SVM. La LIF de gestión registra toda la información de portal, alias y nombre del nodo de destino de iSCSI con el servicio iSNS para una SVM específica.

En el siguiente ejemplo, SVM «`VS1`» utiliza la LIF de gestión de SVM «`VS1_mgmt_lif`» para registrarse en el

servidor iSNS. Durante el registro de iSNS, una SVM envía todas las LIF de iSCSI a través de la LIF de gestión de SVM al servidor iSNS. Una vez completado el registro de iSNS, el servidor iSNS tendrá una lista de todas las LIF que sirven iSCSI en «VS1». Si un clúster contiene varias SVM, cada SVM debe registrarse individualmente con el servidor iSNS para utilizar el servicio iSNS.



En el siguiente ejemplo, después de que el servidor iSNS complete el registro con el destino, el Host A puede detectar todas las LIF para 'VS1' a través del servidor iSNS como se indica en el Paso 1. Una vez que el Host A completa el descubrimiento de las LIF para «VS1», el Host A puede establecer una conexión con cualquiera de las LIF en «VS1», tal como se muestra en el Paso 2. El host A no tiene en cuenta ninguna de las LIF incluidas en «VS2» hasta que la LIF de gestión «VS2_mgmt_LIF» para registros «VS2» en el servidor iSNS.



Sin embargo, si define las listas de acceso de interfaz, el host solo puede usar las LIF definidas en la lista de acceso de interfaz para acceder al destino.

Una vez que se configura inicialmente iSNS, ONTAP actualiza automáticamente el servidor iSNS cuando cambian las opciones de configuración de SVM.

Es posible que se produzca una demora de unos minutos entre el momento en que realiza cambios en la configuración y la hora en que ONTAP envía la actualización al servidor iSNS. Forzar una actualización inmediata de la información de iSNS en el servidor iSNS: `vserver iscsi isns update`

Comandos para gestionar iSNS

ONTAP proporciona comandos para gestionar el servicio iSNS.

| Si desea... | Se usa este comando... |
|---|--|
| Configure un servicio iSNS | <code>vserver iscsi isns create</code> |
| Inicie un servicio iSNS | <code>vserver iscsi isns start</code> |
| Modifique un servicio iSNS | <code>vserver iscsi isns modify</code> |
| Muestra la configuración de servicio iSNS | <code>vserver iscsi isns show</code> |
| Fuerza una actualización de la información de iSNS registrada | <code>vserver iscsi isns update</code> |

| | |
|---------------------------------|--|
| Detenga un servicio iSNS | <code>vserver iscsi isns stop</code> |
| Quite un servicio iSNS | <code>vserver iscsi isns delete</code> |
| Vea la página man de un comando | <code>man <i>command name</i></code> |

Consulte la página de manual de cada comando para obtener más información.

Aprovisionamiento DE SAN con FC

Debe conocer los conceptos importantes necesarios para comprender cómo implementa ONTAP UNA SAN FC.

Cómo se conectan los nodos de destino de FC a la red

Los sistemas de almacenamiento y hosts cuentan con adaptadores para que se puedan conectar a switches FC con cables.

Cuando un nodo está conectado a LA SAN FC, cada SVM registra el nombre de puerto WWPN de su LIF con el servicio de nombres de estructura del switch. ONTAP asigna automáticamente el WWNN de la SVM y el nombre de puerto WWPN de cada LIF.



No se admite la conexión directa a nodos de hosts con FC, se requiere NPIV y esto requiere que se utilice un switch. con sesiones iSCSI, la comunicación funciona con conexiones que están enrutadas de red o de conexión directa. Sin embargo, ONTAP admite ambos métodos.

Cómo se identifican los nodos FC

Cada SVM configurada con FC se identifica con un nombre de nodo WWNN.

Cómo se utilizan los WWPN

Los WWPN identifican cada LIF en una SVM configurada para admitir FC. Estos LIF utilizan puertos FC físicos en cada nodo del clúster, que pueden ser tarjetas objetivo FC, UTA o UTA2 configurados como FC o FCoE en los nodos.

- Crear un iGroup

Los WWPN de los HBA del host se usan para crear un iGroup. Un igroup se utiliza para controlar el acceso del host a una LUN específica. Puede crear un igroup especificando una colección de WWPN de iniciadores en una red de FC. Cuando asigna una LUN en un sistema de almacenamiento a un igroup, puede conceder a todos los iniciadores de ese grupo el acceso a esa LUN. Si el WWPN de un host no está en un igroup que se asigna a una LUN, ese host no tiene acceso a la LUN. Esto significa que los LUN no aparecen como discos en ese host.

También puede crear conjuntos de puertos para que una LUN sea visible solo en puertos de destino específicos. Un conjunto de puertos consta de un grupo de puertos de destino FC. Es posible enlazar un igroup con un conjunto de puertos. Cualquier host del igroup solo puede acceder a las LUN mediante la conexión a los puertos de destino del puerto establecido.

- Identificación exclusiva de LIF FC

Los WWPN identifican de forma única cada interfaz lógica de FC. El sistema operativo del host utiliza la combinación del WWNN y el WWPN para identificar SVM y LIF de FC. Algunos sistemas operativos requieren un enlace persistente para garantizar que la LUN aparece con el mismo ID objetivo en el host.

Cómo funcionan las asignaciones de nombres en todo el mundo

Los nombres de todo el mundo se crean secuencialmente en ONTAP. Sin embargo, debido a la forma en que ONTAP los asigna, puede parecer que están asignados en un orden no secuencial.

Cada adaptador tiene un WWPN y un WWNN preconfigurados, pero ONTAP no usa estos valores preconfigurados. En su lugar, ONTAP asigna sus propios WWPN o WWN, según las direcciones MAC de los puertos Ethernet internos.

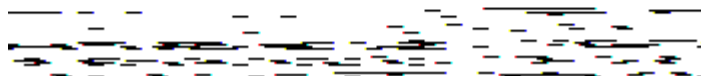
Puede parecer que los nombres internacionales no son secuenciales cuando se asignan por los siguientes motivos:

- Los nombres mundiales se asignan en todos los nodos y las máquinas virtuales de almacenamiento (SVM) del clúster.
- Los nombres liberados en todo el mundo se reciclan y se añaden al grupo de nombres disponibles.

Cómo se identifican los switches FC

Los switches Fibre Channel tienen un nombre de nodo WWNN del dispositivo mismo, y un nombre de puerto WWPN para cada uno de sus puertos.

Por ejemplo, el siguiente diagrama muestra cómo se asignan los WWPN a cada uno de los puertos de un switch Brocade de 16 puertos. Para obtener detalles sobre cómo están numerados los puertos de un switch determinado, consulte la documentación suministrada por el proveedor de ese switch.



Puerto **0**, WWPN 20:**00**:00:60:69:51:06:B4

Puerto **1**, WWPN 20:**01**:00:60:69:51:06:B4

Puerto **14**, WWPN 20:**0e**:00:60:69:51:06:b4

Puerto **15**, WWPN 20:**0f**:00:60:69:51:06:B4

Aprovisionamiento DE SAN con NVMe

A partir de ONTAP 9.4, NVMe/FC es compatible con el entorno SAN. NVMe/FC permite a los administradores de almacenamiento aprovisionar espacios de nombres y subsistemas y, a continuación, asignar los espacios de nombres a subsistemas de, de modo similar al modo en que se aprovisionan y asignan los LUN a iGroups para FC e iSCSI.

Un espacio de nombres NVMe es una cantidad de memoria no volátil que se puede formatear en bloques

lógicos. Los espacios de nombres son el equivalente de LUN para los protocolos FC e iSCSI, y un subsistema NVMe es análogo a un igroup. Los iniciadores asociados pueden acceder a un subsistema NVMe con iniciadores para que los espacios de nombres dentro del subsistema puedan acceder a ellos.



Si bien son análogos en la función, los espacios de nombres de NVMe no admiten todas las funciones compatibles con los LUN.

A partir de ONTAP 9.5 se requiere una licencia para admitir el acceso a datos que mira el host con NVMe. Si se habilita NVMe en ONTAP 9.4, se concede un periodo de gracia de 90 días para adquirir la licencia antes de actualizar a ONTAP 9.5. Si lo tiene **"ONTAP One"**, Las licencias NVMe están incluidas. Puede habilitar la licencia mediante el siguiente comando:

```
system license add -license-code NVMe_license_key
```

Información relacionada

["Informe técnico de NetApp 4684: Implementación y configuración de SAN modernas con NVMe/FC"](#)

Volúmenes SAN

Información general sobre SAN Volumes

ONTAP proporciona tres opciones básicas de aprovisionamiento de volúmenes: Aprovisionamiento ligero, aprovisionamiento ligero y aprovisionamiento ligero. Cada opción utiliza diferentes formas de gestionar el espacio de volumen y los requisitos de espacio para las tecnologías de uso compartido de bloques de ONTAP. Comprender cómo funcionan las opciones le permite elegir la mejor opción para su entorno.



No se recomienda colocar LUN DE SAN y recursos compartidos de NAS en el mismo volumen de FlexVol. Debería aprovisionar volúmenes FlexVol independientes específicamente para sus LUN DE SAN y debería aprovisionar volúmenes FlexVol independientes específicamente para sus recursos compartidos NAS. Esto simplifica la gestión y la replicación y es similar a la forma en la que los volúmenes de FlexVol son compatibles con Active IQ Unified Manager (anteriormente, Unified Manager de OnCommand).

Aprovisionamiento ligero para volúmenes

Cuando se crea un volumen con Thin Provisioning, ONTAP no reserva ningún espacio adicional cuando se crea el volumen. A medida que se escriben datos en el volumen, el volumen solicita el almacenamiento que necesita del agregado para acomodar la operación de escritura. El uso de volúmenes con aprovisionamiento ligero le permite comprometer en exceso su agregado, lo que introduce la posibilidad de que el volumen no pueda asegurar el espacio que necesita cuando el agregado se queda sin espacio libre.

Para crear un volumen de FlexVol con aprovisionamiento fino, debe configurar su `-space-guarantee` opción a `none`.

Aprovisionamiento grueso para volúmenes

Cuando se crea un volumen con aprovisionamiento grueso, ONTAP reserva suficiente almacenamiento del agregado para garantizar que cualquier bloque del volumen se pueda escribir en cualquier momento. Cuando configura un volumen para utilizar este tipo de aprovisionamiento, puede emplear cualquiera de las funcionalidades de eficiencia del almacenamiento de ONTAP, como la compresión y la deduplicación, para compensar los mayores requisitos de almacenamiento inicial.

Para crear un volumen FlexVol con aprovisionamiento grueso, configure su `-space-slo` (objetivo de nivel de servicio) opción a. `thick`.

Aprovisionamiento para volúmenes semigruesos

Cuando se crea un volumen que utiliza aprovisionamiento grueso, ONTAP establece un espacio de almacenamiento aparte del agregado para tener en cuenta el tamaño del volumen. Si el volumen se está quedando sin espacio libre porque las tecnologías de uso compartido de bloques lo están utilizando, ONTAP realiza un esfuerzo para eliminar objetos de datos de protección (copias Snapshot y archivos FlexClone y LUN) para liberar el espacio en el que se encuentran. Siempre que ONTAP pueda eliminar los objetos de datos de protección con la rapidez suficiente como para responder al ritmo del espacio requerido para las sobrescrituras, las operaciones de escritura siguen teniendo éxito. Esto se denomina «mejor esfuerzo».

Nota: no se admite la siguiente funcionalidad en volúmenes que utilizan aprovisionamiento semi-grueso:

- tecnologías de eficiencia del almacenamiento como la deduplicación, la compresión y la compactación
- Transferencia de datos descargados (ODX) de Microsoft

Para crear un volumen de FlexVol con aprovisionamiento semigrueso, establezca su configuración `-space-slo` (objetivo de nivel de servicio) opción a. `semi-thick`.

Utilice con archivos y LUN reservados en el espacio

Un archivo o LUN con reserva de espacio es uno para el cual se asigna el almacenamiento cuando se crea. Históricamente, NetApp ha utilizado el término «LUN aprovisionada mediante thin provisioning» para indicar una LUN para la que se ha deshabilitado la reserva de espacio (LUN sin reservar espacio).

Nota: los archivos sin espacio reservado no se denominan normalmente «ficheros con Thin-Provisioning».

En la tabla siguiente se resumen las principales diferencias en cómo pueden utilizarse las tres opciones de aprovisionamiento de volúmenes con archivos y LUN con espacio reservado:

| Aprovisionamiento de volúmenes | Reserva de espacio de archivos/LUN | Sobrescrituras | Datos de protección 2 | Eficiencia del almacenamiento 3 |
|--------------------------------|------------------------------------|------------------|-----------------------|---------------------------------|
| Grueso | Compatible | Garantizado 1 | Garantizado | Compatible |
| Fino | Sin efecto | Ninguno | Garantizado | Compatible |
| Semi-grueso | Compatible | Mejor esfuerzo 1 | El mejor esfuerzo | No admitido |

Notas

1. La capacidad para garantizar sobrescrituras o proporcionar una garantía de sobrescritura de mejor esfuerzo requiere que la reserva de espacio esté habilitada en la LUN o el archivo.
2. Los datos de protección incluyen copias Snapshot, y los archivos FlexClone y LUN marcados para su eliminación automática (clones de backup).
3. La eficiencia del almacenamiento incluye deduplicación, compresión, cualquier archivo FlexClone y LUN no marcados para su eliminación automática (clones activos), y subarchivos FlexClone (utilizados para la descarga de copia).

Compatibilidad con LUN provisionados mediante thin provisioning de SCSI

ONTAP admite LUN T10 SCSI con thin provisioning, así como LUN con thin provisioning de NetApp. El thin provisioning SCSI T10 permite que las aplicaciones host admitan funciones SCSI como la reclamación de espacio de LUN y las funcionalidades de supervisión de espacio de LUN para entornos de bloques. El thin provisioning SCSI T10 debe ser compatible con su software host SCSI.

Se utiliza `ONTAP space-allocation` Configuración para habilitar o deshabilitar la compatibilidad con thin provisioning T10 en una LUN. Se utiliza `ONTAP space-allocation enable` Configuración para habilitar thin provisioning SCSI T10 en una LUN.

La `[-space-allocation {enabled|disabled}]` En el manual de referencia de comandos de la ONTAP encontrará más información para habilitar o deshabilitar la compatibilidad con el thin provisioning T10 y para habilitar el aprovisionamiento ligero SCSI T10 en una LUN.

"Comandos de ONTAP 9"

Configure las opciones de aprovisionamiento del volumen

Puede configurar un volumen para thin provisioning, thick provisioning o semi-thick provisioning.

Acerca de esta tarea

Ajuste de `-space-slo` opción a. `thick` garantiza lo siguiente:

- El volumen completo se preasigna en el agregado. No puede utilizar el `volume create` o `volume modify` para configurar el volumen `-space-guarantee` opción.
- se reserva el 100% del espacio requerido para sobrescrituras. No puede utilizar el `volume modify` para configurar el volumen `-fractional-reserve` opción

Ajuste de `-space-slo` opción a. `semi-thick` garantiza lo siguiente:

- El volumen completo se preasigna en el agregado. No puede utilizar el `volume create` o `volume modify` para configurar el volumen `-space-guarantee` opción.
- No hay espacio reservado para sobrescrituras. Puede utilizar el `volume modify` para configurar el volumen `-fractional-reserve` opción.
- La eliminación automática de copias Snapshot está habilitada.

Paso

1. Configure las opciones de aprovisionamiento del volumen:

```
volume create -vserver vs1 -volume vol1 -aggregate agg1 -space-slo none|thick|semi-thick -space-guarantee none|volume
```

La `-space-guarantee` de forma predeterminada, la opción es `none` Para sistemas AFF y volúmenes DP distintos de AFF. De lo contrario, se establece de forma predeterminada en `volume`. Para los volúmenes de FlexVol existentes, utilice `volume modify` para configurar las opciones de aprovisionamiento.

El siguiente comando configura vol1 en SVM vs1 para thin provisioning:

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-guarantee none
```

El siguiente comando configura vol1 en SVM vs1 para el aprovisionamiento grueso:

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-slo thick
```

El siguiente comando configura vol1 en SVM vs1 para un aprovisionamiento semigrueso:

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-slo semi-thick
```

Opciones de configuración de volúmenes SAN

Debe configurar varias opciones en el volumen que contiene el LUN. La manera en que establece las opciones de volumen determina la cantidad de espacio disponible para las LUN del volumen.

Crecimiento automático

Puede activar o desactivar Autofila. Si se habilita esta función, el crecimiento automático permite que ONTAP aumente automáticamente el tamaño del volumen hasta un tamaño máximo que se determine previamente. Debe haber espacio disponible en el agregado contenedor para admitir el crecimiento automático del volumen. Por lo tanto, si se habilita el crecimiento automático, se debe supervisar el espacio libre en el agregado que contiene y agregar más cuando se necesite.

No se puede activar el crecimiento automático para admitir la creación de copias Snapshot. Si se intenta crear una copia de Snapshot y hay espacio insuficiente en el volumen, se produce un error en la creación de Snapshot, incluso con el crecimiento automático habilitado.

Si se deshabilita el crecimiento automático, el tamaño del volumen seguirá siendo el mismo.

Autohrink

Puede activar o desactivar la función de reducción automática. Si lo habilita, la función de reducción automática permite a ONTAP reducir automáticamente el tamaño total de un volumen cuando la cantidad de espacio consumido en el volumen disminuye un umbral predeterminado. Esto aumenta la eficiencia de almacenamiento al activar los volúmenes para liberar automáticamente espacio libre no utilizado.

Eliminación automática de Snapshot

La eliminación automática de Snapshot elimina automáticamente las copias Snapshot si se produce alguna de las siguientes situaciones:

- El volumen está casi lleno.
- El espacio de reserva de Snapshot está casi lleno.
- El espacio de reserva de sobrescritura está lleno.

Es posible configurar la eliminación automática de Snapshot para eliminar copias de Snapshot de las más antiguas a las más nuevas, o de las más nuevas a las más antiguas. La eliminación automática de Snapshot no elimina las copias de Snapshot vinculadas a las copias de Snapshot en volúmenes o LUN clonados.

Si el volumen necesita espacio adicional y se habilitó el crecimiento automático y la eliminación automática de Snapshot, de manera predeterminada, ONTAP intenta adquirir el espacio necesario mediante la activación del crecimiento automático por primera vez. Si no se adquiere suficiente espacio a través del crecimiento automático, se activa la eliminación automática de Snapshot.

Reserva de Snapshot

La reserva de Snapshot define la cantidad de espacio en el volumen reservado para las copias de Snapshot. El espacio asignado a la reserva de Snapshot no se puede utilizar con ningún otro fin. Si se utiliza todo el espacio asignado a la reserva de Snapshot, las copias snapshot empiezan a consumir espacio adicional en el volumen.

Requisito para mover volúmenes en entornos SAN

Antes de mover un volumen que contiene LUN o espacios de nombres, debe cumplir ciertos requisitos.

- Para los volúmenes que contienen una o más LUN, debe tener un mínimo de dos rutas por LUN (LIF) conectadas a cada nodo del clúster.

De este modo, se eliminan los puntos únicos de error y el sistema puede sobrevivir a fallos de componentes.

- Para los volúmenes que contienen espacios de nombres, el clúster debe ejecutar ONTAP 9.6 o una versión posterior.

La transferencia de volúmenes no es compatible con configuraciones de NVMe que ejecuten ONTAP 9.5.

Consideraciones para establecer la reserva fraccionaria

La reserva fraccionaria, también denominada *LUN overwrite reserve*, le permite desactivar la reserva de sobrescritura para archivos y LUN reservados de espacio en un volumen de FlexVol. Esto puede ayudarle a maximizar el uso del almacenamiento, pero si su entorno se ve afectado negativamente por errores en las operaciones de escritura debido a la falta de espacio, debe comprender los requisitos que impone esta configuración.

La configuración de reserva fraccionaria se expresa como un porcentaje; los únicos valores válidos son 0 y.. 100 porcentaje. La configuración de reserva fraccionaria es un atributo del volumen.

Estableciendo la reserva fraccionaria en 0 aumenta la utilización del almacenamiento. Sin embargo, una aplicación que acceda a los datos del volumen puede sufrir una interrupción del servicio de los datos si el volumen no tiene espacio libre, incluso con la garantía de volumen establecida en `volume`. Sin embargo, con una configuración de volumen y un uso adecuados, se puede minimizar la posibilidad de que falle la escritura. ONTAP proporciona una garantía de escritura «"best effort"» para volúmenes con reserva fraccionaria establecida en 0 cuando se cumplan *all* de los siguientes requisitos:

- La deduplicación no se está utilizando

- La compresión no se está utilizando
- No se utilizan subarchivos FlexClone
- Todos los archivos de FlexClone y LUN de FlexClone están habilitados para la eliminación automática

Esta no es la configuración predeterminada. Debe habilitar de forma explícita la eliminación automática, ya sea en el momento de la creación o modificando el archivo FlexClone o la LUN de FlexClone después de crearla.

- No se están utilizando la descarga de copias ODX y FlexClone
- La garantía de volumen se establece en `volume`
- La reserva de espacio de la LUN o el archivo es `enabled`
- La reserva de copias Snapshot de volumen se establece en `0`
- La eliminación automática de copias Snapshot de volumen es `enabled` con un nivel de compromiso de `destroy`, una lista de destrucción de `lun_clone, vol_clone, cifs_share, file_clone, sfsr`, y un disparador de `volume`

Esta configuración también garantiza que los archivos FlexClone y las LUN de FlexClone se eliminen cuando sea necesario.

Tenga en cuenta que si la tasa de cambios es alta, en raras ocasiones la eliminación automática de la copia snapshot podría quedarse atrás, lo que dará como resultado que el volumen se quede sin espacio, incluso con todas las opciones de configuración requeridas anteriores en uso.

Además, tiene la opción de usar la funcionalidad de crecimiento automático de volumen para reducir la probabilidad de que las copias de snapshot del volumen deban eliminarse automáticamente. Si se habilita la funcionalidad de crecimiento automático, se debe supervisar el espacio libre en el agregado asociado. Si el agregado está lo suficientemente lleno como para evitar que el volumen crezca, es probable que se eliminen más copias snapshot a medida que se agota el espacio libre del volumen.

Si no puede satisfacer todos los requisitos de configuración anteriores y es necesario garantizar que el volumen no se quede sin espacio, debe establecer el valor de reserva fraccionaria del volumen en `100`. Esto requiere más espacio libre de antemano, pero garantiza que las operaciones de modificación de datos tendrán éxito incluso cuando las tecnologías enumeradas anteriormente estén en uso.

El valor predeterminado y los valores permitidos para la configuración de reserva fraccionaria dependen de la garantía del volumen:

| Garantía de volumen | Reserva fraccionaria predeterminada | Valores permitidos |
|---------------------|-------------------------------------|--------------------|
| Volumen | 100 | 0, 100 |
| Ninguno | 0 | 0, 100 |

Gestión del espacio del host DE SAN

En un entorno con thin provisioning, la gestión del espacio del host completa el proceso de gestión del espacio desde el sistema de almacenamiento que se ha liberado en el sistema de ficheros host.

El sistema de archivos de host contiene metadatos para realizar un seguimiento de los bloques disponibles para almacenar datos nuevos y qué bloques contienen datos válidos que no deben sobrescribirse. Estos metadatos se almacenan en el LUN. Cuando se elimina un archivo en el sistema de archivos host, los metadatos del sistema de archivos se actualizan para marcar los bloques del archivo como espacio libre. El espacio libre total del sistema de archivos se vuelve a calcular para incluir los bloques recién liberados. Para el sistema de almacenamiento, estas actualizaciones de metadatos no aparecen diferentes de cualquier otra escritura que realice el host. Por lo tanto, el sistema de almacenamiento no es consciente de que se han producido eliminaciones.

Esto crea una discrepancia entre la cantidad de espacio libre notificada por el host y la cantidad de espacio libre notificada por el sistema de almacenamiento subyacente. Por ejemplo, suponga que tiene un LUN de 200 GB recién provisionado asignado al host mediante el sistema de almacenamiento. Tanto el host como el sistema de almacenamiento informan de 200 GB de espacio libre. Luego, el host escribe 100 GB de datos. En este momento, tanto el host como el sistema de almacenamiento informan de 100 GB de espacio usado y 100 GB de espacio no utilizado.

A continuación, elimina 50 GB de datos del host. En este momento, su host informará de 50 GB de espacio usado y 150 GB de espacio no utilizado. Sin embargo, el sistema de almacenamiento informará de 100 GB de espacio usado y 100 GB de espacio sin utilizar.

La gestión del espacio en el host utiliza diversos métodos para conciliar la diferencia de espacio entre el host y el sistema de almacenamiento.

Gestión de hosts simplificada con SnapCenter

Es posible utilizar el software SnapCenter para simplificar algunas de las tareas de gestión y protección de datos asociadas con el almacenamiento iSCSI y FC. SnapCenter es un paquete de gestión opcional para los hosts Windows y UNIX.

Puede utilizar el software SnapCenter para crear fácilmente discos virtuales a partir de pools de almacenamiento que pueden distribuirse entre varios sistemas de almacenamiento y para automatizar las tareas de aprovisionamiento del almacenamiento y simplificar el proceso de creación de copias Snapshot y clones a partir de copias Snapshot consistentes con los datos del host.

Consulte la documentación de productos de NetApp para obtener más información acerca de ["SnapCenter"](#).

Enlaces relacionados

["Activar la asignación de espacio para LUN con Thin Provisioning de SCSI"](#)

Acerca de iGroups

Los iGroups son tablas de nombres de WWPN de host de protocolo FC o de nodos de host iSCSI. Puede definir iGroups y asignarlas a LUN para controlar qué iniciadores tienen acceso a las LUN.

Generalmente, desea que todos los puertos de iniciador o iniciadores de software del host tengan acceso a una LUN. Si utiliza software multivía o tiene hosts en clúster, cada puerto iniciador o iniciador de software de cada host en clúster necesita rutas redundantes a la misma LUN.

Es posible crear iGroups para especificar qué iniciadores tienen acceso a las LUN antes o después de crear las LUN, pero debe crear iGroups antes de poder asignar una LUN a un igroup.

Los iGroups pueden tener varios iniciadores, y varios iGroups pueden tener el mismo iniciador. Sin embargo, no puede asignar una LUN a varios iGroups que tengan el mismo iniciador. Un iniciador no puede ser

miembro de iGroups de tipos de configuración distintos.

Ejemplo de cómo los iGroups proporcionan acceso a LUN

Es posible crear varios iGroups para definir qué LUN están disponibles para sus hosts. Por ejemplo, si tiene un clúster de hosts, puede utilizar iGroups para garantizar que determinadas LUN sean visibles solo para un host del clúster o para todos los hosts del clúster.

La siguiente tabla muestra cómo cuatro iGroups dan acceso a las LUN para cuatro hosts diferentes que acceden al sistema de almacenamiento. Los hosts en clúster (Host3 y Host4) son miembros del mismo igroup (group3) y pueden acceder a las LUN asignadas a este igroup. El igroup denominado group4 contiene los WWPN de Host4 para almacenar información local que su socio no debe ver.

| Hosts con WWPN de HBA, IQN o EUIs | grupos de iniciadores | WWPN, IQN, EUIs añadidos a iGroups | LUN asignadas a iGroups |
|---|-----------------------|--|--|
| Host1, ruta única (iniciador de software iSCSI) iqn.1991-05.com.microsoft:host1 | grupo1 | iqn.1991-05.com.microsoft:host1 | /vol/vol2/lun1 |
| Host2, multivía (dos HBA) 10:00:00:00:c9:2b:6b:3c 10:00:00:00:c9:2b:02:3c | grupo 2 | 10:00:00:00:c9:2b:6b:3c 10:00:00:00:c9:2b:02:3c | /vol/vol2/lun2 |
| Host3, multivía, agrupado con host 4 10:00:00:00:c9:2b:32:1b 10:00:00:00:c9:2b:41:02 | grupo 3 | 10:00:00:00:c9:2b:32:1b 10:00:00:00:c9:2b:41:02 10:00:00:00:c9:2b:51:2c 10:00:00:00:c9:2b:47:a2 | /vol/vol2/mtree1/lun3 |
| Host4, multivía, agrupado (no visible para Host3) 10:00:00:00:c9:2b:51:2c 10:00:00:00:c9:2b:47:a2 | grupo 4 | 10:00:00:00:c9:2b:51:2c 10:00:00:00:c9:2b:47:a2 | /vol/vol2/mtree2/lun4 /vol/vol2/mtree1/lun5 |

Especifique WWPN de iniciador y los nombres de nodo iSCSI para un igroup

Puede especificar los nombres de nodo iSCSI y los WWPN de los iniciadores cuando crea un igroup, o bien puede añadirlos más adelante. Si opta por especificar los nombres de nodo iSCSI y los WWPN de iniciador cuando crea la LUN, pueden eliminarse más adelante, si fuera necesario.

Siga las instrucciones de la documentación de Host Utilities para obtener los WWPN y para encontrar los

nombres de los nodos iSCSI asociados con un host específico. En el caso de los hosts que ejecutan el software ESX, utilice Virtual Storage Console.

Virtualización del almacenamiento con la copia de datos descargados de VMware y Microsoft

Información general sobre la descarga de copias de VMware y Microsoft mediante la virtualización del almacenamiento

VMware y Microsoft admiten operaciones de descarga de copias para aumentar el rendimiento y el rendimiento de la red. Debe configurar su sistema para que cumpla los requisitos de los entornos de sistema operativo VMware y Windows para utilizar sus respectivas funciones de descarga de copias.

Al utilizar la descarga de copias de VMware y Microsoft en entornos virtualizados, deben alinearse los LUN. Las LUN desalineadas pueden degradar el rendimiento.

Ventajas de usar un entorno SAN virtualizado

La creación de un entorno virtualizado mediante LIF y máquinas virtuales de almacenamiento (SVM) le permite expandir su entorno SAN a todos los nodos del clúster.

- Gestión distribuida

Puede iniciar sesión en cualquier nodo de la SVM para administrar todos los nodos de un clúster.

- Mayor acceso a los datos

Con MPIO y ALUA, tendrá acceso a los datos a través de cualquier LIF iSCSI o FC activa para la SVM.

- Acceso de LUN controlado

Si utiliza SLM y conjuntos de puertos, puede limitar qué LIF puede utilizar un iniciador para acceder a las LUN.

Cómo funciona el acceso de LUN en un entorno virtualizado

En un entorno virtualizado, las LIF permiten que los hosts (clientes) accedan a las LUN a través de rutas optimizadas y sin optimizar.

Una LIF es una interfaz lógica que conecta la SVM a un puerto físico. Aunque varias SVM pueden tener varios LIF en el mismo puerto, un LIF pertenece a una SVM. Puede acceder a las LUN a través de las LIF de SVM.

Ejemplo de acceso de LUN con una única SVM en un clúster

En el siguiente ejemplo, el host 1 se conecta a LIF1.1 y LIF1.2 en SVM-1 para acceder a LUN1. LIF1.1 utiliza el puerto físico 1:0c y LIF1.2:0c. LIF1.1 y LIF1.2 sólo pertenecen a SVM-1. Si se crea una nueva LUN en el nodo 1 o en el nodo 2, para SVM-1, puede usar estas mismas LIF. Si se crea una nueva SVM, pueden crearse nuevas LIF con los puertos físicos 0c o 0d de ambos nodos.



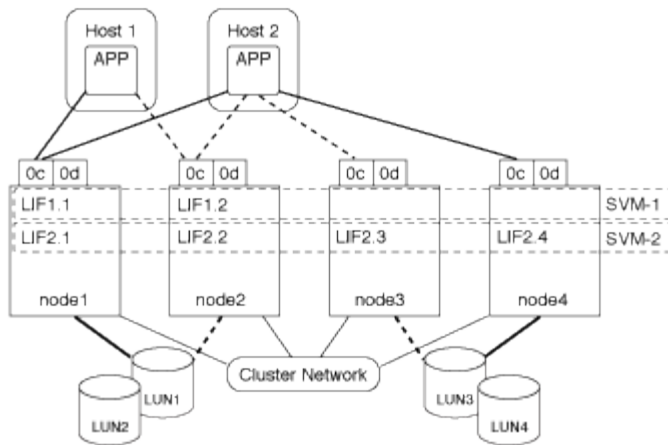
Ejemplo de acceso de la LUN con varias SVM en un clúster

Un puerto físico puede admitir varios LIF que sirven a diferentes SVM. Dado que los LIF están asociados con una SVM determinada, los nodos del clúster pueden enviar el tráfico de datos entrantes a la SVM correcta. En el ejemplo siguiente, cada nodo del 1 al 4 tiene una LIF para SVM-2 utilizando el puerto físico 0c de cada nodo. El host 1 se conecta a LIF1.1 y LIF1.2 en SVM-1 para acceder a LUN1. El host 2 se conecta al LIF2-1 y al LIF2-2 en la SVM-2 para acceder a LUN2. Ambas SVM comparten el puerto físico 0c en los nodos 1 y 2. SVM-2 tiene LIF adicionales que utiliza el host 2 para acceder a las LUN 3 y 4. Estos LIF están utilizando el puerto físico 0c en los nodos 3 y 4. Varias SVM pueden compartir los puertos físicos en los nodos.



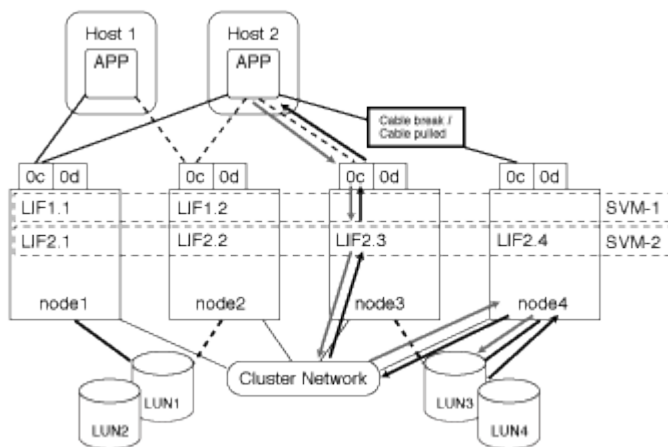
Ejemplo de una ruta activa o optimizada a una LUN desde un sistema host

En una ruta activa o optimizada, el tráfico de datos no viaja a través de la red de clúster; viaja por la ruta más directa a la LUN. La ruta activa o optimizada a LUN1 se realiza a través de LIF1.1 en el nodo 1, utilizando 0c de puerto físico. El host 2 tiene dos rutas activas o optimizadas, una ruta al nodo 1, LIF2.1, que comparte el puerto físico 0c y la otra ruta al nodo 4, LIF2.4, que utiliza el puerto físico 0c.



Ejemplo de una ruta de acceso activa o no optimizada (indirecta) a una LUN desde un sistema host

En una ruta de ruta activa o no optimizada (indirecta), el tráfico de datos viaja por la red de clúster. Este problema se produce solo si todas las rutas activas o optimizadas de un host no están disponibles para manejar el tráfico. Si se pierde la ruta desde el host 2 a la SVM-2 LIF2.4, el acceso a LUN3 y LUN4 atraviesa la red de clúster. El acceso desde el host 2 utiliza LIF2.3 en el nodo 3. A continuación, el tráfico entra en el switch de red de clúster y realiza una copia de seguridad de hasta node4 para acceder a LUN3 y LUN4. A continuación, volverá a atravesar el switch de red del clúster y, a continuación, volverá a pasar por LIF2.3 al host 2. Esta ruta activa o no optimizada se utiliza hasta que se restaura la ruta al LIF2.4 o se establece un nuevo LIF para SVM-2 en otro puerto físico del nodo 4.



=
:allow-uri-read:

Mejore el rendimiento de VMware VAAI para los hosts ESX

ONTAP admite algunas funciones de VMware vStorage APIs for Array Integration (VAAI) cuando el host ESX ejecuta ESX 4.1 o posterior. Estas funciones ayudan a descargar las operaciones del host ESX al sistema de almacenamiento y aumentan el rendimiento de la red. El host ESX habilita las funciones automáticamente en el entorno correcto.

La función VAAI admite los siguientes comandos SCSI:

- EXTENDED_COPY

Esta función permite que el host inicie la transferencia de datos entre las LUN o dentro de una LUN sin

implicar al host en la transferencia de datos. El resultado es guardar los ciclos de CPU de ESX y aumentar el rendimiento de la red. La función de copia ampliada, también conocida como "descarga de copias", se utiliza en situaciones como el clonado de una máquina virtual. Cuando el host ESX lo invoca, la función de descarga de copias copia copia copia copia copia copia los datos del sistema de almacenamiento en lugar de pasar por la red host. La descarga de copias transfiere datos de las siguientes formas:

- Dentro de una LUN
- Entre las LUN de un volumen
- Entre LUN en diferentes volúmenes dentro de una máquina virtual de almacenamiento (SVM)
- Entre LUN de diferentes SVM dentro de un clúster

Si no se puede invocar esta función, el host ESX utiliza automáticamente los comandos READ y WRITE estándar para la operación de copia.

- WRITE_SAME

Esta función libera el trabajo de escribir un patrón repetido, como todos los ceros, a una cabina de almacenamiento. El host ESX utiliza esta función en operaciones como rellenar un archivo sin ceros.

- COMPARE_AND_WRITE

Esta función omite ciertos límites de concurrencia de acceso a archivos, lo que acelera operaciones como el arranque de máquinas virtuales.

Requisitos para usar el entorno VAAI

Las funciones VAAI forman parte del sistema operativo ESX y las invoca automáticamente el host ESX cuando se configura el entorno correcto.

Los requisitos del entorno son los siguientes:

- El host ESX debe ejecutar ESX 4.1 o una versión posterior.
- El sistema de almacenamiento de NetApp que aloja el almacén de datos de VMware debe ejecutar ONTAP.
- (Solo copia de liberación de sobrecarga) el origen y el destino de la operación de copia de VMware se deben alojar en el mismo sistema de almacenamiento dentro del mismo clúster.



La función de descarga de copias no admite en este momento la copia de datos entre almacenes de datos VMware alojados en diferentes sistemas de almacenamiento.

Determinar si ESX admite las funciones de VAAI

Para confirmar si el sistema operativo ESX admite las funciones VAAI, puede comprobar vSphere Client o utilizar cualquier otro medio para acceder al host. ONTAP admite los comandos SCSI de forma predeterminada.

Puede comprobar la configuración avanzada del host ESX para determinar si las funciones de VAAI están habilitadas. La tabla indica qué comandos SCSI corresponden a los nombres de control ESX.

| Comando SCSI | Nombre del control ESX (función VAAI) |
|-----------------|---------------------------------------|
| EXTENDED_COPY | HardwareAcceleratedMove |
| WRITE_SAME | HardwareAcceleratedInit |
| COMPARE_Y_WRITE | HardwareAcceleratedLocking |

Transferencia de datos descargados (ODX) de Microsoft

La transferencia de datos descargados (ODX) de Microsoft, también conocida como *copy flood*, permite transferir datos directamente dentro de un dispositivo de almacenamiento o entre dispositivos de almacenamiento compatibles sin transferir los datos a través del equipo host.

ONTAP admite ODX para los protocolos SMB Y SAN.

En las transferencias de archivos que no tienen ODX, los datos se leen del origen y se transfieren por la red al host. El host transfiere los datos a través de la red al destino. En la transferencia de archivos ODX, los datos se copian directamente del origen al destino sin pasar por el host.

Como las copias descargadas de ODX se realizan directamente entre el origen y el destino, se obtienen importantes beneficios de rendimiento si se realizan copias dentro del mismo volumen, incluido un tiempo de copia más rápido para copias de mismo volumen, reducción del uso de CPU y memoria en el cliente y reducción del uso de ancho de banda de I/O de red. Si las copias se realizan entre volúmenes, es posible que no haya un aumento significativo del rendimiento en comparación con las copias basadas en host.

Para entornos SAN, ODX solo está disponible cuando es compatible tanto con el host como con el sistema de almacenamiento. Los equipos cliente compatibles con ODX y que tengan habilitada ODX automáticamente y de forma transparente utilizan la transferencia de archivos descargados cuando se mueven o copian archivos. ODX se utiliza independientemente de si arrastra y suelta archivos a través del Explorador de Windows o utiliza comandos de copia de archivos de la línea de comandos, o si una aplicación cliente inicia solicitudes de copia de archivos.

Requisitos para usar ODX

Si planea utilizar ODX para descargas de copias, debe estar familiarizado con las consideraciones de compatibilidad de volúmenes, los requisitos del sistema y los requisitos de funcionalidad de software.

Para utilizar ODX, el sistema debe tener lo siguiente:

- ONTAP

ODX se habilita automáticamente en las versiones compatibles de ONTAP.

- Volumen de origen mínimo de 2 GB

Para obtener un rendimiento óptimo, el volumen de origen debe ser mayor que 260 GB.

- Compatibilidad con ODX en el cliente Windows

Windows Server 2012 o posterior admite ODX y Windows 8 o versiones posteriores. La matriz de

interoperabilidad contiene la información más reciente sobre los clientes Windows compatibles.

["Herramienta de matriz de interoperabilidad de NetApp"](#)

- Compatibilidad con aplicaciones de copia para ODX

La aplicación que realiza la transferencia de datos debe ser compatible con ODX. Las operaciones de aplicaciones compatibles con ODX incluyen lo siguiente:

- Las operaciones de gestión de Hyper-V, como la creación y conversión de discos duros virtuales (VHD), la gestión de copias Snapshot y la copia de archivos entre máquinas virtuales
- Operaciones del Explorador de Windows
- Comandos de copia de Windows PowerShell
- Comandos de copia en el símbolo del sistema de Windows

La biblioteca de Microsoft TechNet contiene más información sobre las aplicaciones ODX compatibles en servidores y clientes Windows.

- Si se utilizan volúmenes comprimidos, el tamaño del grupo de compresión debe ser de 8 KB.

No se admite el tamaño del grupo de compresión de 32 KB.

ODX no funciona con los siguientes tipos de volúmenes:

- Volúmenes de origen con capacidades inferiores a 2 GB
- Volúmenes de solo lectura
- ["Volúmenes de FlexCache"](#)



ODX es compatible con los volúmenes de origen FlexCache.

- ["Volúmenes semigruesos aprovisionados"](#)

Requisitos especiales de archivo del sistema

Es posible eliminar los archivos ODX que se encuentran en qtrees. No debe quitar ni modificar ningún otro archivo del sistema ODX a menos que el soporte técnico le indique que lo haga.

Cuando se usa la función ODX, existen archivos del sistema ODX en todos los volúmenes del sistema. Estos archivos permiten una representación puntual de los datos utilizados durante la transferencia ODX. Los siguientes archivos del sistema se encuentran en el nivel raíz de cada volumen que contiene LUN o archivos en los que se ha descargado datos:

- `.copy-offload` (un directorio oculto)
- `.tokens` (archivo debajo del oculto `.copy-offload` directorio)

Puede utilizar el `copy-offload delete-tokens -path dir_path -node node_name` Comando para eliminar un qtree que contiene un archivo ODX.

Casos de uso para ODX

Debe conocer los casos de uso de ODX en SVM para poder determinar en qué circunstancias le proporciona ventajas en rendimiento.

Los servidores y los clientes de Windows que admiten ODX utilizan la descarga de copias como forma predeterminada de copiar datos en servidores remotos. Si el cliente o el servidor Windows no son compatibles con ODX o se produce un error en cualquier momento, la operación de copia o movimiento vuelve a las lecturas y escrituras tradicionales para la operación de copia o movimiento.

Los siguientes casos de uso admiten el uso de copias y movimientos ODX:

- Volumen interno

Los archivos o LUN de origen y destino están dentro del mismo volumen.

- Entre volúmenes, mismo nodo, misma SVM

Los archivos de origen y de destino o las LUN se encuentran en distintos volúmenes ubicados en el mismo nodo. Los datos son propiedad de la misma SVM.

- Entre volúmenes, distintos nodos, misma SVM

Los archivos de origen y de destino o las LUN se encuentran en volúmenes distintos que se encuentran en nodos diferentes. Los datos son propiedad de la misma SVM.

- Entre SVM, mismo nodo

El archivo de origen y los LUN de destino se encuentran en distintos volúmenes ubicados en el mismo nodo. Los datos son propiedad de diferentes SVM.

- Entre SVM, diferentes nodos

El archivo o las LUN de origen y destino se encuentran en distintos volúmenes ubicados en nodos diferentes. Los datos son propiedad de diferentes SVM.

- Entre clústeres

Las LUN de origen y de destino se encuentran en distintos volúmenes ubicados en distintos nodos en varios clústeres. Solo se admite en SAN y no funciona para SMB.

Existen algunos casos de uso especiales adicionales:

- Con la implementación de ODX de ONTAP, se puede utilizar ODX para copiar archivos entre recursos compartidos de SMB y unidades virtuales asociadas a FC o iSCSI.

Puede utilizar el Explorador de Windows, la CLI de Windows o PowerShell, Hyper-V u otras aplicaciones que admiten ODX para copiar o mover archivos sin problemas mediante la descarga de la copia ODX entre recursos compartidos de SMB y LUN conectados, siempre y cuando los recursos compartidos y las LUN del SMB estén en el mismo clúster.

- Hyper-V proporciona algunos casos de uso adicionales para la descarga de copias ODX:

- Se puede utilizar la transferencia de la copia ODX mediante Hyper-V para copiar datos dentro o a través de archivos de disco duro virtual (VHD), o bien copiar datos entre recursos compartidos de SMB asignados y LUN iSCSI conectados dentro del mismo clúster.

Esto permite que las copias de sistemas operativos invitados pasen al almacenamiento subyacente.

- Al crear discos duros virtuales de tamaño fijo, ODX se utiliza para inicializar el disco con ceros,

empleando un token de cero conocido.

- La descarga de copias ODX se utiliza para la migración de almacenamiento de máquinas virtuales si el almacenamiento de origen y destino está en el mismo clúster.



Para aprovechar los casos de uso de un paso a través de la descarga de copias ODX mediante Hyper-V, el sistema operativo invitado debe ser compatible con ODX, mientras que los discos del sistema operativo invitado deben ser discos SCSI respaldados por almacenamiento (tanto SMB COMO SAN) que sean compatibles con ODX. Los discos IDE del sistema operativo invitado no admiten el paso a través de ODX.

Administración de SAN

Aprovisionamiento SAN

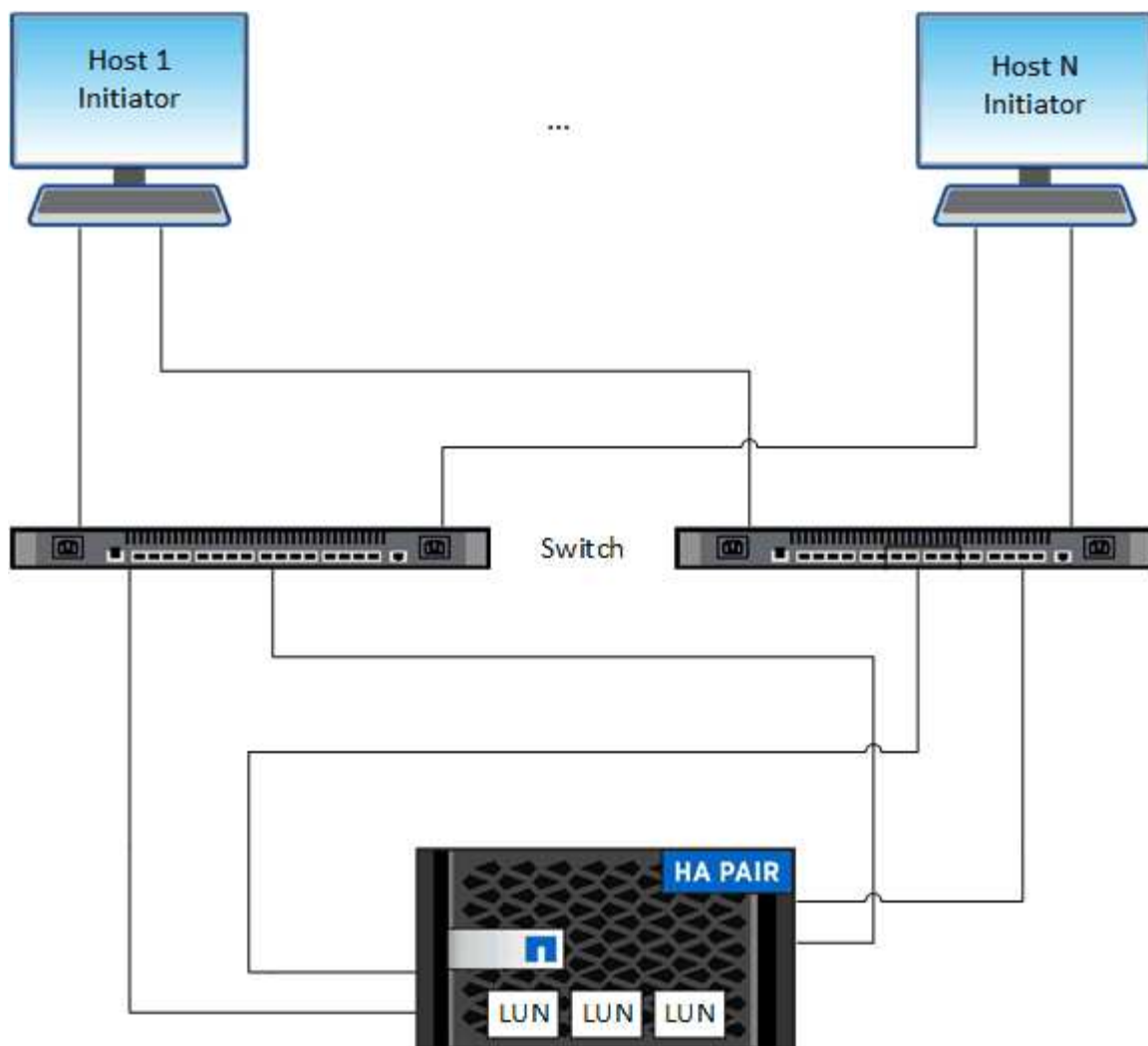
Información general de gestión de San

El contenido de esta sección muestra cómo configurar y gestionar entornos SAN con la interfaz de línea de comandos (CLI) de ONTAP y System Manager en ONTAP 9.7 y versiones posteriores.

Si utiliza la versión clásica de System Manager (disponible solo en ONTAP 9.7 y versiones anteriores), consulte los temas siguientes:

- ["Protocolo iSCSI"](#)
- ["Protocolo FC/FCoE"](#)

Puede utilizar los protocolos iSCSI y FC para proporcionar almacenamiento en un entorno SAN.



Con iSCSI y FC, los destinos de almacenamiento se denominan LUN (unidades lógicas) y se presentan a los hosts como dispositivos de bloque estándar. Puede crear LUN y, a continuación, asignarlas a iGroups. Los iGroups son tablas de WWN de host FC y nombres de nodos de host iSCSI; además, controlan qué iniciadores tienen acceso a qué LUN.

Los destinos FC se conectan a la red a través de switches FC y adaptadores del lado del host y se identifican por nombres de puerto WWPN. Los destinos iSCSI se conectan a la red a través de adaptadores de red Ethernet (NIC) estándar, tarjetas del motor de descarga TCP (TOE) con iniciadores de software, adaptadores de red convergentes (CNA) o adaptadores de host busto (HBA) dedicados y se identifican mediante nombres completos de iSCSI (IQN).

Configurar los switches para FCoE

Debe configurar los switches de FCoE para que el servicio FC pueda ejecutarse en la infraestructura Ethernet existente.

Lo que necesitará

- Debe ser compatible con la configuración SAN.

Para obtener más información acerca de las configuraciones admitidas, consulte ["Herramienta de matriz de interoperabilidad de NetApp"](#).

- Se debe instalar un adaptador de objetivo unificado (UTA) en el sistema de almacenamiento.

Si utiliza un UTA2, debe configurarse en `cna` modo.

- Se debe instalar un adaptador de red convergente (CNA) en el host.

Pasos

1. Use la documentación de su switch para configurar los switches para FCoE.
2. Compruebe que los ajustes de DCB para cada nodo del cluster se han configurado correctamente.

```
run -node node1 -command dcb show
```

Los ajustes de DCB se configuran en el switch. Si los ajustes no son correctos, consulte la documentación del switch.

3. Compruebe que el inicio de sesión FCoE funciona cuando el estado en línea del puerto de destino de FC es `true`.

```
fcip adapter show -fields node,adapter,status,state,speed,fabric-  
established,physical-protocol
```

Si el estado en línea del puerto de destino FC es `false`, consulte la documentación del conmutador.

Información relacionada

- ["Herramienta de matriz de interoperabilidad de NetApp"](#)
- ["Informe técnico de NetApp 3800: Guía de implementación integral de Fibre Channel sobre Ethernet \(FCoE\)"](#)
- ["Guías de configuración de software de Cisco MDS 9000 NX-OS y SAN-OS"](#)
- ["Productos Brocade"](#)

Requisitos del sistema

La configuración de LUN implica crear una LUN, crear un igroup y asignar la LUN al igroup. El sistema debe cumplir con ciertos requisitos previos antes de poder configurar las LUN.

- La matriz de interoperabilidad debe incluir la configuración DE SAN como compatible.
- El entorno SAN debe cumplir con los límites DE configuración de host SAN y controladora especificados en ["Hardware Universe de NetApp"](#) Para su versión del software ONTAP.
- Se debe instalar una versión compatible de Host Utilities.

La documentación de Host Utilities proporciona más información.

- Debe tener LIF SAN en el nodo propietario de LUN y el partner de alta disponibilidad del nodo propietario.

Información relacionada

- ["Herramienta de matriz de interoperabilidad de NetApp"](#)
- ["Configuración de host SAN ONTAP"](#)
- ["Informe técnico de NetApp 4017: Prácticas recomendadas de SAN Fibre Channel"](#)

Qué debe saber antes de crear una LUN

Por qué el tamaño real de las LUN varía ligeramente

Debe tener en cuenta lo siguiente con respecto al tamaño de sus LUN.

- Cuando crea una LUN , el tamaño real de la LUN puede variar ligeramente en función del tipo de SO de la LUN. El tipo de SO LUN no se puede modificar una vez que se crea la LUN.
- Si crea una LUN en el tamaño máximo de LUN, tenga en cuenta que el tamaño real de la LUN puede ser ligeramente menor. ONTAP redondea el límite para ser ligeramente menor.
- Los metadatos de cada LUN requieren aproximadamente 64 KB de espacio en el agregado que lo contiene. Cuando crea una LUN, debe asegurarse de que el agregado que contiene tenga suficiente espacio para los metadatos de la LUN. Si el agregado no contiene espacio suficiente para los metadatos de la LUN, es posible que algunos hosts no puedan acceder a la LUN.

Directrices para asignar ID de LUN

Normalmente, el ID de LUN predeterminado comienza con 0 y se asigna en incrementos de 1 para cada LUN asignada adicional. El host asocia el ID de LUN con la ubicación y el nombre de ruta de la LUN. El rango de números de ID de LUN válidos depende del host. Para obtener información detallada, consulte la documentación proporcionada con las utilidades de host.

Directrices para asignar las LUN a iGroups

- Solo puede asignar una LUN una vez a un igroup.
- Como práctica recomendada, debe asignar una LUN a un solo iniciador específico a través del igroup.
- Puede agregar un solo iniciador a varios iGroups, pero el iniciador solo se puede asignar a una LUN.
- No puede utilizar el mismo ID de LUN para dos LUN asignadas al mismo igroup.
- Debe utilizar el mismo tipo de protocolo para iGroups y conjuntos de puertos.

Compruebe y añada su licencia de protocolo FC o iSCSI

Para poder habilitar el acceso en bloque para una máquina virtual de almacenamiento (SVM) con FC o iSCSI, debe tener una licencia. Las licencias FC e iSCSI están incluidas con ["ONTAP One"](#).

Ejemplo 6. Pasos

System Manager

Si no tiene ONTAP One, verifique y añada su licencia FC o iSCSI con System Manager de ONTAP (9,7 y posterior).

1. En System Manager, seleccione **Clúster > Configuración > Licencias**
2. Si la licencia no aparece en la lista, seleccione  e introduzca la clave de licencia.
3. Seleccione **Agregar**.

CLI

Si no tiene ONTAP One, verifique y añada su licencia FC o iSCSI con la CLI de ONTAP.

1. Compruebe que tiene una licencia activa para FC o iSCSI.

```
system license show
```

| Package | Type | Description | Expiration |
|---------|------|----------------------|------------|
| Base | site | Cluster Base License | - |
| NFS | site | NFS License | - |
| CIFS | site | CIFS License | - |
| iSCSI | site | iSCSI License | - |
| FCP | site | FCP License | - |

2. Si no tiene una licencia activa para FC o iSCSI, añada el código de licencia.

```
license add -license-code <your_license_code>
```

Aprovisionar el almacenamiento SAN

Este procedimiento crea nuevas LUN en una máquina virtual de almacenamiento existente que ya tiene configurado el protocolo FC o iSCSI.

Si necesita crear una máquina virtual de almacenamiento nueva y configurar el protocolo FC o iSCSI, consulte ["Configure una SVM para FC"](#) o ["Configure una SVM para iSCSI"](#).

Si la licencia de FC no está habilitada, aparecen las LIF y SVM en línea pero el estado operativo está inactivo.

Las LUN aparecen como dispositivos de disco para el host.



El acceso asimétrico de unidad lógica (ALUA, Asymmetric Logical Unit Access) siempre está habilitado durante la creación de una LUN. No se puede cambiar la configuración de ALUA.

Debe usar la división en zonas de iniciador único para todas las LIF FC de la SVM a fin de alojar los iniciadores.

A partir de ONTAP 9.8, cuando se aprovisiona el almacenamiento, la calidad de servicio se habilita de forma predeterminada. Puede deshabilitar la calidad de servicio o seleccionar una política de calidad de servicio personalizada durante el proceso de aprovisionamiento o más adelante.

Ejemplo 7. Pasos

System Manager

Crear LUN para proporcionar almacenamiento para un host SAN mediante el protocolo FC o iSCSI con el Administrador del sistema de ONTAP (9.7 y versiones posteriores).

Para completar esta tarea mediante System Manager Classic (disponible con 9.7 y versiones anteriores), consulte ["Configuración iSCSI para Red Hat Enterprise Linux"](#)

Pasos

1. Instale el adecuado ["Utilidades host SAN"](#) en el host.
2. En System Manager, haga clic en **almacenamiento > LUN** y, a continuación, haga clic en **Agregar**.
3. Introduzca la información necesaria para crear la LUN.
4. Puede hacer clic en **más opciones** para realizar cualquiera de las siguientes acciones, dependiendo de su versión de ONTAP.

| Opción | Disponible empezando por |
|--|--------------------------|
| <ul style="list-style-type: none">• Asigne una política de calidad de servicio a las LUN en lugar de al volumen principal<ul style="list-style-type: none">◦ Más opciones > almacenamiento y optimización◦ Seleccione nivel de servicio de rendimiento.◦ Para aplicar la política QoS a LUN individuales en lugar de todo el volumen, seleccione aplicar estos límites de rendimiento a cada LUN.<p>De forma predeterminada, los límites de rendimiento se aplican a nivel de volumen.</p> | ONTAP 9.10.1 |
| <ul style="list-style-type: none">• Cree un nuevo iGroup mediante los iGroups existentes<ul style="list-style-type: none">◦ Más Opciones > INFORMACIÓN de HOST◦ Seleccione Nuevo iGroup utilizando los iGroups existentes.<p>NOTA: El tipo de SO para un igroup que contiene otros grupos de iniciadores no se puede cambiar después de que se haya creado.</p> | ONTAP 9.9.1 |
| <ul style="list-style-type: none">• Añada una descripción a su igroup o iniciador de host <p>La descripción sirve como alias del igroup o el iniciador del host.</p> <ul style="list-style-type: none">◦ Más Opciones > INFORMACIÓN de HOST | ONTAP 9.9.1 |

| | |
|--|-------------|
| <ul style="list-style-type: none"> • Cree el LUN en un volumen existente <p>De manera predeterminada, se crea un nuevo LUN en un volumen nuevo.</p> <ul style="list-style-type: none"> ◦ Más Opciones > Agregar LUN ◦ Seleccione Grupo de LUN. | ONTAP 9.9.1 |
| <ul style="list-style-type: none"> • Deshabilite QoS o elija una política de calidad de servicio personalizada ◦ Más opciones > almacenamiento y optimización ◦ Seleccione nivel de servicio de rendimiento. <p>NOTA: En ONTAP 9.9.1 y posterior, si selecciona una política de QoS personalizada, también puede seleccionar la colocación manual en un nivel local específico.</p> | ONTAP 9,8 |

5. Para FC, dividir los switches de FC en zonas mediante WWPN. Use una zona por iniciador e incluya todos los puertos de destino en cada zona.

6. Detectar las LUN en el host.

Para VMware vSphere, utilice Virtual Storage Console (VSC) para detectar e inicializar los LUN.

7. Inicialice las LUN y, opcionalmente, cree sistemas de archivos.

8. Compruebe que el host puede escribir y leer datos en la LUN.

CLI

Cree LUN para proporcionar almacenamiento para un host SAN mediante el protocolo FC o iSCSI con la CLI de ONTAP.

1. Compruebe que dispone de una licencia para FC o iSCSI.

```
system license show
```

| Package | Type | Description | Expiration |
|---------|------|----------------------|------------|
| Base | site | Cluster Base License | - |
| NFS | site | NFS License | - |
| CIFS | site | CIFS License | - |
| iSCSI | site | iSCSI License | - |
| FCP | site | FCP License | - |

2. Si no tiene una licencia para FC o iSCSI, utilice `license add` comando.

```
license add -license-code <your_license_code>
```

3. Habilite el servicio de protocolo en la SVM:

Para iSCSI:

```
vserver iscsi create -vserver <svm_name> -target-alias <svm_name>
```

Para FC:

```
vserver fcp create -vserver <svm_name> -status-admin up
```

4. Cree dos LIF para las SVM en cada nodo:

```
network interface create -vserver <svm_name> -lif <lif_name> -role  
data -data-protocol <iscsi|fc> -home-node <node_name> -home-port  
<port_name> -address <ip_address> -netmask <netmask>
```

NetApp admite un mínimo de un LIF iSCSI o FC por nodo para cada SVM que sirve datos. Sin embargo, se necesitan dos LIF por nodo para redundancia. Para iSCSI, se recomienda configurar un mínimo de dos LIF por nodo en redes Ethernet independientes.

5. Compruebe que sus LIF se han creado y que su estado operativo es online:

```
network interface show -vserver <svm_name> <lif_name>
```

6. Cree sus LUN:

```
lun create -vserver <svm_name> -volume <volume_name> -lun <lun_name>  
-size <lun_size> -ostype linux -space-reserve <enabled|disabled>
```

El nombre de la LUN no puede superar los 255 caracteres y no puede contener espacios.



La opción NVFAIL se habilita automáticamente cuando se crea una LUN en un volumen.

7. Cree sus iGroups:

```
igroup create -vserver <svm_name> -igroup <igroup_name> -protocol  
<fcp|iscsi|mixed> -ostype linux -initiator <initiator_name>
```

8. Asigne sus LUN a iGroups:

```
lun mapping create -vserver <svm__name> -volume <volume_name> -lun  
<lun_name> -igroup <igroup_name>
```

9. Compruebe que sus LUN están configuradas correctamente:

```
lun show -vserver <svm_name>
```

10. Opcionalmente, ["Cree un conjunto de puertos y enlace a un igroup"](#).
11. Siga los pasos de la documentación de host para habilitar el acceso en bloque en los hosts específicos.
12. Use las utilidades de host para completar la asignación de FC o iSCSI y para detectar las LUN en el host.

Información relacionada

- ["Información general sobre la administración de SAN"](#)
- ["Configuración de host SAN ONTAP"](#)
- ["Consulte y gestione los iGroups SAN en System Manager"](#)
- ["Informe técnico de NetApp 4017: Prácticas recomendadas de SAN Fibre Channel"](#)

Aprovisionamiento de NVMe

Descripción general de NVMe

Es posible usar el protocolo de memoria no volátil rápida (NVMe) para proporcionar almacenamiento en un entorno SAN. El protocolo NVMe está optimizado para el rendimiento con el almacenamiento de estado sólido.

Para NVMe, los destinos de almacenamiento se denominan espacios de nombres. Un espacio de nombres NVMe es una cantidad de almacenamiento no volátil que se puede formatear en bloques lógicos y presentarla a un host como dispositivo de bloques estándar. Se crean espacios de nombres y subsistemas y, a continuación, se asignan los espacios de nombres a los subsistemas de, de modo similar al modo en que se aprovisionan las LUN y se asignan a iGroups para FC e iSCSI.

Los destinos NVMe se conectan a la red a través de una infraestructura FC estándar que utiliza switches FC o una infraestructura TCP estándar que utiliza switches Ethernet y adaptadores del lado del host.

La compatibilidad con NVMe varía según su versión de ONTAP. Consulte ["Compatibilidad y limitaciones de NVMe"](#) para obtener más detalles.

Qué es NVMe

El protocolo expreso de memoria no volátil (NVMe) es un protocolo de transporte que se utiliza para acceder a medios de almacenamiento no volátiles.

NVMe over Fabrics (NVMeoF) es una extensión definida por las especificaciones para NVMe que permite la

comunicación basada en NVMe mediante conexiones distintas de PCIe. Esta interfaz permite conectar gabinetes de almacenamiento externos a un servidor.

NVMe se ha diseñado para proporcionar un acceso eficiente a dispositivos de almacenamiento creados con memoria no volátil, desde la tecnología flash hasta las tecnologías de memoria persistente de mayor rendimiento. De este modo, no tiene las mismas limitaciones que los protocolos de almacenamiento diseñados para las unidades de disco duro. Los dispositivos flash y de estado sólido (SSD) son un tipo de memoria no volátil (NVM). NVM es un tipo de memoria que conserva su contenido durante una interrupción de la alimentación. NVMe es un modo de acceder a esa memoria.

Entre las ventajas de NVMe se incluyen mayores velocidades, productividad, rendimiento y capacidad para la transferencia de datos. Entre las características específicas se encuentran las siguientes:

- NVMe está diseñado para tener hasta 64 000 colas.

Cada cola puede tener hasta 64 000 comandos simultáneos.

- NVMe es compatible con varios proveedores de hardware y software
- NVMe es más productivo con las tecnologías Flash que permiten tiempos de respuesta más rápidos
- NVMe permite solicitudes de datos múltiples para cada «misión» enviada al SSD.

NVMe tarda menos tiempo en decodificar una «misión» y no requiere bloqueo de subprocesos en un programa multiproceso.

- NVMe admite una funcionalidad que evita cuellos de botella a nivel de CPU y posibilita una escalabilidad masiva conforme aumentan los sistemas.

Acerca de los espacios de nombres de NVMe

Un espacio de nombres NVMe es una cantidad de memoria no volátil (NVM) que se puede formatear en bloques lógicos. Los espacios de nombres se usan cuando una máquina virtual de almacenamiento se configura con el protocolo NVMe y es el equivalente de LUN para protocolos FC e iSCSI.

Uno o más espacios de nombres se aprovisionan y están conectados a un host NVMe. Cada espacio de nombres puede admitir distintos tamaños de bloque.

El protocolo NVMe ofrece acceso a los espacios de nombres mediante varias controladoras. El uso de controladores NVMe, que son compatibles con la mayoría de los sistemas operativos, los espacios de nombres de unidades de estado sólido (SSD) aparecen como dispositivos de bloque estándar en los cuales los sistemas de archivos y las aplicaciones se pueden implementar sin ninguna modificación.

Un identificador de espacio de nombres (NSID) es un identificador que utiliza una controladora para proporcionar acceso a un espacio de nombres. Al configurar el NSID para un host o un grupo de hosts, también se puede configurar la accesibilidad a un volumen en un host. Un bloque lógico solo se puede asignar a un único grupo de hosts a la vez, y un grupo de hosts determinado no tiene ningún NSID duplicado.

Acerca de los subsistemas NVMe

Un subsistema NVMe incluye una o más controladoras NVMe, espacios de nombres, puertos del subsistema NVM, un medio de almacenamiento NVM y una interfaz entre la controladora y el medio de almacenamiento NVM. Cuando crea un espacio de nombres NVMe, de forma predeterminada no se asigna a un subsistema. También puede optar por asignarlo a un subsistema nuevo o existente.

Información relacionada

- ["Aprovisione el almacenamiento NVMe"](#)
- ["Asignar un espacio de nombres NVMe a un subsistema"](#)
- ["Configuración de los hosts SAN y los clientes de cloud"](#)

Requisitos para la licencia de NVMe

A partir de ONTAP 9.5, se requiere una licencia para admitir NVMe. Si se habilita NVMe en ONTAP 9.4, se concede un periodo de gracia de 90 días para adquirir la licencia antes de actualizar a ONTAP 9.5.

Puede habilitar la licencia mediante el siguiente comando:

```
system license add -license-code NVMe_license_key
```

Configuración, compatibilidad y limitaciones de NVMe

A partir de ONTAP 9.4, el ["Memoria no volátil rápida \(NVMe\)"](#) el protocolo está disponible para los entornos SAN. FC-NVMe utiliza la misma práctica de configuración física y división en zonas que las redes FC tradicionales pero permite un mayor ancho de banda, un aumento de IOPS y una latencia reducida que FC-SCSI.

Las limitaciones y la compatibilidad de NVMe varían en función de la versión de ONTAP, su plataforma y la configuración. Para obtener detalles sobre su configuración específica, consulte ["Herramienta de matriz de interoperabilidad de NetApp"](#). Para conocer los límites admitidos, consulte ["Hardware Universe"](#).



El número máximo de nodos por clúster está disponible en Hardware Universe bajo **Mezcla de plataformas soportada**.

Configuración

- Puede establecer su configuración NVMe con una sola estructura o multiestructura.
- Debe configurar una LIF de gestión para cada SVM compatible con SAN.
- No se admite el uso de estructuras heterogéneas de switches FC, a excepción de los switches blade integrados.

Las excepciones específicas se enumeran en la ["Herramienta de matriz de interoperabilidad de NetApp"](#).

- Las estructuras en cascada, malla parcial, malla completa, núcleo-borde y director son métodos estándar en el sector para conectar switches FC a una estructura, y todos son compatibles.

Una estructura puede estar compuesta por uno o varios switches y las controladoras de almacenamiento se pueden conectar a varios switches.

Funciones

Las siguientes funciones de NVMe se admiten según la versión de ONTAP.

| | |
|------------------------|-------------------------|
| Iniciando con ONTAP... | Compatibilidad con NVMe |
|------------------------|-------------------------|

| | |
|--------|---|
| 9.12.1 | <p>Configuraciones IP de MetroCluster de 4 nodos en NVMe/FC.</p> <ul style="list-style-type: none"> Las configuraciones de MetroCluster no son compatibles con NVMe antes de la versión 9.12.1. Las configuraciones de MetroCluster no son compatibles con NVMe/TCP. |
| 9.10.1 | Cambiar el tamaño de un espacio de nombres |
| 9.9.1 | <ul style="list-style-type: none"> Los espacios de nombres y LUN coexisten en el mismo volumen. |
| 9,8 | <ul style="list-style-type: none"> Coexistencia con protocolos <p>Pueden existir los protocolos SCSI, NAS y NVMe en la misma máquina virtual de almacenamiento (SVM).</p> <p>Antes de ONTAP 9,8, NVMe puede ser el único protocolo en la SVM.</p> <p>*</p> |
| 9,6 | <ul style="list-style-type: none"> bloques de 512 bytes y bloques de 4096 bytes para espacios de nombres <p>4096 es el valor predeterminado. 512 solo se debe utilizar si el sistema operativo del host no admite bloques de 4096 bytes.</p> <ul style="list-style-type: none"> Movimiento de volúmenes con espacios de nombres asignados |
| 9,5 | Conmutación/retorno al nodo primario de la pareja de HA de múltiples rutas. |

Protocolos

Se admiten los siguientes protocolos NVMe.

| Protocolo | Iniciando con ONTAP... | Permitido por... |
|-----------|------------------------|------------------|
| TCP | 9.10.1 | Predeterminado |
| FC | 9,4 | Predeterminado |

A partir de ONTAP 9,8, puede configurar los protocolos SCSI, NAS y NVMe en la misma máquina virtual de almacenamiento (SVM).

En ONTAP 9,7 y versiones anteriores, NVMe puede ser el único protocolo en la SVM.

Espacios de nombres

Cuando trabaje con espacios de nombres de NVMe, debe tener en cuenta lo siguiente:

- Si pierde datos en una LUN, no se pueden restaurar desde un espacio de nombres o viceversa.
- La garantía de espacio para espacios de nombres es la misma que la garantía de espacio del volumen que contiene.
- No se puede crear un espacio de nombres en una transición de volúmenes desde Data ONTAP en 7-Mode.
- Los espacios de nombres no admiten lo siguiente:
 - Cambio de nombre
 - Movimiento entre volúmenes
 - Copia entre volúmenes
 - Copiar bajo demanda

Limitaciones adicionales

Las configuraciones de NVMe no admiten las siguientes funciones de ONTAP:

- Sincr
- Consola de almacenamiento virtual

Lo siguiente solo se aplica a nodos que ejecutan ONTAP 9.4:

- Las LIF y los espacios de nombres de NVMe deben alojarse en el mismo nodo.
- Debe crearse el servicio NVMe antes de crear la LIF NVMe.

Información relacionada

["Prácticas recomendadas para SAN modernas"](#)

Configure una máquina virtual de almacenamiento para NVMe

Si desea usar el protocolo NVMe en un nodo, debe configurar la SVM específicamente para NVMe.


Antes de empezar

Sus adaptadores FC o Ethernet deben ser compatibles con NVMe. Los adaptadores admitidos figuran en la ["Hardware Universe de NetApp"](#).

Ejemplo 8. Pasos

System Manager

Configure una máquina virtual de almacenamiento para NVMe con ONTAP System Manager (9.7 y posterior).

| Para configurar NVMe en una nueva máquina virtual de almacenamiento | Para configurar NVMe en una máquina virtual de almacenamiento existente |
|--|---|
| <ol style="list-style-type: none">1. En System Manager, haga clic en almacenamiento > Storage VMs y, a continuación, haga clic en Agregar.2. Escriba un nombre para la máquina virtual de almacenamiento.3. Seleccione NVMe para el Protocolo de acceso.4. Seleccione Activar NVMe/FC o Activar NVMe/TCP y Guardar. | <ol style="list-style-type: none">1. En System Manager, haga clic en almacenamiento > Storage VMs.2. Haga clic en la máquina virtual de almacenamiento que desee configurar.3. Haga clic en la ficha Configuración y, a continuación, haga clic en  Junto al protocolo NVMe.4. Seleccione Activar NVMe/FC o Activar NVMe/TCP y Guardar. |

CLI

Configure una máquina virtual de almacenamiento para NVMe con la interfaz de línea de comandos de ONTAP.

1. Si no quiere usar una SVM existente, cree una:

```
vserver create -vserver <SVM_name>
```

- a. Compruebe que la SVM se ha creado:

```
vserver show
```

2. Compruebe que tiene instalados adaptadores compatibles con NVMe o TCP en el clúster:

Para NVMe:

```
network fcp adapter show -data-protocols-supported fc-nvme
```

Para TCP:

```
network port show
```

3. Si utiliza ONTAP 9.7 o una versión anterior, quite todos los protocolos de la SVM:

```
vserver remove-protocols -vserver <SVM_name> -protocols  
iscsi, fcp, nfs, cifs, ndmp
```

A partir de ONTAP 9.8, no es necesario quitar otros protocolos al añadir NVMe.

4. Añada el protocolo NVMe a la SVM:

```
vserver add-protocols -vserver <SVM_name> -protocols nvme
```

5. Si ejecuta ONTAP 9.7 o una versión anterior, compruebe que NVMe sea el único protocolo permitido en la SVM:

```
vserver show -vserver <SVM_name> -fields allowed-protocols
```

NVMe debe ser el único protocolo que se muestra en la `allowed protocols` columna.

6. Cree el servicio NVMe:

```
vserver nvme create -vserver <SVM_name>
```

7. Compruebe que el servicio NVMe se ha creado:

```
vserver nvme show -vserver <SVM_name>
```

La Administrative Status De la SVM debe aparecer como up.

8. Cree una LIF NVMe/FC:

- Para ONTAP 9.9.1 o anterior, FC:

```
network interface create -vserver <SVM_name> -lif <lif_name>  
-role data -data-protocol fc-nvme -home-node <home_node> -home  
-port <home_port>
```

- Para ONTAP 9.10.1 o posterior, FC o TCP:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-service-policy <default-data-nvme-tcp | default-data-nvme-fc>
-data-protocol <fcp | fc-nvme | nvme-tcp> -home-node <home_node>
-home-port <home_port> -status-admin up -failover-policy disabled
-firewall-policy data -auto-revert false -failover-group
<failover_group> -is-dns-update-enabled false
```

9. Cree una LIF NVMe/FC en el nodo del partner de alta disponibilidad:

- Para ONTAP 9.9.1 o anterior, FC:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-role data -data-protocol fc-nvme -home-node <home_node> -home
-port <home_port>
```

- Para ONTAP 9.10.1 o posterior, FC o TCP:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-service-policy <default-data-nvme-tcp | default-data-nvme-fc>
-data-protocol <fcp | fc-nvme | nvme-tcp> -home-node <home_node>
-home-port <home_port> -status-admin up -failover-policy disabled
-firewall-policy data -auto-revert false -failover-group
<failover_group> -is-dns-update-enabled false
```

10. Compruebe que se han creado los LIF NVMe/FC:

```
network interface show -vserver <SVM_name>
```

11. Cree volúmenes en el mismo nodo que el LIF:

```
vol create -vserver <SVM_name> -volume <vol_name> -aggregate
<aggregate_name> -size <volume_size>
```

Si aparece un mensaje de advertencia acerca de la política de eficiencia automática, puede ignorarlo de forma segura.

Aprovisione el almacenamiento NVMe

Utilice estos pasos para crear espacios de nombres y aprovisionar almacenamiento para cualquier host compatible con NVMe en una máquina virtual de almacenamiento existente.

A partir de ONTAP 9.8, cuando se aprovisiona el almacenamiento, la calidad de servicio se habilita de forma predeterminada. Puede deshabilitar la calidad de servicio o seleccionar una política de calidad de servicio personalizada durante el proceso de aprovisionamiento o más adelante.

Antes de empezar

La máquina virtual de almacenamiento debe configurarse para NVMe, y ya se debe configurar el transporte FC o TCP.

System Manager

Con System Manager de ONTAP (9.7 y versiones posteriores), cree espacios de nombres para ofrecer almacenamiento mediante el protocolo NVMe.

Pasos

1. En System Manager, haga clic en **almacenamiento > espacios de nombres NVMe** y, a continuación, haga clic en **Agregar**.

Si necesita crear un subsistema nuevo, haga clic en **más opciones**.

2. Si está ejecutando ONTAP 9.8 o posterior y desea desactivar QoS o elegir una directiva de QoS personalizada, haga clic en **más opciones** y, a continuación, en **almacenamiento y optimización** seleccione **nivel de servicio de rendimiento**.
3. Dividir los switches de FC en zonas mediante WWPN. Use una zona por iniciador e incluya todos los puertos de destino en cada zona.
4. En el host, detecte los nuevos espacios de nombres.
5. Inicialice el espacio de nombres y formatee el sistema de archivos.
6. Verificar que el host puede escribir y leer datos en el espacio de nombres.

CLI

Si usa la interfaz de línea de comandos de ONTAP, cree espacios de nombres para ofrecer almacenamiento con el protocolo NVMe.

Este procedimiento crea un espacio de nombres y un subsistema NVMe en una máquina virtual de almacenamiento existente que ya se configuró para el protocolo NVMe y luego asigna el espacio de nombres al subsistema para permitir el acceso a los datos desde el sistema host.

Si necesita configurar la máquina virtual de almacenamiento para NVMe, consulte ["Configure una SVM para NVMe"](#).

Pasos

1. Compruebe que la SVM esté configurada para NVMe:

```
vserver show -vserver <svm_name> -fields allowed-protocols
```

NVMe debe aparecer debajo de la `allowed-protocols` columna.

2. Cree el espacio de nombres NVMe:

```
vserver nvme namespace create -vserver <svm_name> -path <path> -size <size_of_namespace> -ostype <OS_type>
```

3. Cree el subsistema NVMe:


```
vserver nvme subsystem create -vserver <svm_name> -subsystem  
<name_of_subsystem> -ostype <OS_type>
```

El nombre del subsistema NVMe distingue mayúsculas de minúsculas. Debe contener de 1 a 96 caracteres. Se permiten caracteres especiales.

4. Compruebe que se ha creado el subsistema:

```
vserver nvme subsystem show -vserver <svm_name>
```

La nvme el subsistema debe aparecer debajo de Subsystem columna.

5. Obtenga el NQN del host.
6. Añada el NQN del host al subsistema:

```
vserver nvme subsystem host add -vserver <svm_name> -subsystem  
<subsystem_name> -host-nqn <Host_NQN>
```

7. Asigne el espacio de nombres al subsistema:

```
vserver nvme subsystem map add -vserver <svm_name> -subsystem  
<subsystem_name> -path <path>
```

Un espacio de nombres solo se puede asignar a un subsistema único.

8. Compruebe que el espacio de nombres está asignado al subsistema:

```
vserver nvme namespace show -vserver <svm_name> -instance
```

El subsistema debe aparecer como Attached subsystem.

Asignar un espacio de nombres NVMe a un subsistema

La asignación de un espacio de nombres NVMe a un subsistema permite el acceso a los datos desde el host. Es posible asignar un espacio de nombres NVMe a un subsistema al aprovisionar almacenamiento, o bien puede hacerlo después de que se ha aprovisionado el almacenamiento.

A partir de ONTAP 9.14.1, puede priorizar la asignación de recursos para hosts específicos. De forma predeterminada, cuando se añade un host al subsistema NVMe, se da prioridad regular. Puede usar la interfaz de línea de comandos (CLI) de ONTAP para cambiar manualmente la prioridad predeterminada de regular a alta. Los hosts a los que se asigna una prioridad alta se asignan números de colas de I/O de mayor tamaño y

profundidades de cola.



Si desea dar una prioridad alta a un host que se añadió a un subsistema en ONTAP 9.13.1 o versiones anteriores, puede [cambie la prioridad del host](#).

Antes de empezar

El espacio de nombres y el subsistema ya deben crearse. Si necesita crear un espacio de nombres y un subsistema, consulte "[Aprovisione el almacenamiento NVMe](#)".

Pasos

1. Obtenga el NQN del host.
2. Añada el NQN del host al subsistema:

```
vserver nvme subsystem host add -vserver <SVM_name> -subsystem  
<subsystem_name> -host-nqn <Host_NQN_:subsystem._subsystem_name>
```

Si desea cambiar la prioridad predeterminada del host de normal a alta, use el `-priority high` opción. Esta opción está disponible a partir de ONTAP 9.14.1.

3. Asigne el espacio de nombres al subsistema:

```
vserver nvme subsystem map add -vserver <SVM_name> -subsystem  
<subsystem_name> -path <path>
```

Un espacio de nombres solo se puede asignar a un subsistema único.

4. Compruebe que el espacio de nombres está asignado al subsistema:

```
vserver nvme namespace show -vserver <SVM_name> -instance
```

El subsistema debe aparecer como `Attached subsystem`.

Gestionar las LUN

Editar el grupo de políticas de calidad de servicio de la LUN

A partir de ONTAP 9.10.1, puede usar System Manager para asignar o quitar políticas de calidad de servicio (QoS) en varias LUN a la vez.



Si se asigna la política de calidad de servicio en el nivel del volumen, se debe cambiar en el nivel del volumen. Solo puede editar la política de calidad de servicio en el nivel de LUN si originalmente se asignó en el nivel de LUN.

Pasos

1. En System Manager, haga clic en **almacenamiento > LUN**.

2. Seleccione la LUN o los LUN que desee editar.

Si edita más de una LUN a la vez, las LUN deben pertenecer a la misma máquina virtual de almacenamiento (SVM). Si selecciona los LUN que no pertenecen a la misma SVM, no se muestra la opción para editar el grupo de políticas de calidad de servicio.

3. Haga clic en **más** y seleccione **Editar grupo de políticas QoS**.

Convertir una LUN en un espacio de nombres

A partir de ONTAP 9.11.1, es posible utilizar la interfaz de línea de comandos de ONTAP para convertir sin movimiento un LUN existente a un espacio de nombres NVMe.

Lo que necesitará

- La LUN especificada no debe tener ningún mapa existente en un igroup.
- El LUN no debe estar en una SVM configurada por MetroCluster ni en una relación de SM-BC.
- La LUN no debe ser un extremo de protocolo ni estar vinculada a un extremo de protocolo.
- La LUN no debe tener un prefijo distinto de cero ni un flujo de sufijo.
- La LUN no debe formar parte de una copia Snapshot ni en el lado destino de la relación de SnapMirror como LUN de solo lectura.

Paso

1. Convertir una LUN en un espacio de nombres NVMe:

```
vserver nvme namespace convert-from-lun -vserver -lun-path
```


Desconectar una LUN

A partir de ONTAP 9.10.1, puede utilizar System Manager para desconectar las LUN. Antes de ONTAP 9.10.1, debe utilizar la CLI de ONTAP para desconectar las LUN.

System Manager

Pasos

1. En System Manager, haga clic en **almacenamiento>LUN**.
2. Desconectar una única LUN o varias

| Si desea... | Haga esto... |
|---------------------------|--|
| Desconectar una única LUN | Junto al nombre de la LUN, haga clic en  Y seleccione desconectar . |
| Desconectar varias LUN | <ol style="list-style-type: none">1. Seleccione las LUN que desea desconectar.2. Haga clic en más y seleccione desconectar. |

CLI

Solo puede desconectar una LUN a la vez al utilizar la CLI.

Paso

1. Desconectar la LUN:

```
lun offline <lun_name> -vserver <SVM_name>
```

Cambiar el tamaño de una LUN

Puede aumentar o reducir el tamaño de una LUN.



No se puede cambiar el tamaño de las LUN de Solaris.

Aumentar el tamaño de una LUN

El tamaño al que puede aumentar su LUN varía en función de su versión de ONTAP.

| Versión de ONTAP | Tamaño máximo de LUN |
|-----------------------------------|--|
| ONTAP 9.12.1P2 y posterior | 128 TB para plataformas AFF, FAS y ASA |
| ONTAP 9,8 y versiones posteriores | <ul style="list-style-type: none">• 128 TB para plataformas de cabinas All-Flash SAN (ASA)• 16 TB para plataformas que no son ASA |
| ONTAP 9,5, 9,6 y 9,7 | 16 TB |

| | |
|----------------------|--|
| ONTAP 9.4 o anterior | <p>10 veces el tamaño original de la LUN, pero no superior a 16 TB, que es el tamaño máximo de LUN.</p> <p>Por ejemplo, si crea un LUN de 100 GB, solo puede ampliarlo a 1,000 GB.</p> <p>Es posible que el tamaño máximo real de la LUN no sea exactamente de 16 TB. ONTAP redondea el límite para ser ligeramente menor.</p> |
|----------------------|--|


No es necesario desconectar la LUN para aumentar el tamaño. Sin embargo, después de haber aumentado el tamaño, debe volver a analizar el LUN en el host para que el host reconozca el cambio de tamaño.

Consulte la página Command Reference para el `lun resize` Comando para obtener más información acerca de cómo cambiar el tamaño de una LUN.

Ejemplo 9. Pasos

System Manager

Aumente el tamaño de una LUN con System Manager de ONTAP (9.7 y posterior).

1. En System Manager, haga clic en **almacenamiento > LUN**.
2. Haga clic en  Y seleccione **Editar**.
3. En **almacenamiento y optimización** aumente el tamaño de la LUN y **Guardar**.

CLI

Aumente el tamaño de una LUN con la CLI de ONTAP.

1. Aumentar el tamaño de la LUN:

```
lun resize -vserver <SVM_name> -volume <volume_name> -lun <lun_name>
-size <lun_size>
```

2. Compruebe que ha aumentado el tamaño de LUN:

```
lun show -vserver <SVM_name_>
```

Las operaciones de ONTAP completan el tamaño máximo real de la LUN, de modo que es ligeramente inferior al valor esperado. Además, el tamaño real de la LUN puede variar ligeramente según el tipo de SO de la LUN. Para obtener el valor de tamaño exacto, ejecute los siguientes comandos en el modo avanzado:

```
set -unit B
```

```
lun show -fields max-resize-size -volume volume_name -lun lun_name
```

1. Vuelva a analizar el LUN en el host.
2. Siga la documentación del host para hacer que el tamaño de LUN recién creado sea visible para el sistema de archivos del host.

Reducir el tamaño de una LUN

Antes de reducir el tamaño de una LUN, el host necesita migrar los bloques que contienen los datos de la LUN al límite del tamaño de la LUN más pequeño. Debe utilizar una herramienta como SnapCenter para garantizar que la LUN se disminuye correctamente sin truncar los bloques que contengan datos de LUN. No se recomienda reducir manualmente el tamaño del LUN.

Después de reducir el tamaño del LUN, ONTAP notifica automáticamente al iniciador que el tamaño del LUN ha disminuido. Sin embargo, es posible que se requieran pasos adicionales en el host para que el host reconozca el nuevo tamaño de LUN. Consulte la documentación del host para obtener información específica sobre cómo reducir el tamaño de la estructura del archivo host.

Mover una LUN

Puede mover un LUN entre volúmenes dentro de una máquina virtual de almacenamiento (SVM), pero no puede mover un LUN entre varias SVM. Las LUN movidas entre volúmenes dentro de un SVM se mueven inmediatamente y sin pérdida de conectividad.

Lo que necesitará

Si el LUN utiliza una asignación de LUN selectiva (SLM), debería ["Modifique la lista SLM Reporting-Nodes"](#) Para incluir el nodo de destino y su partner de alta disponibilidad antes de mover el LUN.

Acerca de esta tarea

Las funciones de eficiencia del almacenamiento, como la deduplicación, la compresión y la compactación, no se conservan durante un movimiento de LUN. Se deben volver a aplicar una vez que se haya completado el movimiento de LUN.

La protección de datos mediante copias Snapshot se produce en el nivel de volumen. Por lo tanto, al mover una LUN, ésta se encuentra bajo el esquema de protección de datos del volumen de destino. Si no tiene establecidas copias de Snapshot para el volumen de destino, no se crean copias de Snapshot de la LUN. Además, todas las copias Snapshot de la LUN se conservan en el volumen original hasta que se eliminan dichas copias.

No se puede mover una LUN a los siguientes volúmenes:

- Un volumen de destino de SnapMirror
- El volumen raíz de SVM

No puede mover los siguientes tipos de LUN:

- LUN creada a partir de un archivo
- Una LUN que tiene el estado NVFAIL
- LUN en una relación de uso compartido de carga
- LUN de clase de extremo de protocolo



Para los LUN de Solaris os_TYPE que tienen 1 TB o más, es posible que se agote el tiempo de espera del host durante el movimiento de la LUN. Para este tipo de LUN, tiene que desmontar la LUN antes de iniciar la transición.


Ejemplo 10. Pasos

System Manager

Mueva una LUN con System Manager de ONTAP (9.7 y posterior).

A partir de ONTAP 9.10.1, se puede usar System Manager para crear un volumen nuevo al mover una sola LUN. En ONTAP 9.8 y 9.9.1, el volumen al que se mueve el LUN debe existir antes de iniciar el movimiento de LUN.

Pasos

1. En System Manager, haga clic en **almacenamiento>LUN**.
2. Haga clic con el botón derecho en la LUN que desea mover y, a continuación, haga clic en  Y seleccione **mover LUN**.

En ONTAP 9.10.1, seleccione para mover el LUN a **un volumen existente** o a **Nuevo volumen**.

Si selecciona crear un nuevo volumen, proporcione las especificaciones del volumen.

3. Haga clic en **mover**.

CLI

Mueva una LUN con la CLI de ONTAP.

1. Mover la LUN:

```
lun move start
```

Durante un período muy breve, la LUN puede verse tanto en el volumen de origen como en el de destino. Esto es normal y se resuelve al finalizar el traslado.

2. Realice un seguimiento del estado de la transferencia y compruebe que la finalización es correcta:

```
lun move show
```

Información relacionada

- ["Asignación de LUN selectiva"](#)

Eliminar las LUN

Es posible eliminar una LUN de una máquina virtual de almacenamiento (SVM) si ya no se necesita la LUN.

Lo que necesitará

Se debe quitar la asignación de la LUN de su igroup para poder eliminarla.

Pasos

1. Compruebe que la aplicación o el host no están utilizando la LUN.
2. Desasigne la LUN del igroup:

```
lun mapping delete -vserver <SVM_name> -volume <volume_name> -lun  
<LUN_name> -igroup <igroup_name>
```

3. Elimine la LUN:

```
lun delete -vserver <SVM_name> -volume <volume_name> -lun <LUN_name>
```

4. Compruebe que ha eliminado la LUN:

```
lun show -vserver <SVM_name>
```

| Vserver | Path | State | Mapped | Type | Size |
|---------|-----------------|--------|--------|---------|---------|
| vs5 | /vol/vol16/lun8 | online | mapped | windows | 10.00GB |

Qué debe saber antes de copiar las LUN

Debe ser consciente de ciertas cosas antes de copiar una LUN.

Los administradores de clúster pueden copiar una LUN en máquinas virtuales de almacenamiento (SVM) del clúster mediante el `lun copy` comando. Los administradores de clústeres deben establecer la relación entre iguales de las máquinas virtuales de almacenamiento (SVM) mediante el `vserver peer create` Antes de ejecutar una operación de copia de LUN entre SVM. Debe haber suficiente espacio en el volumen de origen para un clon SIS.

Las LUN de las copias Snapshot se pueden usar como LUN de origen del `lun copy` comando. Cuando se copia una LUN mediante `lun copy` Comando, la copia LUN está disponible inmediatamente para acceso de lectura y escritura. La LUN de origen no se modifica por la creación de una copia LUN. Tanto la LUN de origen como la copia LUN existen como LUN únicas con diferentes números de serie de LUN. Los cambios realizados en la LUN de origen no se reflejan en la copia LUN, y los cambios realizados en la copia LUN no se reflejan en la LUN de origen. La asignación de la LUN de origen no se copia en la nueva LUN; es necesario asignar la copia LUN.

La protección de datos mediante copias Snapshot se produce en el nivel de volumen. Por lo tanto, si copia una LUN en un volumen distinto del volumen de la LUN de origen, la LUN de destino cae en el esquema de protección de datos del volumen de destino. Si no tiene establecidas copias de Snapshot para el volumen de destino, no se crean copias de Snapshot de la copia de LUN.

La copia de LUN es una operación no disruptiva.

No se pueden copiar los siguientes tipos de LUN:

- LUN creada a partir de un archivo
- Una LUN con el estado NVFAIL
- LUN en una relación de uso compartido de carga
- LUN de clase de extremo de protocolo

Examine el espacio configurado y usado de una LUN

Conocer el espacio configurado y el espacio real usado para las LUN puede ayudar a determinar la cantidad de espacio que se puede recuperar al hacer la reclamación de espacio, la cantidad de espacio reservado que contiene datos, y el tamaño total configurado en comparación con el tamaño real usado para una LUN.

Paso

1. Vea el espacio configurado en comparación con el espacio real usado para una LUN:

```
lun show
```

En el siguiente ejemplo, se muestra el espacio configurado en comparación con el espacio real utilizado por las LUN en la máquina virtual de almacenamiento (SVM) vs3:

```
lun show -vserver vs3 -fields path, size, size-used, space-reserve
```

| vserver | path | size | space-reserve | size-used |
|---------|-----------------------|---------|---------------|-----------|
| vs3 | /vol/vol0/lun1 | 50.01GB | disabled | 25.00GB |
| vs3 | /vol/vol0/lun1_backup | 50.01GB | disabled | 32.15GB |
| vs3 | /vol/vol0/lun2 | 75.00GB | disabled | 0B |
| vs3 | /vol/volspace/lun0 | 5.00GB | enabled | 4.50GB |

4 entries were displayed.

Activar la asignación de espacio para LUN con Thin Provisioning de SCSI

Si el host admite thin provisioning de SCSI, puede habilitar la asignación de espacio para LUN de SCSI con Thin Provisioning en ONTAP. Cuando se habilita la asignación de espacio, ONTAP notifica al host cuando el volumen se ha quedado sin espacio y el LUN del volumen no puede aceptar escrituras. ONTAP también recupera espacio automáticamente cuando el host elimina datos.

En los hosts que no admiten thin provisioning SCSI, cuando el volumen que contiene LUN se queda sin espacio y no se puede aumentar automáticamente, ONTAP desconecta la LUN. En los hosts compatibles con el thin provisioning SCSI, ONTAP no desconecta la LUN cuando se queda sin espacio. La LUN permanece en línea en modo de solo lectura, y se le notifica al host que la LUN ya no puede aceptar escrituras.

Además, cuando se eliminan datos en un host que admite thin provisioning SCSI, la gestión de espacio en el host identifica los bloques de datos eliminados en el sistema de archivos del host y emite automáticamente

uno o más SCSI UNMAP los comandos para liberar los bloques correspondientes en el sistema de almacenamiento.

Antes de empezar

Para permitir la asignación de espacio, el host debe admitir thin provisioning de SCSI. El thin provisioning de SCSI utiliza el aprovisionamiento de bloques lógicos tal como se define en el estándar SCSI SBC-3. Solo los hosts que admiten este estándar pueden utilizar thin provisioning SCSI en ONTAP.

Los siguientes hosts actualmente admiten thin provisioning de SCSI cuando habilita la asignación de espacio:

- Citrix XenServer 6,5 y posterior
- ESXi 5,0 y versiones posteriores
- Kernel UEK de Oracle Linux 6,2 o posterior
- RHEL 6,2 y posterior
- SLES11 y posterior
- Solaris 11,1 y posterior
- Windows

Acerca de esta tarea

De manera predeterminada, la asignación de espacio está deshabilitada para todas las LUN. Debe desconectar la LUN para permitir la asignación de espacio; después debe realizar la detección en el host para que el host reconozca que se ha habilitado la asignación de espacio.

Pasos

1. Desconecte la LUN.

```
lun modify -vserver vservice_name -volume volume_name -lun lun_name  
-state offline
```

2. Activar asignación de espacio:

```
lun modify -vserver _vserver_name_ -volume _volume_name_ -lun _lun_name_  
-space-allocation enabled
```

3. Compruebe que la asignación de espacio está activada:

```
lun show -vserver _vserver_name_ -volume _volume_name_ -lun _lun_name_  
-fields space-allocation
```

4. Conectar la LUN:

```
lun modify -vserver _vserver_name_ -volume _volume_name_ -lun _lun_name_  
-state online
```

5. En el host, vuelva a analizar todos los discos para garantizar que el cambio en el `-space-allocation` la opción se detecta correctamente.

Controle y supervise el rendimiento de I/O de las LUN utilizando la calidad de servicio de almacenamiento

Puede controlar el rendimiento de entrada/salida (I/O) a las LUN asignando LUN a los grupos de políticas de calidad de servicio de almacenamiento. Es posible controlar el rendimiento de I/O para garantizar que las cargas de trabajo alcancen objetivos de rendimiento específicos o reducir una carga de trabajo que afecte negativamente a otras cargas de trabajo.

Acerca de esta tarea

Los grupos de directivas aplican un límite máximo de rendimiento (por ejemplo, 100 MB/s). Puede crear un grupo de políticas sin especificar un rendimiento máximo, lo que permite supervisar el rendimiento antes de controlar la carga de trabajo.

También puede asignar máquinas virtuales de almacenamiento (SVM) con volúmenes de FlexVol y LUN a grupos de políticas.

Tenga en cuenta los siguientes requisitos sobre la asignación de una LUN a un grupo de políticas:

- La LUN debe estar contenida en la SVM a la que pertenece el grupo de políticas.

La SVM se especifica al crear el grupo de políticas.

- Si asigna un LUN a un grupo de políticas, no puede asignar el volumen o la SVM que contiene el LUN a un grupo de políticas.

Para obtener más información acerca de cómo usar la calidad de servicio de almacenamiento, consulte ["Referencia de administración del sistema"](#).

Pasos

1. Utilice la `qos policy-group create` comando para crear un grupo de políticas.
2. Utilice la `lun create` o el `lun modify` con el `-qos-policy-group` Parámetro para asignar una LUN a un grupo de políticas.
3. Utilice la `qos statistics` comandos para ver datos de rendimiento.
4. Si es necesario, utilice `qos policy-group modify` comando para ajustar el límite máximo de rendimiento del grupo de políticas.

Herramientas disponibles para supervisar sus LUN de forma efectiva

Hay herramientas disponibles para ayudarle a supervisar de forma efectiva las LUN y evitar quedarse sin espacio.

- Active IQ Unified Manager es una herramienta gratuita que le permite gestionar todo el almacenamiento en todos los clústeres del entorno.
- System Manager es una interfaz gráfica de usuario integrada en ONTAP que le permite gestionar manualmente las necesidades de almacenamiento en el nivel del clúster.
- OnCommand Insight presenta una única vista de la infraestructura de almacenamiento y le permite

configurar la supervisión automática, alertas e informes cuando sus LUN, volúmenes y agregados se están quedando sin espacio de almacenamiento.

Funcionalidades y restricciones de los LUN convertidos

En un entorno SAN, es necesario interrumpir el servicio durante la transición de un volumen de 7-Mode a ONTAP. Debe apagar los hosts para completar la transición. Después de la transición, debe actualizar las configuraciones de host para poder empezar a servir datos en ONTAP

Debe programar una ventana de mantenimiento durante la cual puede apagar los hosts y completar la transición.

Las LUN que se han realizado la transición de Data ONTAP en 7-Mode a ONTAP tienen ciertas funcionalidades y restricciones que afectan a la forma en que se pueden gestionar las LUN.

Puede hacer lo siguiente con las LUN convertidas:

- Vea la LUN mediante `lun show` comando
- Vea el inventario de LUN convertidos desde el volumen de 7-Mode con el `transition 7-mode show` comando
- Restaure un volumen a partir de una copia de Snapshot de 7-Mode

Al restaurar el volumen, se realiza la transición de todas las LUN capturadas en la copia Snapshot

- Restaure un único LUN de una copia Snapshot de 7-Mode mediante la `snapshot restore-file` comando
- Crear un clon de una LUN en una copia Snapshot de 7-Mode
- Restaure un rango de bloques a partir de una LUN capturada en una copia Snapshot de 7-Mode
- Cree un FlexClone del volumen mediante una copia snapshot de 7-Mode

No se puede hacer lo siguiente con las LUN convertidas:

- Acceda a los clones de LUN respaldados por copias de Snapshot capturados en el volumen

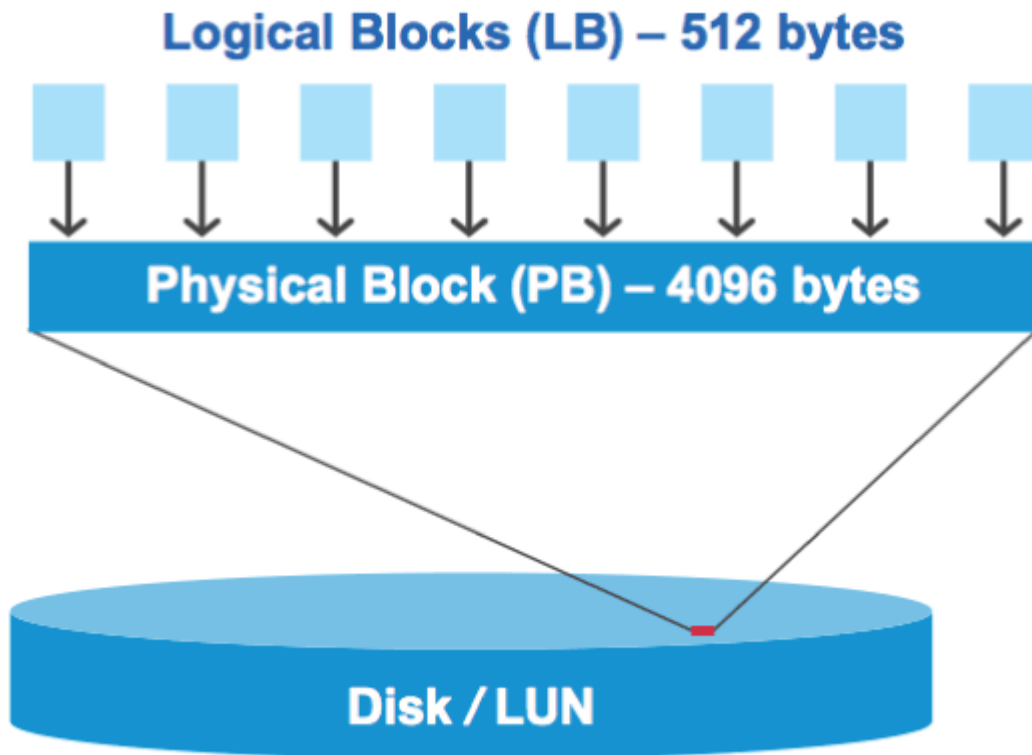
Información relacionada

["Transición basada en copias"](#)

Alineación incorrecta de I/O en la descripción general de las LUN alineadas correctamente

ONTAP podría informar de desalineación de I/O en LUN alineadas correctamente. En general, estas advertencias de mala alineación pueden ignorarse mientras tenga la confianza de que su LUN está correctamente aprovisionada y que la tabla de particiones es correcta.

Los LUN y los discos duros proporcionan almacenamiento como bloques. Como el tamaño de bloque de los discos del host es de 512 bytes, los LUN presentan bloques de ese tamaño al host a la vez que utilizan bloques de más grandes de 4 KB para almacenar datos. El bloque de datos de 512 bytes que usa el host se conoce como un bloque lógico. El bloque de datos de 4 KB que utiliza la LUN para almacenar datos se conoce como un bloque físico. Esto significa que hay ocho bloques lógicos de 512 bytes en cada bloque físico de 4



El sistema operativo host puede iniciar una operación de I/o de lectura o escritura en cualquier bloque lógico. Las operaciones de I/o solo se consideran alineadas cuando comienzan en el primer bloque lógico del bloque físico. Si una operación de I/o se inicia en un bloque lógico que no es también el inicio de un bloque físico, la I/o se considera mal alineada. ONTAP detecta automáticamente los errores de alineación y los informa en la LUN. Sin embargo, la presencia de I/o mal alineadas no significa necesariamente que la unidad lógica tampoco esté alineada. Es posible que se notifique una I/o mal alineada en las LUN alineadas correctamente.

Si necesita más investigación, consulte el artículo de la base de conocimientos ["¿Cómo identificar las I/o no alineadas en las LUN?"](#)

Para obtener más información sobre las herramientas para corregir problemas de alineación, consulte la siguiente documentación: +

- ["Utilidades unificadas de host de Windows 7.1"](#)
- ["Guía de instalación y administración de Virtual Storage Console para VMware vSphere"](#)

Alinear las operaciones de I/o con los tipos de SO de LUN

Para ONTAP 9,7 o anterior, debe usar la LUN de ONTAP recomendada `ostype` Valor que mejor se adapta a su sistema operativo para lograr una alineación de E/S con el esquema de particiones de SO.

El esquema de partición empleado por el sistema operativo host es un factor importante que contribuye a los desalineamientos de E/S. Algunas LUN de ONTAP `ostype` los valores utilizan un desplazamiento especial denominado «'prefix'» para habilitar la alineación del esquema de partición predeterminado utilizado por el sistema operativo host.



En algunas circunstancias, puede que se requiera una tabla de particiones personalizadas para lograr la alineación de las operaciones de I/O. Sin embargo, para `ostype` valores con un valor de «'prefijo'» mayor que 0, Es posible que una partición personalizada cree E/S mal alineadas

Para obtener más información acerca de las LUN aprovisionadas en ONTAP 9,7 o versiones anteriores, consulte el artículo de la base de conocimientos ["Cómo identificar las I/O no alineadas en las LUN"](#).



De forma predeterminada, las nuevas LUN que se aprovisionan en ONTAP 9,8 o una versión posterior tienen un tamaño de prefijo y sufijo de cero para todos los tipos de sistema operativo de LUN. De forma predeterminada, las I/O deben alinearse con el SO del host compatible.

Consideraciones especiales sobre la alineación de E/S para Linux

Las distribuciones de Linux ofrecen una amplia variedad de formas de usar un LUN, como dispositivos sin formato para bases de datos, varios administradores de volúmenes y sistemas de archivos. No es necesario crear particiones en un LUN cuando se usa como dispositivo sin configurar o como volumen físico en un volumen lógico.

Para RHEL 5 y versiones anteriores y SLES 10 y anteriores, si la LUN se utilizará sin un administrador de volúmenes, debe realizar particiones en la LUN para tener una partición que comienza en un desplazamiento alineado, que es un sector que es un múltiplo de ocho bloques lógicos.

Consideraciones especiales sobre la alineación de I/O para las LUN de Solaris

Es necesario tener en cuenta varios factores a la hora de determinar si se debe usar el `solaris ostype` o la `solaris_efi ostype`.

Consulte ["Guía de instalación y administración de Solaris Host Utilities"](#) para obtener información detallada.

Los LUN de arranque de ESX no están alineados

ONTAP suele informar de las LUN utilizadas como LUN de arranque de ESX como mal alineadas. ESX crea varias particiones en el LUN de arranque, por lo que es muy difícil realizar una alineación. Las LUN de arranque de ESX mal alineadas no suelen ser un problema de rendimiento, ya que la cantidad total de I/O mal alineadas es pequeña. Suponiendo que la LUN se provisionara correctamente con VMware `ostype`, no se necesita ninguna acción.

Información relacionada

["Alineación de disco/partición del sistema de archivos de máquina virtual invitada para VMware vSphere, otros entornos virtuales y los sistemas de almacenamiento de NetApp"](#)

Formas de abordar problemas cuando las LUN se desconectan

Cuando no hay espacio disponible para las escrituras, las LUN se desconectan para conservar la integridad de los datos. Las LUN pueden quedarse sin espacio y desconectarse por varios motivos, y hay varias formas de abordar el problema.

| Si... | Le permite... |
|--|---|
| El agregado está lleno | <ul style="list-style-type: none"> • Añada más discos. • Utilice la <code>volume modify</code> comando para reducir un volumen que tiene espacio disponible. • Si tiene volúmenes con garantía de espacio que tienen espacio disponible, cambie la garantía de espacio de volumen a <code>none</code> con la <code>volume modify</code> comando. |
| El volumen está lleno, pero hay espacio disponible en el agregado que contiene | <ul style="list-style-type: none"> • Para los volúmenes de garantía de espacio, utilice <code>volume modify</code> comando para aumentar el tamaño del volumen. • Para volúmenes con Thin Provisioning, utilice <code>volume modify</code> comando para aumentar el tamaño máximo del volumen. <p>Si no se habilita el crecimiento automático de un volumen, se debe usar <code>volume modify -autogrow-mode</code> para habilitar la función.</p> <ul style="list-style-type: none"> • Elimine copias Snapshot manualmente con el <code>volume snapshot delete</code> o utilice el <code>volume snapshot autodelete modify</code> Comando para eliminar automáticamente copias Snapshot. |

Información relacionada

["Gestión de discos y niveles locales \(agregado\)"](#)

["Gestión de almacenamiento lógico"](#)

Solucione problemas de LUN iSCSI que no están visibles en el host

Los LUN de iSCSI aparecen como discos locales para el host. Si los LUN del sistema de almacenamiento no están disponibles como discos en el host, debe comprobar los ajustes de configuración.

| Ajuste de configuración | Qué hacer |
|-------------------------|---|
| Cableado | Compruebe que los cables entre el host y el sistema de almacenamiento estén conectados correctamente. |

| Ajuste de configuración | Qué hacer |
|--------------------------------|---|
| Conectividad de la red | <p>Compruebe que hay conectividad TCP/IP entre el host y el sistema de almacenamiento.</p> <ul style="list-style-type: none"> Desde la línea de comandos del sistema de almacenamiento, haga ping a las interfaces del host que se utilizan para iSCSI: <pre>ping -node node_name -destination host_ip_address_for_iSCSI</pre> <ul style="list-style-type: none"> En la línea de comandos del host, realice una ping en las interfaces del sistema de almacenamiento que se utilizan para iSCSI: <pre>ping -node node_name -destination host_ip_address_for_iSCSI</pre> |
| Requisitos del sistema | <p>Compruebe que los componentes de su configuración están cualificados. Además, compruebe que tiene el nivel correcto de paquete de servicio, la versión del iniciador, la versión de ONTAP y otros requisitos del sistema operativo host. La matriz de interoperabilidad contiene los requisitos del sistema más actualizados.</p> |
| Tramas gigantes | <p>Si utiliza tramas gigantes en la configuración, compruebe que se hayan habilitado tramas gigantes en todos los dispositivos de la ruta de red: La NIC Ethernet del host, el sistema de almacenamiento y todos los switches.</p> |
| Estado del servicio iSCSI | <p>Compruebe que el servicio iSCSI tiene licencia y se ha iniciado en el sistema de almacenamiento.</p> |
| Inicio de sesión del iniciador | <p>Compruebe que el iniciador ha iniciado sesión en el sistema de almacenamiento. Si la <code>iscsi initiator show</code> el resultado del comando no muestra ningún iniciador con sesión iniciada. compruebe la configuración del iniciador en el host. Compruebe también que el sistema de almacenamiento está configurado como destino del iniciador.</p> |
| Nombres de nodos iSCSI (IQN) | <p>Compruebe que está usando los nombres de nodo iniciador correctos en la configuración de igroup. En el host, puede usar las herramientas y los comandos del iniciador para mostrar el nombre del nodo iniciador. Los nombres de los nodos del iniciador configurados en el igroup y el host deben coincidir.</p> |
| Asignaciones de LUN | <p>Compruebe que las LUN se han asignado a un igroup. En la consola del sistema de almacenamiento, puede usar uno de los siguientes comandos:</p> <ul style="list-style-type: none"> <code>lun mapping show</code> Muestra todas las LUN y los iGroups a los que se les han asignado. <code>lun mapping show -igroup</code> Muestra las LUN asignadas a un igroup específico. |

| Ajuste de configuración | Qué hacer |
|-------------------------|---|
| Los LIF iSCSI permiten | Compruebe que las interfaces lógicas iSCSI están habilitadas. |

Información relacionada

["Herramienta de matriz de interoperabilidad de NetApp"](#)

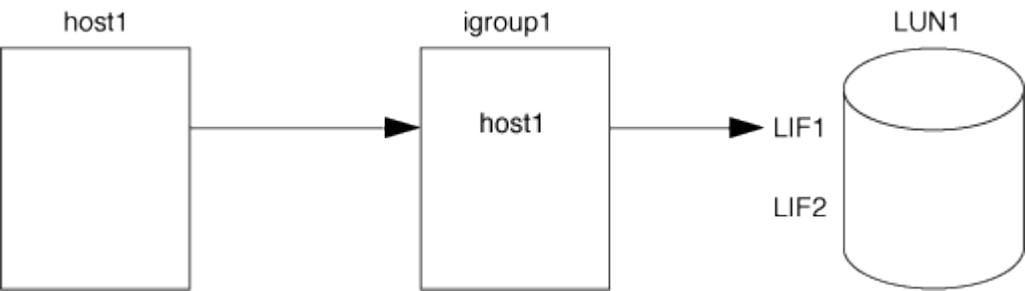
Gestione iGroups y conjuntos de puertos

Formas de limitar el acceso LUN con conjuntos de puertos e iGroups

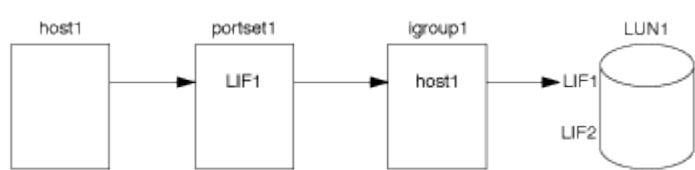
Además de utilizar la asignación de LUN selectiva (SLM), puede limitar el acceso a sus LUN a través de iGroups y conjuntos de puertos.

Los conjuntos de puertos se pueden utilizar con SLM para restringir aún más el acceso de ciertos destinos a ciertos iniciadores. Cuando se utiliza SLM con conjuntos de puertos, se podrá acceder a los LUN en el conjunto de puertos del nodo que posee la LUN y en el partner de alta disponibilidad de ese nodo.

En el ejemplo siguiente, initiator1 no tiene un conjunto de puertos. Sin un conjunto de puertos, initiator1 puede acceder a LUN1 a través de LIF1 y LIF2.



Puede limitar el acceso a LUN1 mediante un conjunto de puertos. En el ejemplo siguiente, initiator1 sólo puede acceder a LUN1 a través de LIF1. Sin embargo, initiator1 no puede acceder a LUN1 a través de LIF2 porque LIF2 no está en portset1.



Información relacionada

- [Asignación de LUN selectiva](#)
- [Cree un conjunto de puertos y enlace a un igroup](#)

Consulte y gestione iniciadores E iGroups SAN

Es posible usar System Manager para ver y gestionar los iGroups y los iniciadores.

Acerca de esta tarea

- Los iGroups identifican qué hosts pueden acceder a LUN específicas del sistema de almacenamiento.
- Después de crear un iniciador e iGroups, también puede editarlos o eliminarlos.

- Para gestionar los iniciadores y los grupos de iniciadores SAN, puede realizar las tareas siguientes:
 - [\[view-manage-san-igroups\]](#)
 - [\[view-manage-san-inits\]](#)

Consulte y gestione los iGroups SAN

Puede usar System Manager para ver una lista de iGroups. En la lista, es posible ejecutar operaciones adicionales.

Pasos

1. En el Administrador del sistema, haga clic en **hosts > grupos de iniciadores DE SAN**.


La página muestra una lista de iGroups. Si la lista es grande, puede ver páginas adicionales de la lista haciendo clic en los números de página en la esquina inferior derecha de la página.

Las columnas muestran información diversa sobre los iGroups. A partir de 9.11.1, también se muestra el estado de conexión del igroup. Pase el ratón sobre las alertas de estado para ver detalles.

2. (Opcional): Puede realizar las siguientes tareas haciendo clic en los iconos de la esquina superior derecha de la lista:
 - **Buscar**
 - **Descargar** la lista.
 - **Mostrar o Ocultar** columnas en la lista.
 - **Filtrar** los datos de la lista.

3. Es posible realizar operaciones de la lista:
 - Haga clic en  **Add** para añadir un igroup.
 - Haga clic en el nombre del igroup para ver la página **Overview** que muestra detalles sobre el igroup.

En la página **Overview**, puede ver las LUN asociadas con el igroup, y puede iniciar las operaciones para crear las LUN y asignarlas. Haga clic en **All SAN Initiators** para volver a la lista principal.

- Pase el ratón sobre el igroup y, a continuación, haga clic en  junto al nombre de un igroup para editar o eliminar el igroup.
- Pase el ratón sobre el área que se encuentra a la izquierda del nombre del igroup y, a continuación, active la casilla de comprobación. Si hace clic en **+Agregar al iGroup**, puede añadir ese igroup a otro igroup.
- En la columna **Storage VM**, haga clic en el nombre de una VM de almacenamiento para ver detalles sobre ella.

Consulte y gestione iniciadores DE SAN

Puede usar System Manager para ver una lista de iniciadores. En la lista, es posible ejecutar operaciones adicionales.

Pasos

1. En el Administrador del sistema, haga clic en **hosts > grupos de iniciadores DE SAN**.

La página muestra una lista de iGroups.

2. Para ver los iniciadores, realice lo siguiente:

- Haga clic en la ficha **iniciadores FC** para ver una lista de iniciadores FC.
- Haga clic en la ficha **iSCSI Initiators** para ver una lista de iniciadores iSCSI.

Las columnas muestran diversa información sobre los iniciadores.

A partir de 9.11.1, se muestra también el estado de conexión del iniciador. Pase el ratón sobre las alertas de estado para ver detalles.

3. (Opcional): Puede realizar las siguientes tareas haciendo clic en los iconos de la esquina superior derecha de la lista:

- **Buscar** la lista de iniciadores en particular.
- **Descargar** la lista.
- **Mostrar** o **Ocultar** columnas en la lista.
- **Filtrar** los datos de la lista.

Cree un igroup anidado

A partir de ONTAP 9.9.1, es posible crear un igroup que esté compuesto por otros iGroups existentes.

1. En el Administrador del sistema, haga clic en **Host > grupos de iniciadores SAN** y, a continuación, haga clic en **Agregar**.
2. Introduzca el igroup **Nombre** y **Descripción**.

La descripción sirve como alias del igroup.

3. Seleccione **Storage VM** y **Host System**.



El tipo de sistema operativo de un igroup anidado no se puede cambiar una vez que se crea el igroup.

4. En **Miembros del iGroup** seleccione **Grupo iniciador existente**.

Puede utilizar **Buscar** para buscar y seleccionar los iGroups que desea agregar.

Asigne iGroups a varias LUN

A partir de ONTAP 9.9.1, puede asignar iGroups a dos o más LUN simultáneamente.

1. En System Manager, haga clic en **almacenamiento > LUN**.
2. Seleccione las LUN que desea asignar.
3. Haga clic en **más** y, a continuación, haga clic en **asignar a iGroups**.



Los iGroups seleccionados se agregan a las LUN seleccionadas. Las asignaciones preexistentes no se sobrescriben.

Cree un conjunto de puertos y enlace a un igroup

Además de utilizar "[Asignación de LUN selectiva \(SLM\)](#)", Puede crear un conjunto de puertos y enlazar el conjunto de puertos a un igroup para limitar aún más qué LIF puede usar un iniciador para acceder a una LUN.

Si no se vincula un conjunto de puertos a un igroup, todos los iniciadores del igroup pueden acceder a las LUN asignadas a través de todas las LIF del nodo al que pertenece la LUN y al partner de alta disponibilidad del nodo propietario.

Lo que necesitará

Debe tener al menos un LIF y un igroup.

A menos que utilice grupos de interfaces, se recomiendan dos LIF para redundancia tanto de iSCSI como de FC. Solo se recomienda un LIF para los grupos de interfaces.

Acerca de esta tarea

Es ventajoso utilizar conjuntos de puertos con SLM cuando tiene más de dos LIF en un nodo y desea restringir un iniciador determinado a un subconjunto de LIF. Sin conjuntos de puertos, todos los destinos del nodo podrán acceder a ellos con acceso a la LUN a través del nodo al que pertenece la LUN y del partner de alta disponibilidad del nodo propietario.

Ejemplo 11. Pasos

System Manager

A partir de ONTAP 9.10.1, es posible usar System Manager para crear conjuntos de puertos y vincularlos a iGroups.

Si necesita crear un conjunto de puertos y vincularlo a un igroup en una versión de ONTAP anterior a 9.10.1, debe usar el procedimiento de la CLI de ONTAP.

1. En System Manager, haga clic en **Red > Descripción general > Portsets** y, a continuación, en **Agregar**.
2. Introduzca la información del nuevo conjunto de puertos y haga clic en **Agregar**.
3. Haga clic en **hosts > grupos de iniciadores SAN**.
4. Para enlazar el conjunto de puertos con un nuevo igroup, haga clic en **Add**.

Para enlazar el conjunto de puertos a un igroup existente, seleccione el igroup, haga clic en **Y**, a continuación, haga clic en **Editar iGroup**.

Información relacionada

["Consulte y gestione los iniciadores y los iGroups"](#)

CLI

1. Cree un conjunto de puertos que contenga las LIF correspondientes:

```
portset create -vserver vsample_name -portset portset_name -protocol
protocol -port-name port_name
```

Si usa FC, especifique el `protocol` parámetro como `fc`. Si utiliza iSCSI, especifique el `protocol` parámetro como `iscsi`.

2. Enlace el igroup al conjunto de puertos:

```
lun igroup bind -vserver vsample_name -igroup igroup_name -portset
portset_name
```

3. Compruebe que sus conjuntos de puertos y LIF son correctos:

```
portset show -vserver vsample_name
```

| Vserver | Portset | Protocol | Port Names | Igroups |
|---------|----------|----------|------------|---------|
| vs3 | portset0 | iscsi | lif0,lif1 | igroup1 |

Gestionar conjuntos de puertos


Además de ["Asignación de LUN selectiva \(SLM\)"](#), Puede utilizar conjuntos de puertos para limitar aún más qué LIF puede utilizar un iniciador para acceder a una LUN.

A partir de ONTAP 9.10.1, es posible usar System Manager para cambiar las interfaces de red asociadas con los conjuntos de puertos y eliminar los conjuntos de puertos.

Cambiar las interfaces de red asociadas a un conjunto de puertos

1. En System Manager, seleccione **Network > Overview > Portsets**.
2. Seleccione el conjunto de puertos que desea editar luego , Luego seleccione **Editar Portset**.

Eliminar un conjunto de puertos

1. En System Manager, haga clic en **Red > Descripción general > Portsets**.
2. Para eliminar un solo conjunto de puertos, seleccione el conjunto de puertos y, a continuación, seleccione  Y, a continuación, seleccione **Eliminar conjuntos de puertos**.

Para eliminar varios conjuntos de puertos, seleccione los conjuntos de puertos y haga clic en **Eliminar**.

Información general sobre asignación de LUN selectiva

La asignación selectiva de LUN (SLM) reduce el número de rutas desde el host hacia el LUN. Con SLM, cuando se crea una nueva asignación de LUN, el LUN solo se puede acceder a través de las rutas del nodo al que pertenece la LUN y su partner de alta disponibilidad.

SLM permite gestionar un solo igroup por host y también admite operaciones de movimiento de LUN no disruptivas que no requieren manipulación del conjunto de puertos o reasignación de LUN.

"Conjuntos de puertos" Se puede utilizar con SLM para restringir aún más el acceso de determinados destinos a determinados iniciadores. Cuando se utiliza SLM con conjuntos de puertos, se podrá acceder a los LUN en el conjunto de puertos del nodo que posee la LUN y en el partner de alta disponibilidad de ese nodo.

SLM está habilitado de forma predeterminada en todos los mapas de LUN nuevos.

Determinar si SLM está habilitado en una asignación de LUN

Si su entorno tiene una combinación de LUN creadas en una versión de ONTAP 9 y LUN que han realizado la transición desde versiones anteriores, puede que deba determinar si la asignación de LUN selectiva (SLM) está habilitada en una LUN concreta.

Puede utilizar la información que se muestra en el resultado del `lun mapping show -fields reporting-nodes, node` Comando para determinar si SLM está habilitado en la asignación de LUN. Si SLM no está habilitado, se muestra "-" en las celdas bajo la columna "nodos de portabilidad" de la salida del comando. Si SLM está habilitado, la lista de nodos que se muestran bajo la columna "nodos" se duplica en la columna "nodos de portabilidad".

Modifique la lista nodos de informes de SLM

Si mueve un LUN o un volumen que contiene LUN a otra pareja de alta disponibilidad (ha) dentro del mismo clúster, debe modificar la lista de nodos de generación de informes de asignación de LUN selectiva (SLM) antes de iniciar el movimiento para garantizar que se mantengan las rutas de LUN activas y optimizadas.

Pasos

1. Añada el nodo de destino y su nodo asociado a la lista Reporting-Nodes del volumen o del agregado:

```
lun mapping add-reporting-nodes -vserver _vserver_name_ -path _lun_path_  
-igroup _igroup_name_ [-destination-aggregate _aggregate_name_|-  
destination-volume _volume_name_]
```

Si tiene una convención de nomenclatura coherente, puede modificar varias asignaciones de LUN al mismo tiempo mediante *igroup_prefix** en lugar de *igroup_name*.

2. Vuelva a analizar el host para detectar las rutas recién añadidas.
3. Si el sistema operativo lo requiere, añada las rutas nuevas a la configuración de I/O de red multivía (MPIO).
4. Ejecute el comando para la operación de movimiento necesaria y espere a que finalice la operación.
5. Compruebe que se está prestando servicio a E/S a través de la ruta activa/optimizada:

```
lun mapping show -fields reporting-nodes
```

6. Elimine el propietario anterior de la LUN y su nodo asociado de la lista de nodos de generación de informes:

```
lun mapping remove-reporting-nodes -vserver _vserver_name_ -path  
_lun_path_ -igroup _igroup_name_ -remote-nodes
```

7. Compruebe que la LUN se ha eliminado del mapa de LUN existente:

```
lun mapping show -fields reporting-nodes
```

8. Elimine las entradas obsoletas del dispositivo para el sistema operativo host.
9. Si es necesario, cambie los archivos de configuración de accesos múltiples.
10. Vuelva a analizar el host para verificar la eliminación de las rutas antiguas.
Consulte la documentación del host para ver los pasos específicos para volver a analizar los hosts.

Gestionar el protocolo iSCSI

Configure su red para obtener el mejor rendimiento

Las redes Ethernet varían en gran medida en cuanto al rendimiento. Se puede maximizar el rendimiento de la red utilizada para iSCSI mediante la selección de valores de configuración específicos.

Pasos

1. Conecte los puertos de host y de almacenamiento a la misma red.

Se recomienda conectarse a los mismos conmutadores. No se debe usar el enrutamiento.

2. Seleccione los puertos de mayor velocidad disponibles y dedícalos a iSCSI.

Los puertos de 10 GbE son los mejores. Los puertos de 1 GbE son el mínimo.

3. Desactive el control de flujo Ethernet para todos los puertos.

Debería ver "[Gestión de redes](#)" Para utilizar la CLI para configurar el control de flujo del puerto Ethernet.

4. Habilitar tramas gigantes (normalmente MTU de 9000).

Todos los dispositivos de la ruta de datos, incluidos los iniciadores, los destinos y los switches, deben admitir tramas gigantes. De lo contrario, al habilitar tramas gigantes se reduce realmente el rendimiento de red considerablemente.

Configure una SVM para iSCSI

Para configurar una máquina virtual de almacenamiento (SVM) para iSCSI, debe crear LIF para la SVM y asignar el protocolo iSCSI a esas LIF.


Acerca de esta tarea

Necesita un mínimo de un LIF iSCSI por nodo para cada SVM que sirva datos con el protocolo iSCSI. Para redundancia, debe crear al menos dos LIF por nodo.

Ejemplo 12. Pasos

System Manager

Configuración de una máquina virtual de almacenamiento para iSCSI con ONTAP System Manager (9.7 y posterior).

| Para configurar iSCSI en un nuevo equipo virtual de almacenamiento | Para configurar iSCSI en un equipo virtual de almacenamiento existente |
|---|--|
| <ol style="list-style-type: none">1. En System Manager, haga clic en almacenamiento > Storage VMs y, a continuación, haga clic en Agregar.2. Escriba un nombre para la máquina virtual de almacenamiento.3. Seleccione iSCSI para el Protocolo de acceso.4. Haga clic en Activar iSCSI e introduzca la dirección IP y la máscara de subred de la interfaz de red. + cada nodo debe tener al menos dos interfaces de red.5. Haga clic en Guardar. | <ol style="list-style-type: none">1. En System Manager, haga clic en almacenamiento > Storage VMs.2. Haga clic en la máquina virtual de almacenamiento que desee configurar.3. Haga clic en la ficha Configuración y, a continuación, haga clic en  Junto al protocolo iSCSI.4. Haga clic en Activar iSCSI e introduzca la dirección IP y la máscara de subred de la interfaz de red. + cada nodo debe tener al menos dos interfaces de red.5. Haga clic en Guardar. |

CLI

Configuración de una máquina virtual de almacenamiento para iSCSI con la interfaz de línea de comandos de ONTAP.

1. Habilite las SVM para que escuche el tráfico de iSCSI:

```
vserver iscsi create -vserver vserver_name -target-alias vserver_name
```

2. Cree una LIF para las SVM de cada nodo que utilice para iSCSI:

- Para ONTAP 9,6 y versiones posteriores:

```
network interface create -vserver vserver_name -lif lif_name -data  
-protocol iscsi -service-policy default-data-iscsi -home-node node_name  
-home-port port_name -address ip_address -netmask netmask
```

- Para ONTAP 9,5 y versiones anteriores:

```
network interface create -vserver vserver_name -lif lif_name -role data  
-data-protocol iscsi -home-node node_name -home-port port_name -address  
ip_address -netmask netmask
```

3. Compruebe que ha configurado las LIF correctamente:

```
network interface show -vserver vserver_name
```

4. Compruebe que iSCSI esté en funcionamiento y que el IQN objetivo para esa SVM:

```
vserver iscsi show -vserver vserver_name
```

5. Desde el host, cree sesiones iSCSI con sus LIF.

Información relacionada

["Informe técnico de NetApp 4080: Prácticas recomendadas para SAN moderno"](#)

Definir un método de política de seguridad para un iniciador

Puede definir una lista de iniciadores y sus métodos de autenticación. También puede modificar el método de autenticación predeterminado que se aplica a los iniciadores que no tienen un método de autenticación definido por el usuario.

Acerca de esta tarea

Puede generar contraseñas únicas utilizando algoritmos de directivas de seguridad en el producto o especificar manualmente las contraseñas que desea utilizar.



No todos los iniciadores admiten contraseñas secretas CHAP hexadecimales.

Pasos

1. Utilice la `vserver iscsi security create` comando para crear un método de política de seguridad para un iniciador.

```
vserver iscsi security create -vserver vs2 -initiator ign.1991-05.com.microsoft:host1 -auth-type CHAP -user-name bob1 -outbound-user-name bob2
```

2. Siga los comandos de la pantalla para añadir las contraseñas.

Crea un método de directiva de seguridad para el iniciador `ign.1991-05.com.microsoft:host1` con nombres de usuario y contraseñas CHAP entrantes y salientes.

Información relacionada

- [Cómo funciona la autenticación iSCSI](#)
- [Autenticación CHAP](#)

Eliminar un servicio iSCSI para una SVM

Es posible eliminar un servicio iSCSI para una SVM si ya no se necesita.

Lo que necesitará

El estado de administración del servicio iSCSI debe estar en el estado «inactivo» antes de poder eliminar un servicio iSCSI. Puede mover el estado de administración a hacia abajo con `vserver iscsi modify` comando.

Pasos

1. Utilice la `vserver iscsi modify` Comando para detener la actividad de I/O de la LUN.

```
vserver iscsi modify -vserver vs1 -status-admin down
```

2. Utilice la `vserver iscsi delete` Comando para quitar el servicio iscsi de la SVM.

```
vserver iscsi delete -vserver vs_1
```

3. Utilice la `vserver iscsi show command` Para verificar si ha eliminado el servicio iSCSI de la SVM.

```
vserver iscsi show -vserver vs1
```

Obtenga más detalles en las recuperaciones de errores de sesión iSCSI

Al aumentar el nivel de recuperación de errores de la sesión iSCSI, es posible recibir información más detallada sobre las recuperaciones de errores de iSCSI. El uso de un nivel de recuperación de errores más alto puede provocar una reducción menor en el rendimiento de la sesión iSCSI.

Acerca de esta tarea

De manera predeterminada, ONTAP se configura para utilizar el nivel de recuperación de errores 0 para sesiones iSCSI. Si está usando un iniciador cualificado para el nivel de recuperación de errores 1 o 2, puede optar por aumentar el nivel de recuperación de errores. El nivel de recuperación de error de sesión modificado afecta solo a las sesiones recién creadas y no afecta a las sesiones existentes.

A partir de ONTAP 9,4, el `max-error-recovery-level` la opción no es compatible con `iscsi show y.. iscsi modify` comandos.

Pasos

1. Entrar al modo avanzado:

```
set -privilege advanced
```

2. Compruebe la configuración actual mediante la `iscsi show` comando.

```
iscsi show -vserver vs3 -fields max-error-recovery-level
```

```
vserver max-error-recovery-level
-----
vs3      0
```

3. Cambie el nivel de recuperación de error mediante el `iscsi modify` comando.

```
iscsi modify -vserver vs3 -max-error-recovery-level 2
```

Registre la SVM en un servidor iSNS

Puede utilizar el `vserver iscsi isns` Comando para configurar la máquina virtual de almacenamiento (SVM) para registrarse en un servidor iSNS.

Acerca de esta tarea

La `vserver iscsi isns create` El comando configura la SVM para registrarse en el servidor iSNS. La

SVM no proporciona comandos que permitan configurar o gestionar el servidor iSNS. Para gestionar el servidor iSNS, puede usar las herramientas de administración del servidor o la interfaz que proporcione el proveedor para el servidor iSNS.

Pasos

1. En el servidor iSNS, asegúrese de que el servicio iSNS esté activo y disponible para su servicio.
2. Cree la LIF de gestión de SVM en un puerto de datos:

```
network interface create -vserver SVM_name -lif lif_name -role data -data  
-protocol none -home-node home_node_name -home-port home_port -address  
IP_address -netmask network_mask
```

3. Cree un servicio iSCSI en la SVM si todavía no existe ninguno:

```
vserver iscsi create -vserver SVM_name
```

4. Compruebe que el servicio iSCSI se ha creado correctamente:

```
iscsi show -vserver SVM_name
```

5. Compruebe que existe una ruta predeterminada para la SVM:

```
network route show -vserver SVM_name
```

6. Si no hay ninguna ruta predeterminada para la SVM, cree una ruta predeterminada:

```
network route create -vserver SVM_name -destination destination -gateway  
gateway
```

7. Configure la SVM para registrarse con el servicio iSNS:

```
vserver iscsi isns create -vserver SVM_name -address IP_address
```

Se admiten las familias de direcciones IPv4 e IPv6. La familia de direcciones del servidor iSNS debe ser la misma que la de la LIF de gestión de SVM.

Por ejemplo, no puede conectar una LIF de gestión anSVM con una dirección IPv4 a un servidor iSNS con una dirección IPv6.

8. Compruebe que el servicio iSNS esté en ejecución:

```
vserver iscsi isns show -vserver SVM_name
```

9. Si el servicio iSNS no está en ejecución, inícielo:

```
vserver iscsi isns start -vserver SVM_name
```

Resuelva los mensajes de error de iSCSI en el sistema de almacenamiento

Hay varios mensajes de error comunes relacionados con iSCSI que se pueden ver con el `event log show` comando. Debe saber qué significan estos mensajes y qué puede hacer para resolver los problemas que identifican.

La siguiente tabla contiene los mensajes de error más comunes e instrucciones para resolverlos:

| Mensaje | Explicación | Qué hacer |
|---|--|---|
| ISCSI: network interface identifier disabled for use; incoming connection discarded | El servicio iSCSI no está habilitado en la interfaz. | Puede utilizar el <code>iscsi interface enable</code> Comando para habilitar el servicio iSCSI en la interfaz. Por ejemplo: <code>iscsi interface enable -vserver vs1 -lif lif1</code> |
| ISCSI: Authentication failed for initiator nodename | CHAP no está configurado correctamente para el iniciador especificado. | Debe comprobar la configuración de CHAP; no puede usar el mismo nombre de usuario y contraseña para la configuración de entrada y salida en el sistema de almacenamiento: <ul style="list-style-type: none"> • Las credenciales entrantes en el sistema de almacenamiento deben coincidir con las credenciales salientes en el iniciador. • Las credenciales salientes en el sistema de almacenamiento deben coincidir con las credenciales entrantes del iniciador. |

Habilitar o deshabilitar la recuperación tras fallos automática de LIF de iSCSI

Después de actualizar a ONTAP 9.11.1 o una versión posterior, debe habilitar manualmente la conmutación por error automática de LIF en todas las LIF de iSCSI creadas en ONTAP 9.10.1 o una versión anterior.

A partir de ONTAP 9.11.1, puede habilitar la recuperación automática tras fallos de LIF para LIF iSCSI en plataformas de cabinas SAN all-flash. Si se produce una recuperación tras fallos de almacenamiento, el LIF de iSCSI se migra automáticamente desde su nodo o puerto principal a su puerto o nodo de alta disponibilidad asociado y, a continuación, una vez finalizada la recuperación tras fallos. O bien, si el puerto para LIF iSCSI deja de estar en buen estado, la LIF se migra automáticamente a un puerto en buen estado de su nodo inicial actual y de nuevo a su puerto original cuando el estado del puerto vuelve a estar en buen estado. El habilita las cargas de trabajo SAN que se ejecutan en iSCSI para reanudar el servicio de I/O más rápido después de que se experimenta una conmutación al nodo de respaldo.

En ONTAP 9.11.1 y versiones posteriores, de forma predeterminada, los LIF iSCSI recién creados se habilitan para la conmutación automática por error de LIF si se cumple alguna de las siguientes condiciones:

- No hay ningún LIF de iSCSI en la SVM
- Todos los LIF de iSCSI en la SVM están habilitados para la conmutación al respaldo automática de LIF

Activar recuperación tras fallos automática de LIF iSCSI

De manera predeterminada, las LIF de iSCSI creadas en ONTAP 9.10.1 y versiones anteriores no están habilitadas para la conmutación automática por error de LIF. Si hay LIF de iSCSI en la SVM que no están habilitados para la conmutación automática al respaldo de LIF, los LIF creados recientemente no se habilitarán para la conmutación automática por error de LIF. Si la recuperación tras fallos automática de LIF no está habilitada y existe un evento de recuperación tras fallos, los LIF de iSCSI no migrarán.

Más información acerca de ["Recuperación tras fallos y restauración de LIF"](#).

Paso

1. Habilitar la recuperación automática tras fallos en una LIF iSCSI:

```
network interface modify -vserver SVM_name -lif iscsi_lif -failover-policy sfo-partner-only -auto-revert true
```

Para actualizar todos los LIF iSCSI en la SVM, utilice `-lif*` en lugar de `lif`.

Desactive la recuperación tras fallos automática de LIF de iSCSI

Si anteriormente habilitó conmutación por error automática de LIF de iSCSI en LIF iSCSI creadas en ONTAP 9.10.1 o una versión anterior, tiene la opción de deshabilitarla.

Paso

1. Desactive la recuperación automática tras fallos para una LIF iSCSI:

```
network interface modify -vserver SVM_name -lif iscsi_lif -failover-policy disabled -auto-revert false
```

Para actualizar todos los LIF iSCSI en la SVM, utilice `-lif*` en lugar de `lif`.

Información relacionada

- ["Cree una LIF"](#)
- Manualmente ["Migre una LIF"](#)
- Manualmente ["Revierte una LIF a su puerto de inicio"](#)
- ["Configure los ajustes de recuperación tras fallos en un LIF"](#)

Gestione el protocolo FC

Configure una SVM para FC

Para configurar una máquina virtual de almacenamiento (SVM) para FC, debe crear LIF para la SVM y asignar el protocolo FC a esas LIF.

Antes de empezar

Debe tener una licencia de FC (["Incluido con ONTAP One"](#)) y debe estar activado. Si la licencia de FC no está habilitada, aparecen las LIF y SVM en línea pero el estado operativo es `down`. Para que los LIF y SVM estén

operativos, el servicio FC debe estar habilitado. Debe usar la división en zonas de iniciador único para todas las LIF FC de la SVM a fin de alojar los iniciadores.


Acerca de esta tarea

NetApp admite un mínimo de un LIF de FC por nodo para cada SVM que sirve datos con el protocolo FC. Debe usar dos LIF por nodo y dos estructuras, con un LIF por nodo conectado. De este modo se proporciona redundancia en la capa del nodo y en la estructura.

Ejemplo 13. Pasos

System Manager

Configuración de una máquina virtual de almacenamiento para iSCSI con ONTAP System Manager (9.7 y posterior).

| Para configurar FC en un nuevo equipo virtual de almacenamiento | Para configurar FC en una máquina virtual de almacenamiento existente |
|--|--|
| <ol style="list-style-type: none">1. En System Manager, haga clic en almacenamiento > Storage VMs y, a continuación, haga clic en Agregar.2. Escriba un nombre para la máquina virtual de almacenamiento.3. Seleccione FC para Protocolo de acceso.4. Haga clic en Habilitar FC. + los puertos FC se asignan automáticamente.5. Haga clic en Guardar. | <ol style="list-style-type: none">1. En System Manager, haga clic en almacenamiento > Storage VMs.2. Haga clic en la máquina virtual de almacenamiento que desee configurar.3. Haga clic en la ficha Configuración y, a continuación, haga clic en  Junto al protocolo FC.4. Haga clic en Activar FC e introduzca la dirección IP y la máscara de subred de la interfaz de red. + los puertos FC se asignan automáticamente.5. Haga clic en Guardar. |

CLI

1. Habilite el servicio FC en la SVM:

```
vserver fcp create -vserver vserver_name -status-admin up
```

2. Cree dos LIF para las SVM en cada nodo que sirva FC:

- Para ONTAP 9,6 y versiones posteriores:

```
network interface create -vserver vserver_name -lif lif_name -data  
-protocol fcp -service-policy default-data-fcp -home-node node_name  
-home-port port_name -address ip_address -netmask netmask -status-admin  
up
```

- Para ONTAP 9,5 y versiones anteriores:

```
network interface create -vserver vserver_name -lif lif_name -role data  
-data-protocol fcp -home-node node_name -home-port port
```

3. Compruebe que sus LIF se han creado y que su estado operativo es online:

```
network interface show -vserver vserver_name lif_name
```

Información relacionada

["Soporte de NetApp"](#)

["Herramienta de matriz de interoperabilidad de NetApp"](#)

Eliminar un servicio de FC para una SVM

Es posible eliminar un servicio de FC para una SVM si ya no se necesita.

Lo que necesitará

El estado de administración debe ser «inactivo» antes de poder eliminar un servicio FC para una SVM. Puede establecer el estado de administración en inactivo con cualquiera de los dos `vserver fcp modify` o el `vserver fcp stop` comando.

Pasos

- 1. Utilice la `vserver fcp stop` Comando para detener la actividad de I/o de la LUN.

```
vserver fcp stop -vserver vs_1
```

- 2. Utilice la `vserver fcp delete` Comando para quitar el servicio de la SVM.

```
vserver fcp delete -vserver vs_1
```

- 3. Utilice la `vserver fcp show` Para verificar si ha eliminado el servicio FC de la SVM:

```
vserver fcp show -vserver vs_1
```

Configuraciones de MTU recomendadas para tramas gigantes de FCoE

Para Fibre Channel sobre Ethernet (FCoE), las tramas gigantes para la porción del adaptador Ethernet de la CNA deben configurarse en 9000 MTU. Las tramas gigantes para la parte del adaptador FCoE de CNA se deben configurar en más de 1500 MTU. Solo configure las tramas gigantes si el iniciador, el destino y todos los switches intermedios admiten y están configurados para tramas gigantes.

Gestione el protocolo NVMe

Inicie el servicio NVMe para una SVM

Para poder utilizar el protocolo NVMe en la máquina virtual de almacenamiento (SVM), se debe iniciar el servicio NVMe en la SVM.

Antes de empezar

Debe permitirse NVMe como protocolo en el sistema.

Se admiten los siguientes protocolos NVMe:

| Protocolo | Comenzando con ... | Permitido por... |
|-----------|--------------------|------------------|
| TCP | ONTAP 9.10.1 | Predeterminado |
| FCP | ONTAP 9,4 | Predeterminado |

Pasos

1. Cambie la configuración del privilegio a avanzado:

```
set -privilege advanced
```

2. Compruebe que NVMe se permite como protocolo:

```
vserver nvme show
```

3. Cree el servicio de protocolo NVMe:

```
vserver nvme create
```

4. Inicie el servicio de protocolo NVMe en la SVM:

```
vserver nvme modify -status -admin up
```

Elimine el servicio NVMe de una SVM

Si es necesario, puede eliminar el servicio NVMe de su máquina virtual de almacenamiento (SVM).

Pasos

1. Cambie la configuración del privilegio a avanzado:

```
set -privilege advanced
```

2. Detenga el servicio NVMe en la SVM:

```
vserver nvme modify -status -admin down
```

3. Elimine el servicio NVMe:


```
vserver nvme delete
```

Cambiar el tamaño de un espacio de nombres

A partir de ONTAP 9.10.1, se puede utilizar la interfaz de línea de comandos ONTAP para aumentar o reducir el tamaño de un espacio de nombres NVMe. Es posible usar System Manager para aumentar el tamaño de un espacio de nombres NVMe.

Aumentar el tamaño de un espacio de nombres

System Manager

1. Haga clic en **almacenamiento > espacios de nombres NVMe**.
2. Hoover el espacio de nombres que desea aumentar, haga clic en , a continuación, haga clic en **Editar**.
3. En **CAPACIDAD**, cambie el tamaño del espacio de nombres.

CLI

1. Introduzca el siguiente comando: `vserver nvme namespace modify -vserver SVM_name -path path -size new_size_of_namespace`

Reducir el tamaño de un espacio de nombres

Se debe usar la CLI de ONTAP para reducir el tamaño de un espacio de nombres NVMe.

1. Cambie la configuración del privilegio a avanzado:

```
set -privilege advanced
```

2. Reducir el tamaño del espacio de nombres:

```
vserver nvme namespace modify -vserver SVM_name -path namespace_path -size new_size_of_namespace
```

Convertir un espacio de nombres en una LUN

A partir de ONTAP 9.11.1, se puede utilizar la interfaz de línea de comandos de ONTAP para convertir un espacio de nombres NVMe existente en una LUN.

Antes de empezar

- El espacio de nombres NVMe especificado no debe tener ningún mapa existente a un subsistema.
- El espacio de nombres no debe formar parte de una copia Snapshot ni de la relación de SnapMirror en el lado de destino como espacio de nombres de solo lectura.
- Dado que los espacios de nombres de NVMe solo son compatibles con plataformas y tarjetas de red específicas, esta función solo funciona con hardware específico.

Pasos

1. Introduzca el siguiente comando para convertir un espacio de nombres NVMe en una LUN:

```
lun convert-from-namespace -vserver -namespace-path
```

Configure la autenticación en banda a través de NVMe

A partir de ONTAP 9.12.1, se puede utilizar la interfaz de línea de comandos (CLI) de ONTAP para configurar la autenticación en banda (segura), bidireccional y unidireccional entre un host NVMe y una controladora mediante los protocolos NVMe/TCP y NVMe/FC mediante la autenticación DH-HMAC-CHAP. A partir de ONTAP 9.14.1, la autenticación

en banda se puede configurar en System Manager.

Para configurar la autenticación en banda, cada host o controladora debe estar asociado con una clave DH-HMAC-CHAP que es una combinación de NQN del host o controladora NVMe y un secreto de autenticación configurado por el administrador. Para que un host o una controladora NVMe autentiquen a su par, deben conocer la clave asociada con el par.

En la autenticación unidireccional, se configura una clave secreta para el host, pero no para la controladora. En la autenticación bidireccional, se configura una clave secreta para el host y la controladora.

SHA-256 es la función hash predeterminada y 2048 bits es el grupo DH predeterminado.

System Manager

A partir de ONTAP 9.14.1, se puede usar System Manager para configurar la autenticación en banda mientras se crea o actualiza un subsistema NVMe, se crean o clonan espacios de nombres NVMe, o bien se añaden grupos de coherencia con nuevos espacios de nombres NVMe.

Pasos

1. En el Administrador del sistema, haga clic en **Hosts > Subsistema NVMe** y, a continuación, haga clic en **Agregar**.
2. Añada el nombre del subsistema NVMe y seleccione la máquina virtual de almacenamiento y el sistema operativo del host.
3. Introduzca el NQN del host.
4. Seleccione **Usar autenticación en banda** junto al Host NQN.
5. Proporcione el secreto del host y el secreto de la controladora.

La clave DH-HMAC-CHAP es una combinación del NQN del host o controladora NVMe y un secreto de autenticación configurado por el administrador.

6. Seleccione la función hash y el grupo DH preferidos para cada host.

Si no selecciona una función hash y un grupo DH, SHA-256 se asigna como función hash predeterminada y 2048 bits se asigna como grupo DH predeterminado.

7. Opcionalmente, haga clic en **Agregar** y repita los pasos según sea necesario para agregar más host.
8. Haga clic en **Guardar**.
9. Para verificar que la autenticación en banda está habilitada, haga clic en **System Manager > Hosts > Subsistema NVMe > Grid > Vista Peek**.

Un icono de clave transparente junto al nombre del host indica que el modo unidireccional está activado. Una clave opaca junto al nombre del host indica que el modo bidireccional está activado.

CLI

Pasos

1. Añada la autenticación DH-HMAC-CHAP al subsistema NVMe:

```
vserver nvme subsystem host add -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn> -dhchap-host-secret
<authentication_host_secret> -dhchap-controller-secret
<authentication_controller_secret> -dhchap-hash-function <sha-
256|sha-512> -dhchap-group <none|2048-bit|3072-bit|4096-bit|6144-
bit|8192-bit>
```

2. Compruebe que el protocolo de autenticación CHAP DH-HMAC se ha agregado al host:

```
vserver nvme subsystem host show
```

```

[ -dhchap-hash-function {sha-256|sha-512} ] Authentication Hash
Function
[ -dhchap-dh-group {none|2048-bit|3072-bit|4096-bit|6144-bit|8192-
bit} ]
Diffie-Hellman
Group
[ -dhchap-mode {none|unidirectional|bidirectional} ]
Authentication Mode

```

3. Compruebe que la autenticación CHAP DH-HMAC se ejecutó durante la creación de la controladora NVMe:

```
vserver nvme subsystem controller show
```

```

[ -dhchap-hash-function {sha-256|sha-512} ] Authentication Hash
Function
[ -dhchap-dh-group {none|2048-bit|3072-bit|4096-bit|6144-bit|8192-
bit} ]
Diffie-Hellman
Group
[ -dhchap-mode {none|unidirectional|bidirectional} ]
Authentication Mode

```

Deshabilite la autenticación en banda sobre NVMe

Si configuró la autenticación en banda a través de NVMe mediante DH-HMAC-CHAP, puede optar por deshabilitarla en cualquier momento.

Si va a revertir desde ONTAP 9.12.1 o posterior a ONTAP 9.12.0 o una versión anterior, debe deshabilitar la autenticación en banda antes de revertir. Si la autenticación en banda con DH-HMAC-CHAP no está desactivada, se producirá un error en la reversión.

Pasos

1. Quite el host del subsistema para deshabilitar la autenticación DH-HMAC-CHAP:

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

2. Compruebe que el protocolo de autenticación DH-HMAC-CHAP se ha eliminado del host:

```
vserver nvme subsystem host show
```

3. Vuelva a agregar el host al subsistema sin autenticación:

```
vserver nvme subsystem host add vserver <svm_name> -subsystem  
<subsystem> -host-nqn <host_nqn>
```

Cambiar la prioridad del host de NVMe

A partir de ONTAP 9.14.1, puede configurar su subsistema NVMe para priorizar la asignación de recursos para hosts específicos. De forma predeterminada, cuando se agrega un host al subsistema, se le asigna una prioridad regular. Los hosts a los que se asigna una prioridad alta se asignan números de colas de I/O de mayor tamaño y profundidades de cola.

Puede usar la interfaz de línea de comandos (CLI) de ONTAP para cambiar manualmente la prioridad predeterminada de regular a alta. Para cambiar la prioridad asignada a un host, debe eliminar el host del subsistema y volver a añadirlo.

Pasos

1. Compruebe que la prioridad de host se ha establecido en Regular:

```
vserver nvme show-host-priority
```

2. Elimine el host del subsistema:

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem  
<subsystem> -host-nqn <host_nqn>
```

3. Compruebe que el host se ha eliminado del subsistema:

```
vserver nvme subsystem host show
```

4. Vuelva a agregar el host al subsistema con prioridad alta:

```
vserver nvme subsystem host add -vserver <SVM_name> -subsystem  
<subsystem_name> -host-nqn <Host_NQN_:subsystem._subsystem_name>  
-priority high
```

Gestionar la detección automática de hosts de controladoras NVMe/TCP

A partir de ONTAP 9.14.1, la detección de host de las controladoras con el protocolo NVMe/TCP se automatiza de forma predeterminada en las estructuras basadas en IP.

Habilite la detección de host automatizada de las controladoras NVMe/TCP

Si deshabilitó la detección de hosts automatizada anteriormente, pero sus necesidades cambiaron, es posible volver a habilitarla.

Pasos

1. Entre en el modo de privilegio avanzado:

```
set -privilege advanced
```

2. Habilitar detección automatizada:

```
vserver nvme modify -vserver <vserver_name> -mdns-service-discovery  
-enabled true
```

3. Compruebe que la detección automatizada de controladoras NVMe/TCP está habilitada.

```
vserver nvme show
```

Deshabilite la detección automática de host de las controladoras NVMe/TCP

Si no necesita controladoras NVMe/TCP para que el host lo detecte automáticamente y detecta el tráfico de multidifusión no deseado en la red, debe deshabilitar esta funcionalidad.

Pasos

1. Entre en el modo de privilegio avanzado:

```
set -privilege advanced
```

2. Desactivar la detección automatizada:

```
vserver nvme modify -vserver <vserver_name> -mdns-service-discovery  
-enabled false
```

3. Verifique que la detección automatizada de las controladoras NVMe/TCP está deshabilitada.

```
vserver nvme show
```


Deshabilitar identificador de máquina virtual de host NVMe

A partir de ONTAP 9.14.1, de forma predeterminada, ONTAP admite la capacidad de los hosts NVMe/FC para identificar las máquinas virtuales con un identificador único y para que los hosts NVMe/FC supervisen la utilización de los recursos de las máquinas virtuales. Esto mejora la generación de informes y la solución de problemas del host.

Puede utilizar el arranque para desactivar esta funcionalidad.

Paso

1. Desactive el identificador de la máquina virtual:

```
bootargs set fct_sli_appid_off <port>, <port>
```

En el ejemplo siguiente se deshabilita el VMID en el puerto 0g y en el puerto 0i.

```
bootargs set fct_sli_appid_off 0g,0i  
  
fct_sli_appid_off == 0g,0i
```

Gestione sistemas con adaptadores de FC

Gestione sistemas con adaptadores de FC

Hay comandos disponibles para gestionar los adaptadores FC integrados y las tarjetas adaptadoras FC. Estos comandos se pueden utilizar para configurar el modo del adaptador, mostrar información del adaptador y cambiar la velocidad.

La mayoría de los sistemas de almacenamiento tienen adaptadores FC integrados que se pueden configurar como iniciadores o destinos. También puede utilizar tarjetas adaptadoras de FC configuradas como iniciadores o destinos. Los iniciadores se conectan a las bandejas de discos del back-end y posiblemente a cabinas de almacenamiento externas (FlexArray). Los destinos se conectan solo a switches FC. Tanto los puertos HBA de destino FC como la velocidad del puerto del switch deben configurarse con el mismo valor y no deben configurarse en modo automático.

Información relacionada

["CONFIGURACIÓN DE SAN"](#)

Comandos para gestionar adaptadores de FC

Puede usar comandos FC para gestionar adaptadores de destino FC, adaptadores de iniciador FC y adaptadores de FC integrados para su controladora de almacenamiento. Los mismos comandos se utilizan para gestionar adaptadores de FC para el protocolo FC y el protocolo FC-NVMe.

Los comandos de adaptador del iniciador de FC solo funcionan en el nivel del nodo. Debe utilizar el `run -node node_name` Antes de poder utilizar los comandos del adaptador del iniciador de FC.

Comandos para gestionar los adaptadores de destino de FC

| Si desea... | Se usa este comando... |
|--|---|
| Muestra información del adaptador de FC en un nodo | <code>network fcp adapter show</code> |
| Modifique los parámetros del adaptador de destino FC | <code>network fcp adapter modify</code> |
| Muestra información sobre el tráfico del protocolo FC | <code>run -node <i>node_name</i> sysstat -f</code> |
| Muestra el tiempo que se ha ejecutado el protocolo FC | <code>run -node <i>node_name</i> uptime</code> |
| Mostrar la configuración y el estado del adaptador | <code>run -node <i>node_name</i> sysconfig -v <i>adapter</i></code> |
| Compruebe qué tarjetas de expansión están instaladas y si hay algún error de configuración | <code>run -node <i>node_name</i> sysconfig -ac</code> |
| Ver una página de manual de un comando | <code>man <i>command_name</i></code> |

Comandos para gestionar los adaptadores de iniciador de FC

| Si desea... | Se usa este comando... |
|--|---|
| Muestra información de todos los iniciadores y sus adaptadores en un nodo | <code>run -node <i>node_name</i> storage show adapter</code> |
| Mostrar la configuración y el estado del adaptador | <code>run -node <i>node_name</i> sysconfig -v <i>adapter</i></code> |
| Compruebe qué tarjetas de expansión están instaladas y si hay algún error de configuración | <code>run -node <i>node_name</i> sysconfig -ac</code> |

Comandos para gestionar los adaptadores de FC internos

| Si desea... | Se usa este comando... |
|--|--|
| Muestra el estado de los puertos FC internos | <code>run -node <i>node_name</i> system hardware unified-connect show</code> |

Configure los adaptadores de FC

Cada puerto FC integrado se puede configurar de forma individual como iniciador o destino. Los puertos en determinados adaptadores de FC también se pueden configurar de forma individual como un puerto de destino o como un puerto iniciador, al igual que

los puertos FC integrados. Hay disponible una lista de adaptadores que se pueden configurar para el modo de destino en ["Hardware Universe de NetApp"](#).

El modo de destino se utiliza para conectar los puertos a iniciadores FC. El modo iniciador se usa para conectar los puertos a unidades de cinta, bibliotecas de cintas o almacenamiento de terceros con la virtualización de FlexArray o con importación de LUN externa (FLI).

Los mismos pasos se utilizan cuando se configuran los adaptadores de FC para el protocolo FC y el protocolo FC-NVMe. Sin embargo, solo ciertos adaptadores de FC admiten FC-NVMe. Consulte ["Hardware Universe de NetApp"](#) Para obtener una lista de los adaptadores que admiten el protocolo FC-NVMe.

Configure los adaptadores de FC para el modo de destino

Pasos

1. Desconectar el adaptador:

```
node run -node node_name storage disable adapter adapter_name
```

Si el adaptador no se desconecta, también puede quitar el cable del puerto de adaptador correspondiente del sistema.

2. Cambie el adaptador del iniciador al destino:

```
system hardware unified-connect modify -t target -node node_name adapter adapter_name
```

3. Reinicie el nodo que aloja el adaptador que cambió.
4. Compruebe que el puerto de destino tiene la configuración correcta:

```
network fcp adapter show -node node_name
```

5. Conectar su adaptador:

```
network fcp adapter modify -node node_name -adapter adapter_port -state up
```

Configure los adaptadores de FC para el modo iniciador

Lo que necesitará

- Las LIF del adaptador deben eliminarse de cualquier conjunto de puertos de los que pertenezcan.
- Todas las LIF de todas las máquinas virtuales de almacenamiento (SVM) que utilizan el puerto físico que se va a modificar deben migrarse o destruirse antes de cambiar la personalidad del puerto físico de destino a iniciador.



NVMe/FC no admite el modo iniciador.

Pasos

1. Quite todas las LIF del adaptador:

```
network interface delete -vserver SVM_name -lif LIF_name,LIF_name
```

2. Desconectar el adaptador:

```
network fcp adapter modify -node node_name -adapter adapter_port -status-admin  
down
```

Si el adaptador no se desconecta, también puede quitar el cable del puerto de adaptador correspondiente del sistema.

3. Cambie el adaptador del destino al iniciador:

```
system hardware unified-connect modify -t initiator adapter_port
```

4. Reinicie el nodo que aloja el adaptador que cambió.
5. Compruebe que los puertos FC estén configurados en estado correcto para la configuración:

```
system hardware unified-connect show
```

6. Vuelva a conectar el adaptador:

```
node run -node node_name storage enable adapter adapter_port
```

Ver la configuración de adaptador

Puede utilizar comandos específicos para ver información sobre sus adaptadores FC/UTA.

Adaptador de destino FC

Paso

1. Utilice la `network fcp adapter show` comando para mostrar información del adaptador: `network fcp adapter show -instance -node node1 -adapter 0a`

El resultado muestra información de configuración del sistema y información del adaptador para cada ranura que se utiliza.

Adaptador de destino unificado (UTA) X1143A-R6

Pasos

1. Arranque la controladora sin los cables conectados.
2. Ejecute el `system hardware unified-connect show` comando para ver la configuración del puerto y los módulos.
3. Consulte la información del puerto antes de configurar el CNA y los puertos.

Cambie el puerto UTA2 del modo CNA al modo FC

Debe cambiar el puerto UTA2 del modo adaptador de red convergente (CNA) al modo Fibre Channel (FC) para admitir el iniciador de FC y el modo de destino de FC. Debe cambiar la personalidad del modo CNA al modo FC cuando necesite cambiar el medio físico que conecta el puerto a su red.

Pasos

1. Desconectar el adaptador:

```
network fcp adapter modify -node node_name -adapter adapter_name -status-admin
down
```

2. Cambie el modo de puerto:

```
ucadmin modify -node node_name -adapter adapter_name -mode fcp
```

3. Reinicie el nodo y a continuación, active el adaptador:

```
network fcp adapter modify -node node_name -adapter adapter_name -status-admin
up
```

4. Notifique a su administrador o VIF Manager que elimine o quite el puerto, según corresponda:

- Si el puerto se utiliza como puerto de inicio de una LIF, es miembro de un grupo de interfaces (ifgrp) o una VLAN de host, un administrador debe hacer lo siguiente:
 - i. Mueva las LIF, quite el puerto del ifgrp o elimine las VLAN respectivamente.
 - ii. Elimine manualmente el puerto ejecutando el `network port delete` comando.

Si la `network port delete` error del comando, el administrador debe solucionar los errores y volver a ejecutar el comando.

- Si el puerto no se usa como puerto de inicio de una LIF, no es miembro de un ifgrp y no aloja VLAN, el gestor VIF debería eliminar el puerto de sus registros en el momento del reinicio.

Si el administrador VIF no quita el puerto, el administrador debe quitarlo manualmente después del reinicio usando la `network port delete` comando.

```
net-f8040-34::> network port show
```

```
Node: net-f8040-34-01
```

| Port | IPspace | Broadcast | Domain | Link | MTU | Speed (Mbps) Admin/Oper | Health Status |
|-------|---------|-----------|--------|------|------|----------------------------|------------------|
| ----- | ----- | ----- | ----- | ---- | ---- | ----- | |
| ----- | | | | | | | |
| ... | | | | | | | |
| e0i | Default | Default | | down | 1500 | auto/10 | - |
| e0f | Default | Default | | down | 1500 | auto/10 | - |
| ... | | | | | | | |

```
net-f8040-34::> ucadmin show
```

| | | | Current | Current | Pending | Pending |
|-----------------|---------|-------|---------|---------|---------|---------|
| Admin | | | | | | |
| Node | Adapter | Mode | Type | Mode | Type | |
| Status | | | | | | |
| ----- | ----- | ----- | ----- | ----- | ----- | ----- |
| ----- | | | | | | |
| net-f8040-34-01 | 0e | cna | target | - | - | |
| offline | | | | | | |

```

net-f8040-34-01 0f cna target - -
offline
...

net-f8040-34::> network interface create -vs net-f8040-34 -lif m
-role
node-mgmt-home-node net-f8040-34-01 -home-port e0e -address 10.1.1.1
-netmask 255.255.255.0

net-f8040-34::> network interface show -fields home-port, curr-port

vserver lif                home-port curr-port
-----
Cluster net-f8040-34-01_clus1 e0a        e0a
Cluster net-f8040-34-01_clus2 e0b        e0b
Cluster net-f8040-34-01_clus3 e0c        e0c
Cluster net-f8040-34-01_clus4 e0d        e0d
net-f8040-34
      cluster_mgmt          e0M          e0M
net-f8040-34
      m                      e0e          e0i
net-f8040-34
      net-f8040-34-01_mgmt1 e0M          e0M
7 entries were displayed.

net-f8040-34::> ucadmin modify local 0e fc

Warning: Mode on adapter 0e and also adapter 0f will be changed to
fc.
Do you want to continue? {y|n}: y
Any changes will take effect after rebooting the system. Use the
"system node reboot" command to reboot.

net-f8040-34::> reboot local
(system node reboot)

Warning: Are you sure you want to reboot node "net-f8040-34-01"?
{y|n}: y

```

5. Compruebe que tiene instalado el SFP+ correcto:

```
network fcp adapter show -instance -node -adapter
```

Para CNA, se debe usar un SFP Ethernet de 10 GB. Para FC, se debe usar un SFP de 8 GB o un SFP de 16 GB antes de cambiar la configuración en el nodo.

Cambie los módulos ópticos del adaptador de destino CNA/UTA2

Debe cambiar los módulos ópticos del adaptador de destino unificado (CNA/UTA2) para admitir el modo de personalidad seleccionado para el adaptador.

Pasos

1. Verifique el SFP+ actual utilizado en la tarjeta. A continuación, reemplace el SFP+ actual por el SFP+ adecuado para la personalidad preferida (FC o CNA).
2. Retire los módulos ópticos actuales del adaptador X1143A-R6.
3. Inserte los módulos correctos para la óptica del modo de personalidad preferido (FC o CNA).
4. Compruebe que tiene instalado el SFP+ correcto:

```
network fcp adapter show -instance -node -adapter
```

Los módulos SFP+ admitidos y los cables de cobre (Twinax) de la Marca Cisco se enumeran en el *Hardware Universe*.

Información relacionada

["Hardware Universe de NetApp"](#)

Configuraciones de puertos compatibles para los adaptadores X1143A-R6

El modo de destino FC es la configuración predeterminada para los puertos de adaptador X1143A-R6. Sin embargo, los puertos de este adaptador se pueden configurar como puertos Ethernet y FCoE de 10 GB o como puertos FC de 16 GB.

Cuando se configura para Ethernet y FCoE, los adaptadores X1143A-R6 admiten el tráfico de destino NIC y FCoE simultáneo en el mismo puerto de 10 GBE. Cuando se configura para FC, cada par de dos puertos que comparte el mismo ASIC se puede configurar individualmente para modo iniciador FC o destino FC. Esto significa que un solo adaptador X1143A-R6 puede admitir el modo objetivo FC en un par de dos puertos y el modo iniciador de FC en otro par de dos puertos.

Información relacionada

["Hardware Universe de NetApp"](#)

["CONFIGURACIÓN DE SAN"](#)

Configure los puertos

Para configurar el adaptador de objetivo unificado (X1143A-R6), debe configurar los dos puertos adyacentes en el mismo chip en el mismo modo Personality.

Pasos

1. Configure los puertos según sea necesario para Fibre Channel (FC) o el adaptador de red convergente (CNA) mediante el `system node hardware unified-connect modify` comando.
2. Conecte los cables adecuados para FC o Ethernet de 10 GB.
3. Compruebe que tiene instalado el SFP+ correcto:

```
network fcp adapter show -instance -node -adapter
```

Para CNA, se debe usar un SFP Ethernet de 10 GB. Para FC, se debe usar un SFP de 8 GB o un SFP de 16 GB, a partir de la estructura de FC al que se está conectando.

Evite la pérdida de conectividad cuando utilice el adaptador X1133A-R6

Puede evitar la pérdida de conectividad durante un error en el puerto configurando el sistema con rutas redundantes en HBA X1133A-R6 independientes.

El HBA X1133A-R6 es un adaptador FC de 4 puertos y 16 GB que consta de dos pares de dos puertos. El adaptador X1133A-R6 se puede configurar como modo de destino o modo de iniciador. Cada par de 2 puertos se admite con un único ASIC (por ejemplo, el puerto 1 y el puerto 2 en ASIC 1 y el puerto 3 y el puerto 4 en ASIC 2). Ambos puertos en un único ASIC deben configurarse para funcionar en el mismo modo, tanto en modo objetivo como en modo iniciador. Si se produce un error con el ASIC que admite un par, ambos puertos del par se desconectan.

Para evitar esta pérdida de conectividad, puede configurar el sistema con rutas redundantes para separar los HBA X1133A-R6, o con rutas redundantes a los puertos compatibles con diferentes ASIC en el HBA.

Administre LIF para todos los protocolos SAN

Administre LIF para todos los protocolos SAN

Los iniciadores deben usar I/O multivía (MPIO) y el acceso asimétrico de unidades lógicas (ALUA) para la capacidad de conmutación por error para los clústeres de un entorno SAN. Si falla un nodo, los LIF no migran ni asumen las direcciones IP del nodo del compañero que ha fallado. En su lugar, el software MPIO, mediante ALUA en el host, es responsable de seleccionar las rutas adecuadas para el acceso de las LUN a través de LIF.

Debe crear una o varias rutas iSCSI desde cada nodo de una pareja de ha, utilizando interfaces lógicas (LIF) para permitir el acceso a las LUN a las que presta servicio el par de alta disponibilidad. Debe configurar un LIF de gestión para cada máquina virtual de almacenamiento (SVM) compatible con SAN.

La conexión directa o el uso de switches Ethernet es compatible con la conectividad. Debe crear LIF para ambos tipos de conectividad.

- Debe configurar un LIF de gestión para cada máquina virtual de almacenamiento (SVM) compatible con SAN.
Puede configurar dos LIF por nodo, uno para cada estructura que se usa con FC y para separar redes Ethernet para iSCSI.

Una vez creadas las LIF, pueden eliminarse de conjuntos de puertos, moverse a diferentes nodos en una máquina virtual de almacenamiento (SVM) y eliminarse.

Información relacionada

- ["Configurar LIF overveiw"](#)
- ["Cree una LIF"](#)

Configure una LIF NVMe

Deben satisfacerse ciertos requisitos al configurar las LIF de NVMe.

Antes de empezar

El adaptador de FC en el que se crea la LIF debe admitir NVMe. Los adaptadores admitidos se enumeran en ["Hardware Universe"](#).

Acerca de esta tarea

A partir de ONTAP 9.12.1 y versiones posteriores, puede configurar dos LIF NVMe por nodo en un máximo de 12 nodos. En ONTAP 9.11.1 y versiones anteriores, puede configurar dos LIF NVMe por nodo en un máximo de dos nodos.

Se aplican las siguientes reglas al crear una LIF NVMe:

- NVMe puede ser el único protocolo de datos en las LIF de datos.
- Debe configurar una LIF de gestión para cada SVM que sea compatible con SAN.
- Para ONTAP 9,5 y versiones posteriores, debe configurar un LIF NVMe en el nodo que contiene el espacio de nombres y en el partner de alta disponibilidad del nodo.
- Solo para ONTAP 9.4:
 - Las LIF y los espacios de nombres de NVMe deben alojarse en el mismo nodo.
 - Solo se puede configurar un LIF de datos NVMe por SVM.

Pasos

1. Cree la LIF:

```
network interface create -vserver <SVM_name> -lif <LIF_name> -role  
<LIF_role> -data-protocol {fc-nvme|nvme-tcp} -home-node <home_node>  
-home-port <home_port>
```



NVME/TCP está disponible a partir de ONTAP 9.10.1 y versiones posteriores.

2. Compruebe que la LIF se ha creado:

```
network interface show -vserver <SVM_name>
```

Después de la creación, las LIF NVMe/TCP reciben la detección en el puerto 8009.

Qué debe saber antes de mover una LIF SAN

Solo debe realizar un movimiento LIF si está cambiando el contenido del clúster, por ejemplo, agregar nodos al clúster o eliminar nodos del clúster. Si realiza un movimiento de LIF, no necesita volver a crear una zona de la estructura de FC ni crear nuevas sesiones iSCSI entre los hosts conectados del clúster y la nueva interfaz de destino.

No puede mover un LIF DE SAN mediante el `network interface move` comando. El movimiento de LIF DE SAN debe realizarse desconectando el LIF, trasladando el LIF a otro nodo o puerto raíz y, a continuación, volviendo a conectarlo en su nueva ubicación. El acceso asimétrico de Unidad lógica (ALUA, Asymmetric Logical Unit Access) proporciona rutas redundantes y selección automática de rutas como parte de cualquier solución SAN de ONTAP. Por lo tanto, no se produce ninguna interrupción de I/O cuando se desconecta el LIF

para dicho movimiento. El host simplemente reintenta y, a continuación, mueve I/O a otra LIF.

Con el movimiento LIF, puede hacer lo siguiente de forma no disruptiva:

- Sustituya un par de alta disponibilidad de un clúster por un par de alta disponibilidad actualizado de manera que los hosts que acceden a los datos de las LUN sean transparentes
- Actualizar una tarjeta de interfaz de destino
- Traslade los recursos de una máquina virtual de almacenamiento (SVM) de un conjunto de nodos de un clúster a otro conjunto de nodos del clúster

Quite una LIF DE SAN de un conjunto de puertos

Si la LIF que desea eliminar o mover está en un conjunto de puertos, debe quitar la LIF del conjunto de puertos antes de poder eliminar o mover la LIF.

Acerca de esta tarea

Debe realizar el Paso 1 del siguiente procedimiento sólo si hay un LIF en el conjunto de puertos. No puede quitar la última LIF de un conjunto de puertos si el conjunto de puertos está vinculado a un iGroup. De lo contrario, puede empezar con Paso 2 si hay varias LIF en el conjunto de puertos.

Pasos

1. Si solo hay una LIF en el conjunto de puertos, utilice `lun igroup unbind` comando para desvincular el puerto establecido del igroup.



Cuando se desvincula un iGroup de un conjunto de puertos, todos los iniciadores del iGroup tienen acceso a todas las LUN de destino asignadas al iGroup en todas las interfaces de red.

```
cluster1::>lun igroup unbind -vserver vs1 -igroup ig1
```

2. Utilice la `lun portset remove` Comando para quitar la LIF del conjunto de puertos.

```
cluster1::> port set remove -vserver vs1 -portset ps1 -port-name lif1
```

Mover un LIF SAN

Si un nodo tiene que desconectarse, puede mover un LIF SAN para conservar la información de configuración, como su WWPN, y evitar volver a dividir en zonas la estructura de switches. Como hay que desconectar un LIF SAN antes de trasladarlo, el tráfico del host debe depender de software multivía del host para ofrecer un acceso no disruptivo a la LUN. Puede mover LIF SAN a cualquier nodo de un clúster, pero no puede mover estas entre máquinas virtuales de almacenamiento (SVM).

Lo que necesitará

Si el LIF es miembro de un conjunto de puertos, es necesario haber eliminado el LIF del conjunto de puertos antes de poder mover el LIF a un nodo diferente.

Acerca de esta tarea

El nodo de destino y el puerto físico de un LIF que desee mover deben estar en la misma estructura de FC o red Ethernet. Si mueve un LIF a otra estructura que no haya tenido una zona adecuada o si mueve un LIF a

una red Ethernet que no tenga conectividad entre un iniciador iSCSI y un destino, no será posible acceder a la LUN cuando vuelva a estar en línea.

Pasos

1. Vea el estado administrativo y operativo de la LIF:

```
network interface show -vserver vserver_name
```

2. Cambie el estado de la LIF a. down (sin conexión):

```
network interface modify -vserver vserver_name -lif LIF_name -status-admin  
down
```

3. Asigne a la LIF un nodo y un puerto nuevos:

```
network interface modify -vserver vserver_name -lif LIF_name -home-node  
node_name -home-port port_name
```

4. Cambie el estado de la LIF a. up (en línea):

```
network interface modify -vserver vserver_name -lif LIF_name -status-admin up
```

5. Compruebe los cambios:

```
network interface show -vserver vserver_name
```

Eliminar una LIF en un entorno SAN

Antes de eliminar una LIF, debe asegurarse de que el host conectado a la LIF pueda acceder a las LUN a través de otra ruta.

Lo que necesitará

Si la LIF que desea eliminar es miembro de un conjunto de puertos, primero debe quitar la LIF del conjunto de puertos antes de poder eliminar la LIF.

System Manager

Elimine una LIF con el Administrador del sistema de ONTAP (9.7 y posterior).

Pasos

1. En System Manager, haga clic en **Red > Descripción general** y, a continuación, seleccione **interfaces de red**.
2. Seleccione la máquina virtual de almacenamiento desde la que desea eliminar la LIF.
3. Haga clic en **⋮** Y seleccione **Eliminar**.

CLI

Elimine una LIF con la CLI de ONTAP.

Pasos

1. Compruebe el nombre de la LIF y el puerto actual que se va a eliminar:

```
network interface show -vserver vs1 -lif lif1
```

2. Elimine la LIF:

```
network interface delete
```

```
network interface delete -vserver vs1 -lif lif1
```

3. Compruebe que ha eliminado la LIF:

```
network interface show
```

```
network interface show -vserver vs1
```

| Logical Status | Network | Current | Current Is |
|-------------------|------------|-----------------|-------------|
| Vserver Interface | Admin/Oper | Address/Mask | Node Port |
| Home | | | |
| ----- | ----- | ----- | ----- |
| vs1 | | | |
| lif2 | up/up | 192.168.2.72/24 | node-01 e0b |
| true | | | |
| lif3 | up/up | 192.168.2.73/24 | node-01 e0b |
| true | | | |

Requisitos de LIF de SAN para añadir nodos a un clúster

Debe tener en cuenta determinadas consideraciones al añadir nodos a un clúster.

- Debe crear LIF en los nuevos nodos del modo que corresponda antes de crear LUN en esos nuevos nodos.

- Debe detectar estas LIF desde los hosts según lo dictado por la pila del host y el protocolo.
- Debe crear LIF en los nodos nuevos de modo que los movimientos de la LUN y los volúmenes sean posibles sin utilizar la red de interconexión de clúster.

Configure LIF iSCSI para devolver el FQDN al host iSCSI SendTargets Discovery Operation

A partir de ONTAP 9, las LIF iSCSI se pueden configurar para que devuelvan un nombre de dominio completo (FQDN) cuando un sistema operativo host envía una operación de detección SendTargets iSCSI. Devolver un FQDN es útil cuando hay un dispositivo de traducción de direcciones de red (NAT) entre el sistema operativo host y el servicio de almacenamiento.

Acerca de esta tarea

Las direcciones IP de un lado del dispositivo NAT no tienen sentido en el otro lado, pero FQDN puede tener significado en ambos lados.



El límite de interoperabilidad del valor FQDN es de 128 caracteres en todo el sistema operativo host.

Pasos

1. Cambie la configuración del privilegio a avanzado:

```
set -privilege advanced
```

2. Configure los LIF iSCSI para devolver el FQDN:

```
vserver iscsi interface modify -vserver SVM_name -lif iscsi_LIF_name
-sendtargets_fqdn FQDN
```

En el ejemplo siguiente, los LIF iSCSI están configurados para devolver storagehost-005.example.com como el FQDN.

```
vserver iscsi interface modify -vserver vs1 -lif vs1_iscsi1 -sendtargets-fqdn
storagehost-005.example.com
```

3. Compruebe que sendTargets sea el FQDN:

```
vserver iscsi interface show -vserver SVM_name -fields sendtargets-fqdn
```

En este ejemplo, storagehost-005.example.com se muestra en el campo de salida sendTargets-fqdn.

```
cluster::vserver*> vserver iscsi interface show -vserver vs1 -fields
sendtargets-fqdn
vserver lif          sendtargets-fqdn
-----
vs1      vs1_iscsi1  storagehost-005.example.com
vs1      vs1_iscsi2  storagehost-006.example.com
```

Información relacionada

Combinaciones de configuración recomendadas de volúmenes y archivos o LUN

Información general de las combinaciones de configuración de volúmenes y archivos o LUN recomendadas

Existen combinaciones específicas de configuraciones de volumen y archivo de FlexVol o LUN que puede utilizar, en función de sus requisitos de aplicación y administración. Comprender los beneficios y los costos de estas combinaciones puede ayudarlo a determinar la combinación adecuada de configuración de volúmenes y LUN para su entorno.

Se recomiendan las siguientes combinaciones de configuración de volúmenes y LUN:

- Archivos reservados de espacio o LUN con aprovisionamiento de volumen grueso
- Archivos sin espacio reservado o LUN con thin provisioning de volumen
- Archivos reservados de espacio o LUN con aprovisionamiento de volumen grueso

Puede utilizar thin provisioning SCSI en sus LUN junto con cualquiera de estas combinaciones de configuración.

Archivos reservados de espacio o LUN con aprovisionamiento de volumen grueso

Beneficios:

- Se garantizan todas las operaciones de escritura en los archivos con espacio reservado; no se producen errores debido a la falta de espacio.
- No existen restricciones sobre las tecnologías de eficiencia del almacenamiento y protección de datos en el volumen.

Costos y limitaciones:

- Debe reservar espacio suficiente desde el agregado hacia delante para admitir el volumen considerablemente aprovisionado.
- El espacio es igual al doble del tamaño de la LUN se asigna desde el volumen en el momento de creación de la LUN.

Archivos sin espacio reservado o LUN con thin provisioning de volumen

Beneficios:

- No existen restricciones sobre las tecnologías de eficiencia del almacenamiento y protección de datos en el volumen.
- El espacio se asigna solo como se utiliza.

Costos y restricciones:

- No se garantizan las operaciones de escritura; pueden fallar si el volumen se queda sin espacio libre.
- Debe gestionar eficazmente el espacio libre del agregado para evitar que el agregado se quede sin espacio libre.

Beneficios:

Se reserva menos espacio inicial que para el aprovisionamiento de volúmenes gruesos y se ofrece una garantía de escritura de mejor esfuerzo.

Costos y restricciones:

- Las operaciones de escritura pueden fallar con esta opción.

Puede mitigar este riesgo equilibrando correctamente el espacio libre en el volumen frente a la volatilidad de los datos.

- No puede confiar en la retención de objetos de protección de datos como copias Snapshot, archivos FlexClone y LUN.
- No se pueden utilizar funcionalidades de eficiencia del almacenamiento con uso compartido de bloques de ONTAP que no se pueden eliminar automáticamente, incluida la deduplicación, la compresión y la descarga ODX/copia.

Determinar la combinación correcta de configuración de volumen y LUN para su entorno

Responder a algunas preguntas básicas acerca de su entorno puede ayudarle a determinar la mejor configuración de LUN y volumen FlexVol para su entorno.

Acerca de esta tarea

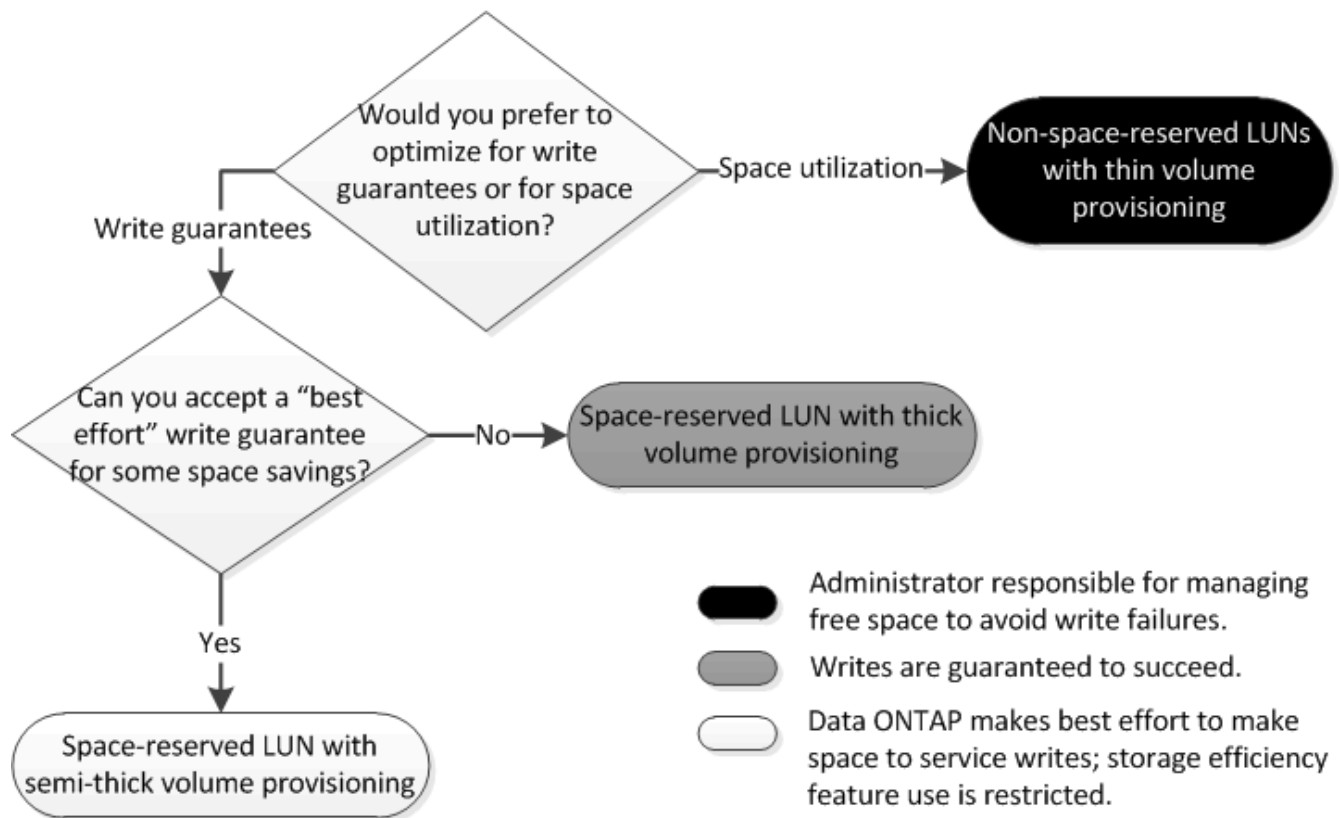
Puede optimizar su configuración de LUN y volúmenes para un uso máximo del almacenamiento o para la seguridad de garantías de escritura. En función de sus requisitos de utilización del almacenamiento y su capacidad para supervisar y reponer espacio libre rápidamente, debe determinar el volumen de FlexVol y los volúmenes LUN adecuados para su instalación.



No es necesario un volumen separado para cada LUN.

Paso

1. Use el siguiente árbol de decisiones para determinar la mejor combinación de configuración de volumen y LUN para su entorno:



Calcule la tasa de crecimiento de datos de las LUN

Necesita conocer la velocidad a la que crecen sus datos de LUN con el tiempo para determinar si debe utilizar LUN reservadas para el espacio o LUN no reservadas para el espacio.

Acerca de esta tarea

Si tiene una tasa alta y constante de crecimiento de datos, puede que las LUN con reserva de espacio sean una mejor opción. Si tiene una tasa baja de crecimiento de datos, debe plantearse poner en marcha LUN sin reservar espacio.

Puede utilizar herramientas como OnCommand Insight para calcular la tasa de crecimiento de datos o puede calcularla manualmente. Los siguientes pasos son para el cálculo manual.

Pasos

1. Configure un LUN con reserva de espacio.
2. Supervise los datos en la LUN durante un período establecido, como una semana.

Asegúrese de que el período de monitorización sea lo suficientemente largo como para formar una muestra representativa de los aumentos que se producen regularmente en el crecimiento de datos. Por ejemplo, es posible que usted tenga constantemente un gran crecimiento de datos a final de cada mes.

3. Cada día, registre en GB cuánto crecen sus datos.
4. Al final de su período de monitoreo, agregue los totales para cada día juntos, y luego divida por el número de días en su período de monitoreo.

Este cálculo genera la tasa media de crecimiento.

Ejemplo

En este ejemplo, necesita una LUN de 200 GB. Decide supervisar la LUN durante una semana y registrar los siguientes cambios diarios en sus datos:

- Domingo: 20 GB
- Lunes: 18 GB
- Martes: 17 GB
- Miércoles: 20 GB
- Jueves: 20 GB
- Viernes: 23 GB
- Sábado: 22 GB

En este ejemplo, la tasa de crecimiento es $(20+18+17+20+20+23+22) / 7 = 20$ GB al día.

Opción de configuración para archivos reservados espacio o LUN con volúmenes aprovisionados con thick-Provisioning

Esta combinación de configuración de volumen y archivo de FlexVol o LUN ofrece la capacidad de utilizar tecnologías de eficiencia del almacenamiento y no le requiere supervisar de forma activa el espacio libre, ya que se asigna suficiente espacio de antemano.

Las siguientes opciones de configuración son necesarias para configurar un archivo o LUN con espacio reservado en un volumen mediante el aprovisionamiento grueso:

| Ajuste del volumen | Valor |
|------------------------------------|--|
| Garantizado | Volumen |
| Reserva fraccionaria | 100 |
| Reserva de Snapshot | Cualquiera |
| Eliminación automática de Snapshot | Opcional |
| Crecimiento automático | Opcional; si está habilitado, el espacio libre del agregado debe supervisarse de forma activa. |

| Configuración de archivo o LUN | Valor |
|--------------------------------|----------|
| Reserva de espacio | Activado |

Configuración para archivos que no estén reservados espacio o LUN con volúmenes con thin provisioning

Esta combinación de configuración de volumen y archivo FlexVol o LUN requiere la cantidad más pequeña de almacenamiento que se asigne de antemano, pero requiere la

gestión activa del espacio libre para evitar errores debido a la falta de espacio.

Los siguientes ajustes de configuración son necesarios para configurar un LUN o archivos sin espacio reservado en un volumen con thin provisioning:

| Ajuste del volumen | Valor |
|------------------------------------|------------|
| Garantizado | Ninguno |
| Reserva fraccionaria | 0 |
| Reserva de Snapshot | Cualquiera |
| Eliminación automática de Snapshot | Opcional |
| Crecimiento automático | Opcional |

| Configuración de archivo o LUN | Valor |
|--------------------------------|---------------|
| Reserva de espacio | Deshabilitado |

Consideraciones adicionales

Cuando el volumen o el agregado se queda sin espacio, se puede producir un error en las operaciones de escritura en el archivo o la LUN.

Si no desea supervisar activamente el espacio libre tanto del volumen como del agregado, debe habilitar la fila automática para el volumen y establecer el tamaño máximo para el volumen en el tamaño del agregado. En esta configuración, se debe supervisar el espacio libre del agregado de forma activa, pero no es necesario supervisar el espacio libre del volumen.

Configuración para archivos reservados espacio o LUN con aprovisionamiento de volúmenes semigruesos

Esta combinación de configuración de volumen y archivo o LUN de FlexVol requiere que haya menos almacenamiento que la combinación completamente aprovisionada, pero impone restricciones sobre las tecnologías de eficiencia que se pueden utilizar para el volumen. Las sobrescrituras se realizan de acuerdo con el mejor esfuerzo posible para esta combinación de configuración.

Las siguientes opciones de configuración son necesarias para configurar un LUN con reserva de espacio en un volumen mediante el aprovisionamiento semi-grueso:

| Ajuste del volumen | Valor |
|----------------------|---------|
| Garantizado | Volumen |
| Reserva fraccionaria | 0 |

| Ajuste del volumen | Valor |
|------------------------------------|---|
| Reserva de Snapshot | 0 |
| Eliminación automática de Snapshot | Activado, con un nivel de compromiso de destrucción, una lista de destrucción que incluye todos los objetos, el activador establecido en volumen y todos los LUN y archivos FlexClone habilitados para la eliminación automática. |
| Crecimiento automático | Opcional; si está habilitado, el espacio libre del agregado debe supervisarse de forma activa. |

| Configuración de archivo o LUN | Valor |
|--------------------------------|----------|
| Reserva de espacio | Activado |

Restricciones tecnológicas

No se pueden usar las siguientes tecnologías de eficiencia del almacenamiento de volumen para esta combinación de configuración:

- Compresión
- Deduplicación
- Descarga de copias ODX y FlexClone
- LUN y archivos de FlexClone no marcados para eliminación automática (clones activos)
- Subarchivos FlexClone
- ODX/descarga de copias

Consideraciones adicionales

Al emplear esta combinación de configuración deben tenerse en cuenta los siguientes hechos:

- Cuando el volumen que admite que la LUN se ejecuta con poco espacio, se destruyen los datos de protección (LUN y archivos de FlexClone, copias Snapshot).
- Es posible que se agote el tiempo de espera de las operaciones de escritura y se produzca un error en ellas cuando el volumen se queda sin espacio libre.

De forma predeterminada, la compresión se habilita para las plataformas AFF. Debe deshabilitar explícitamente la compresión en cualquier volumen para el que desee utilizar aprovisionamiento de media en una plataforma AFF.

Protección de DATOS SAN

Información general sobre los métodos de protección de datos en entornos SAN

Puede proteger sus datos realizando copias de ellos para que estén disponibles para su restauración en caso de eliminación accidental, fallos en las aplicaciones, daños en los

datos o desastres. En función de sus necesidades de backup y protección de datos, ONTAP ofrece una variedad de métodos que le permiten proteger sus datos.

Continuidad del negocio de SnapMirror (SM-BC)

A partir de la disponibilidad general de ONTAP 9.9.1, proporciona un objetivo de tiempo de recuperación cero (objetivo de tiempo de recuperación nulo) o conmutación por error de aplicaciones transparente (TAF) para permitir la recuperación automática tras fallos de aplicaciones vitales para el negocio en entornos SAN. SM-BC requiere la instalación de ONTAP Mediator 1,2 en una configuración con dos clústeres AFF o dos clústeres de cabina SAN all-flash (ASA).

["Documentación de NetApp: Continuidad empresarial de SnapMirror"](#)

Copia Snapshot

Le permite crear, programar y mantener manualmente o de forma automática varios backups de sus LUN. Las copias Snapshot utilizan solo una cantidad mínima de espacio en el volumen adicional y no tienen ningún coste de rendimiento. Si sus datos de LUN se modifican o eliminan por error, esos datos pueden restaurarse de forma rápida y sencilla a partir de una de las copias Snapshot más recientes.

LUN de FlexClone (se requiere licencia de FlexClone)

Proporciona copias puntuales editables de otra LUN en un volumen activo o en una copia Snapshot. Un clon y su primario se pueden modificar de forma independiente sin que se vean afectados.

SnapRestore (se requiere licencia)

Le permite realizar una recuperación de datos bajo solicitud y rápida, que gestiona el espacio de manera eficiente desde copias Snapshot en todo un volumen. Puede utilizar SnapRestore para restaurar una LUN a un estado conservado anterior sin reiniciar el sistema de almacenamiento.

Copias de mirroring para la protección de datos (se requiere licencia de SnapMirror)

Ofrece recuperación ante desastres asíncrona, ya que le permite crear periódicamente copias Snapshot de los datos del volumen, copiar estas copias Snapshot a través de una red de área local o de área amplia a un volumen asociado, normalmente en otro clúster, y conservar dichas copias Snapshot. La copia reflejada del volumen de partner proporciona disponibilidad y restauración de datos desde el momento de la última copia de Snapshot, si los datos del volumen de origen se pierden o se dañan.

Backups de SnapVault (se requiere licencia de SnapMirror)

Ofrece un almacenamiento eficiente y retención de backups a largo plazo. Las relaciones de SnapVault permiten realizar un backup de las copias de Snapshot seleccionadas de los volúmenes en un volumen de destino y conservar los backups.

Si realiza backups a cinta y operaciones de archivado, puede ponerlas en marcha en los datos de los que ya se ha realizado un backup en el volumen secundario de SnapVault.

SnapDrive para Windows o UNIX (se requiere una licencia de SnapDrive)

Configura el acceso a las LUN, gestiona las LUN y gestiona las copias snapshot del sistema de almacenamiento directamente desde hosts de Windows o UNIX.

Backup y recuperación en cinta nativos

ONTAP admite la mayoría de las unidades de cinta existentes, así como un método para que los proveedores de cintas añadan dinámicamente soporte para nuevos dispositivos. ONTAP también es compatible con el protocolo de cinta magnética remota (RMT), lo que permite la copia de seguridad y la recuperación en cualquier sistema capaz.

Información relacionada

["Documentación de NetApp: SnapDrive para UNIX"](#)

["Documentación de NetApp: SnapDrive para Windows \(versiones actuales\)"](#)

["Protección de datos mediante backup en cinta"](#)

Efecto de mover o copiar una LUN en copias Snapshot

Efecto de mover o copiar una LUN en la información general sobre copias Snapshot

Las copias Snapshot se crean en el nivel de los volúmenes. Si copia o mueve una LUN a otro volumen, la política de copia de Snapshot del volumen de destino se aplica al volumen copiado o movido. Si no se establecen copias Snapshot para el volumen de destino, no se crearán copias Snapshot de la LUN movida o copiada.

Restaura un solo LUN de una copia Snapshot

Puede restaurar un único LUN a partir de una copia Snapshot sin restaurar todo el volumen que contiene la única LUN. Puede restaurar el LUN en su lugar o a una nueva ruta en el volumen. La operación restaura solo el LUN único sin que se vean afectados otros archivos o LUN del volumen. También puede restaurar archivos con secuencias.

Lo que necesitará

- Debe tener suficiente espacio en el volumen para completar la operación de restauración:
 - Si va a restaurar una LUN con la reserva de espacio donde la reserva fraccionaria es 0%, necesitará un tamaño más que el de la LUN restaurada.
 - Si va a restaurar una LUN con la reserva de espacio donde la reserva fraccionaria es del 100%, necesitará el doble del tamaño de la LUN restaurada.
 - Si va a restaurar una LUN que no tiene espacio reservado, solo necesita el espacio real utilizado para la LUN restaurada.
- Se debe haber creado una copia Snapshot de la LUN de destino.

Si la operación de restauración falla, es posible que la LUN de destino se trunque. En estos casos, puede usar la copia Snapshot para evitar la pérdida de datos.

- Se debe haber creado una copia Snapshot de la LUN de origen.

En raras ocasiones, la restauración de LUN puede generar un error y, con ello, la LUN de origen no se puede utilizar. Si esto sucede, puede usar la copia Snapshot para devolver la LUN al estado justo antes del intento de restauración.

- La LUN de destino y la LUN de origen deben tener el mismo tipo de SO.

Si la LUN de destino tiene un tipo de sistema operativo diferente de la LUN de origen, el host puede perder el acceso a los datos a la LUN de destino después de la operación de restauración.

Pasos

1. Desde el host, detenga todo el acceso del host a la LUN.
2. Desmonte la LUN en su host para que el host no pueda acceder a la LUN.
3. Desasigne la LUN:

```
lun mapping delete -vserver vserver_name -volume volume_name -lun lun_name  
-igroup igroup_name
```

4. Determine la copia Snapshot en la que desea restaurar la LUN:

```
volume snapshot show -vserver vserver_name -volume volume_name
```

5. Cree una copia Snapshot de la LUN antes de restaurar la LUN:

```
volume snapshot create -vserver vserver_name -volume volume_name -snapshot  
snapshot_name
```

6. Restaure el LUN especificado en un volumen:

```
volume snapshot restore-file -vserver vserver_name -volume volume_name  
-snapshot snapshot_name -path lun_path
```

7. Siga los pasos de la pantalla.
8. Si es necesario, conectar la LUN:

```
lun modify -vserver vserver_name -path lun_path -state online
```

9. Si es necesario, reasigne la LUN:

```
lun mapping create -vserver vserver_name -volume volume_name -lun lun_name  
-igroup igroup_name
```

10. Desde el host, vuelva a montar la LUN.
11. Desde el host, reinicie el acceso a la LUN.

Restaure todas las LUN de un volumen a partir de una copia Snapshot

Puede utilizar `volume snapshot restore` Comando para restaurar todas las LUN de un volumen especificado desde una copia Snapshot.

Pasos

1. Desde el host, detenga todo el acceso del host a las LUN.

El uso de SnapRestore sin detener todo el acceso de host a las LUN del volumen puede provocar daños en los datos y errores del sistema.

2. Desmonte las LUN de ese host para que el host no pueda acceder a las LUN.

3. Desasigne sus LUN:

```
lun mapping delete -vserver vserver_name -volume volume_name -lun lun_name  
-igroup igroup_name
```

4. Para determinar la copia Snapshot en la que desea restaurar el volumen:

```
volume snapshot show -vserver vserver_name -volume volume_name
```

5. Cambie la configuración de privilegios a avanzada:

```
set -privilege advanced
```

6. Restaure sus datos:

```
volume snapshot restore -vserver vserver_name -volume volume_name -snapshot  
snapshot_name
```

7. Siga las instrucciones que aparecen en pantalla.

8. Reasigne sus LUN:

```
lun mapping create -vserver vserver_name -volume volume_name -lun lun_name  
-igroup igroup_name
```

9. Compruebe que sus LUN están en línea:

```
lun show -vserver vserver_name -path lun_path -fields state
```

10. Si sus LUN no están en línea, conectarlos:

```
lun modify -vserver vserver_name -path lun_path -state online
```

11. Cambie la configuración de privilegio a admin:

```
set -privilege admin
```

12. Desde el host, vuelva a montar las LUN.

13. Desde el host, reinicie el acceso a sus LUN.

Elimine una o más copias Snapshot existentes de un volumen

Puede eliminar manualmente una o varias copias Snapshot existentes del volumen. Se recomienda hacerlo si se necesita más espacio en el volumen.

Pasos

1. Utilice la `volume snapshot show` Comando para verificar qué copias de Snapshot desea eliminar.

```
cluster::> volume snapshot show -vserver vs3 -volume vol3
```

| Vserver | Volume | Snapshot | Size | ---Blocks--- | |
|---------|--------|-----------------------|-------|--------------|-------|
| | | | | Total% | Used% |
| vs3 | vol3 | | | | |
| | | snap1.2013-05-01_0015 | 100KB | 0% | 38% |
| | | snap1.2013-05-08_0015 | 76KB | 0% | 32% |
| | | snap2.2013-05-09_0010 | 76KB | 0% | 32% |
| | | snap2.2013-05-10_0010 | 76KB | 0% | 32% |
| | | snap3.2013-05-10_1005 | 72KB | 0% | 31% |
| | | snap3.2013-05-10_1105 | 72KB | 0% | 31% |
| | | snap3.2013-05-10_1205 | 72KB | 0% | 31% |
| | | snap3.2013-05-10_1305 | 72KB | 0% | 31% |
| | | snap3.2013-05-10_1405 | 72KB | 0% | 31% |
| | | snap3.2013-05-10_1505 | 72KB | 0% | 31% |

10 entries were displayed.

2. Utilice la `volume snapshot delete` Comando para eliminar copias Snapshot.

| Si desea... | Introduzca este comando... |
|-----------------------------------|---|
| Elimine una sola copia Snapshot | <code>volume snapshot delete -vserver svm_name -volume vol_name -snapshot snapshot_name</code> |
| Elimine varias copias Snapshot | <code>volume snapshot delete -vserver svm_name -volume vol_name -snapshot snapshot_name1[, snapshot_name2,...]</code> |
| Elimine todas las copias Snapshot | <code>volume snapshot delete -vserver svm_name -volume vol_name -snapshot *</code> |

En el siguiente ejemplo se eliminan todas las copias Snapshot del volumen vol3.

```
cluster::> volume snapshot delete -vserver vs3 -volume vol3 *
```

10 entries were acted on.

Use LUN FlexClone para proteger sus datos

Use LUN FlexClone para proteger la descripción general de sus datos

Una LUN FlexClone es una copia puntual modificable de otra LUN en un volumen activo

o en una copia Snapshot. El clon y su primario se pueden modificar de forma independiente sin que se vean afectados.

Una LUN FlexClone comparte espacio inicialmente con su LUN principal. De forma predeterminada, la LUN FlexClone hereda el atributo de espacio reservado de la LUN principal. Por ejemplo, si la LUN principal no está reservada a espacio, la LUN FlexClone también está sin la reserva de espacio de forma predeterminada. Sin embargo, puede crear una LUN FlexClone sin reservar espacio desde un elemento principal que es una LUN con reserva de espacio.

Cuando se clona una LUN, el uso compartido de bloques se produce en segundo plano y no se puede crear una copia de Snapshot de volumen hasta que haya finalizado el uso compartido de bloques.

Debe configurar el volumen para habilitar la función de eliminación automática de LUN de FlexClone con el `volume snapshot autodelete modify` comando. De lo contrario, si desea que las LUN de FlexClone se eliminen automáticamente pero el volumen no está configurado para la eliminación automática de FlexClone, no se elimina ninguna de las LUN de FlexClone.

Al crear una LUN de FlexClone, la función de eliminación automática de la LUN de FlexClone está deshabilitada de manera predeterminada. Debe habilitarla manualmente en cada LUN de FlexClone antes de que esa LUN de FlexClone se pueda eliminar de forma automática. Si utiliza aprovisionamiento de volúmenes semigruesos y desea obtener la garantía de escritura «mejor esfuerzo» proporcionada por esta opción, debe poner a disposición LUN de `all` FlexClone para su eliminación automática.



Cuando crea una LUN de FlexClone a partir de una copia Snapshot, la LUN se divide automáticamente de la copia Snapshot con un proceso en segundo plano con gestión eficiente del espacio, de modo que la LUN no siga dependiendo de la copia Snapshot o consuma espacio adicional. Si no ha finalizado esta división en segundo plano y esta copia snapshot se elimina automáticamente, esa LUN de FlexClone se elimina aunque haya deshabilitado la función de eliminación automática de FlexClone para esa LUN de FlexClone. Una vez finalizada la división en segundo plano, la LUN de FlexClone no se elimina ni siquiera si se elimina esa copia snapshot.

Información relacionada

["Gestión de almacenamiento lógico"](#)

Razones para utilizar LUN de FlexClone

Puede utilizar las LUN FlexClone para crear varias copias de lectura/escritura de una LUN.

Se recomienda hacerlo por los siguientes motivos:

- Debe crear una copia temporal de una LUN para fines de pruebas.
- Debe realizar una copia de sus datos disponibles a usuarios adicionales sin tener que darles acceso a los datos de producción.
- Desea crear un clon de una base de datos para operaciones de manipulación y proyección, al mismo tiempo que se conservan los datos originales sin alterarlos.
- Desea acceder a un subconjunto específico de los datos de una LUN (un volumen lógico o un sistema de archivos específicos de un grupo de volúmenes, O un archivo específico o un conjunto de archivos en un sistema de archivos) y cópielos en la LUN original, sin restaurar el resto de datos de la LUN original. Esto funciona en sistemas operativos que son compatibles con el montaje de las LUN y un clon de la LUN al mismo tiempo. SnapDrive para UNIX lo admite con el `snap connect` comando.

- Necesita varios hosts DE arranque SAN con el mismo sistema operativo.

Cómo un volumen de FlexVol puede reclamar espacio libre con la configuración de eliminación automática

Puede activar la configuración de eliminación automática de un volumen FlexVol para eliminar automáticamente archivos FlexClone y LUN FlexClone. Al habilitar la eliminación automática, se puede recuperar una cantidad de espacio libre objetivo en el volumen cuando un volumen está casi lleno.

Puede configurar un volumen para que comience a eliminar automáticamente archivos FlexClone y LUN FlexClone cuando el espacio libre en el volumen disminuya por debajo de un valor de umbral determinado y deje de eliminar automáticamente clones cuando se reclame una cantidad de espacio libre objetivo en el volumen. Aunque, no puede especificar el valor de umbral que inicia la eliminación automática de clones, puede especificar si un clon es apto para su eliminación y puede especificar la cantidad de espacio libre objetivo para un volumen.

Un volumen elimina automáticamente los archivos FlexClone y las LUN FlexClone cuando el espacio libre en el volumen disminuye por debajo de un umbral determinado y cuando se cumplen los siguientes requisitos:

- La función de eliminación automática está habilitada para el volumen que contiene los archivos FlexClone y las LUN FlexClone.

Para habilitar la funcionalidad de eliminación automática para un volumen de FlexVol, se puede usar la `volume snapshot autodelete modify` comando. Debe configurar el `-trigger` parámetro a `volume 0. snap_reserve` Para que un volumen elimine automáticamente archivos FlexClone y LUN FlexClone.

- La función de eliminación automática está activada para los archivos de FlexClone y las LUN de FlexClone.

Puede activar la eliminación automática para un archivo FlexClone o una LUN FlexClone mediante el `file clone create` con el `-autodelete` parámetro. Como resultado, puede conservar algunos archivos FlexClone y LUN FlexClone deshabilitando la eliminación automática de los clones y asegurándose de que otras opciones de configuración del volumen no anulen la configuración del clon.

Configurar un volumen FlexVol para que elimine automáticamente archivos FlexClone y LUN FlexClone

Es posible habilitar un volumen FlexVol para eliminar automáticamente archivos de FlexClone y LUN FlexClone con la eliminación automática habilitada cuando el espacio libre en el volumen disminuye por debajo de un umbral en particular.

Lo que necesitará

- El volumen FlexVol debe contener archivos FlexClone y LUN FlexClone, y debe estar en línea.
- El volumen FlexVol no debe ser un volumen de solo lectura.

Pasos

1. Permita la eliminación automática de archivos de FlexClone y LUN de FlexClone en el volumen de FlexVol mediante el `volume snapshot autodelete modify` comando.
 - Para la `-trigger` parámetro, puede especificar `volume 0. snap_reserve`.

- Para la `-destroy-list` parámetro, debe especificar siempre `lun_clone,file_clone` independientemente de si desea eliminar solo un tipo de clon.

El siguiente ejemplo muestra cómo puede habilitar volume vol1 para activar la eliminación automática de archivos FlexClone y LUN de FlexClone para la reclamación de espacio hasta que el 25% del volumen esté compuesto por espacio libre:

```
cluster1::> volume snapshot autodelete modify -vserver vs1 -volume  
vol1 -enabled true -commitment disrupt -trigger volume -target-free  
-space 25 -destroy-list lun_clone,file_clone  
  
Volume modify successful on volume:vol1
```



Al habilitar la eliminación automática de volúmenes de FlexVol, si establece el valor de `-commitment` parámetro a `destroy`, Todos los archivos FlexClone y las LUN FlexClone con `-autodelete` parámetro establecido en `true` puede eliminarse cuando el espacio libre en el volumen disminuya por debajo del valor de umbral especificado. Sin embargo, los archivos FlexClone y las LUN FlexClone con el `-autodelete` parámetro establecido en `false` no se eliminará.

2. Compruebe que la eliminación automática de archivos FlexClone y LUN de FlexClone está activada en el volumen de FlexVol mediante el `volume snapshot autodelete show` comando.

El siguiente ejemplo muestra que el volumen vol1 está activado para la eliminación automática de archivos FlexClone y LUN FlexClone:

```
cluster1::> volume snapshot autodelete show -vserver vs1 -volume vol1  
  
Vserver Name: vs1  
Volume Name: vol1  
Enabled: true  
Commitment: disrupt  
Defer Delete: user_created  
Delete Order: oldest_first  
Defer Delete Prefix: (not specified)*  
Target Free Space: 25%  
Trigger: volume  
Destroy List: lun_clone,file_clone  
Is Constituent Volume: false
```

3. Asegúrese de que la eliminación automática esté habilitada para los archivos de FlexClone y las LUN FlexClone del volumen que desea eliminar siguiendo estos pasos:
 - a. Permitir la eliminación automática de un archivo FlexClone o una LUN FlexClone concretos mediante el `volume file clone autodelete` comando.

Puede forzar la eliminación automática de un archivo FlexClone o una LUN de FlexClone mediante la

volume file clone autodelete con el `-force` parámetro.

El ejemplo siguiente muestra que la eliminación automática de la LUN de FlexClone `lun1_clone` contenida en el volumen `vol1` está habilitada:

```
cluster1:> volume file clone autodelete -vserver vs1 -clone-path  
/vol/vol1/lun1_clone -enabled true
```

Puede activar la eliminación automática cuando crea archivos FlexClone y LUN de FlexClone.

- b. Compruebe que el archivo FlexClone o la LUN de FlexClone están activados para eliminación automática mediante la `volume file clone show-autodelete` comando.

El ejemplo siguiente muestra que la LUN de FlexClone `lun1_clone` está habilitada para eliminación automática:

```
cluster1:> volume file clone show-autodelete -vserver vs1 -clone  
-path vol/vol1/lun1_clone  
  
Name: vs1  
Path: vol/vol1/lun1_clone  
  
**Autodelete Enabled: true**
```

Para obtener más información acerca del uso de los comandos, consulte las páginas man correspondientes.

Clonar las LUN de un volumen activo

Para crear copias de sus LUN, debe clonar las LUN en el volumen activo. Estas LUN FlexClone son copias legibles y editables de las LUN originales en el volumen activo.

Lo que necesitará

Debe instalar una licencia de FlexClone. Esta licencia se incluye con ["ONTAP One"](#).

Acerca de esta tarea

Un LUN FlexClone con reserva de espacio requiere tanto espacio como la LUN principal con reserva de espacio. Si la LUN FlexClone no está reservada para el espacio, debe asegurarse de que el volumen tenga suficiente espacio para acomodar los cambios en la LUN FlexClone.

Pasos

1. Debe haber verificado que las LUN no están asignadas a un igroup o que se escriben en antes de crear el clon.
2. Utilice la `lun show` Comando para comprobar que la LUN existe.

```
lun show -vserver vs1
```

| Vserver | Path | State | Mapped | Type | Size |
|---------|----------------|--------|----------|---------|---------|
| vs1 | /vol/vol1/lun1 | online | unmapped | windows | 47.07MB |

3. Utilice la `volume file clone create` Comando para crear la LUN FlexClone.

```
volume file clone create -vserver vs1 -volume vol1 -source-path lun1
-destination-path/lun1_clone
```

Si necesita que la LUN de FlexClone esté disponible para su eliminación automática, tendrá que incluir `-autodelete true`. Si crea este LUN FlexClone en un volumen mediante el aprovisionamiento semi-grueso, debe habilitar la eliminación automática para todas las LUN de FlexClone.

4. Utilice la `lun show` Comando para verificar que ha creado una LUN.

```
lun show -vserver vs1
```

| Vserver | Path | State | Mapped | Type | Size |
|---------|----------------------|--------|----------|---------|---------|
| vs1 | /vol/volX/lun1 | online | unmapped | windows | 47.07MB |
| vs1 | /vol/volX/lun1_clone | online | unmapped | windows | 47.07MB |

Crear LUN FlexClone a partir de una copia snapshot en un volumen

Puede usar una copia snapshot del volumen para crear copias FlexClone de las LUN. Las copias FlexClone de las LUN son legibles y editables.

Lo que necesitará

Debe instalar una licencia de FlexClone. Esta licencia se incluye con ["ONTAP One"](#).

Acerca de esta tarea

La LUN FlexClone hereda el atributo de reservas de espacio de la LUN principal. Un LUN FlexClone con reserva de espacio requiere tanto espacio como la LUN principal con reserva de espacio. Si la LUN FlexClone no está reservada para el espacio, el volumen debe tener espacio suficiente para acomodar los cambios en el clon.

Pasos

1. Compruebe que la LUN no está asignada ni se está escribiendo en.
2. Cree una copia Snapshot del volumen que contenga las LUN:

```
volume snapshot create -vserver vserver_name -volume volume_name -snapshot
snapshot_name
```

Debe crear una copia Snapshot (la copia Snapshot que realiza la copia) de la LUN que desea clonar.

3. Cree la LUN FlexClone a partir de la copia Snapshot:

```
file clone create -vserver vserver_name -volume volume_name -source-path
source_path -snapshot-name snapshot_name -destination-path destination_path
```

Si necesita que la LUN de FlexClone esté disponible para su eliminación automática, tendrá que incluir `-autodelete true`. Si crea este LUN FlexClone en un volumen mediante el aprovisionamiento semi-grueso, debe habilitar la eliminación automática para todas las LUN de FlexClone.

4. Compruebe que la LUN de FlexClone es correcta:

```
lun show -vserver vserver_name
```

| Vserver | Path | State | Mapped | Type | Size |
|---------|---------------------------|--------|----------|---------|---------|
| vs1 | /vol/vol1/lun1_clone | online | unmapped | windows | 47.07MB |
| vs1 | /vol/vol1/lun1_snap_clone | online | unmapped | windows | 47.07MB |

Evitar que se elimine automáticamente un archivo FlexClone o una LUN de FlexClone específica

Si configura un volumen FlexVol para eliminar automáticamente archivos FlexClone y LUN FlexClone, es posible eliminar cualquier clon que se ajuste a los criterios que especifique. Si tiene archivos FlexClone o LUN FlexClone específicos que desea conservar, puede excluirlos del proceso automático de eliminación de FlexClone.

Lo que necesitará

Debe instalar una licencia de FlexClone. Esta licencia se incluye con ["ONTAP One"](#).

Acerca de esta tarea

Cuando se crea un archivo FlexClone o una LUN de FlexClone, se deshabilita de forma predeterminada la configuración de eliminación automática del clon. Los archivos FlexClone y las LUN FlexClone con eliminación automática desactivada se conservan cuando se configura un volumen FlexVol para eliminar automáticamente los clones para reclamar espacio en el volumen.



Si establece la `commitment` nivele el volumen a `try` o `disrupt`, Puede conservar de forma individual archivos de FlexClone o LUN de FlexClone desactivando la eliminación automática de dichos clones. Sin embargo, si establece la `commitment` nivele el volumen a `destroy` y las listas de destrucción incluyen `lun_clone`, `file_clone`, La configuración de volumen anula la configuración de clon y todos los archivos FlexClone y las LUN FlexClone se pueden eliminar independientemente de la configuración de eliminación automática de los clones.

Pasos

1. Evite que un archivo FlexClone o una LUN de FlexClone específicos se eliminen automáticamente mediante el `volume file clone autodelete` comando.

El ejemplo siguiente muestra cómo puede deshabilitar la eliminación automática para FlexClone LUN `lun1_clone` contenido en `vol1`:

```
cluster1::> volume file clone autodelete -vserver vs1 -volume vol1  
-clone-path lun1_clone -enable false
```

No se puede eliminar automáticamente un archivo FlexClone o una LUN FlexClone con la eliminación automática para reclamar espacio en el volumen.

2. Compruebe que la eliminación automática está deshabilitada para el archivo FlexClone o la LUN FlexClone mediante el `volume file clone show-autodelete` comando.

El ejemplo siguiente muestra que la eliminación automática es falsa para la LUN FlexClone `lun1_clone`:

```
cluster1::> volume file clone show-autodelete -vserver vs1 -clone-path  
vol/vol1/lun1_clone  
  
Name: vs1  
vol/vol1/lun1_clone  
Enabled: false  
  
Vserver  
Clone Path:  
Autodelete
```

Configuración y uso de backups de SnapVault en un entorno SAN

Configuración y uso de los backups de SnapVault en una descripción general del entorno SAN

La configuración y el uso de SnapVault en un entorno SAN son muy similares a la configuración y el uso en un entorno NAS, pero para restaurar las LUN en un entorno SAN se requieren procedimientos especiales.

Los backups de SnapVault contienen un conjunto de copias de solo lectura de un volumen de origen. En un entorno SAN, siempre realiza un backup de volúmenes completos en el volumen secundario de SnapVault, no de LUN individuales.

El procedimiento para crear e inicializar la relación de SnapVault entre un volumen primario que contiene LUN y un volumen secundario que actúa como un backup de SnapVault es idéntico al procedimiento utilizado con los volúmenes FlexVol utilizados para protocolos de archivos. Este procedimiento se describe detalladamente en ["Protección de datos"](#).

Es importante garantizar que las LUN de las que se realiza el backup tengan un estado coherente antes de que se creen y copien al volumen secundario de SnapVault. Automatizar la creación de copias Snapshot con SnapCenter garantiza que la aplicación original pueda usar las LUN de backup.

Existen tres opciones básicas para restaurar LUN a partir de un volumen secundario de SnapVault:

- Puede asignar un LUN directamente desde el volumen secundario de SnapVault y conectar un host a la LUN para acceder al contenido de dicha LUN.

La LUN es de solo lectura y solo se puede asignar de la copia Snapshot más reciente en el backup de SnapVault. Se pierden las reservas persistentes y otros metadatos de los LUN. Si lo desea, puede utilizar

un programa de copia en el host para copiar el contenido de la LUN nuevamente en la LUN original si aún está accesible.

La LUN tiene un número de serie diferente a la LUN de origen.

- Es posible clonar cualquier copia Snapshot en el volumen secundario SnapVault en un nuevo volumen de lectura y escritura.

A continuación, puede asignar cualquiera de las LUN del volumen y conectar un host a la LUN para acceder al contenido del LUN. Si lo desea, puede utilizar un programa de copia en el host para copiar el contenido de la LUN nuevamente en la LUN original si aún está accesible.

- Puede restaurar todo el volumen que contiene el LUN desde cualquier copia Snapshot en el volumen secundario de SnapVault.

La restauración de todo el volumen sustituye a todas las LUN y todos los archivos del volumen. Se pierden todas las nuevas LUN creadas desde que se creó la copia Snapshot.

Las LUN conservan su asignación, números de serie, UUID y reservas persistentes.

Acceda a una copia de LUN de solo lectura desde un backup de SnapVault

Puede acceder a una copia de solo lectura de una LUN de la última copia de Snapshot de un backup de SnapVault. El ID de LUN, la ruta y el número de serie son diferentes de la LUN de origen y deben asignarse primero. Las reservas persistentes, las asignaciones de LUN y los iGroups no se replican en el volumen secundario de SnapVault.

Lo que necesitará

- Debe inicializarse la relación de SnapVault y la última copia Snapshot del volumen secundario de SnapVault debe contener la LUN deseada.
- La máquina virtual de almacenamiento (SVM) que contiene el backup de SnapVault debe tener una o varias LIF con el protocolo SAN deseado accesible desde el host utilizado para acceder a la copia de LUN.
- Si piensa acceder a las copias de LUN directamente desde el volumen secundario de SnapVault, debe crear los iGroups en la SVM de SnapVault con antelación.

Es posible acceder a un LUN directamente desde el volumen secundario de SnapVault sin tener que restaurar o clonar primero el volumen que contiene la LUN.

Acerca de esta tarea

Si una nueva copia Snapshot se añade al volumen secundario SnapVault mientras tiene una LUN asignada de una copia Snapshot anterior, el contenido de la LUN asignada cambia. La LUN sigue asignada con los mismos identificadores, pero los datos se toman de la nueva copia Snapshot. Si cambia el tamaño de LUN, algunos hosts detectan automáticamente el cambio de tamaño; los hosts Windows requieren que se vuelva a analizar el disco para recoger cualquier cambio de tamaño.

Pasos

1. Ejecute el `lun show` Comando para enumerar los LUN disponibles en el volumen secundario de SnapVault.

En este ejemplo, puede ver tanto las LUN originales en el volumen primario srcvola como las copias en el volumen secundario de SnapVault dstvolB:


```
cluster::> lun show
```

| Vserver | Path | State | Mapped | Type | Size |
|----------|--------------------|--------|----------|---------|---------|
| ----- | ----- | ----- | ----- | ----- | ----- |
| vserverA | /vol/srcvolA/lun_A | online | mapped | windows | 300.0GB |
| vserverA | /vol/srcvolA/lun_B | online | mapped | windows | 300.0GB |
| vserverA | /vol/srcvolA/lun_C | online | mapped | windows | 300.0GB |
| vserverB | /vol/dstvolB/lun_A | online | unmapped | windows | 300.0GB |
| vserverB | /vol/dstvolB/lun_B | online | unmapped | windows | 300.0GB |
| vserverB | /vol/dstvolB/lun_C | online | unmapped | windows | 300.0GB |

```
6 entries were displayed.
```

2. Si el igroup del host deseado no existe en la SVM que contiene el volumen secundario de SnapVault, ejecute el `igroup create` comando para crear un igroup.

Este comando crea un igroup para un host Windows que utiliza el protocolo iSCSI:

```
cluster::> igroup create -vserver vserverB -igroup temp_igroup  
-protocol iscsi -ostype windows  
-initiator iqn.1991-05.com.microsoft:hostA
```

3. Ejecute el `lun mapping create` Comando para asignar la copia LUN deseada al igroup.

```
cluster::> lun mapping create -vserver vserverB -path /vol/dstvolB/lun_A  
-igroup temp_igroup
```

4. Conecte el host a la LUN y acceda al contenido de la LUN como desee.

Restaurar un solo LUN a partir de un backup de SnapVault

Es posible restaurar un solo LUN a una nueva ubicación o a la ubicación original. Puede restaurar desde cualquier copia Snapshot en el volumen secundario de SnapVault. Para restaurar la LUN en la ubicación original, primero debe restaurarla en una nueva ubicación y, a continuación, copiarla.

Lo que necesitará

- Debe inicializarse la relación de SnapVault, y el volumen secundario de SnapVault debe contener una copia Snapshot adecuada para restaurar.
- La máquina virtual de almacenamiento (SVM) que contiene el volumen secundario de SnapVault debe tener una o más LIF con el protocolo SAN deseado a los que se puede acceder desde el host que se utiliza para acceder a la copia de LUN.
- Los iGroups ya deben existir en la SVM de SnapVault.

Acerca de esta tarea

El proceso incluye crear un clon de volumen de lectura y escritura a partir de una copia Snapshot en el volumen secundario de SnapVault. Puede utilizar la LUN directamente desde el clon, o bien puede copiar de nuevo el contenido de la LUN a su ubicación original.

La LUN del clon tiene una ruta y un número de serie diferentes a la LUN original. No se conservan las reservas persistentes.

Pasos

- 1. Ejecute el `snapmirror show` Comando para verificar el volumen secundario que contiene el backup de SnapVault.

```
cluster::> snapmirror show
```

| Source Path | Type | Dest Path | Mirror State | Relation Status | Total Progress | Healthy | Last Updated |
|------------------|------|------------------|--------------|-----------------|----------------|---------|--------------|
| vserverA:srcvolA | XDP | vserverB:dstvolB | Snapmirrored | Idle | - | true | - |

- 2. Ejecute el `volume snapshot show` Comando para identificar la copia Snapshot desde la que desea restaurar la LUN.

```
cluster::> volume snapshot show
```

| Vserver | Volume | Snapshot | State | Size | Total% | Used% |
|----------|---------|-----------------------|-------|-------|--------|-------|
| vserverB | dstvolB | snap2.2013-02-10_0010 | valid | 124KB | 0% | 0% |
| | | snap1.2013-02-10_0015 | valid | 112KB | 0% | 0% |
| | | snap2.2013-02-11_0010 | valid | 164KB | 0% | 0% |

- 3. Ejecute el `volume clone create` Comando para crear un clon de lectura y escritura a partir de la copia Snapshot que desea.

El clon de volumen se crea en el mismo agregado que el backup de SnapVault. Debe haber suficiente espacio en el agregado para almacenar el clon.

```
cluster::> volume clone create -vserver vserverB
    -flexclone dstvolB_clone -type RW -parent-volume dstvolB
    -parent-snapshot daily.2013-02-10_0010
[Job 108] Job succeeded: Successful
```

4. Ejecute el `lun show` Comando para mostrar las LUN del clon del volumen.

```
cluster::> lun show -vserver vserverB -volume dstvolB_clone
```

| Vserver | Path | State | Mapped | Type |
|----------|--------------------------|--------|----------|---------|
| vserverB | /vol/dstvolB_clone/lun_A | online | unmapped | windows |
| vserverB | /vol/dstvolB_clone/lun_B | online | unmapped | windows |
| vserverB | /vol/dstvolB_clone/lun_C | online | unmapped | windows |

3 entries were displayed.

5. Si el `igroup` del host deseado no existe en la SVM que contiene el backup de SnapVault, ejecute el `igroup create` comando para crear un `igroup`.

En este ejemplo, se crea un `igroup` para un host Windows que utiliza el protocolo iSCSI:

```
cluster::> igroup create -vserver vserverB -igroup temp_igroup  
-protocol iscsi -ostype windows  
-initiator iqn.1991-05.com.microsoft:hostA
```

6. Ejecute el `lun mapping create` Comando para asignar la copia LUN deseada al `igroup`.

```
cluster::> lun mapping create -vserver vserverB  
-path /vol/dstvolB_clone/lun_C -igroup temp_igroup
```

7. Conecte el host a la LUN y acceda al contenido de la LUN, según lo desee.

La LUN es de lectura y escritura y se puede utilizar en lugar de la LUN original. Dado que el número de serie de la LUN es diferente, el host lo interpreta como un LUN diferente al original.

8. Use un programa de copia en el host para copiar el contenido de la LUN nuevamente en la LUN original.

Restaurar todos los LUN de un volumen a partir de un backup de SnapVault

Si necesita restaurar uno o varios LUN de un volumen desde un backup de SnapVault, puede restaurar el volumen completo. La restauración del volumen afecta a todos los LUN del volumen.

Lo que necesitará

Debe inicializarse la relación de SnapVault, y el volumen secundario de SnapVault debe contener una copia Snapshot adecuada para restaurar.

Acerca de esta tarea

Si se restaura un volumen completo, este volverá al estado que tenía cuando se hizo la copia Snapshot. Si se agregó una LUN al volumen después de la copia Snapshot, esa LUN se elimina durante el proceso de

restauración.

Después de restaurar el volumen, las LUN siguen asignadas a los iGroups a los que se asignaron justo antes de la restauración. La asignación de LUN puede ser diferente del mapa en el momento de la copia Snapshot. Se conservan las reservas persistentes en los LUN de clústeres de hosts.

Pasos

- 1. Detenga las operaciones de I/o en todos los LUN del volumen.
- 2. Ejecute el `snapmirror show` Comando para verificar el volumen secundario que contiene el volumen secundario de SnapVault.

```
cluster::> snapmirror show
```

| Source Path | Type | Dest Path | Mirror State | Relation Status | Total Progress | Healthy | Last Updated |
|------------------|------|------------------|--------------|-----------------|----------------|---------|--------------|
| vserverA:srcvolA | XDP | vserverB:dstvolB | Snapmirrored | Idle | - | true | - |

- 3. Ejecute el `volume snapshot show` Comando para identificar la copia Snapshot desde la que desea restaurar.

```
cluster::> volume snapshot show
```

| Vserver | Volume | Snapshot | State | Size | Total% | Used% |
|----------|---------|-----------------------|-------|-------|--------|-------|
| vserverB | dstvolB | snap2.2013-02-10_0010 | valid | 124KB | 0% | 0% |
| | | snap1.2013-02-10_0015 | valid | 112KB | 0% | 0% |
| | | snap2.2013-02-11_0010 | valid | 164KB | 0% | 0% |

- 4. Ejecute el `snapmirror restore` y especifique el `-source-snapshot` Opción para especificar la copia Snapshot que se usará.

El destino que se especifica para la restauración es el volumen original al que se va a restaurar.

```
cluster::> snapmirror restore -destination-path vserverA:srcvolA
        -source-path vserverB:dstvolB -source-snapshot daily.2013-02-10_0010

Warning: All data newer than Snapshot copy hourly.2013-02-11_1205 on
volume vserverA:src_volA will be deleted.
Do you want to continue? {y|n}: y
[Job 98] Job is queued: snapmirror restore from source
"vserverB:dstvolB" for the snapshot daily.2013-02-10_0010.
```

5. Si va a compartir LUN en un clúster de hosts, restaure las reservas persistentes en los LUN de los hosts afectados.

Restaurar un volumen a partir de un backup de SnapVault

En el siguiente ejemplo, la LUN llamada lun_D se agregó al volumen después de crear la copia Snapshot. Después de restaurar todo el volumen a partir de la copia Snapshot, lun_D ya no aparece.

En la `lun show` Resultado del comando, puede ver las LUN en el srcvolA del volumen primario y las copias de solo lectura de esas LUN en el volumen secundario de SnapVault dstvolB. No hay copia de lun_D en el backup de SnapVault.

```
cluster::> lun show
```

| Vserver | Path | State | Mapped | Type | Size |
|----------|--------------------|--------|----------|---------|---------|
| vserverA | /vol/srcvolA/lun_A | online | mapped | windows | 300.0GB |
| vserverA | /vol/srcvolA/lun_B | online | mapped | windows | 300.0GB |
| vserverA | /vol/srcvolA/lun_C | online | mapped | windows | 300.0GB |
| vserverA | /vol/srcvolA/lun_D | online | mapped | windows | 250.0GB |
| vserverB | /vol/dstvolB/lun_A | online | unmapped | windows | 300.0GB |
| vserverB | /vol/dstvolB/lun_B | online | unmapped | windows | 300.0GB |
| vserverB | /vol/dstvolB/lun_C | online | unmapped | windows | 300.0GB |

7 entries were displayed.

```
cluster::> snapmirror restore -destination-path vserverA:srcvolA
-source-path vserverB:dstvolB
-source-snapshot daily.2013-02-10_0010
```

Warning: All data newer than Snapshot copy hourly.2013-02-11_1205 on volume vserverA:src_volA will be deleted.

Do you want to continue? {y|n}: y

[Job 98] Job is queued: snapmirror restore from source "vserverB:dstvolB" for the snapshot daily.2013-02-10_0010.

```
cluster::> lun show
```

| Vserver | Path | State | Mapped | Type | Size |
|----------|--------------------|--------|----------|---------|---------|
| vserverA | /vol/srcvolA/lun_A | online | mapped | windows | 300.0GB |
| vserverA | /vol/srcvolA/lun_B | online | mapped | windows | 300.0GB |
| vserverA | /vol/srcvolA/lun_C | online | mapped | windows | 300.0GB |
| vserverB | /vol/dstvolB/lun_A | online | unmapped | windows | 300.0GB |
| vserverB | /vol/dstvolB/lun_B | online | unmapped | windows | 300.0GB |
| vserverB | /vol/dstvolB/lun_C | online | unmapped | windows | 300.0GB |

6 entries were displayed.

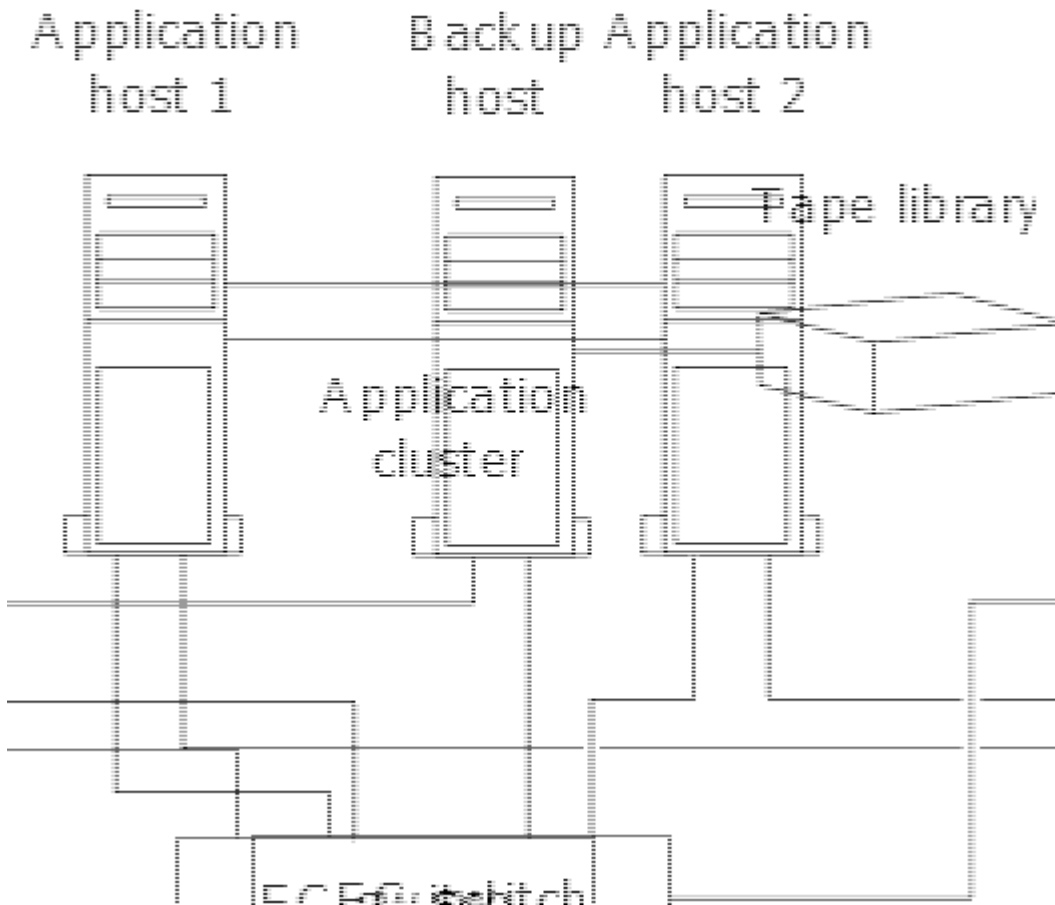
Una vez que se restaura el volumen secundario del SnapVault, el volumen de origen ya no contiene lun_D. No es necesario volver a asignar las LUN en el volumen de origen después de la restauración porque estas se siguen asignando.

Cómo se puede conectar un sistema de backup de host al sistema de almacenamiento primario

Se puede lanzar backups de sistemas SAN a cinta a través de un host de backup independiente para evitar que el rendimiento se resienta en el host de aplicaciones.

Es imprescindible mantener separados los datos DE SAN y NAS con fines de backup. La siguiente figura

muestra la configuración física recomendada para un sistema de backup host al sistema de almacenamiento principal. Debe configurar los volúmenes como solo SAN. Las LUN pueden quedar limitadas a un único volumen o las LUN pueden propagarse por varios volúmenes o sistemas de almacenamiento.



Los volúmenes de un host pueden consistir en una única LUN asignada desde el sistema de almacenamiento o de varias LUN mediante un gestor de volúmenes, como VxVM en sistemas HP-UX.

Realice un backup de una LUN a través de un sistema de backup del host

Es posible usar un LUN clonado de una copia Snapshot como datos de origen para el sistema de backup host.

Lo que necesitará

Debe haber una LUN de producción y asignarse a un igroup que incluya el nombre de nodo WWPN o iniciador del servidor de aplicaciones. La LUN también se debe formatear y es accesible para el host

Pasos

1. Guarde el contenido de los búferes del sistema de archivos del host en el disco.

Se puede utilizar el comando provisto por el sistema operativo del host, o bien se puede utilizar SnapDrive para Windows y SnapDrive para UNIX. También puede optar por hacer que este paso forme parte de su script de procesamiento previo de la copia DE seguridad DE SAN.

2. Utilice la `volume snapshot create` Comando para crear una copia Snapshot de la LUN de producción.

```
volume snapshot create -vserver vs0 -volume vol3 -snapshot vol3_snapshot
```

```
-comment "Single snapshot" -foreground false
```

3. Utilice la `volume file clone create` Comando para crear un clon de la LUN de producción.

```
volume file clone create -vserver vs3 -volume vol3 -source-path lun1 -snapshot  
-name snap_vol3 -destination-path lun1_backup
```

4. Utilice la `lun igroup create` Comando para crear un igroup que incluye el WWPN del servidor de backup.

```
lun igroup create -vserver vs3 -igroup igroup3 -protocol fc -ostype windows  
-initiator 10:00:00:00:c9:73:5b:91
```

5. Utilice la `lun mapping create` Comando para asignar el clon de LUN que creó en el paso 3 al host de backup.

```
lun mapping create -vserver vs3 -volume vol3 -lun lun1_backup -igroup igroup3
```

Puede optar por hacer que este paso forme parte de la secuencia de comandos de posprocesamiento de su aplicación DE backup SAN.

6. Desde el host, detectar el nuevo LUN y hacer que el sistema de archivos esté disponible para el host.

Puede optar por hacer que este paso forme parte de la secuencia de comandos de posprocesamiento de su aplicación DE backup SAN.

7. Realice un backup de los datos del clon LUN desde el host de backup a cinta con la aplicación de backup SAN.

8. Utilice la `lun modify` Comando para desconectar el clon de la LUN.

```
lun modify -vserver vs3 -path /vol/vol3/lun1_backup -state offline
```

9. Utilice la `lun delete` Para quitar el clon LUN.

```
lun delete -vserver vs3 -volume vol3 -lun lun1_backup
```

10. Utilice la `volume snapshot delete` Comando para quitar la copia Snapshot.

```
volume snapshot delete -vserver vs3 -volume vol3 -snapshot vol3_snapshot
```

Referencia para la configuración DE SAN

Información general de la configuración DE SAN

Una red de área de almacenamiento (SAN) consta de una solución de almacenamiento conectada a los hosts a través de un protocolo de transporte SAN como iSCSI o FC. Puede configurar el SAN para que su solución de almacenamiento se conecte a los hosts mediante uno o varios switches. Si utiliza iSCSI, también puede configurar su SAN de modo que su solución de almacenamiento se conecte directamente al host sin necesidad de switch.

En una SAN, varios hosts, mediante diferentes sistemas operativos, como Windows, Linux o UNIX, pueden acceder a la solución de almacenamiento a la vez. Puede utilizar ["Asignación de LUN selectiva"](#) y.. ["conjuntos de puertos"](#) limitar el acceso a los datos entre los hosts y el almacenamiento.

Para iSCSI, la topología de red entre la solución de almacenamiento y los hosts se denomina red. Para FC, FC/NVMe y FCoE La topología de red entre la solución de almacenamiento y los hosts se conoce como estructura. Para crear redundancia, que le proteja de la pérdida de acceso a los datos, debería configurar la SAN con parejas de alta disponibilidad en una configuración multired o multiestructura. Las configuraciones que utilizan nodos únicos o redes/estructuras únicas no son totalmente redundantes, por lo que no se recomiendan.

Después de configurar la SAN, puede ["Aprovisione almacenamiento para iSCSI o FC"](#), o usted puede ["Aprovisione almacenamiento para FC/NVMe"](#). Luego puede conectarse a los hosts para comenzar a reparar datos.

La compatibilidad con el protocolo SAN varía en función de la versión de ONTAP, su plataforma y la configuración. Para obtener detalles sobre su configuración específica, consulte ["Herramienta de matriz de interoperabilidad de NetApp"](#).

Información relacionada

- ["Descripción de la administración de San"](#)
- ["Configuración, compatibilidad y limitaciones de NVMe"](#)

Configuraciones de iSCSI

Formas de configurar hosts SAN iSCSI

Debe configurar la configuración de iSCSI con parejas de alta disponibilidad (HA) que se conecten directamente a sus hosts SAN iSCSI o que se conecten a los hosts a través de uno o más switches IP.

["Parejas de HA"](#) Se definen como los nodos de generación de informes para las rutas Active/Optimized y Active/Unoptimizadas que usarán los hosts para acceder a las LUN. Varios hosts, utilizando diferentes sistemas operativos, como Windows, Linux o UNIX, pueden acceder al almacenamiento al mismo tiempo. Los hosts requieren que se instale y configure una solución multivía compatible con ALUA. Los sistemas operativos compatibles y las soluciones multivía se pueden verificar en el ["Herramienta de matriz de interoperabilidad de NetApp"](#).

En una configuración de varias redes, existen dos o más switches que conectan los hosts con el sistema de almacenamiento. Se recomiendan las configuraciones de varias redes porque son totalmente redundantes. En una configuración de red única, hay un switch que conecta los hosts al sistema de almacenamiento. Las configuraciones de red única no son totalmente redundantes.



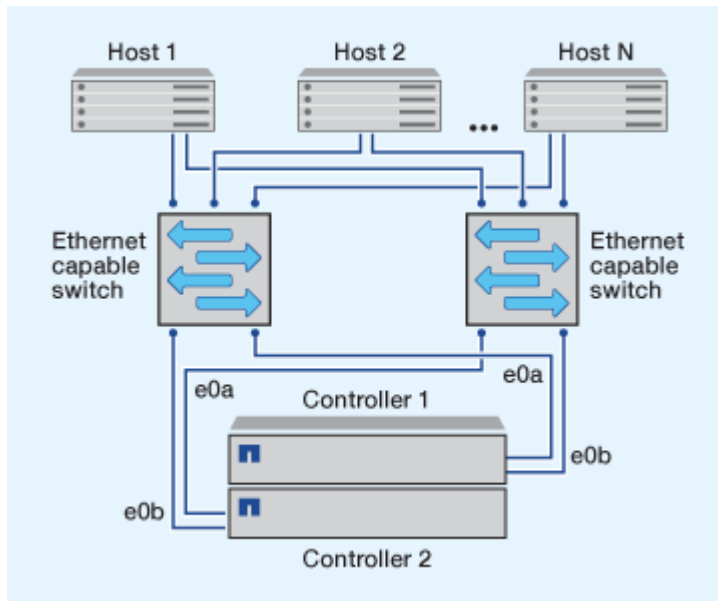
["Configuraciones de nodo único"](#) no se recomiendan porque no proporcionan la redundancia necesaria para admitir tolerancia a fallos y operaciones no disruptivas.

Información relacionada

- Vea cómo ["Asignación de LUN selectiva \(SLM\)"](#) Limita las rutas que se utilizan para acceder a las LUN que pertenece a una pareja de alta disponibilidad.
- Descubra ["LIF SAN"](#).
- Obtenga más información sobre ["Ventajas de las VLAN en iSCSI"](#).

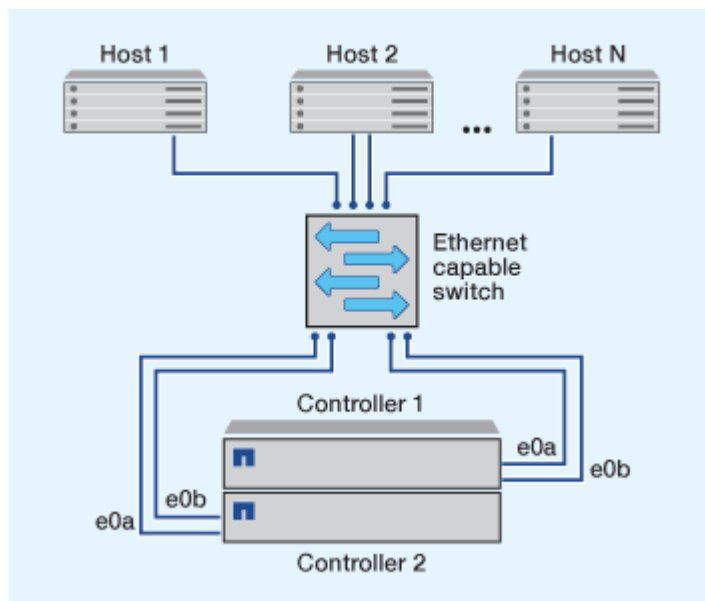
Configuraciones iSCSI multired

En las configuraciones de pares de alta disponibilidad de varias redes, dos o más switches conectan el par de alta disponibilidad con uno o más hosts. Dado que hay varios switches, esta configuración es completamente redundante.



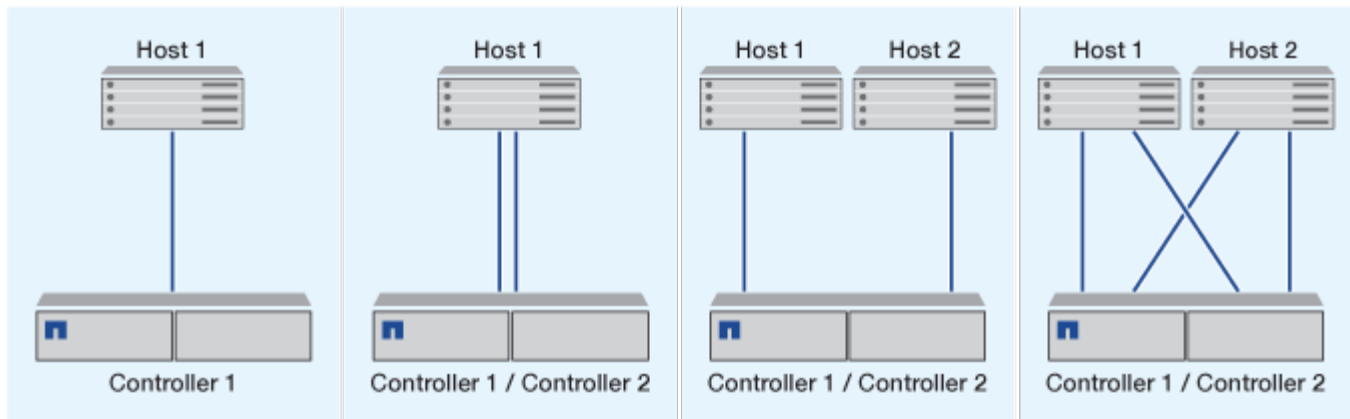
Configuraciones iSCSI de red única

En las configuraciones de pares de alta disponibilidad de red única, un switch conecta el par de alta disponibilidad a uno o varios hosts. Dado que hay un único switch, esta configuración no es completamente redundante.



Configuración iSCSI de conexión directa

En una configuración de conexión directa, uno o varios hosts están conectados directamente a las controladoras.



Ventajas de usar VLAN en configuraciones iSCSI

Una VLAN consta de un grupo de puertos switch agrupados en un dominio de difusión. Una VLAN puede estar en un único switch o puede abarcar varios chasis de switch. Las VLAN estáticas y dinámicas le permiten aumentar la seguridad, aislar problemas y limitar las rutas disponibles en la infraestructura de red IP.

Cuando se implementan VLAN en infraestructuras de redes IP grandes, se obtienen las siguientes ventajas:

- Mayor seguridad.

VLAN le permite aprovechar la infraestructura existente a la vez que proporciona una seguridad mejorada porque limitan el acceso entre diferentes nodos de una red Ethernet o SAN IP.

- Fiabilidad mejorada de la red Ethernet y SAN IP mediante el aislamiento de los problemas.
- Reducción del tiempo de resolución de problemas limitando el espacio del problema.
- Reducción del número de rutas disponibles a un puerto de destino iSCSI en particular.
- Reducción del número máximo de rutas que utiliza un host.

El hecho de tener demasiadas rutas ralentiza los tiempos de reconexión. Si un host no tiene una solución multivía, puede utilizar VLAN para permitir solo una ruta.

VLAN dinámicas

Las VLAN dinámicas se basan en direcciones MAC. Puede definir una VLAN especificando la dirección MAC de los miembros que desea incluir.

Las VLAN dinámicas proporcionan flexibilidad y no requieren la asignación a los puertos físicos en los que el dispositivo está conectado físicamente al conmutador. Puede mover un cable de un puerto a otro sin tener que configurar la VLAN de nuevo.

VLAN estáticas

Las VLAN estáticas se basan en puertos. El switch y el puerto del switch se utilizan para definir la VLAN y sus miembros.

Las VLAN estáticas ofrecen una seguridad mejorada porque no es posible romper las VLAN mediante la suplantación de control de acceso a medios (MAC). Sin embargo, si alguien tiene acceso físico al switch, el reemplazo de un cable y la reconfiguración de la dirección de red puede permitir el acceso.

En algunos entornos, es más fácil crear y gestionar VLAN estáticas que las VLAN dinámicas. Esto es debido a que las VLAN estáticas requieren que solo se especifique el switch y el identificador de puerto, en lugar de la dirección MAC de 48 bits. Además, puede etiquetar los rangos de puertos del switch con el identificador de VLAN.

Configuraciones de FC

Formas de configurar los hosts SAN FC y FC-NVMe

Es recomendable configurar sus hosts SAN FC y FC-NVMe usando pares de alta disponibilidad y un mínimo de dos switches. Esto proporciona redundancia en las capas de la estructura y del sistema de almacenamiento para admitir tolerancia a fallos y operaciones no disruptivas. No puede conectar directamente hosts SAN FC o FC-NVMe a parejas de alta disponibilidad sin utilizar un switch.

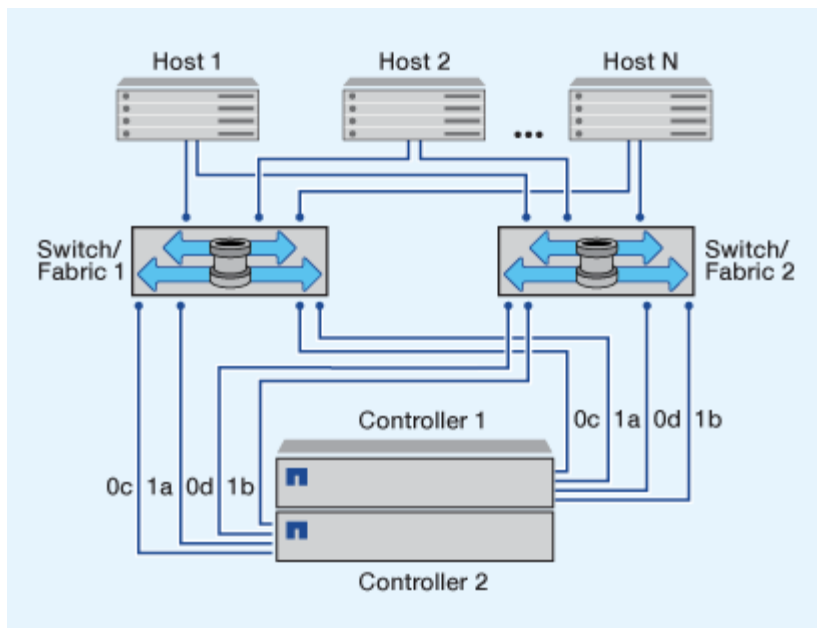
Las estructuras en cascada, malla parcial, malla completa, núcleo-borde y director son métodos estándar en el sector para conectar switches FC a una estructura, y todos son compatibles. No se admite el uso de estructuras heterogéneas de switches FC, a excepción de los switches blade integrados. Las excepciones específicas se enumeran en la ["Herramienta de matriz de interoperabilidad"](#). Una estructura puede estar compuesta por uno o varios switches y las controladoras de almacenamiento se pueden conectar a varios switches.

Varios hosts, utilizando diferentes sistemas operativos, como Windows, Linux o UNIX, pueden acceder a las controladoras de almacenamiento al mismo tiempo. Los hosts requieren que se instale y configure una solución multivía compatible. Los sistemas operativos compatibles y las soluciones multivía se pueden verificar en la herramienta de matriz de interoperabilidad.

Configuraciones FC y FC-NVMe multiestructura

En las configuraciones de par de alta disponibilidad multiestructura, existen dos o más switches que conectan pares de alta disponibilidad a uno o varios hosts. Para mayor simplicidad, la siguiente figura de par de alta disponibilidad multiestructura solo muestra dos estructuras, pero puede tener dos o más estructuras en cualquier configuración de estructura múltiple.

Los números de puerto de destino FC (0C, 0d, 1a, 1b) que aparecen en las ilustraciones son ejemplos. Los números de puerto reales varían según el modelo de su nodo de almacenamiento y si usa adaptadores de expansión.

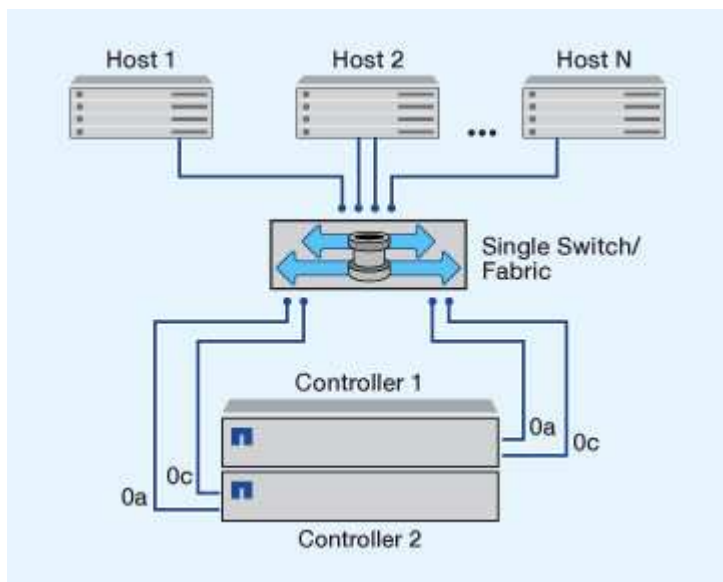


Configuraciones FC y FC-NVMe de estructura única

En configuraciones de pareja de alta disponibilidad de estructura única, existe una estructura que conecta ambas controladoras en el par de alta disponibilidad a uno o varios hosts. Dado que los hosts y las controladoras están conectados a través de un único switch, las configuraciones de par de alta disponibilidad de estructura única no son totalmente redundantes.

Los números de puerto de destino FC (0A, 0C) que aparecen en las ilustraciones son ejemplos. Los números de puerto reales varían según el modelo de su nodo de almacenamiento y si usa adaptadores de expansión.

Todas las plataformas que admiten las configuraciones FC admiten configuraciones de par de alta disponibilidad de estructura única.



"Configuraciones de nodo único" no se recomiendan porque no proporcionan la redundancia necesaria para admitir tolerancia a fallos y operaciones no disruptivas.

Información relacionada

- Vea cómo ["Asignación de LUN selectiva \(SLM\)"](#) Limita las rutas que se utilizan para acceder a las LUN que pertenece a una pareja de alta disponibilidad.
- Descubra ["LIF SAN"](#).

Prácticas recomendadas para la configuración del switch FC

Para obtener el mejor rendimiento, debe tener en cuenta ciertas prácticas recomendadas al configurar el switch de FC.

Una configuración permanente de la velocidad es la mejor práctica para las configuraciones de switch FC, especialmente en grandes estructuras, porque ofrece el mejor rendimiento para recompilaciones de estructuras y puede ahorrar mucho tiempo. Aunque la autonegociación ofrece la mayor flexibilidad, la configuración del switch de FC no siempre funciona del modo esperado y añade tiempo a la secuencia general de compilación de estructura.

Todos los switches que están conectados a la estructura deben ser compatibles con la virtualización de N_Port ID (NPIV) y deben tener NPIV habilitado. ONTAP utiliza NPIV para presentar destinos de FC a una estructura.

Para obtener más detalles sobre qué entornos se admiten, consulte ["Herramienta de matriz de interoperabilidad de NetApp"](#).

Para ver las prácticas recomendadas para FC e iSCSI, consulte ["Informe técnico de NetApp 4080: Prácticas recomendadas para SAN moderno"](#).

Número admitido de saltos de FC

El número máximo de saltos de FC admitidos entre un host y el sistema de almacenamiento depende del proveedor de switch y de la compatibilidad del sistema de almacenamiento para las configuraciones de FC.

Los saltos son el número de switches presentes en la ruta que va del iniciador (host) al destino (sistema de almacenamiento). Cisco también se refiere a este valor como el *diámetro de LA estructura DE SAN*.

| Cambiar proveedor | Número de saltos admitidos |
|-------------------|--|
| Brocade | 7 GbE para FC, 5 GbE para FCoE |
| Cisco | 7 para FC, hasta 3 de los switches pueden ser switches FCoE. |

Información relacionada

["Descargas de NetApp: Documentos de matriz de escalabilidad de Brocade"](#)

["Descargas de NetApp: Documentos de matriz de escalabilidad de Cisco"](#)

Velocidades admitidas en el puerto de destino FC

Los puertos de destino FC pueden configurarse para que funcionen a diferentes velocidades. Debe configurar la velocidad del puerto de destino para que coincida con la velocidad del dispositivo al que se conecta. Todos los puertos de destino utilizados por

un host determinado deben configurarse con la misma velocidad.

Los puertos de destino FC se pueden utilizar para las configuraciones FC-NVMe exactamente del mismo modo que se utilizan para las configuraciones FC.

Debe configurar la velocidad del puerto de destino para que coincida con la velocidad del dispositivo al que se conecta en vez de utilizar la autonegociación. Un puerto configurado para la autonegociación puede tardar más en volver a conectarse después de una toma de control/devolución u otra interrupción.

Puede configurar los puertos internos y los adaptadores de expansión para que se ejecuten a la velocidad siguiente. Cada controladora y puerto del adaptador de expansión se pueden configurar de forma individual para diferentes velocidades según sea necesario.

| Puertos de 4 GB | Puertos de 8 GB | Puertos de 16 GB | Puertos de 32 GB |
|--|--|---|--|
| <ul style="list-style-type: none">• 4 GB• 2 GB• 1 GB | <ul style="list-style-type: none">• 8 GB• 4 GB• 2 GB | <ul style="list-style-type: none">• 16 GB• 8 GB• 4 GB | <ul style="list-style-type: none">• 32 GB• 16 GB• 8 GB |



Los puertos UTA2 pueden utilizar un adaptador SFP+ de 8 GB para admitir velocidades de 8, 4 y 2 GB, si fuera necesario.

Recomendaciones de configuración de los puertos de destino FC

Para obtener el mejor rendimiento y la mayor disponibilidad, debe usar la configuración recomendada de puertos de destino FC.

En la siguiente tabla, se muestra el orden de uso de puertos preferido para los puertos de destino FC y FC-NVMe integrados. Para los adaptadores de expansión, los puertos FC deben propagarse para no usar el mismo ASIC para la conectividad. El orden de ranura preferido se muestra en la "[Hardware Universe de NetApp](#)" Para la versión del software ONTAP que utiliza el controlador.

FC-NVMe es compatible con los siguientes modelos:

- AFF A300



Los puertos internos de AFF A300 no son compatibles con FC-NVMe.

- AFF A700
- AFF A700s
- AFF A800



Los sistemas FAS2520 no tienen puertos FC integrados y no admiten adaptadores complementarios.

| Controladora | Pares de puertos con ASIC compartido | Número de puertos de destino: Puertos preferidos |
|---|--------------------------------------|--|
| FAS9000, AFF A700, AFF A700s y AFF A800 | Ninguno | Todos los puertos de datos están en adaptadores de expansión. Consulte " Hardware Universe de NetApp " si quiere más información. |
| 8080, 8060 y 8040 | 0e+0f 0g+0h | 1: 0e 2: 0e, 0g 3: 0e, 0g, 0h 4: 0e, 0g, 0f, 0h |
| FAS8200 y AFF A300 | 0g+0h | 1: 0g 2: 0g, 0h |
| 8020 | 0c+0d | 1: 0c 2: 0c, 0d |
| 62xx | 0a+0b 0c+0d | 1: 0a 2: 0a, 0c 3: 0a, 0c, 0b 4: 0a, 0c, 0b, 0d |
| 32xx | 0c+0d | 1: 0c 2: 0c, 0d |
| FAS2554, FAS2552, FAS2600 series, FAS2720, FAS2750, AFF A200 y AFF A220 | 0c+0d 0e+0f | 1: 0c 2: 0c, 0e 3: 0c, 0e, 0d 4: 0c, 0e, 0d, 0f |

Gestione sistemas con adaptadores de FC

Información general sobre la gestión de sistemas con adaptadores de FC

Hay comandos disponibles para gestionar los adaptadores FC integrados y las tarjetas adaptadoras FC. Estos comandos se pueden utilizar para configurar el modo del adaptador, mostrar información del adaptador y cambiar la velocidad.

La mayoría de los sistemas de almacenamiento tienen adaptadores FC integrados que se pueden configurar como iniciadores o destinos. También puede utilizar tarjetas adaptadoras de FC configuradas como iniciadores o destinos. Los iniciadores se conectan a las bandejas de discos del back-end y posiblemente a cabinas de almacenamiento externas (FlexArray). Los destinos se conectan solo a switches FC. Tanto los puertos HBA de destino FC como la velocidad del puerto del switch deben configurarse con el mismo valor y no deben configurarse en modo automático.

Comandos para gestionar adaptadores de FC

Puede usar comandos FC para gestionar adaptadores de destino FC, adaptadores de iniciador FC y adaptadores de FC integrados para su controladora de almacenamiento. Los mismos comandos se utilizan para gestionar adaptadores de FC para el protocolo FC y el protocolo FC-NVMe.

Los comandos de adaptador del iniciador de FC solo funcionan en el nivel del nodo. Debe utilizar el `run -node node_name` Antes de poder utilizar los comandos del adaptador del iniciador de FC.

Comandos para gestionar los adaptadores de destino de FC

| Si desea... | Se usa este comando... |
|--|---|
| Muestra información del adaptador de FC en un nodo | <code>network fcp adapter show</code> |
| Modifique los parámetros del adaptador de destino FC | <code>network fcp adapter modify</code> |
| Muestra información sobre el tráfico del protocolo FC | <code>run -node node_name sysstat -f</code> |
| Muestra el tiempo que se ha ejecutado el protocolo FC | <code>run -node node_name uptime</code> |
| Mostrar la configuración y el estado del adaptador | <code>run -node node_name sysconfig -v adapter</code> |
| Compruebe qué tarjetas de expansión están instaladas y si hay algún error de configuración | <code>run -node node_name sysconfig -ac</code> |
| Ver una página de manual de un comando | <code>man command_name</code> |

Comandos para gestionar los adaptadores de iniciador de FC

| Si desea... | Se usa este comando... |
|---|---|
| Muestra información de todos los iniciadores y sus adaptadores en un nodo | <code>run -node node_name storage show adapter</code> |
| Mostrar la configuración y el estado del adaptador | <code>run -node node_name sysconfig -v adapter</code> |

| Si desea... | Se usa este comando... |
|--|---|
| Compruebe qué tarjetas de expansión están instaladas y si hay algún error de configuración | <code>run -node <i>node_name</i> sysconfig -ac</code> |

Comandos para gestionar los adaptadores de FC internos

| Si desea... | Se usa este comando... |
|--|--|
| Muestra el estado de los puertos FC internos | <code>system node hardware unified-connect show</code> |

Configure los adaptadores de FC para el modo iniciador

Puede configurar puertos FC individuales de adaptadores integrados y determinadas tarjetas adaptadoras FC para el modo iniciador. El modo iniciador se usa para conectar los puertos a unidades de cinta, bibliotecas de cintas o almacenamiento de terceros con la virtualización de FlexArray o con importación de LUN externa (FLI).

Lo que necesitará

- Las LIF del adaptador deben eliminarse de cualquier conjunto de puertos de los que pertenezcan.
- Todas las LIF de todas las máquinas virtuales de almacenamiento (SVM) que utilizan el puerto físico que se va a modificar deben migrarse o destruirse antes de cambiar la personalidad del puerto físico de destino a iniciador.

Acerca de esta tarea

Cada puerto FC integrado se puede configurar de forma individual como iniciador o destino. Los puertos en determinados adaptadores de FC también se pueden configurar de forma individual como un puerto de destino o como un puerto iniciador, al igual que los puertos FC integrados. Hay disponible una lista de adaptadores que se pueden configurar para el modo de destino en ["Hardware Universe de NetApp"](#).



NVMe/FC no admite el modo iniciador.

Pasos

1. Quite todas las LIF del adaptador:

```
network interface delete -vserver SVM_name -lif lif_name,lif_name
```

2. Desconectar el adaptador:

```
network fcp adapter modify -node node_name -adapter adapter_port -status-admin down
```

Si el adaptador no se desconecta, también puede quitar el cable del puerto de adaptador correspondiente del sistema.

3. Cambie el adaptador del destino al iniciador:

```
system hardware unified-connect modify -t initiator adapter_port
```

4. Reinicie el nodo que aloja el adaptador que cambió.
5. Compruebe que los puertos FC estén configurados en estado correcto para la configuración:

```
system hardware unified-connect show
```

6. Vuelva a conectar el adaptador:

```
node run -node node_name storage enable adapter adapter_port
```

Configure los adaptadores de FC para el modo de destino

Puede configurar puertos FC individuales de adaptadores integrados y determinadas tarjetas adaptadoras FC para el modo destino. El modo de destino se utiliza para conectar los puertos a iniciadores FC.

Acerca de esta tarea

Cada puerto FC integrado se puede configurar de forma individual como iniciador o destino. Los puertos en determinados adaptadores de FC también se pueden configurar de forma individual como un puerto de destino o como un puerto iniciador, al igual que los puertos FC integrados. Hay disponible una lista de adaptadores que se pueden configurar para el modo de destino en ["Hardware Universe de NetApp"](#).

Los mismos pasos se utilizan cuando se configuran los adaptadores de FC para el protocolo FC y el protocolo FC-NVMe. Sin embargo, solo ciertos adaptadores de FC admiten FC-NVMe. Consulte ["Hardware Universe de NetApp"](#) Para obtener una lista de los adaptadores que admiten el protocolo FC-NVMe.

Pasos

1. Desconectar el adaptador:

```
node run -node node_name storage disable adapter adapter_name
```

Si el adaptador no se desconecta, también puede quitar el cable del puerto de adaptador correspondiente del sistema.

2. Cambie el adaptador del iniciador al destino:

```
system node hardware unified-connect modify -t target -node node_name adapter adapter_name
```

3. Reinicie el nodo que aloja el adaptador que cambió.
4. Compruebe que el puerto de destino tiene la configuración correcta:

```
network fcp adapter show -node node_name
```

5. Conectar su adaptador:

```
network fcp adapter modify -node node_name -adapter adapter_port -state up
```

Muestra información sobre un adaptador de destino de FC

Puede utilizar el `network fcp adapter show` Comando para mostrar la información de la configuración del sistema y del adaptador de cualquier adaptador de FC en el

sistema.

Paso

1. Muestra información sobre el adaptador de FC mediante el `network fcp adapter show` comando.

El resultado muestra información de configuración del sistema y información del adaptador para cada ranura que se utiliza.

```
network fcp adapter show -instance -node node1 -adapter 0a
```

Cambie la velocidad del adaptador de FC

Debe configurar la velocidad del puerto de destino del adaptador para que coincida con la velocidad del dispositivo al que se conecta, en vez de utilizar la autonegociación. Un puerto configurado para la autonegociación puede tardar más tiempo en reconectar después de una toma de control/devolución u otra interrupción.

Lo que necesitará

Todos los LIF que utilizan este adaptador como puerto de inicio deben estar desconectados.

Acerca de esta tarea

Dado que esta tarea abarca todas las máquinas virtuales de almacenamiento (SVM) y todos los LIF de un clúster, debe utilizar el `-home-port` y.. `-home-lif` parámetros para limitar el alcance de esta operación. Si no utiliza estos parámetros, la operación se aplica a todas las LIF del clúster, lo que podría no ser deseable.

Pasos

1. Desconecte todas las LIF de este adaptador:

```
network interface modify -vserver * -lif * { -home-node node1 -home-port 0c }  
-status-admin down
```

2. Desconectar el adaptador:

```
network fcp adapter modify -node node1 -adapter 0c -state down
```

Si el adaptador no se desconecta, también puede quitar el cable del puerto de adaptador correspondiente del sistema.

3. Determine la velocidad máxima del adaptador de puerto:

```
fcp adapter show -instance
```

No puede modificar la velocidad del adaptador más allá de la velocidad máxima.

4. Cambie la velocidad del adaptador:

```
network fcp adapter modify -node node1 -adapter 0c -speed 16
```

5. Conectar el adaptador:

```
network fcp adapter modify -node node1 -adapter 0c -state up
```

6. Conectar todas las LIF del adaptador:

```
network interface modify -vserver * -lif * { -home-node node1 -home-port 0c }  
-status-admin up
```

Puertos FC compatibles

El número de puertos FC integrados y puertos CNA/UTA2 configurados para FC varía según el modelo de la controladora. Los puertos FC también están disponibles mediante adaptadores de expansión de destino FC admitidos o tarjetas UTA2 adicionales configuradas con adaptadores FC SFP+.

Puertos FC, UTA y UTA2 integrados

- Los puertos integrados se pueden configurar de forma individual como puertos FC de destino o de iniciador.
- El número de puertos FC integrados varía según el modelo de la controladora.

La ["Hardware Universe de NetApp"](#) Contiene una lista completa de puertos FC integrados en cada modelo de controladora.

- Los sistemas FAS2520 no son compatibles con FC.

Puertos FC de adaptador de ampliación de destino

- Los adaptadores de expansión de destino disponibles difieren según el modelo de la controladora.

La ["Hardware Universe de NetApp"](#) contiene una lista completa de los adaptadores de expansión de destino para cada modelo de controladora.

- Los puertos de algunos adaptadores de ampliación de FC se configuran como iniciadores o destinos de fábrica y no se pueden cambiar.

Los demás se pueden configurar de forma individual como puertos FC de destino o de iniciador, al igual que los puertos FC incorporados. Hay una lista completa disponible en ["Hardware Universe de NetApp"](#).

Evite la pérdida de conectividad cuando utilice el adaptador X1133A-R6

Puede evitar la pérdida de conectividad durante un error en el puerto configurando el sistema con rutas redundantes en HBA X1133A-R6 independientes.

El HBA X1133A-R6 es un adaptador FC de 4 puertos y 16 GB que consta de dos pares de dos puertos. El adaptador X1133A-R6 se puede configurar como modo de destino o modo de iniciador. Cada par de 2 puertos se admite con un único ASIC (por ejemplo, el puerto 1 y el puerto 2 en ASIC 1 y el puerto 3 y el puerto 4 en ASIC 2). Ambos puertos en un único ASIC deben configurarse para funcionar en el mismo modo, tanto en modo objetivo como en modo iniciador. Si se produce un error con el ASIC que admite un par, ambos puertos del par se desconectan.

Para evitar esta pérdida de conectividad, puede configurar el sistema con rutas redundantes para separar los HBA X1133A-R6, o con rutas redundantes a los puertos compatibles con diferentes ASIC en el HBA.

Información general sobre las configuraciones de puertos admitidas para los adaptadores X1143A-R6

De manera predeterminada, el adaptador X1143A-R6 se configura en el modo objetivo FC, pero puede configurar sus puertos como puertos Ethernet y FCoE de 10 GB (CNA) o como puertos de destino o iniciador FC de 16 GB. Esto requiere distintos adaptadores de SFP+.

Cuando se configura para Ethernet y FCoE, los adaptadores X1143A-R6 admiten el tráfico de destino NIC y FCoE simultáneo en el mismo puerto de 10 GBE. Cuando se configura para FC, cada par de dos puertos que comparte el mismo ASIC se puede configurar individualmente para modo iniciador FC o destino FC. Esto significa que un solo adaptador X1143A-R6 puede admitir el modo objetivo FC en un par de dos puertos y el modo iniciador de FC en otro par de dos puertos. Los pares de puertos conectados al mismo ASIC deben configurarse en el mismo modo.

En el modo FC, el adaptador X1143A-R6 se comporta como cualquier dispositivo FC existente con velocidades de hasta 16 Gbps. En el modo CNA, se puede utilizar el adaptador X1143A-R6 para el tráfico NIC y FCoE simultáneo que comparta el mismo puerto 10 GbE. El modo CNA solo admite el modo de destino FC para la función FCoE.

Configure los puertos

Para configurar el adaptador de objetivo unificado (X1143A-R6), debe configurar los dos puertos adyacentes en el mismo chip en el mismo modo Personality.

Pasos

1. Configure los puertos según sea necesario para Fibre Channel (FC) o el adaptador de red convergente (CNA) mediante el `system node hardware unified-connect modify` comando.
2. Conecte los cables adecuados para FC o Ethernet de 10 GB.
3. Compruebe que tiene instalado el SFP+ correcto:

```
network fcp adapter show -instance -node -adapter
```

Para CNA, se debe usar un SFP Ethernet de 10 GB. Para FC, se debe usar un SFP de 8 GB o un SFP de 16 GB, a partir de la estructura de FC al que se está conectando.

Cambie el puerto UTA2 del modo CNA al modo FC

Debe cambiar el puerto UTA2 del modo adaptador de red convergente (CNA) al modo Fibre Channel (FC) para admitir el iniciador de FC y el modo de destino de FC. Debe cambiar la personalidad del modo CNA al modo FC cuando necesite cambiar el medio físico que conecta el puerto a su red.

Pasos

1. Desconectar el adaptador:

```
network fcp adapter modify -node node_name -adapter adapter_name -status-admin  
down
```

2. Cambie el modo de puerto:

```
ucadmin modify -node node_name -adapter adapter_name -mode fcp
```

3. Reinicie el nodo y a continuación, active el adaptador:

```
network fcp adapter modify -node node_name -adapter adapter_name -status-admin  
up
```

4. Notifique a su administrador o VIF Manager que elimine o quite el puerto, según corresponda:

- Si el puerto se utiliza como puerto de inicio de una LIF, es miembro de un grupo de interfaces (ifgrp) o una VLAN de host, un administrador debe hacer lo siguiente:
 - i. Mueva las LIF, quite el puerto del ifgrp o elimine las VLAN respectivamente.
 - ii. Elimine manualmente el puerto ejecutando el `network port delete` comando.

Si la `network port delete` error del comando, el administrador debe solucionar los errores y volver a ejecutar el comando.

- Si el puerto no se usa como puerto de inicio de una LIF, no es miembro de un ifgrp y no aloja VLAN, el gestor VIF debería eliminar el puerto de sus registros en el momento del reinicio.

Si el administrador VIF no quita el puerto, el administrador debe quitarlo manualmente después del reinicio usando la `network port delete` comando.

```
net-f8040-34::> network port show
```

```
Node: net-f8040-34-01
```

| Port | IPspace | Broadcast | Domain | Link | MTU | Speed (Mbps) Admin/Oper | Health Status |
|------|---------|-----------|--------|------|------|----------------------------|------------------|
| ... | | | | | | | |
| e0i | Default | Default | | down | 1500 | auto/10 | - |
| e0f | Default | Default | | down | 1500 | auto/10 | - |
| ... | | | | | | | |

```
net-f8040-34::> ucadmin show
```

| Node | Adapter | Current Mode | Current Type | Pending Mode | Pending Type | Admin |
|-----------------|---------|-----------------|-----------------|-----------------|-----------------|-------|
| Status | | | | | | |
| net-f8040-34-01 | 0e | cna | target | - | - | |
| offline | | | | | | |
| net-f8040-34-01 | 0f | cna | target | - | - | |

```

offline
...

net-f8040-34::> network interface create -vs net-f8040-34 -lif m
-role
node-mgmt-home-node net-f8040-34-01 -home-port e0e -address 10.1.1.1
-netmask 255.255.255.0


net-f8040-34::> network interface show -fields home-port, curr-port

vserver lif                               home-port curr-port
-----
Cluster net-f8040-34-01_clus1 e0a          e0a
Cluster net-f8040-34-01_clus2 e0b          e0b
Cluster net-f8040-34-01_clus3 e0c          e0c
Cluster net-f8040-34-01_clus4 e0d          e0d
net-f8040-34
      cluster_mgmt          e0M          e0M
net-f8040-34
      m                      e0e          e0i
net-f8040-34
      net-f8040-34-01_mgmt1 e0M          e0M
7 entries were displayed.


net-f8040-34::> ucadmin modify local 0e fc

Warning: Mode on adapter 0e and also adapter 0f will be changed to
fc.
Do you want to continue? {y|n}: y
Any changes will take effect after rebooting the system. Use the
"system node reboot" command to reboot.


net-f8040-34::> reboot local
(system node reboot)


Warning: Are you sure you want to reboot node "net-f8040-34-01"?
{y|n}: y

```

5. Compruebe que tiene instalado el SFP+ correcto:

```
network fcp adapter show -instance -node -adapter
```

Para CNA, se debe usar un SFP Ethernet de 10 GB. Para FC, se debe usar un SFP de 8 GB o un SFP de 16 GB antes de cambiar la configuración en el nodo.

Cambie los módulos ópticos del adaptador de destino CNA/UTA2

Debe cambiar los módulos ópticos del adaptador de destino unificado (CNA/UTA2) para admitir el modo de personalidad seleccionado para el adaptador.

Pasos

1. Verifique el SFP+ actual utilizado en la tarjeta. A continuación, reemplace el SFP+ actual por el SFP+ adecuado para la personalidad preferida (FC o CNA).
2. Retire los módulos ópticos actuales del adaptador X1143A-R6.
3. Inserte los módulos correctos para la óptica del modo de personalidad preferido (FC o CNA).
4. Compruebe que tiene instalado el SFP+ correcto:

```
network fcp adapter show -instance -node -adapter
```

Los módulos SFP+ compatibles y los cables de cobre de Marca Cisco (Twinax) se enumeran en la ["Hardware Universe de NetApp"](#).

Ver la configuración de adaptador

Para ver la configuración del adaptador de destino unificado (X1143A-R6), debe ejecutar el `system hardware unified-connect show` comando para mostrar todos los módulos de la controladora.

Pasos

1. Arranque la controladora sin los cables conectados.
2. Ejecute el `system hardware unified-connect show` comando para ver la configuración del puerto y los módulos.
3. Consulte la información del puerto antes de configurar el CNA y los puertos.

Configuraciones de FCoE

Formas de configurar la información general sobre FCoE

FCoE puede configurarse de diversas formas mediante switches FCoE. FCoE no admite las configuraciones de conexión directa.

Todas las configuraciones de FCoE tienen estructura doble, son completamente redundantes y requieren un software multivía en el lado del host. En todas las configuraciones de FCoE, puede tener varios switches FCoE y FC en la ruta entre el iniciador y el destino, hasta el límite máximo de saltos. Para conectar los switches entre sí, deben ejecutar una versión de firmware que admita ISL de Ethernet. Cada host de cualquier configuración de FCoE se puede configurar con un sistema operativo diferente.

Las configuraciones de FCoE requieren switches Ethernet que admitan explícitamente las funciones de FCoE. Las configuraciones de FCoE se validan mediante el mismo proceso de interoperabilidad y garantía de calidad que los switches FC. Las configuraciones admitidas se muestran en la matriz de interoperabilidad. Algunos de los parámetros incluidos en estas configuraciones admitidas son el modelo de switch, el número de switches que puede ponerse en marcha en una sola estructura y la versión de firmware del switch compatible.

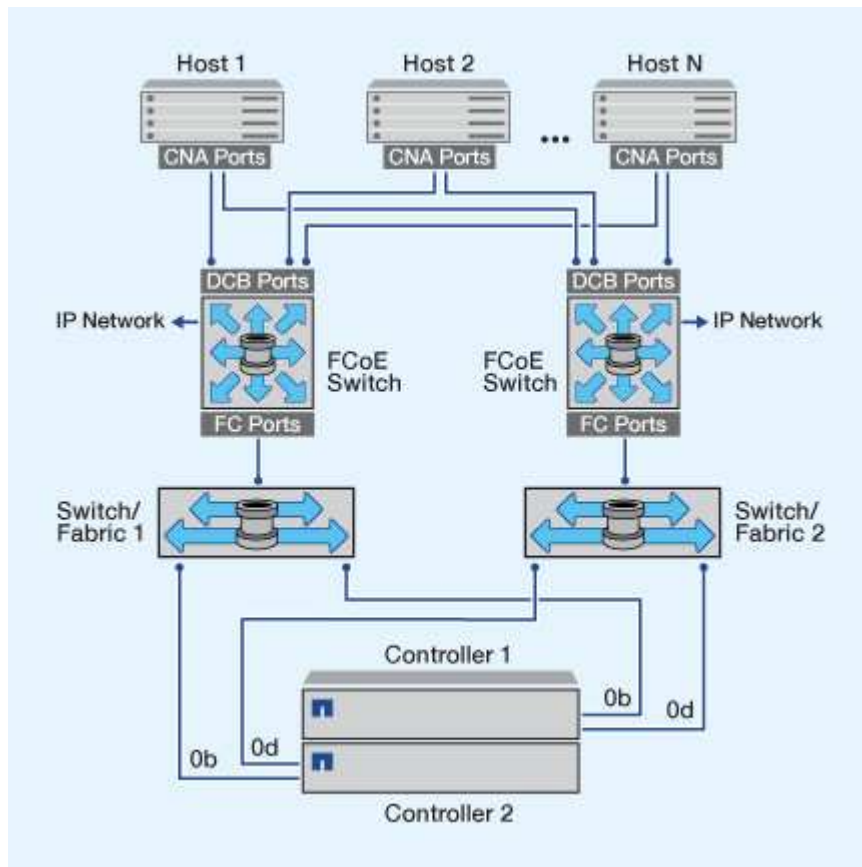
Los números de puertos del adaptador de ampliación de destino FC en las ilustraciones son ejemplos. Los números de puerto reales pueden variar, según las ranuras de expansión en las que se hayan instalado los

adaptadores de expansión de destino FCoE.

Iniciador FCoE a destino FC

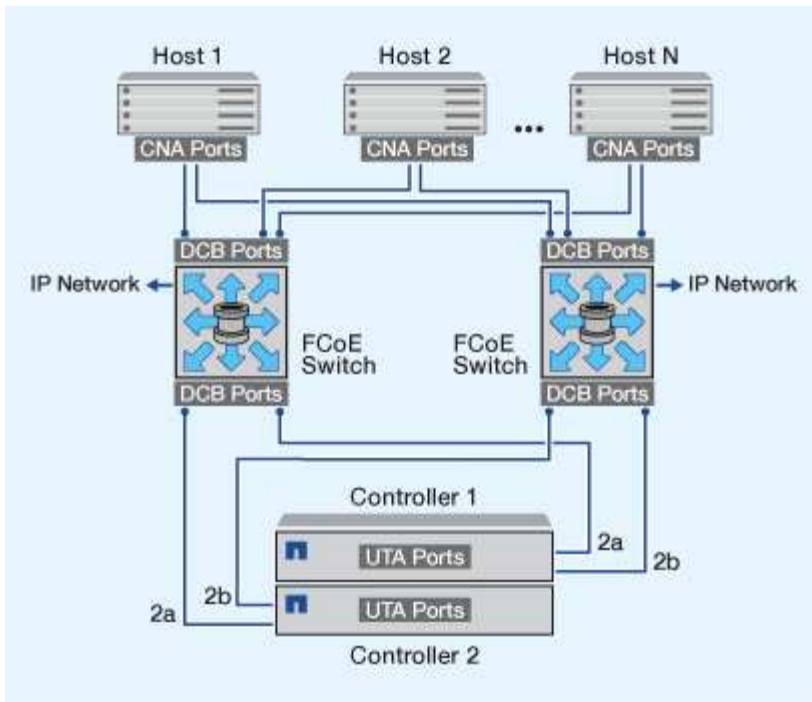
Con iniciadores FCoE (CNA) puede conectar hosts a ambas controladoras en un par de alta disponibilidad mediante switches FCoE a puertos de destino FC. El switch FCoE debe tener también puertos FC. El iniciador FCoE del host siempre se conecta al switch FCoE. El switch FCoE puede conectarse directamente al destino FC o conectarse al destino FC a través de switches FC.

En la siguiente ilustración, se muestran las CNA del host conectadas a un switch FCoE y luego a un switch de FC antes de conectarse al par de alta disponibilidad:



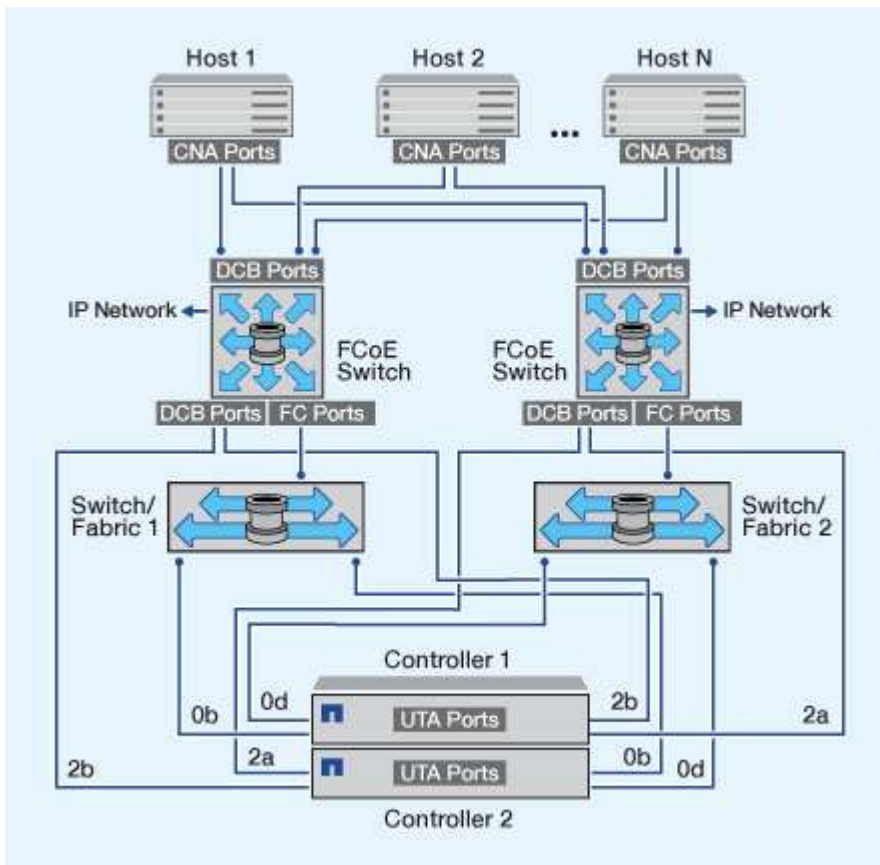
Iniciador de FCoE a destino de FCoE

Con los iniciadores FCoE del host (CNA) es posible conectar los hosts a ambas controladoras en una pareja de alta disponibilidad a los puertos de destino FCoE (también denominados UTA o 2 s) a través de los switches FCoE.



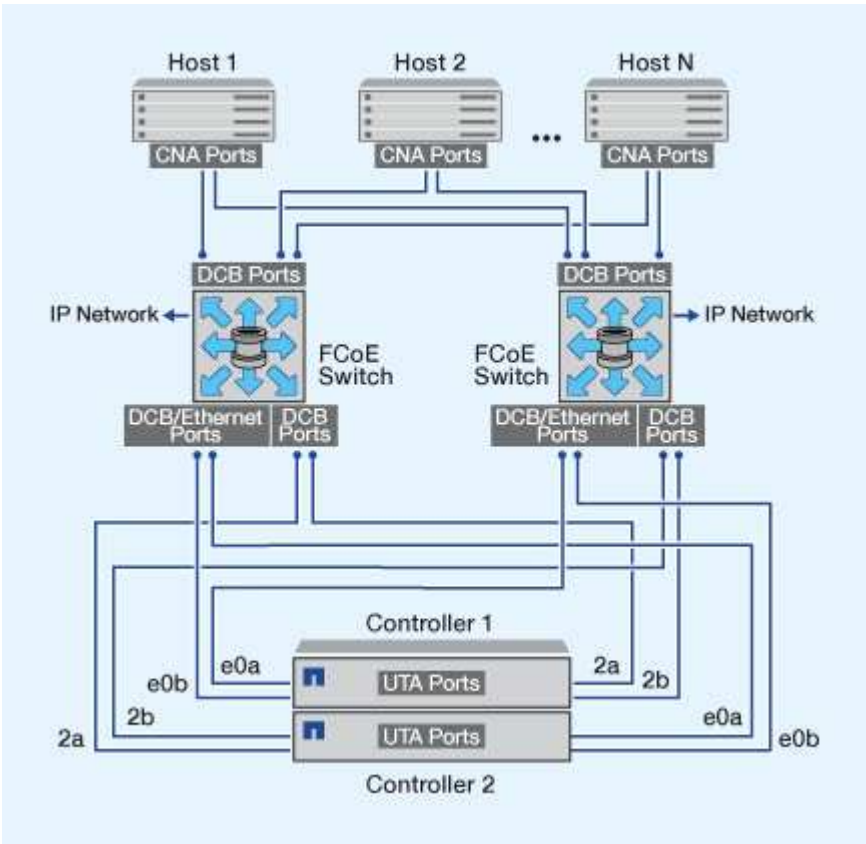
Iniciador FCoE para destinos de FCoE y FC

Con los iniciadores FCoE del host (CNA) es posible conectar los hosts a ambas controladoras en un par de alta disponibilidad a los puertos de destino FCoE y FC (también denominados UTA o UTA 2) a través de los switches FCoE.



Combinación de FCoE y los protocolos de almacenamiento IP

Con los iniciadores FCoE del host (CNA) es posible conectar los hosts a ambas controladoras en una pareja de alta disponibilidad a los puertos de destino FCoE (también denominados UTA o 2 s) a través de los switches FCoE. Los puertos FCoE no pueden usar la agregación tradicional de enlaces a un único switch. Los switches de Cisco admiten un tipo especial de agregación de enlaces (Virtual Port Channel) que admite FCoE. Un canal de puerto virtual agrega vínculos individuales a dos switches. También puede utilizar Canales de puerto virtual para otro tráfico Ethernet. Los puertos que se utilizan para el tráfico aparte de FCoE, como NFS, SMB, iSCSI y otro tráfico Ethernet, pueden utilizar puertos Ethernet habituales en los switches FCoE.



Combinaciones de iniciadores y objetivos de FCoE

Se admiten ciertas combinaciones de iniciadores y destinos FC tradicionales y FCoE.

Iniciadores FCoE

Es posible utilizar iniciadores de FCoE en equipos host con destinos FCoE y FC tradicionales en controladoras de almacenamiento. El iniciador FCoE del host debe conectarse a un switch FCoE DCB (Data Center Bridging); no se admite la conexión directa a un destino.

En la siguiente tabla se enumeran las combinaciones compatibles:

| Iniciador | Destino | Compatible? |
|-----------|---------|-------------|
| FC | FC | Sí |
| FC | FCoE | Sí |

| Iniciador | Destino | Compatible? |
|-----------|---------|-------------|
| FCoE | FC | Sí |
| FCoE | FCoE | Sí |

Destinos FCoE

Puede combinar puertos de destino FCoE con puertos FC de 4 GB, 8 GB o 16 GB en la controladora de almacenamiento, independientemente de si los puertos FC son adaptadores de destino adicionales o puertos integrados. Puede tener adaptadores de destino FCoE y FC en la misma controladora de almacenamiento.



Aún se aplican las reglas para combinar los puertos FC internos y de ampliación.

Número de saltos admitidos por FCoE

El número máximo de saltos de Fibre Channel over Ethernet (FCoE) admitidos entre un host y el sistema de almacenamiento depende del proveedor de switches y de la compatibilidad del sistema de almacenamiento para las configuraciones FCoE.

Los saltos son el número de switches presentes en la ruta que va del iniciador (host) al destino (sistema de almacenamiento). La documentación de Cisco Systems también se refiere a este valor como el *diameter de LA estructura SAN*.

Para FCoE, puede tener switches FCoE conectados a switches FC.

Para las conexiones FCoE integrales, los switches FCoE deben ejecutar una versión de firmware que admita enlaces entre switches Ethernet (ISL).

En la siguiente tabla, se enumeran los números máximos de saltos admitidos:

| Cambiar proveedor | Número de saltos admitidos |
|-------------------|---|
| Brocade | 7 para FC 5 para FCoE |
| Cisco | 7 Hasta 3 switches pueden ser switches FCoE. |

División en zonas de Fibre Channel y FCoE

Información general sobre la división en zonas de Fibre Channel y FCoE

Una zona FC, FC-NVMe o FCoE es una agrupación lógica de uno o varios puertos dentro de una estructura. Para que los dispositivos puedan verse entre sí, conectarse, crear sesiones entre sí y comunicarse, ambos puertos necesitan tener una pertenencia a una zona común. Se recomienda la división en zonas de un solo iniciador.

Motivos para dividir en zonas

- La división en zonas reduce o elimina la *comunicación entre zonas* entre los HBA del iniciador.

Esto ocurre incluso en entornos pequeños y es uno de los mejores argumentos para implementar la zonificación. Los subconjuntos lógicos de la estructura creados por la división en zonas eliminan los problemas de la comunicación por zonas.

- La división en zonas reduce el número de rutas disponibles a un puerto FC, FC-NVMe o FCoE en particular y reduce el número de rutas entre un host y una LUN en particular que se puede ver.

Por ejemplo, algunas soluciones multivía del SO del host tienen limitado el número de rutas que pueden gestionar. La división en zonas puede reducir el número de zonas que ve un controlador multivía de SO. Si un host no tiene una solución multivía instalada, debe verificar que solo pueda verse una ruta a un LUN mediante la división en zonas en la estructura o una combinación de asignación de LUN selectiva (SLM) y conjuntos de puertos en la SVM.

- La división en zonas aumenta la seguridad al limitar el acceso y la conectividad a los puntos finales que comparten una zona común.

Los puertos que no tienen zonas en común no se pueden comunicar entre sí.

- La división en zonas mejora la fiabilidad DE SAN aislando los problemas que se producen y contribuye a reducir el tiempo de resolución de problemas limitando el espacio disponible.

Recomendaciones para la división en zonas

- Debe implementar la división en zonas en cualquier momento, si cuatro o más hosts están conectados a UNA SAN, o si SLM no se implementa en los nodos de una SAN.
- Aunque es posible aplicar la división en zonas de nombre de nodo WWNN con algunos proveedores de switch, se requiere la división en zonas de nombres de puerto WWPN para definir correctamente un puerto específico y utilizar NPIV con eficacia.
- Debe limitar el tamaño de la zona mientras mantiene la capacidad de gestión.

Es posible superponer varias zonas para limitar el tamaño. Idealmente se debería definir una zona para cada host o cada clúster de hosts.

- Debe utilizar la división en zonas de un único iniciador para eliminar la comunicación entre zonas de los HBA del iniciador.

División en zonas basada en World Wide Name

La división en zonas basada en nombre WWN especifica el nombre WWN de los miembros que se incluirán en la zona. Al dividir en zonas en ONTAP, debe usar la división en zonas de nombre de puerto WWPN.

La división en zonas de nombres de puerto WWPN aporta flexibilidad porque el acceso no está determinado por el lugar físico de conexión entre el dispositivo y la estructura. Puede mover un cable de un puerto a otro sin tener que configurar las zonas de nuevo.

Para las rutas Fibre Channel a controladoras de almacenamiento que ejecutan ONTAP, asegúrese de que sus switches se dividen mediante los WWPN de las interfaces lógicas (LIF) objetivo, no los WWPN de los puertos físicos en el nodo. Para obtener más información acerca de las LIF, consulte la *Guía de gestión de redes ONTAP*.

Zonas individuales

En la configuración recomendada de la división por zonas, hay un iniciador de host por zona. La zona consta de un puerto de iniciador de host y uno o varios LIF de destino en los nodos de almacenamiento que proporcionan acceso a las LUN hasta el número deseado de rutas por destino. Esto significa que los hosts que acceden a los mismos nodos no pueden ver los puertos del otro, pero cada iniciador puede acceder a cualquier nodo.

Debería añadir todas las LIF de la máquina virtual de almacenamiento (SVM) a la zona con el iniciador del host. Esto le permite mover volúmenes o LUN sin editar sus zonas existentes ni crear zonas nuevas.

Para las rutas Fibre Channel a los nodos que ejecutan ONTAP, asegúrese de que sus switches se dividen mediante los WWPN de las interfaces lógicas (LIF) objetivo, no los WWPN de los puertos físicos en el nodo. Los WWPN de los puertos físicos comienzan por «'50» y los WWPN de las LIF empiezan por «'20».

División en zonas de estructura única

En una configuración de estructura única, puede seguir conectando cada iniciador de host a cada nodo de almacenamiento. Se requiere un software multivía en el host para administrar varias rutas. Cada host debería tener dos iniciadores para que la multivía ofrezca resiliencia en la solución.

Cada iniciador debería tener como mínimo un LIF desde cada nodo a el que pueda acceder el iniciador. La división en zonas debe permitir al menos una ruta desde el iniciador de host al par de nodos del clúster para proporcionar una ruta para la conectividad de LUN. Esto significa que cada iniciador del host podría tener solo un LIF de destino por nodo en su configuración de zonas. Si hay algún requisito para la multivía en el mismo nodo o en varios nodos del clúster, cada nodo tendrá varias LIF por nodo en su configuración de zona. Esto permite que el host siga teniendo acceso a sus LUN si un nodo falla o se mueve un volumen que contiene la LUN a un nodo diferente. Esto también requiere que los nodos de generación de informes se establezcan correctamente.

Se admiten las configuraciones de estructura única, pero no se consideran de alta disponibilidad. El error de un componente único puede provocar la pérdida del acceso a los datos.

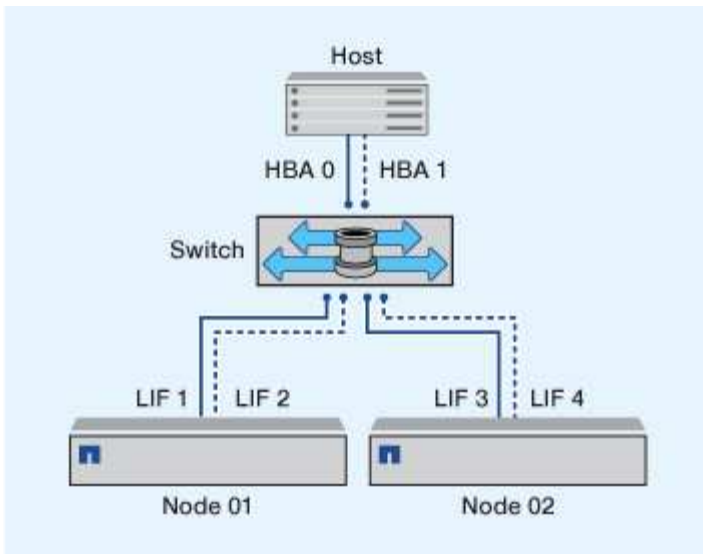
En la figura siguiente, el host tiene dos iniciadores y está ejecutando un software multivía. Hay dos zonas:



La convención de nomenclatura utilizada en esta figura es solo una recomendación de una posible convención de nomenclatura que puede usar para su solución de ONTAP.

- Zona 1: HBA 0, LIF_1 y LIF_3
- Zona 2: HBA 1, LIF_2 y LIF_4

Si la configuración incluía más nodos, las LIF de los nodos adicionales se incluirían en estas zonas.



En este ejemplo también puede tener las cuatro LIF en cada zona. En ese caso, las zonas serían las siguientes:

- Zona 1: HBA 0, LIF_1, LIF_2, LIF_3 y LIF_4
- Zona 2: HBA 1, LIF_1, LIF_2, LIF_3 y LIF_4



El sistema operativo host y el software multivía deben ser compatibles con el número de rutas compatibles que se están utilizando para acceder a las LUN de los nodos. Para determinar el número de rutas utilizadas para acceder a las LUN de los nodos, consulte la sección Límites de configuración DE SAN.

Información relacionada

["Hardware Universe de NetApp"](#)

División en zonas de pares de alta disponibilidad de estructura doble

En configuraciones de estructura doble, puede conectar cada iniciador de host a cada nodo del clúster. Cada iniciador de host utiliza un switch diferente para acceder a los nodos del clúster. Se requiere un software multivía en el host para administrar varias rutas.

Las configuraciones de estructura doble se consideran de alta disponibilidad porque se mantiene el acceso a los datos en caso de que falle un único componente.

En la figura siguiente, el host tiene dos iniciadores y está ejecutando un software multivía. Hay dos zonas. SLM se configura de modo que todos los nodos se consideran nodos de generación de informes.



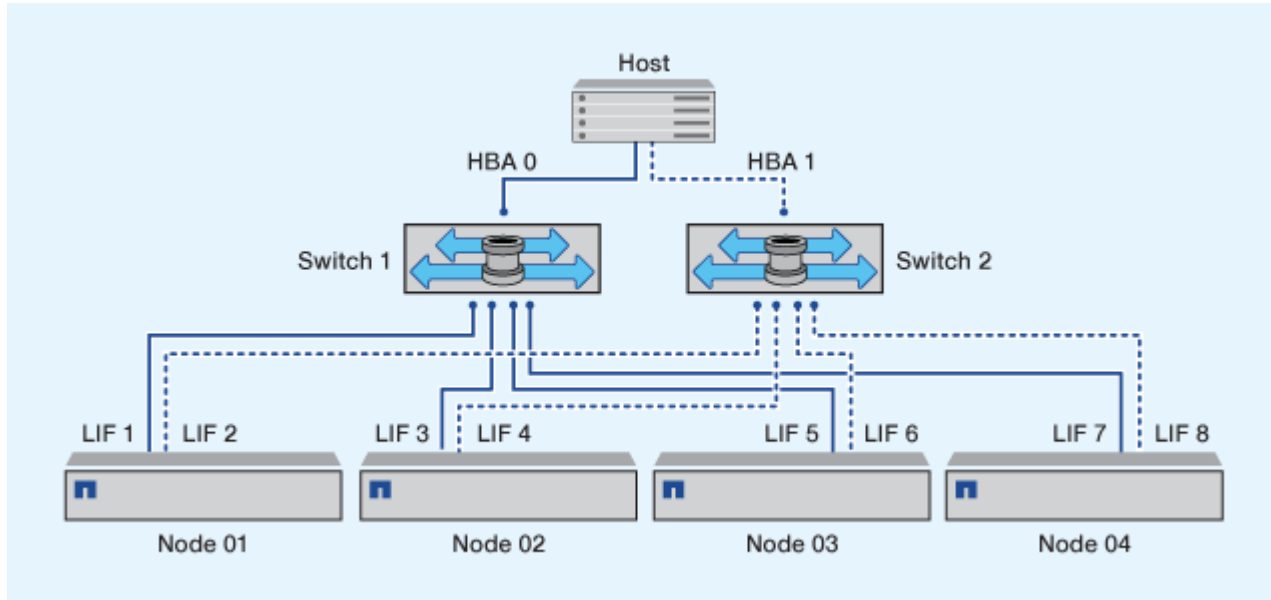
La convención de nomenclatura utilizada en esta figura es solo una recomendación de una posible convención de nomenclatura que puede usar para su solución de ONTAP.

- Zona 1: HBA 0, LIF_1, LIF_3, LIF_5 y LIF_7
- Zona 2: HBA 1, LIF_2, LIF_4, LIF_6 y LIF_8

Cada iniciador de host se zonas mediante un switch diferente. Se accede a la zona 1 a través del conmutador 1. Se accede a la zona 2 a través del conmutador 2.

Cada iniciador puede acceder a una LIF en todos los nodos. Esto permite que el host siga teniendo acceso a sus LUN si un nodo da error. Los SVM tienen acceso a todos los LIF iSCSI y FC de todos los nodos de una solución en clúster según el ajuste de asignación de LUN selectiva (SLM) y la configuración del nodo de generación de informes. Puede utilizar la división en zonas de SLM, conjuntos de puertos o switch de FC para reducir el número de rutas de una SVM al host y el número de rutas de una SVM a un LUN.

Si la configuración incluía más nodos, las LIF de los nodos adicionales se incluirían en estas zonas.



El sistema operativo host y el software multivía tienen que admitir el número de rutas que se están utilizando para acceder a las LUN en los nodos.

Información relacionada

["Hardware Universe de NetApp"](#)

Restricciones de división en zonas para switches Cisco FC y FCoE

Cuando se usan switches Fibre Channel y FCoE de Cisco, una única zona estructural no debe contener más de un LIF de destino para el mismo puerto físico. Si hay varias LIF en el mismo puerto en la misma zona, es posible que los puertos LIF no puedan recuperarse de una pérdida de conexión.

Los switches FC normales se utilizan para el protocolo FC-NVMe exactamente del mismo modo que se utilizan para el protocolo FC.

- Varios LIF para los protocolos FC y FCoE, pueden compartir puertos físicos en un nodo siempre y cuando se encuentren en zonas diferentes.
- FC-NVMe y FCoE no pueden compartir el mismo puerto físico.
- FC y FC-NVMe pueden compartir el mismo puerto físico de 32 GB.
- Los switches FC y FCoE de Cisco requieren que cada LIF de un puerto dado esté en una zona separada de los otros LIF de ese puerto.
- Una sola zona puede tener tanto LIF FC como FCoE. Una zona puede contener un LIF de todos los puertos de destino del clúster, pero tenga cuidado de no superar los límites de ruta del host y verificar la configuración de SLM.

- Los LIF de diferentes puertos físicos pueden estar en la misma zona.
- Los switches de Cisco requieren que se separen las LIF.

Aunque no es necesario, se recomienda separar las LIF para todos los switches

Requisitos para configuraciones SAN compartidas

Las configuraciones DE SAN compartidas se definen como hosts conectados tanto a los sistemas de almacenamiento de ONTAP como a los de otros proveedores. Siempre que se cumplan varios requisitos, se admitirá el acceso a sistemas de almacenamiento de ONTAP y sistemas de almacenamiento de otros proveedores desde un único host.

Para todos los sistemas operativos host, se recomienda usar adaptadores independientes para conectarse a los sistemas de almacenamiento de cada proveedor. El uso de adaptadores independientes reduce las posibilidades de que existan conflictos entre controladores y configuraciones. En el caso de las conexiones con un sistema de almacenamiento ONTAP, el modelo de adaptador, la BIOS, el firmware y el controlador deben aparecer como compatibles con la herramienta de matriz de interoperabilidad de NetApp.

Debe configurar los valores de tiempo de espera necesarios o recomendados y otros parámetros de almacenamiento para el host. Debe instalar siempre el software de NetApp o aplicar en último lugar los ajustes de NetApp.

- Para AIX, debe aplicar los valores de la versión de AIX Host Utilities que se enumeran en la herramienta de matriz de interoperabilidad para la configuración.
- En el caso de ESX, debe aplicar la configuración del host mediante Virtual Storage Console para VMware vSphere.
- Para HP-UX, debe usar la configuración de almacenamiento predeterminada de HP-UX.
- Para Linux, debe aplicar los valores de la versión de Linux Host Utilities que se enumeran en la herramienta de matriz de interoperabilidad para la configuración.
- Para Solaris, debe aplicar los valores de la versión de Solaris Host Utilities que se enumeran en la herramienta de matriz de interoperabilidad para su configuración.
- Para Windows, debe instalar la versión de Windows Host Utilities que se muestra en la herramienta de matriz de interoperabilidad para la configuración.

Información relacionada

["Herramienta de matriz de interoperabilidad de NetApp"](#)

Configuraciones SAN en un entorno MetroCluster

Configuraciones SAN en un entorno MetroCluster

Debe tener en cuenta determinados aspectos que se deben tener en cuenta al utilizar configuraciones DE SAN en un entorno de MetroCluster.

- Las configuraciones de MetroCluster no son compatibles con las configuraciones VSAN «enrutadas» de estructura FC de interfaz.
- A partir de ONTAP 9.12.1, las configuraciones IP de MetroCluster de cuatro nodos son compatibles con NVMe/FC. Las configuraciones de MetroCluster no son compatibles con NVMe/TCP. Las configuraciones de MetroCluster no son compatibles con NVMe antes de ONTAP 9.12.1.

- La configuración de MetroCluster admite otros protocolos SAN, como iSCSI, FC y FCoE.
- Al usar las configuraciones del cliente SAN, debe comprobar si se incluye alguna consideraciones especiales para las configuraciones de MetroCluster en las notas que se proporcionan en la ["Herramienta de matriz de interoperabilidad de NetApp" \(IMT\)](#).
- Los sistemas operativos y las aplicaciones deben proporcionar una resiliencia de I/O de 120 segundos para admitir la conmutación por cierre automática no planificada de MetroCluster y la conmutación de sitios iniciada por tiebreaker o de Mediator.
- MetroCluster utiliza los mismos WWPN en ambos lados de LA SAN front-end.

Información relacionada

- ["Comprender la protección de datos y la recuperación ante desastres de MetroCluster"](#)
- ["Artículo de la base de conocimientos: ¿Cuáles son las consideraciones de compatibilidad del host AIX en una configuración de MetroCluster?"](#)
- ["Artículo de la base de conocimientos: Consideraciones de compatibilidad del host Solaris en una configuración de MetroCluster"](#)

Evite la superposición de puertos entre la conmutación de sitios y la conmutación de estado

En un entorno SAN, puede configurar los switches de interfaz para evitar la superposición cuando el puerto antiguo se desconecta y el nuevo puerto se conecta.

Durante la conmutación de sitios, el puerto FC del sitio superviviente podría iniciar sesión en la estructura antes de que la estructura haya detectado que el puerto FC del sitio de desastre está sin conexión y ha eliminado este puerto de los servicios de nombre y directorio.

Si el puerto FC del desastre aún no se ha eliminado, el intento de inicio de sesión estructural del puerto FC del sitio superviviente podría ser rechazado debido a un WWPN duplicado. Este comportamiento de los switches FC puede cambiarse para respetar el inicio de sesión del dispositivo anterior y no el existente. Debe comprobar los efectos de este comportamiento en otros dispositivos de estructura. Póngase en contacto con el proveedor de switches para obtener más información.

Elija el procedimiento correcto según el tipo de interruptor.

Ejemplo 14. Pasos

Switch Cisco

1. Conéctese al switch e inicie sesión.
2. Entrar al modo de configuración:

```
switch# config t  
switch(config)#
```

3. Sobrescribir la primera entrada del dispositivo en la base de datos del servidor de nombres con el nuevo dispositivo:

```
switch(config)# no fcns reject-duplicate-pwvn vsan 1
```

4. En los switches que ejecutan NX-OS 8.x, confirme que el tiempo de espera de inactividad de flogi está configurado en cero:

- a. Visualizar la temporal de inactividad:

```
switch(config)# show flogi interval info \\\ i quiesce
```

```
Stats:  fs flogi quiesce timerval:  0
```

- b. Si la salida en el paso anterior no indica que el tiempo es cero, entonces configúrelo en cero:

```
switch(config)# flogi scale enable
```

```
switch(config)$ flogi quiesce timeout 0
```

Switch Brocade

1. Conéctese al switch e inicie sesión.
2. Introduzca el switchDisable comando.
3. Introduzca el configure y pulse y en el prompt de.

```
F-Port login parameters (yes, y, no, n): [no] y
```

4. Seleccione el ajuste 1:

```
- 0: First login take precedence over the second login (default)  
- 1: Second login overrides first login.  
- 2: the port type determines the behavior  
Enforce FLOGI/FDISC login: (0..2) [0] 1
```

5. Responda a las preguntas restantes o pulse **Ctrl + D**.

6. Introduzca el `switchEnable` comando.

Información relacionada

["Realizar la conmutación de sitios para pruebas o mantenimiento"](#)

Compatibilidad con host para accesos múltiples

Compatibilidad con host para información general sobre multivía

ONTAP siempre utiliza ALUA (Asymmetric Logical Unit Access) para las rutas FC e iSCSI. Asegúrese de utilizar configuraciones host que sean compatibles con ALUA para los protocolos FC e iSCSI.

A partir de la conmutación por error/retorno de una pareja de ha multivía de ONTAP 9.5, se admite la configuración de NVMe mediante Asynchronous Namespace Access (ANA). En ONTAP 9.4, NVMe solo admite una ruta desde el host al destino. El host de aplicación debe gestionar la conmutación por error en la ruta a su partner de alta disponibilidad (ha).

Para obtener información sobre qué configuraciones de host específicas admiten ALUA o ANA, consulte ["Herramienta de matriz de interoperabilidad de NetApp"](#) y.. ["Configuración de host SAN ONTAP"](#) para el sistema operativo del host.

Cuando se requiere un software multivía para el host

Si hay más de una ruta desde las interfaces lógicas (LIF) de la máquina virtual de almacenamiento hasta la estructura, se requiere un software multivía. Se requiere un software multivía en el host siempre que el host pueda acceder a una LUN a través de más de una ruta.

El software multivía presenta un disco único al sistema operativo para todas las rutas que se dirigen a una LUN. Sin un software multivía, el sistema operativo trataría cada una de las partes como un disco independiente, lo cual provocaría daños en los datos.

Se considera que su solución tiene varias rutas si dispone de alguna de las siguientes opciones:

- Un único puerto iniciador del host conectando varios LIF SAN en la SVM
- Varios puertos de iniciador conectando a un único LIF SAN en la SVM
- Varios puertos de iniciador conectando varios LIF SAN en la SVM

Se recomienda el software multivía en configuraciones de alta disponibilidad. Además de la asignación selectiva de LUN, se recomienda usar la división en zonas o los conjuntos de puertos de switch FC para limitar las rutas utilizadas para acceder a las LUN.

El software multivía también se conoce como software MPIO (I/o multivía).

Número recomendado de rutas desde el host a los nodos en el clúster

No debe exceder de ocho rutas desde el host a cada nodo del clúster, prestando atención al número total de rutas compatibles con el sistema operativo del host y la

multivía utilizada en el host.

Debe tener un mínimo de dos rutas por LUN conectadas a cada nodo de generación de informes a través de la asignación de LUN selectiva (SLM) que utiliza la máquina virtual de almacenamiento (SVM) del clúster. De este modo, se eliminan los puntos únicos de error y el sistema puede sobrevivir a fallos de componentes.

Si tiene cuatro o más nodos en el clúster o más de cuatro puertos de destino que utilizan las SVM en cualquiera de los nodos, Puede usar los siguientes métodos para limitar el número de rutas que se pueden utilizar para acceder a las LUN de los nodos de modo que no supere el máximo recomendado de ocho rutas.

- SLM

SLM reduce el número de rutas entre el host y la LUN solo a rutas del nodo que posee el LUN y el partner de alta disponibilidad del nodo propietario. SLM está habilitado de forma predeterminada.

- Conjuntos de puertos para iSCSI
- Asignaciones de igroup de FC desde el host
- División en zonas de switches FC

Información relacionada

["Administración de SAN"](#)

Límites de configuración

Determinar el número de nodos compatibles para las configuraciones SAN

El número de nodos por clúster que admite ONTAP varía en función de la versión de ONTAP, los modelos de controladora de almacenamiento del clúster y el protocolo de los nodos del clúster.

Acerca de esta tarea

Si alguno de los nodos del clúster está configurado para FC, FC-NVMe, FCoE o iSCSI, ese clúster se limita a los límites de nodos SAN. Los límites de nodos basados en las controladoras de su clúster se enumeran en *Hardware Universe*.

Pasos

1. Vaya a ["Hardware Universe de NetApp"](#).
2. Haga clic en **plataformas** en la parte superior izquierda (junto al botón **Inicio**) y seleccione el tipo de plataforma.
3. Seleccione la casilla de verificación junto a su versión de ONTAP.

Se mostrará una nueva columna para que pueda elegir sus plataformas.

4. Active las casillas junto a las plataformas utilizadas en su solución.
5. Anule la selección de la casilla de verificación **Seleccionar todo** en la columna **Seleccionar las especificaciones**.
6. Active la casilla de verificación **nodos máximos por clúster (NAS/SAN)**.
7. Haga clic en **Mostrar resultados**.

Información relacionada

Determinar el número de hosts compatibles por clúster en configuraciones FC y FC-NVMe

El número máximo de hosts SAN que se pueden conectar a un clúster varía en gran medida según su combinación específica de varios atributos de clúster, como el número de hosts conectados a cada nodo del clúster, iniciadores por host, sesiones por host y nodos en el clúster.

Acerca de esta tarea

Para las configuraciones de FC y FC-NVMe, debe usar el número de anexos de destino del iniciador (ITN) en el sistema para determinar si puede añadir más hosts al clúster.

Un ITN representa una ruta desde el iniciador del host hasta el destino del sistema de almacenamiento. El número máximo de ITN por nodo en las configuraciones de FC y FC-NVMe es 2,048. Siempre que esté por debajo del número máximo de ITN, puede continuar agregando hosts al clúster.

Para determinar el número de ITN utilizados en su clúster, realice los siguientes pasos para cada nodo del clúster.

Pasos

1. Identificar todas las LIF de un nodo determinado.
2. Ejecute el siguiente comando para cada LIF en el nodo:

```
fc initiator show -fields wwpn, lif
```

El número de entradas que se muestran en la parte inferior del resultado del comando representa el número de ITN para esa LIF.

3. Registre el número de ITN que se muestran para cada LIF.
4. Añada el número de ITN para cada LIF de todos los nodos del clúster.

Este total representa el número de ITN de su clúster.

Determinar el número admitido de hosts en configuraciones iSCSI

El número máximo de hosts SAN que se pueden conectar en configuraciones iSCSI varía en gran medida en función de su combinación específica de varios atributos de clúster, como el número de hosts conectados a cada nodo del clúster, iniciadores por host, inicios de sesión por host y nodos en el clúster.

Acerca de esta tarea

El número de hosts que se pueden conectar directamente a un nodo o que se pueden conectar mediante uno o más switches depende del número de puertos Ethernet disponibles. El número de puertos Ethernet disponibles está determinado por el modelo de la controladora y el número y tipo de adaptadores instalados en la controladora. El número de puertos Ethernet admitidos para controladoras y adaptadores está disponible en *Hardware Universe*.

Para todas las configuraciones de clústeres multinodo, debe determinar el número de sesiones iSCSI por nodo para saber si puede añadir más hosts al clúster. Siempre que el clúster se encuentre por debajo del número máximo de sesiones iSCSI por nodo, puede continuar añadiendo hosts al clúster. El número máximo

de sesiones iSCSI por nodo varía en función de los tipos de controladoras del clúster.

Pasos

1. Identificar todos los grupos de portal de destino en el nodo.
2. Compruebe el número de sesiones iSCSI para cada grupo de portales de destino del nodo:

```
iscsi session show -tpgroup tpgroup
```

El número de entradas que se muestra en la parte inferior del resultado del comando representa el número de sesiones iSCSI para ese grupo de portales de destino.

3. Registre el número de sesiones iSCSI que se muestran para cada grupo de portales de destino.
4. Agregue el número de sesiones iSCSI para cada grupo de portales de destino en el nodo.

El total representa la cantidad de sesiones iSCSI en el nodo.

Límites de configuración de switch de FC

Los switches de Fibre Channel tienen límites máximos de configuración, incluyendo el número de inicios de sesión compatibles por puerto, grupo de puertos, blade y switch. Los proveedores de switch documentan sus propios límites.

Cada interfaz lógica de FC (LIF) se registra en un puerto del switch de FC. El número total de inicios de sesión desde un único destino en el nodo es igual al número de LIF más un inicio de sesión para el puerto físico subyacente. No supere los límites de configuración del proveedor del switch para inicios de sesión u otros valores de configuración. Esto también contiene true para los iniciadores que se utilizan en el lado del host en entornos virtualizados con NPIV habilitado. No supere los límites de configuración del proveedor del switch para inicios de sesión para el destino o los iniciadores que se están utilizando en la solución.

Límites del switch Brocade

Encontrará los límites de configuración de los switches Brocade en las *Brocade Scalability Guidelines*.

Límites de switches de Cisco Systems

Puede encontrar los límites de configuración para switches de Cisco en la ["Límites de configuración de Cisco"](#) Guía para su versión del software de switch de Cisco.

Visión general de profundidad de cola

Es posible que deba ajustar la profundidad de la cola FC en el host para obtener los valores máximos de ITN por nodo y de «fan-in» de puertos FC. El número máximo de LUN y el número de HBA que pueden conectarse a un puerto de FC están limitados por la profundidad de cola disponible en los puertos de destino FC.

Acerca de esta tarea

La profundidad de cola es el número de solicitudes de I/O (comandos SCSI) que se pueden poner en cola a la vez en una controladora de almacenamiento. Cada solicitud de I/O del HBA del iniciador del host al adaptador de destino de la controladora de almacenamiento consume una entrada de cola. Normalmente, una mayor profundidad de cola equivale a un mejor rendimiento. Sin embargo, si se alcanza la profundidad máxima de cola del controlador de almacenamiento, ese controlador de almacenamiento rechaza los comandos entrantes

devolviendo una respuesta QFULL a ellos. Si un gran número de hosts acceden a un controlador de almacenamiento, debe planificar cuidadosamente para evitar las condiciones de QFULL, lo que reduce significativamente el rendimiento del sistema y puede provocar errores en algunos sistemas.

En una configuración con varios iniciadores (hosts), todos los hosts deben tener profundidades de cola similares. Debido a la desigualdad en la profundidad de cola entre los hosts conectados a la controladora de almacenamiento a través del mismo puerto objetivo, los hosts con profundidades de cola más pequeñas se ven privados del acceso a los recursos por parte de hosts con profundidades de cola más grandes.

Se pueden hacer las siguientes recomendaciones generales sobre las profundidades de cola de "tuning":

- Para sistemas pequeños y medianos, use una profundidad de cola HBA de 32.
- Para sistemas grandes, utilice una profundidad de cola de HBA de 128.
- Para casos excepcionales o pruebas de rendimiento, utilice una profundidad de cola de 256 para evitar posibles problemas de cola.
- Todos los hosts deben tener las profundidades de cola establecidas en valores similares para proporcionar un acceso igual a todos los hosts.
- Para evitar pérdidas de rendimiento o errores, no se debe exceder la profundidad de cola de puertos FC de destino de la controladora de almacenamiento.

Pasos

1. Cuente el número total de iniciadores de FC de todos los hosts que se conectan a un puerto de destino de FC.
2. Multiplique por 128.
 - Si el resultado es inferior a 2,048, establezca la profundidad de cola de todos los iniciadores en 128. Hay 15 hosts con un iniciador conectado a cada uno de los dos puertos de destino de la controladora de almacenamiento. $15 \times 128 = 1,920$. Como 1,920 es menor que el límite total de profundidad de cola de 2,048, puede establecer la profundidad de cola de todos los iniciadores en 128.
 - Si el resultado es superior a 2,048, vaya al paso 3. Tiene 30 hosts con un iniciador conectado a cada uno de dos puertos de destino de la controladora de almacenamiento. $30 \times 128 = 3,840$. Dado que 3,840 es mayor que el límite total de profundidad de cola de 2,048, debe elegir una de las opciones del paso 3 para la corrección.
3. Seleccione una de las siguientes opciones para añadir más hosts a la controladora de almacenamiento.
 - Opción 1:
 - i. Añada más puertos de destino FC.
 - ii. Redistribuya los iniciadores de FC.
 - iii. Repita los pasos 1 y 2.

La profundidad de cola deseada de 3,840 excede la profundidad de cola disponible por puerto. Para solucionarlo, puede añadir un adaptador de destino FC de dos puertos a cada controladora y volver a dividir los switches de FC de modo que 15 de sus 30 hosts se conecten a un conjunto de puertos y los 15 hosts restantes se conecten a un segundo conjunto de puertos. La profundidad de cola por puerto se reduce a $15 \times 128 = 1,920$.
 - Opción 2:
 - i. Designar a cada huésped como «grande» o «centro comercial» basándose en su necesidad prevista de I/O.
 - ii. Multiplique el número de iniciadores grandes por 128.

- iii. Multiplique el número de iniciadores pequeños por 32.
- iv. Añada los dos resultados juntos.
- v. Si el resultado es inferior a 2,048, establezca la profundidad de cola de los hosts grandes en 128 y la profundidad de cola de los hosts pequeños en 32.
- vi. Si el resultado es aún mayor que 2,048 por puerto, reduzca la profundidad de cola por iniciador hasta que la profundidad total de la cola sea inferior o igual a 2,048.



Para estimar la profundidad de cola necesaria para obtener un determinado rendimiento de I/O por segundo, utilice esta fórmula:

Profundidad de cola necesaria = (número de operaciones de I/O por segundo) × (tiempo de respuesta)

Por ejemplo, si necesita 40,000 E/S por segundo con un tiempo de respuesta de 3 milisegundos, la profundidad de cola necesaria = $40,000 \times (.003) = 120$.

El número máximo de hosts que se pueden conectar a un puerto de destino es 64 si decide limitar la profundidad de cola a la recomendación básica de 32. Sin embargo, si decide tener una profundidad de cola de 128, puede haber un máximo de 16 hosts conectados a un puerto de destino. Cuanto mayor sea la profundidad de la cola, menos hosts serán compatibles con un único puerto de destino. Si su requisito es tal que no pueda comprometer la profundidad de cola, debería obtener más puertos de destino.

La profundidad de cola deseada de 3,840 excede la profundidad de cola disponible por puerto. Cuenta con 10 hosts «grandes» que tienen unas necesidades elevadas de I/O de almacenamiento y 20 hosts «de centros comerciales» con necesidades bajas de I/O. Configure la profundidad de la cola del iniciador en los hosts grandes en 128 y la profundidad de la cola del iniciador en los hosts pequeños en 32.

La profundidad total de la cola resultante es de $(10 \times 128) + (20 \times 32) = 1,920$.

Puede distribuir la profundidad de cola disponible de forma equitativa entre cada iniciador.

La profundidad de cola resultante por iniciador es de $2,048 \div 30 = 68$.

Establecer profundidades de cola en hosts SAN

Es posible que deba cambiar las profundidades de cola del host para alcanzar los valores máximos de ITN por nodo y de fan-in de puertos FC.

Hosts AIX

Puede cambiar la profundidad de cola en los hosts AIX mediante el `chdev` comando. Cambios realizados mediante `chdev` el comando persiste durante todos los reinicios.

Ejemplos:

- Para cambiar la profundidad de cola del dispositivo `hdisk7`, utilice el siguiente comando:

```
chdev -l hdisk7 -a queue_depth=32
```

- Para cambiar la profundidad de cola del HBA `fcs0`, utilice el siguiente comando:

```
chdev -l fcs0 -a num_cmd_elems=128
```

El valor predeterminado para `num_cmd_elems` es 200. El valor máximo es 2.048.



Es posible que sea necesario desconectar el HBA para cambiar `num_cmd_elems` a continuación, vuelva a conectarlo en línea mediante el `rmdev -l fcs0 -R y..makdev -l fcs0 -P` comandos.

Hosts HP-UX

Puede cambiar la profundidad de la cola de dispositivos o LUN en hosts HP-UX mediante el parámetro kernel `scsi_max_qdepth`. Puede cambiar la profundidad de la cola del HBA mediante el parámetro kernel `max_fcp_reqs`.

- El valor predeterminado para `scsi_max_qdepth` es 8. El valor máximo es 255.

`scsi_max_qdepth` puede cambiarse dinámicamente en un sistema en ejecución mediante el `-u` en la `kmtune` comando. El cambio será efectivo para todos los dispositivos del sistema. Por ejemplo, utilice el siguiente comando para aumentar la profundidad de la cola de LUN a 64:

```
kmtune -u -s scsi_max_qdepth=64
```

Es posible cambiar la profundidad de la cola para archivos de dispositivo individuales mediante `scsictl` comando. Cambios mediante `scsictl` el comando no persiste entre reinicios del sistema. Para ver y cambiar la profundidad de cola de un archivo de dispositivo concreto, ejecute el siguiente comando:

```
scsictl -a /dev/rdisk/c2t2d0
```

```
scsictl -m queue_depth=16 /dev/rdisk/c2t2d0
```

- El valor predeterminado para `max_fcp_reqs` es 512. El valor máximo es 1024.

El kernel debe ser reconstruido y el sistema debe ser reiniciado para los cambios a `max_fcp_reqs` para que surta efecto. Para cambiar la profundidad de cola del HBA a 256, por ejemplo, utilice el siguiente comando:

```
kmtune -u -s max_fcp_reqs=256
```

Hosts Solaris

Puede establecer la profundidad de cola LUN y HBA para los hosts Solaris.

- Para profundidad de cola de LUN: El número de LUN en uso en un host multiplicado por el acelerador de por LUN (profundidad de cola de lun) debe ser menor o igual que el valor de profundidad de cola del GT en el host.
- Para profundidad de cola en una pila Sun: Los controladores nativos no permiten por LUN o por destino `max_throttle` Ajustes en el nivel del HBA. El método recomendado para establecer el `max_throttle` El valor de los controladores nativos se encuentra en el nivel VID_PID (por tipo de dispositivo) de la `/kernel/drv/sd.conf` y `/kernel/drv/ssd.conf` archivos. La utilidad de host establece este valor en 64 para configuraciones de MPxIO y 8 para configuraciones de Veritas DMP.

Pasos

1. # `cd/kernel/drv`

2. `# vi lpfc.conf`
3. Busque `/tft-queue (/tgt-queue)`

```
tgt-queue-depth=32
```



El valor predeterminado se establece en 32 durante la instalación.

4. Establezca el valor deseado en función de la configuración de su entorno.
5. Guarde el archivo.
6. Reinicie el host con el `sync; sync; sync; reboot -- -r` comando.

Hosts VMware para un HBA QLogic

Utilice la `esxcfg-module` Comando para cambiar la configuración de tiempo de espera de HBA. Actualizar manualmente la `esx.conf` no se recomienda el archivo.

Pasos

1. Inicie sesión en la consola de servicio como usuario raíz.
2. Utilice la `#vmkload_mod -l` Comando para verificar qué módulo Qlogic HBA está cargado actualmente.
3. Para una instancia única de un HBA Qlogic, ejecute el siguiente comando:

```
#esxcfg-module -s ql2xmaxqdepth=64 qla2300_707
```



En este ejemplo se utiliza el módulo `qla2300_707`. Utilice el módulo adecuado basado en la salida de `vmkload_mod -l`.

4. Guarde los cambios con el siguiente comando:

```
#!/usr/sbin/esxcfg-boot -b
```

5. Reinicie el servidor con el siguiente comando:

```
#reboot
```

6. Confirme los cambios con los siguientes comandos:

a. `#esxcfg-module -g qla2300_707`

b. `qla2300_707 enabled = 1 options = 'ql2xmaxqdepth=64'`

VMware host para un HBA Emulex

Utilice la `esxcfg-module` Comando para cambiar la configuración de tiempo de espera de HBA. Actualizar manualmente la `esx.conf` no se recomienda el archivo.

Pasos

1. Inicie sesión en la consola de servicio como usuario raíz.
2. Utilice la `#vmkload_mod -l grep lpfc` Comando para verificar qué HBA de Emulex está cargado actualmente.

3. Para una única instancia de un HBA de Emulex, introduzca el siguiente comando:

```
#esxcfg-module -s lpfc0_lun_queue_depth=16 lpfcdd_7xx
```



Dependiendo del modelo de HBA, el módulo puede ser lpfcdd_7xx o lpfcdd_732. El comando anterior utiliza el módulo lpfcdd_7xx. Debe utilizar el módulo adecuado en función del resultado de `vmkload_mod -l`.

Si se ejecuta este comando, la profundidad de la cola de LUN es 16 para el HBA que representa lpfc0.

4. Para varias instancias de un HBA Emulex, ejecute el siguiente comando:

```
a esxcfg-module -s "lpfc0_lun_queue_depth=16 lpfc1_lun_queue_depth=16"
lpfcdd_7xx
```

La profundidad de cola de LUN para lpfc0 y la profundidad de cola de LUN para lpfc1 está establecida en 16.

5. Introduzca el siguiente comando:

```
#esxcfg-boot -b
```

6. Reinicie mediante `#reboot`.

Host Windows para un HBA Emulex

En hosts Windows, puede utilizar el LPUTILNT Utilidad para actualizar la profundidad de cola para los HBA de Emulex.

Pasos

1. Ejecute el LPUTILNT utilidad ubicada en C:\WINNT\system32 directorio.
2. Seleccione **parámetros de accionamiento** en el menú de la derecha.
3. Desplácese hacia abajo y haga doble clic en **QueueDepth**.



Si está configurando **QueueDepth** superior a 150, también es necesario aumentar adecuadamente el siguiente valor del Registro de Windows:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\lpxnnds\Parameters\Device\NumberOfRequests
```

Hosts Windows para un HBA Qlogic

En hosts Windows, puede utilizar el SANsurfer Utilidad HBA Manager para actualizar las profundidades de cola para HBA Qlogic.

Pasos

1. Ejecute el SANsurfer Utilidad del gestor de HBA.
2. Haga clic en **Puerto HBA > Ajustes**.
3. Haga clic en **Configuración avanzada del puerto HBA** en el cuadro de lista.

4. Actualice el `Execution Throttle` parámetro.

Hosts Linux para HBA Emulex

Puede actualizar las profundidades de cola de un HBA Emulex en un host Linux. Para que las actualizaciones sean persistentes entre reinicios, debe crear una nueva imagen de disco RAM y reiniciar el host.

Pasos

1. Identificar los parámetros de profundidad de cola que se van a modificar:

```
modinfo lpfc|grep queue_depth
```

Se muestra la lista de parámetros de profundidad de cola con su descripción. Dependiendo de la versión del sistema operativo, puede modificar uno o más de los siguientes parámetros de profundidad de cola:

- `lpfc_lun_queue_depth`: Número máximo de comandos FC que se pueden poner en cola para una LUN específica (uint)
- `lpfc_hba_queue_depth`: Número máximo de comandos FC que se pueden poner en cola en un HBA lpfc (uint)
- `lpfc_tgt_queue_depth`: Número máximo de comandos FC que se pueden poner en cola en un puerto de destino específico (uint)

La `lpfc_tgt_queue_depth` El parámetro sólo se aplica a sistemas Red Hat Enterprise Linux 7.x, sistemas SUSE Linux Enterprise Server 11 SP4 y sistemas 12.x.

2. Actualice las profundidades de cola agregando los parámetros de profundidad de cola al `/etc/modprobe.conf` Archivo para un sistema Red Hat Enterprise Linux 5.x y para `/etc/modprobe.d/scsi.conf` Archivo para un sistema Red Hat Enterprise Linux 6.x o 7.x, o SUSE Linux Enterprise Server 11.x o 12.x.

Según la versión del sistema operativo, puede agregar uno o varios de los siguientes comandos:

- `options lpfc lpfc_hba_queue_depth=new_queue_depth`
- `options lpfc lpfc_lun_queue_depth=new_queue_depth`
- `options lpfc lpfc_tgt_queue_depth=new_queue_depth`

3. Cree una nueva imagen de disco RAM y, a continuación, reinicie el host para que las actualizaciones persistan entre reinicios.

Para obtener más información, consulte ["Administración del sistema"](#) Para su versión del sistema operativo Linux.

4. Compruebe que los valores de profundidad de cola se han actualizado para cada parámetro de profundidad de cola que haya modificado:

```
root@localhost ~]#cat /sys/class/scsi_host/host5/lpfc_lun_queue_depth
30
```

Se muestra el valor actual de la profundidad de cola.

Hosts Linux para HBA QLogic

Puede actualizar la profundidad de la cola de dispositivos de un controlador QLogic en un host Linux. Para que las actualizaciones sean persistentes entre reinicios, debe crear una nueva imagen de disco RAM y reiniciar el host. Puede usar la GUI de gestión de HBA de QLogic o la interfaz de línea de comandos (CLI) para modificar la profundidad de la cola de HBA de QLogic.

Esta tarea muestra cómo utilizar la interfaz de línea de comandos del HBA QLogic para modificar la profundidad de la cola del HBA QLogic

Pasos

1. Identifique el parámetro de profundidad de cola del dispositivo que se va a modificar:

```
modinfo qla2xxx | grep ql2xmaxqdepth
```

Solo puede modificar la `ql2xmaxqdepth` Parámetro de profundidad de cola, que indica la profundidad máxima de cola que se puede establecer para cada LUN. El valor predeterminado es 64 para RHEL 7.5 y versiones posteriores. El valor predeterminado es 32 para RHEL 7.4 y anteriores.

```
root@localhost ~]# modinfo qla2xxx|grep ql2xmaxqdepth
parm:          ql2xmaxqdepth:Maximum queue depth to set for each LUN.
Default is 64. (int)
```

2. Actualice el valor de profundidad de la cola del dispositivo:

- Si desea que las modificaciones sean persistentes, realice los siguientes pasos:
 - i. Actualice las profundidades de cola agregando el parámetro de profundidad de cola al `/etc/modprobe.conf` Archivo para un sistema Red Hat Enterprise Linux 5.x y para `/etc/modprobe.d/scsi.conf` Archivo para un sistema Red Hat Enterprise Linux 6.x o 7.x, o SUSE Linux Enterprise Server 11.x o 12.x: `options qla2xxx ql2xmaxqdepth=new_queue_depth`
 - ii. Cree una nueva imagen de disco RAM y, a continuación, reinicie el host para que las actualizaciones persistan entre reinicios.

Para obtener más información, consulte ["Administración del sistema"](#) Para su versión del sistema operativo Linux.

- Si solo desea modificar el parámetro para la sesión actual, ejecute el siguiente comando:

```
echo new_queue_depth > /sys/module/qla2xxx/parameters/ql2xmaxqdepth
```

En el siguiente ejemplo, la profundidad de cola se establece en 128.

```
echo 128 > /sys/module/qla2xxx/parameters/ql2xmaxqdepth
```

3. Compruebe que se actualizan los valores de profundidad de cola:

```
cat /sys/module/qla2xxx/parameters/ql2xmaxqdepth
```

Se muestra el valor actual de la profundidad de cola.

4. Modifique la profundidad de la cola del HBA QLogic actualizando el parámetro firmware `Execution Throttle` Desde el BIOS del HBA QLogic.

a. Inicie sesión en la CLI de gestión de los HBA de QLogic:

```
/opt/QLogic_Corporation/QConvergeConsoleCLI/qauccli
```

b. En el menú principal, seleccione `Adapter Configuration` opción.

```
[root@localhost ~]#  
/opt/QLogic_Corporation/QConvergeConsoleCLI/qauccli  
Using config file:  
/opt/QLogic_Corporation/QConvergeConsoleCLI/qauccli.cfg  
Installation directory: /opt/QLogic_Corporation/QConvergeConsoleCLI  
Working dir: /root
```

```
QConvergeConsole
```

```
CLI - Version 2.2.0 (Build 15)
```

```
Main Menu
```

```
1: Adapter Information  
**2: Adapter Configuration**  
3: Adapter Updates  
4: Adapter Diagnostics  
5: Monitoring  
6: FabricCache CLI  
7: Refresh  
8: Help  
9: Exit
```

```
Please Enter Selection: 2
```

c. En la lista de parámetros de configuración del adaptador, seleccione `HBA Parameters` opción.


```

1:  Adapter Alias
2:  Adapter Port Alias
**3:  HBA Parameters**
4:  Persistent Names (udev)
5:  Boot Devices Configuration
6:  Virtual Ports (NPIV)
7:  Target Link Speed (iidDMA)
8:  Export (Save) Configuration
9:  Generate Reports
10:  Personality
11:  FEC
(p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)
Please Enter Selection: 3

```

d. Seleccione el puerto HBA necesario de la lista de puertos HBA.

```

Fibre Channel Adapter Configuration

HBA Model QLE2562 SN: BFD1524C78510
  1: Port 1: WWPN: 21-00-00-24-FF-8D-98-E0 Online
  2: Port 2: WWPN: 21-00-00-24-FF-8D-98-E1 Online
HBA Model QLE2672 SN: RFE1241G81915
  3: Port 1: WWPN: 21-00-00-0E-1E-09-B7-62 Online
  4: Port 2: WWPN: 21-00-00-0E-1E-09-B7-63 Online

(p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)
Please Enter Selection: 1

```

Se muestran los detalles del puerto del HBA.

e. En el menú HBA Parameters, seleccione la Display HBA Parameters para ver el valor actual de Execution Throttle opción.

El valor predeterminado de Execution Throttle la opción es 65535.

```

HBA Parameters Menu

=====
HBA          : 2 Port: 1
SN           : BFD1524C78510
HBA Model    : QLE2562
HBA Desc.    : QLE2562 PCI Express to 8Gb FC Dual Channel
FW Version   : 8.01.02

```

```
WWPN          : 21-00-00-24-FF-8D-98-E0
WWNN          : 20-00-00-24-FF-8D-98-E0
Link          : Online
```

```
=====
```

- 1: Display HBA Parameters
- 2: Configure HBA Parameters
- 3: Restore Defaults

```
(p or 0: Previous Menu; m or 98: Main Menu; x or 99: Quit)
Please Enter Selection: 1
```

```
-----
```

```
-----
```

```
HBA Instance 2: QLE2562 Port 1 WWPN 21-00-00-24-FF-8D-98-E0 PortID 03-
07-00
Link: Online
```

```
-----
```

```
-----
```

```
Connection Options          : 2 - Loop Preferred, Otherwise Point-to-
Point
Data Rate                   : Auto
Frame Size                  : 2048
Hard Loop ID                : 0
Loop Reset Delay (seconds)  : 5
Enable Host HBA BIOS        : Enabled
Enable Hard Loop ID         : Disabled
Enable FC Tape Support      : Enabled
Operation Mode              : 0 - Interrupt for every I/O completion
Interrupt Delay Timer (100us) : 0
**Execution Throttle        : 65535**
Login Retry Count           : 8
Port Down Retry Count       : 30
Enable LIP Full Login       : Enabled
Link Down Timeout (seconds) : 30
Enable Target Reset         : Enabled
LUNs Per Target             : 128
Out Of Order Frame Assembly : Disabled
Enable LR Ext. Credits      : Disabled
Enable Fabric Assigned WWN  : N/A
```

```
Press <Enter> to continue:
```

- a. Pulse **Intro** para continuar.
- b. En el menú HBA Parameters, seleccione la Configure HBA Parameters Opción para modificar los parámetros del HBA.

- c. En el menú Configurar parámetros, seleccione `Execute Throttle` y actualice el valor de este parámetro.

Configure Parameters Menu

```
=====
HBA          : 2 Port: 1
SN           : BFD1524C78510
HBA Model    : QLE2562
HBA Desc.    : QLE2562 PCI Express to 8Gb FC Dual Channel
FW Version   : 8.01.02
WWPN         : 21-00-00-24-FF-8D-98-E0
WWNN         : 20-00-00-24-FF-8D-98-E0
Link         : Online
=====

1: Connection Options
2: Data Rate
3: Frame Size
4: Enable HBA Hard Loop ID
5: Hard Loop ID
6: Loop Reset Delay (seconds)
7: Enable BIOS
8: Enable Fibre Channel Tape Support
9: Operation Mode
10: Interrupt Delay Timer (100 microseconds)
11: Execution Throttle
12: Login Retry Count
13: Port Down Retry Count
14: Enable LIP Full Login
15: Link Down Timeout (seconds)
16: Enable Target Reset
17: LUNs per Target
18: Enable Receive Out Of Order Frame
19: Enable LR Ext. Credits
20: Commit Changes
21: Abort Changes

(p or 0: Previous Menu; m or 98: Main Menu; x or 99: Quit)
Please Enter Selection: 11
Enter Execution Throttle [1-65535] [65535]: 65500
```

- d. Pulse **Intro** para continuar.

- e. En el menú Configurar parámetros, seleccione `Commit Changes` opción para guardar los cambios.

f. Salga del menú.

Gestión del almacenamiento de objetos S3

Conozca el soporte de S3 en ONTAP 9

Información general de la configuración de S3

A partir de ONTAP 9.8, puede habilitar un servidor de almacenamiento de objetos ONTAP simple Storage Service (S3) en un clúster de ONTAP.

ONTAP es compatible con dos casos prácticos en las instalaciones para dar servicio al almacenamiento de objetos S3:

- Organización en niveles FabricPool para un bloque en el clúster local (nivel a un bloque local) o clúster remoto (nivel de cloud).
- Acceso de aplicación de cliente S3 a un bloque del clúster local o de un clúster remoto.

A partir de ONTAP 9.14.1, puede habilitar un servidor de almacenamiento de objetos S3 en una SVM en un agregado reflejado o no reflejado en configuraciones de IP y FC de MetroCluster.

A partir de ONTAP 9.12.1, se puede habilitar un servidor de almacenamiento de objetos S3 en una SVM en un agregado no reflejado en una configuración IP de MetroCluster. Para obtener más información sobre las limitaciones de los agregados no reflejados en las configuraciones IP de MetroCluster, consulte ["Consideraciones sobre los agregados no reflejados"](#).

Debe usar estos procedimientos si desea configurar el almacenamiento de objetos S3 de la siguiente manera:

- Desea proporcionar almacenamiento de objetos S3 desde un clúster existente que ejecuta ONTAP.

ONTAP S3 es adecuado si se desean funcionalidades de S3 en los clústeres existentes sin necesidad de hardware ni gestión adicionales. Sin embargo, el software NetApp StorageGRID sigue siendo la solución insignia de NetApp para el almacenamiento de objetos. Para obtener más información, consulte ["Documentación de StorageGRID"](#).

- Tiene privilegios de administrador de clúster, no de administrador de SVM.

Configuración de S3 con System Manager y la interfaz de línea de comandos de ONTAP

Puede configurar y gestionar ONTAP S3 con System Manager y la interfaz de línea de comandos de ONTAP. Cuando se habilita S3 y se crean bloques con System Manager, ONTAP selecciona los valores predeterminados de prácticas recomendadas para simplificar la configuración. Si es necesario especificar parámetros de configuración, se recomienda usar la CLI de ONTAP. Si configura el servidor y los bloques de S3 desde la CLI, puede seguir gestionarlos con System Manager si lo desea, o viceversa.

Cuando se crea un bloque de S3 con System Manager, ONTAP configura un nivel de servicio de rendimiento predeterminado que es el más alto disponible en el sistema. Por ejemplo, en un sistema AFF, el valor predeterminado sería **extremo**. Los niveles de servicio de rendimiento son grupos de políticas de calidad de servicio (QoS) adaptativas predefinidos. En lugar de uno de los niveles de servicio predeterminados, puede especificar un grupo de políticas de calidad de servicio personalizado o ningún grupo de políticas.

Los grupos de políticas de calidad de servicio adaptativas predefinidos son:

- **Extreme**: Se utiliza para aplicaciones que esperan la latencia más baja y el rendimiento más alto.

- **Rendimiento:** Se utiliza para aplicaciones con necesidades de rendimiento y latencia modestos.
- **Valor:** Se utiliza para aplicaciones para las que el rendimiento y la capacidad son más importantes que la latencia.
- **Personalizado:** Especifique una política de QoS personalizada o ninguna política de QoS.

Si selecciona **usar para clasificación por niveles**, no se seleccionan niveles de servicio de rendimiento y el sistema intenta seleccionar medios de bajo costo con un rendimiento óptimo para los datos organizados por niveles.

Consulte también: "[Utilice grupos de políticas de calidad de servicio adaptativos](#)".

ONTAP intenta aprovisionar este bloque en niveles locales que tengan los discos más adecuados para cumplir el nivel de servicio elegido. Sin embargo, si necesita especificar qué discos se incluirán en el bloque, considere la configuración del almacenamiento de objetos S3 desde la CLI especificando los niveles locales (agregado). Si configura el servidor S3 desde la CLI, puede seguir gestionarlo con System Manager si lo desea.

Si desea la capacidad de especificar qué agregados se utilizan para bloques, solo puede hacerlo mediante la CLI.

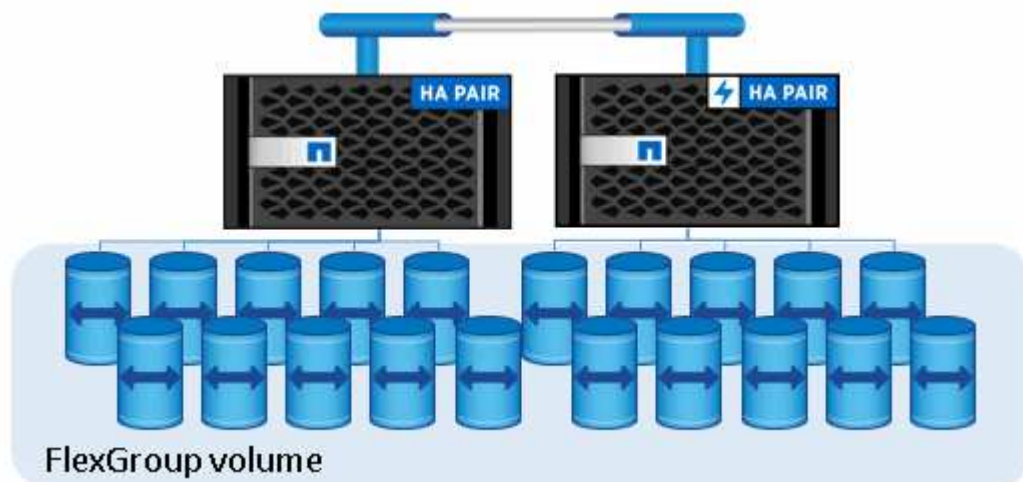
Configuración de bloques de S3 en Cloud Volumes ONTAP

Si desea servir bloques de Cloud Volumes ONTAP, se recomienda encarecidamente seleccionar manualmente los agregados subyacentes para garantizar que solo utilicen un nodo. El uso de agregados de ambos nodos puede afectar al rendimiento, ya que los nodos se encuentran en zonas de disponibilidad separadas geográficamente y, por lo tanto, pueden estar expuestos a problemas de latencia. Por lo tanto, en entornos Cloud Volumes ONTAP, debería hacerlo [Configurar cubos de S3 desde la interfaz de línea de comandos](#).

De lo contrario, los servidores S3 en Cloud Volumes ONTAP están configurados y mantenidos de la misma forma en Cloud Volumes ONTAP que en entornos locales.

Arquitectura

En ONTAP, la arquitectura subyacente para un bloque es un volumen FlexGroup, un espacio de nombres único que está compuesto por varios volúmenes constituyentes, pero que se gestiona como un único volumen.



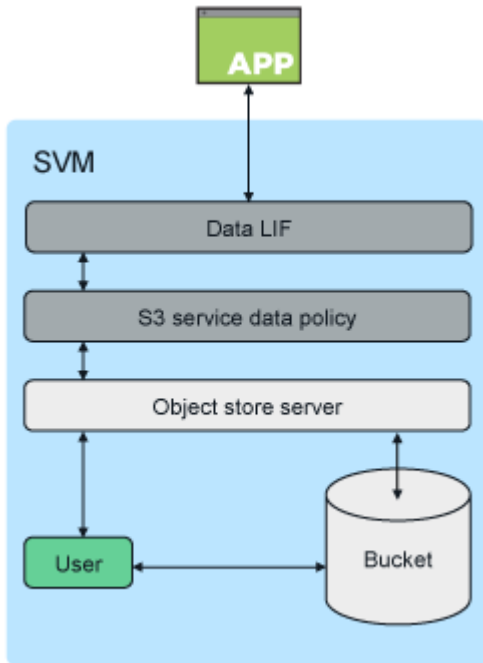
Los bloques solo están limitados por los máximos físicos del hardware subyacente, los máximos

arquitectónicos podrían ser mayores. Los bloques pueden aprovechar el tamaño elástico de FlexGroup para hacer crecer automáticamente un componente de un volumen FlexGroup si se está quedando sin espacio. Existe un límite de 1000 bloques por volumen de FlexGroup, o 1/3 de la capacidad del volumen de FlexGroup (para hacer frente al crecimiento de datos en bloques).



No se permite acceso al protocolo NAS o SAN al volumen FlexGroup que contiene bloques S3.

El acceso al bloque se proporciona a través de usuarios autorizados y aplicaciones cliente.



Casos de uso

Existen tres casos prácticos principales para el acceso de clientes a los servicios ONTAP S3:

- Para sistemas ONTAP que utilizan ONTAP S3 como nivel de capacidad de FabricPool remota (cloud)

El servidor y el bloque de S3 que contienen el nivel de capacidad (para datos *fríos*) se encuentran en un clúster diferente al nivel de rendimiento (para datos *hot*).

- Para los sistemas ONTAP que usan ONTAP S3 como nivel de FabricPool local

El servidor y el bloque de S3 que contiene el nivel de capacidad están en el mismo clúster, pero en un par de alta disponibilidad diferente, al nivel de rendimiento.

- Para aplicaciones de cliente S3 externas

ONTAP S3 da servicio a las aplicaciones cliente S3 que se ejecutan en sistemas que no son de NetApp.

Se recomienda proporcionar acceso a buckets de ONTAP S3 mediante HTTPS. Cuando HTTPS está habilitado, se requieren certificados de seguridad para una integración correcta con SSL/TLS. A continuación, se requieren claves secretas y de acceso de los usuarios clientes para autenticar el usuario con ONTAP S3, así como para autorizar los permisos de acceso de los usuarios para operaciones en ONTAP S3. La aplicación de cliente también debe tener acceso al certificado de CA raíz (el certificado firmado del servidor

ONTAP S3) para poder autenticar el servidor y crear una conexión segura entre el cliente y el servidor.

Los usuarios se crean dentro de la SVM habilitada para S3 y sus permisos de acceso se pueden controlar a nivel de bloque o SVM; es decir, se puede otorgar acceso a uno o más bloques dentro de la SVM.

De forma predeterminada, HTTPS está habilitado en los servidores ONTAP S3. Es posible deshabilitar HTTPS y habilitar HTTP para el acceso de cliente, en cuyo caso no se requiere la autenticación con certificados de CA. Sin embargo, cuando se habilita HTTP y HTTPS está deshabilitado, todas las comunicaciones con el servidor ONTAP S3 se envían por la red en texto sin cifrar.

Para obtener más información, consulte ["Informe técnico: S3 en las prácticas recomendadas de ONTAP"](#)

Información relacionada

["Gestión de volúmenes de FlexGroup"](#)

Planificación

Compatibilidad de versiones de ONTAP para el almacenamiento de objetos S3

ONTAP es compatible con el almacenamiento de objetos S3 para entornos locales que comienzan con ONTAP 9.8. Cloud Volumes ONTAP admite el almacenamiento de objetos S3 para entornos cloud que empiezan por ONTAP 9.9.1.

Compatibilidad de S3 con Cloud Volumes ONTAP

ONTAP S3 está configurado y funciona igual en Cloud Volumes ONTAP que en entornos locales, con una excepción:

- Los agregados subyacentes deben ser solo de un nodo. Más información acerca de ["Creación de bloques en entornos CVO"](#).

| Proveedor de cloud | Versión de ONTAP |
|--------------------|--------------------------------------|
| Azure | ONTAP 9.9.1 y versiones posteriores |
| AWS | ONTAP 9.11.0 y versiones posteriores |
| Google Cloud | ONTAP 9.12.1 y versiones posteriores |

Vista previa pública de S3 en ONTAP 9.7

En ONTAP 9.7, el almacenamiento de objetos S3 se introdujo como una vista previa pública. Esta versión no estaba destinada a entornos de producción y ya no se actualizará a partir de ONTAP 9.8. Solo ONTAP 9.8 y las versiones posteriores admiten el almacenamiento de objetos S3 en entornos de producción.

Los bloques de S3 creados con la vista previa pública de 9.7 pueden usarse en ONTAP 9.8 y versiones posteriores, pero no pueden aprovechar las mejoras de funciones. Si ha creado bloques con la vista previa pública de 9.7, debe migrar el contenido de esos bloques a 9.8 bloques para garantizar el soporte de la función, la seguridad y las mejoras de rendimiento.

Acciones compatibles con ONTAP S3

Las acciones de ONTAP S3 son compatibles con las API DE REST estándar de S3

excepto que se indica a continuación. Para obtener más detalles, consulte ["Referencia de la API de Amazon S3"](#).

Operaciones de bloques

Las siguientes operaciones son compatibles en ONTAP mediante las API S3 de AWS:

| Funcionamiento del cucharón | Soporte de ONTAP empezando por |
|---------------------------------|--|
| CreateBucket | ONTAP 9.11.1 |
| DeleteBucket | ONTAP 9.11.1 |
| DeleteBucketPolicy | ONTAP 9.12.1 |
| GetBucketAcl | ONTAP 9,8 |
| GetBucketLifecycleConfiguration | ONTAP 9.13.1 * solo se admiten acciones de caducidad |
| GetBucketLocation | ONTAP 9.10.1 |
| GetBucketPolicy | ONTAP 9.12.1 |
| Segmento de cabeza | ONTAP 9,8 |
| ListCuchers | ONTAP 9,8 |
| Control de versiones de lista | ONTAP 9.11.1 |
| ListObjectVersions | ONTAP 9.11.1 |
| PutBucket | <ul style="list-style-type: none">• ONTAP 9.11.1• ONTAP 9,8: Solo compatible con API DE REST DE ONTAP |
| PutBucketLifecycleConfiguration | ONTAP 9.13.1 * solo se admiten acciones de caducidad |
| Política de PutBucketPolicy | ONTAP 9.12.1 |

Operaciones de objeto

A partir de ONTAP 9.9.1, ONTAP S3 admite el etiquetado y los metadatos de objetos.

- PutObject y CreateMultipartUpload incluyen pares clave-valor mediante `x-amz-meta-<key>`.

Por ejemplo: `x-amz-meta-project: ontap_s3`.

- GetObject. Y HeadObject devuelven metadatos definidos por el usuario.
- A diferencia de los metadatos, las etiquetas se pueden leer independientemente de los objetos mediante:
 - PutObjectEtiquetado
 - GetObjectEtiquetado
 - DeleteObjectTagging

A partir de ONTAP 9.11.1, ONTAP S3 admite el control de versiones de objetos y acciones asociadas con

estas API de ONTAP:

- GetBucketVersioning
- ListBucketVersions
- PutBucketVersioning

| Operación de objeto | Soporte de ONTAP empezando por |
|----------------------------|--------------------------------|
| AbortMultipartUpload | ONTAP 9,8 |
| CompleteMultipartUpload | ONTAP 9,8 |
| CopyObject | ONTAP 9.12.1 |
| CreateMultipartUpload | ONTAP 9,8 |
| DeleteObject | ONTAP 9,8 |
| DeleteObjects | ONTAP 9.11.1 |
| DeleteObjectTagging | ONTAP 9.9.1 |
| GetBucketVersioning | ONTAP 9.11.1 |
| GetObject | ONTAP 9,8 |
| GetObjectAcl | ONTAP 9,8 |
| GetObjectRetention | ONTAP 9.14.1 |
| GetObjectEtiquetado | ONTAP 9.9.1 |
| Objeto principal | ONTAP 9,8 |
| ListMultipartUpload | ONTAP 9,8 |
| ListObjects | ONTAP 9,8 |
| ListObjectsV2 | ONTAP 9,8 |
| ListBucketVersions | ONTAP 9.11.1 |
| ListParts | ONTAP 9,8 |
| PutBucketVersioning | ONTAP 9.11.1 |
| Objeto de puta | ONTAP 9,8 |
| PutObjectLockConfiguration | ONTAP 9.14.1 |
| PutObjectRetention | ONTAP 9.14.1 |
| PutObjectEtiquetado | ONTAP 9.9.1 |
| UploadPart | ONTAP 9,8 |
| UploadPartCopy | ONTAP 9.12.1 |

Normativas de grupo

Estas operaciones no son específicas de S3 y generalmente se asocian a procesos de identidad y gestión (IAM). ONTAP admite estos comandos, pero no utiliza las API DE REST del IAM.

- Crear política
- Directiva de AttachGroup

Gestión de usuarios

Estas operaciones no son específicas de S3 y generalmente se asocian con procesos IAM.

- CreateUser
- Deleteuser
- CreateGroup
- DeleteGroup

Interoperabilidad de ONTAP S3

El servidor ONTAP S3 interactúa de manera normal con otras funcionalidades de ONTAP, excepto que se indica en esta tabla.

| Área de operación | Compatible | No admitido |
|---------------------|--|--|
| Cloud Volumes ONTAP | <ul style="list-style-type: none"> • Clientes de Azure en ONTAP 9.9.1 y versiones posteriores • Clientes de AWS en ONTAP 9.11.0 y versiones posteriores • Clientes de Google Cloud en ONTAP 9.12.1 y versiones posteriores | <ul style="list-style-type: none"> • Cloud Volumes ONTAP para cualquier cliente en ONTAP 9.8 y versiones anteriores |
| Protección de datos | <ul style="list-style-type: none"> • Cloud Sync • "Control de versiones de objetos" (A partir de ONTAP 9.11.1) • "SnapMirror S3" (A partir de ONTAP 9.10.1) • Configuraciones de IP de MetroCluster (comenzando por ONTAP 9.12.1) • SnapLock (versión inicial de ONTAP 9.14.1) • WORM (a partir de ONTAP 9.14.1) | <ul style="list-style-type: none"> • Codificación de borrado • Gestión de la vida útil de la información • NDMP • SMTape • SnapMirror Cloud • Recuperación ante desastres de SVM • SyncMirror • Copias Snapshot creadas por el usuario |

| Área de operación | Compatible | No admitido |
|-----------------------------------|--|--|
| Cifrado | <ul style="list-style-type: none"> • Cifrado de agregados de NetApp (NAE) • Cifrado de volúmenes de NetApp (NVE) • Cifrado en almacenamiento de NetApp (NSE) • TLS/SSL | <ul style="list-style-type: none"> • ESCORIA |
| Eficiencia del almacenamiento | <ul style="list-style-type: none"> • Deduplicación • Compresión • Compactación | <ul style="list-style-type: none"> • Eficiencias a nivel de agregados • Clon de volumen del volumen de FlexGroup que contiene bloques ONTAP S3 |
| Virtualización del almacenamiento | - | Virtualización FlexArray de NetApp |
| Calidad de servicio (QoS) | <ul style="list-style-type: none"> • Máximos de calidad de servicio (techos) • Mínimos de calidad de servicio (pisos) | - |
| Características adicionales | <ul style="list-style-type: none"> • "Auditar eventos S3" (A partir de ONTAP 9.10.1) | <ul style="list-style-type: none"> • Volúmenes de FlexCache • FPolicy • Qtrees • Cuotas |

Soluciones de terceros validadas con ONTAP S3

NetApp ha validado las siguientes soluciones de terceros para su uso con ONTAP S3. Si la solución que busca no aparece en la lista, póngase en contacto con su representante de cuentas de NetApp.

Soluciones de terceros validadas en ONTAP S3

NetApp ha probado estas soluciones en colaboración con los partners correspondientes.

- Amazon SageMaker
- Cliente Apache Hadoop S3A
- Apache Kafka
- CommVault (V11)
- Confluent Kafka
- Red Hat Quay

- RUBRIK
- Copo de nieve
- Trino
- Veeam (V12)

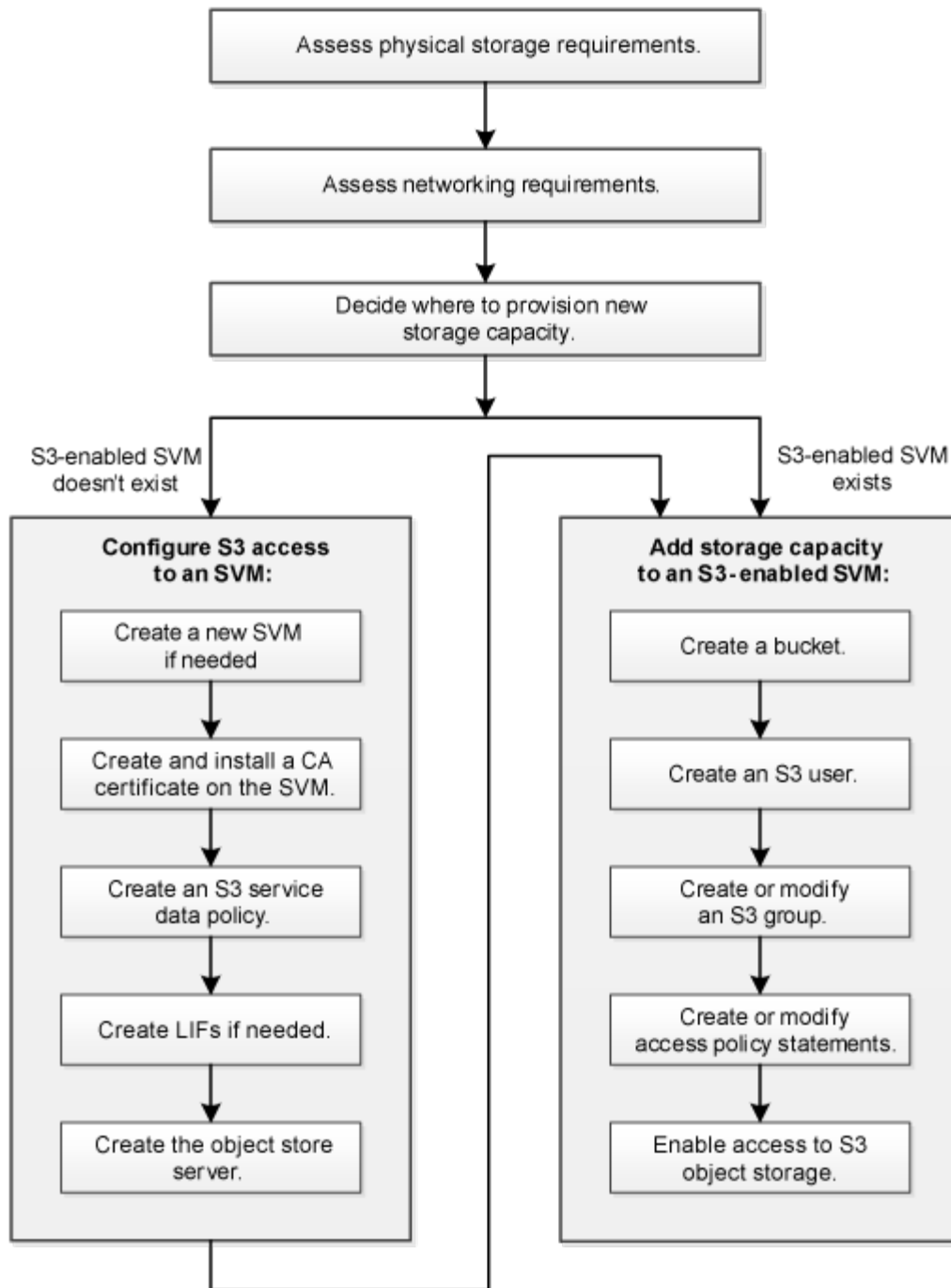
Configurar

Acerca del proceso de configuración de S3

Flujo de trabajo de configuración de S3

La configuración de S3 implica evaluar los requisitos de almacenamiento físico y de red y, a continuación, elegir un flujo de trabajo específico para su objetivo: Configurar el acceso S3 a una SVM nueva o existente, o añadir un bloque y usuarios a una SVM existente que ya esté completamente configurada para acceder a S3.

Cuando configura el acceso S3 a una nueva máquina virtual de almacenamiento mediante System Manager, se le pedirá que introduzca información de certificados y de redes, y que la máquina virtual de almacenamiento y el servidor de almacenamiento de objetos S3 se crean en una única operación.



Evaluar los requisitos de almacenamiento físico

Antes de aprovisionar el almacenamiento S3 para clientes, debe asegurarse de que haya espacio suficiente en los agregados existentes para el nuevo almacén de objetos. Si no lo hay, puede añadir discos a los agregados existentes o crear nuevos agregados del tipo y la ubicación que desee.

Acerca de esta tarea

Cuando se crea un bloque de S3 en una SVM con la función S3 habilitada, se crea automáticamente un volumen FlexGroup para admitir el bloque. Puede dejar a ONTAP Select los agregados y componentes de FlexGroup automáticamente (predeterminado) o puede seleccionar los agregados subyacentes y los componentes de FlexGroup usted mismo.

Si decide especificar los agregados y los componentes de FlexGroup; por ejemplo, si tiene requisitos de rendimiento específicos para los discos subyacentes, debe asegurarse de que la configuración de su agregado sea conforme a las directrices de prácticas recomendadas para aprovisionar un volumen de FlexGroup. Obtenga más información:

- ["Gestión de volúmenes de FlexGroup"](#)
- ["Informe técnico de NetApp 4571-a: Mejores prácticas para los volúmenes ONTAP FlexGroup de NetApp"](#)

Si está sirviendo bloques de Cloud Volumes ONTAP, se recomienda encarecidamente que seleccione manualmente los agregados subyacentes para garantizar que estén usando solo un nodo. El uso de agregados de ambos nodos puede afectar al rendimiento, ya que los nodos se encuentran en zonas de disponibilidad separadas geográficamente y, por lo tanto, pueden estar expuestos a problemas de latencia. Descubra ["Creación de bloques para Cloud Volumes ONTAP"](#).

Puede usar el servidor ONTAP S3 para crear un nivel de capacidad FabricPool local, es decir, en el mismo clúster que el nivel de rendimiento. Esto puede resultar útil, por ejemplo, si tiene discos SSD conectados a un par de alta disponibilidad y desea colocar en niveles los datos *fríos* en discos HDD de otro par de alta disponibilidad. En este caso de uso, el servidor de S3 y el bloque que contiene el nivel de capacidad local deben estar, por lo tanto, en un par de alta disponibilidad diferente al nivel de rendimiento. La organización en niveles local no es compatible en clústeres de un nodo ni de dos nodos.

Pasos

1. Mostrar el espacio disponible en los agregados existentes:

```
storage aggregate show
```

Si hay un agregado con espacio suficiente o la ubicación de nodos necesaria, registre su nombre para la configuración de S3.

```
cluster-1::> storage aggregate show
```

| Aggregate | Size | Available | Used% | State | #Vols | Nodes | RAID | Status |
|-----------|---------|-----------|-------|--------|-------|-------|----------|--------|
| aggr_0 | 239.0GB | 11.13GB | 95% | online | 1 | node1 | raid_dp, | normal |
| aggr_1 | 239.0GB | 11.13GB | 95% | online | 1 | node1 | raid_dp, | normal |
| aggr_2 | 239.0GB | 11.13GB | 95% | online | 1 | node2 | raid_dp, | normal |
| aggr_3 | 239.0GB | 11.13GB | 95% | online | 1 | node2 | raid_dp, | normal |
| aggr_4 | 239.0GB | 238.9GB | 95% | online | 5 | node3 | raid_dp, | normal |
| aggr_5 | 239.0GB | 239.0GB | 95% | online | 4 | node4 | raid_dp, | normal |

```
6 entries were displayed.
```

2. Si no hay agregados con suficiente espacio o la ubicación de nodos necesaria, añada discos a un agregado existente mediante el uso de `storage aggregate add-disks` o cree un nuevo agregado con el `storage aggregate create` comando.

Evaluar los requisitos de red

Antes de proporcionar almacenamiento S3 a los clientes, debe verificar que la red esté correctamente configurada para cumplir los requisitos de aprovisionamiento de S3.

Antes de empezar

Deben configurarse los siguientes objetos de red de clúster:

- Puertos físicos y lógicos
- Dominios de retransmisión
- Subredes (si es necesario)
- Espacios IP (según se requiera, además del espacio IP predeterminado)
- Grupos de conmutación por error (según sea necesario, además del grupo de conmutación por error predeterminado para cada dominio de retransmisión).
- Firewalls externos

Acerca de esta tarea

Para los niveles de capacidad de FabricPool remota (cloud) y los clientes S3 remotos, debe usar una SVM de datos y configurar LIF de datos. Para los niveles de cloud de FabricPool, también se deben configurar las LIF de interconexión de clústeres; no es necesaria la relación de clústeres entre iguales.

Para los niveles de capacidad locales de FabricPool, debe utilizar la SVM del sistema (denominada «'Cluster'»), pero tiene dos opciones para la configuración de LIF:

- Puede usar las LIF de clúster.

En esta opción, no se necesita ninguna otra configuración de LIF, pero habrá un aumento en el tráfico en los LIF del clúster. Además, el nivel local no será accesible para otros clústeres.

- Se pueden usar LIF de datos e interconexión de clústeres.

Esta opción requiere una configuración adicional, lo que incluye habilitar las LIF para el protocolo S3, pero también será posible acceder al nivel local como nivel de cloud de FabricPool remoto a otros clústeres.

Pasos

1. Mostrar los puertos físicos y virtuales disponibles:

```
network port show
```

- Cuando sea posible, debe utilizar el puerto con la velocidad más alta para la red de datos.
- Todos los componentes de la red de datos deben tener la misma configuración de MTU para obtener el mejor rendimiento.

2. Si tiene pensado utilizar un nombre de subred para asignar la dirección IP y el valor de máscara de red para una LIF, compruebe que la subred existe y que tenga suficientes direcciones disponibles:

```
network subnet show
```

Las subredes contienen un grupo de direcciones IP que pertenecen a la misma subred de capa 3. Las subredes se crean mediante la `network subnet create` comando.

3. Mostrar espacios IP disponibles:

```
network ipspace show
```

Puede usar el espacio IP predeterminado o un espacio IP personalizado.

4. Si desea usar direcciones IPv6, compruebe que IPv6 esté habilitado en el clúster:

```
network options ipv6 show
```

Si es necesario, puede habilitar IPv6 con el `network options ipv6 modify` comando.

Decidir dónde aprovisionar la nueva capacidad de almacenamiento S3

Antes de crear un bloque de S3 nuevo, debe decidir si colocarlo en una SVM nueva o existente. Esta decisión determina su flujo de trabajo.

Opciones

- Si desea aprovisionar un bloque en una SVM nueva o una SVM que no esté habilitada para S3, complete los pasos en los temas siguientes.

["Cree una SVM para S3"](#)

["Cree un bloque para S3"](#)

Aunque S3 puede coexistir en una SVM con NFS y SMB, es posible que elija crear una SVM nueva si se cumple alguna de las siguientes afirmaciones:

- Es la primera vez que habilita S3 en un clúster.
- Tiene SVM existentes en un clúster en el que no desea habilitar la compatibilidad con S3.
- Tiene una o varias SVM con la función S3 habilitada en un clúster y desea otro servidor S3 con diferentes características de rendimiento.
Después de habilitar S3 en la SVM, proceda a aprovisionar un bloque.

- Si desea aprovisionar el bloque inicial o un bloque adicional en una SVM existente habilitada para S3, complete los pasos del siguiente tema.

["Cree un bloque para S3"](#)

Configure el acceso S3 a una SVM

Cree una SVM para S3

Aunque S3 puede coexistir con otros protocolos en una SVM, es posible que desee crear una SVM nueva para aislar el espacio de nombres y la carga de trabajo.

Acerca de esta tarea

Si solo va a proporcionar almacenamiento de objetos S3 desde una SVM, el servidor S3 no requiere ninguna configuración de DNS. Sin embargo, puede configurar DNS en la SVM si se usan otros protocolos.

Cuando configura el acceso S3 a una nueva máquina virtual de almacenamiento mediante System Manager, se le pedirá que introduzca información de certificados y de redes, y que la máquina virtual de

almacenamiento y el servidor de almacenamiento de objetos S3 se crean en una única operación.

Ejemplo 15. Pasos

System Manager

Debe estar preparado para introducir el nombre del servidor S3 como un nombre de dominio completo (FQDN), que los clientes usarán para el acceso S3. El FQDN del servidor S3 no debe comenzar por un nombre de bloque.


Debe estar preparado para introducir direcciones IP para los datos de roles de interfaz.

Si utiliza un certificado firmado por una CA externa, se le pedirá que lo introduzca durante este procedimiento, también tendrá la opción de usar un certificado generado por el sistema.

1. Habilite S3 en una máquina virtual de almacenamiento.

- a. Agregue un nuevo equipo virtual de almacenamiento: Haga clic en **almacenamiento > Storage VMs** y, a continuación, haga clic en **Add**.

Si se trata de un sistema nuevo sin equipos virtuales de almacenamiento existentes: Haga clic en **Panel > Configurar protocolos**.

Si va a agregar un servidor S3 a un equipo virtual de almacenamiento existente: Haga clic en **almacenamiento > Storage VMs**, seleccione una máquina virtual de almacenamiento, haga clic en **Configuración** y, a continuación, haga clic en  En **S3**.

- a. Haga clic en **Activar S3** y, a continuación, introduzca el nombre del servidor S3.
- b. Seleccione el tipo de certificado.

Tanto si selecciona un certificado generado por el sistema como uno propio, será necesario para el acceso de los clientes.

- c. Introduzca las interfaces de red.

2. Si seleccionó el certificado generado por el sistema, la información del certificado se muestra cuando se confirma la creación de la máquina virtual de almacenamiento nueva. Haga clic en **Descargar** y guárdelo para acceder a los clientes.
- La clave secreta no se volverá a mostrar.
 - Si necesita de nuevo la información del certificado: Haga clic en **almacenamiento > Storage VMs**, seleccione la VM de almacenamiento y haga clic en **Configuración**.

CLI

1. Compruebe que S3 tiene licencia en el clúster:

```
system license show -package s3
```

Si no lo está, póngase en contacto con su representante de ventas.

2. Cree una SVM:

```
vserver create -vserver <svm_name> -subtype default -rootvolume
<root_volume_name> -aggregate <aggregate_name> -rootvolume-security
-style unix -language C.UTF-8 -data-services <data-s3-server>
-ipospace <ipospace_name>
```

- Utilice el valor UNIX del `-rootvolume-security-style` opción.
- Utilice el C.UTF-8 predeterminado `-language` opción.
- La `ipospace` el ajuste es opcional.

3. Compruebe la configuración y el estado de la SVM recién creada:

```
vserver show -vserver <svm_name>
```

La `Vserver Operational State` el campo debe mostrar la `running` estado. Si muestra la `initializing` estado, significa que hubo un error en algunas operaciones intermedias, como la creación del volumen raíz, y que debe eliminarse la SVM y volver a crearla.

Ejemplos

El siguiente comando crea una SVM para acceder a los datos en el espacio IP `ipospaceA`:

```
cluster-1::> vserver create -vserver svm1.example.com -rootvolume
root_svm1 -aggregate aggr1 -rootvolume-security-style unix -language
C.UTF-8 -data-services _data-s3-server_ -ipospace ipospaceA
```

```
[Job 2059] Job succeeded:
Vserver creation completed
```

El siguiente comando muestra que se creó una SVM con un volumen raíz de 1 GB, y se inició automáticamente y está en `running` estado. El volumen raíz tiene una política de exportación predeterminada que no incluye reglas, por lo que el volumen raíz no se exporta tras la creación. De forma predeterminada, la cuenta de usuario de `vsadmin` se crea y está en la `locked` estado. El rol `vsadmin` se asigna a la cuenta de usuario de `vsadmin` predeterminada.

```

cluster-1::> vserver show -vserver svm1.example.com
                                Vserver: svm1.example.com
                                Vserver Type: data
                                Vserver Subtype: default
                                Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736

                                Root Volume: root_svm1
                                Aggregate: aggr1
                                NIS Domain: -
                                Root Volume Security Style: unix
                                LDAP Client: -
                                Default Volume Language Code: C.UTF-8
                                Snapshot Policy: default
                                Comment:
                                Quota Policy: default
                                List of Aggregates Assigned: -
                                Limit on Maximum Number of Volumes allowed: unlimited
                                Vserver Admin State: running
                                Vserver Operational State: running
                                Vserver Operational State Stopped Reason: -
                                Allowed Protocols: nfs, cifs
                                Disallowed Protocols: -
                                QoS Policy Group: -
                                Config Lock: false
                                IPspace Name: ipspaceA

```

Cree e instale un certificado de CA en la SVM

Se requiere un certificado de la entidad de certificación (CA) para habilitar el tráfico HTTPS desde clientes S3 a la SVM habilitada para S3.

Acerca de esta tarea

Aunque es posible configurar un servidor S3 para que use únicamente HTTP y, aunque es posible configurar clientes sin requisitos de certificado de CA, es una práctica recomendada proteger el tráfico HTTPS a servidores ONTAP S3 con un certificado de CA.

Un certificado de CA no es necesario para un caso de uso de organización en niveles local, donde el tráfico de IP pasa únicamente por las LIF del clúster.

Las instrucciones de este procedimiento crearán e instalarán un certificado autofirmado de ONTAP. También se admiten certificados DE CA de proveedores externos; consulte la documentación de autenticación de administrador para obtener más información.

"Autenticación de administrador y RBAC"

Consulte `security certificate` páginas de manual para opciones de configuración adicionales.

Pasos

1. Cree un certificado digital autofirmado:

```
security certificate create -vserver svm_name -type root-ca -common-name  
ca_cert_name
```

La `-type root-ca` Opción crea e instala un certificado digital autofirmado para firmar otros certificados actuando como entidad de certificación (CA).

La `-common-name` La opción crea el nombre de la entidad de certificación (CA) de la SVM y se utilizará al generar el nombre completo del certificado.

El tamaño predeterminado del certificado es de 2048 bits.

Ejemplo

```
cluster-1::> security certificate create -vserver svm1.example.com -type  
root-ca -common-name svm1_ca
```

```
The certificate's generated name for reference:  
svm1_ca_159D1587CE21E9D4_svm1_ca
```

Cuando se muestre el nombre generado del certificado; asegúrese de guardarlo para pasos posteriores de este procedimiento.

2. Genere una solicitud de firma de certificación:

```
security certificate generate-csr -common-name s3_server_name  
[additional_options]
```

La `-common-name` El parámetro de la solicitud de firma debe ser el nombre del servidor S3 (FQDN).

Puede proporcionar la ubicación y otra información detallada sobre la SVM si lo desea.

Se le solicitará que conserve una copia de su solicitud de certificado y la clave privada para futuras consultas.

3. Firme la CSR con SVM_CA para generar el certificado de S3 Server:

```
security certificate sign -vserver svm_name -ca ca_cert_name -ca-serial  
ca_cert_serial_number [additional_options]
```

Escriba las opciones de comando que ha utilizado en pasos anteriores:

- `-ca` — el nombre común de la CA que introdujo en el paso 1.
- `-ca-serial` — el número de serie de CA desde el Paso 1. Por ejemplo, si el nombre del certificado de CA es `svm1_CA_159D1587CE21E9D4_svm1_ca`, el número de serie es `159D1587CE21E9D4`.

De forma predeterminada, el certificado firmado caducará en 365 días. Puede seleccionar otro valor y especificar otros detalles de firma.

Cuando se le solicite, copie e introduzca la cadena de solicitud de certificado que guardó en el paso 2.

Se muestra un certificado firmado; guárdelo para un uso posterior.

4. Instale el certificado firmado en la SVM habilitada para S3:

```
security certificate install -type server -vserver svm_name
```

Cuando se le solicite, introduzca el certificado y la clave privada.

Puede introducir certificados intermedios si desea una cadena de certificados.

Cuando se muestren la clave privada y el certificado digital firmado por CA, guárdelos para referencia futura.

5. Obtenga el certificado de clave pública:

```
security certificate show -vserver svm_name -common-name ca_cert_name -type  
root-ca -instance
```

Guarde el certificado de clave pública para la configuración posterior del cliente.

Ejemplo

```

cluster-1::> security certificate show -vserver svm1.example.com -common
-name svm1_ca -type root-ca -instance

                Name of Vserver: svm1.example.com
        FQDN or Custom Common Name: svm1_ca
    Serial Number of Certificate: 159D1587CE21E9D4
        Certificate Authority: svm1_ca
            Type of Certificate: root-ca
(DEPRECATED)-Certificate Subtype: -
        Unique Certificate Name: svm1_ca_159D1587CE21E9D4_svm1_ca
Size of Requested Certificate in Bits: 2048
        Certificate Start Date: Thu May 09 10:58:39 2020
        Certificate Expiration Date: Fri May 08 10:58:39 2021
        Public Key Certificate: -----BEGIN CERTIFICATE-----
MIIDZ ...==
-----END CERTIFICATE-----

                Country Name: US
        State or Province Name:
                Locality Name:
                Organization Name:
                Organization Unit:
Contact Administrator's Email Address:
                Protocol: SSL
                Hashing Function: SHA256
        Self-Signed Certificate: true
        Is System Internal Certificate: false

```

Cree una política de datos de servicio de S3

Puede crear políticas de servicio para los servicios de gestión y datos de S3. Se necesita una política de datos de servicio de S3 para habilitar el tráfico de datos de S3 en las LIF.

Acerca de esta tarea

Es necesaria una política de datos de servicio de S3 si se usan LIF de datos y LIF de interconexión de clústeres. No es necesario si utiliza LIF de clúster para el caso de uso de organización en niveles local.

Cuando se especifica una política de servicio para una LIF, la política se usa para construir un rol predeterminado, una política de conmutación por error y una lista de protocolos de datos para la LIF.

Aunque se pueden configurar varios protocolos para las SVM y LIF, lo mejor es que S3 sea el único protocolo cuando ofrece datos de objetos.

Pasos

1. Cambie la configuración del privilegio a avanzado:

```
set -privilege advanced
```


2. Crear una política de datos de servicio:

```
network interface service-policy create -vserver svm_name -policy policy_name
-services data-core,data-s3-server
```

La data-core y.. data-s3-server Los servicios son los únicos necesarios para habilitar ONTAP S3, aunque se pueden incluir otros servicios según sea necesario.

Cree LIF de datos

Si creó una SVM nueva, las LIF dedicadas que crea para el acceso S3 deberían ser LIF de datos.

Antes de empezar

- El puerto de red físico o lógico subyacente debe haber sido configurado para el administrador up estado.
- Si tiene pensado utilizar un nombre de subred para asignar la dirección IP y el valor de máscara de red para una LIF, la subred ya debe existir.

Las subredes contienen un grupo de direcciones IP que pertenecen a la misma subred de capa 3. Se crean mediante la `network subnet create` comando.

- Debe haber la política de servicio de LIF.

Acerca de esta tarea

- Puede crear tanto LIF IPv4 como IPv6 en el mismo puerto de red.
- Si tiene un gran número de LIF en su clúster, puede verificar la capacidad de LIF admitida en el clúster mediante el `network interface capacity show` Comando y la capacidad de LIF admitida en cada nodo mediante el `network interface capacity details show` (en el nivel de privilegio avanzado).
- Si va a habilitar la organización en niveles de capacidad de FabricPool remota (cloud), también debe configurar las LIF de interconexión de clústeres.

Pasos

1. Cree una LIF:

```
network interface create -vserver svm_name -lif lif_name -service-policy
service_policy_names -home-node node_name -home-port port_name {-address
IP_address -netmask IP_address | -subnet-name subnet_name} -firewall-policy
data -auto-revert {true|false}
```

- `-home-node` Es el nodo al que devuelve el LIF cuando el `network interface revert` El comando se ejecuta en la LIF.

También puede especificar si el LIF debería volver automáticamente al nodo raíz y al puerto raíz con el `-auto-revert` opción.

- `-home-port` Es el puerto físico o lógico al que devuelve la LIF cuando el `network interface revert` El comando se ejecuta en la LIF.
- Puede especificar una dirección IP con el `-address` y.. `-netmask` o puede habilitar la asignación desde una subred con `-subnet_name` opción.

- Al usar una subred para suministrar la dirección IP y la máscara de red, si la subred se definió con una puerta de enlace, se añadirá automáticamente a la SVM una ruta predeterminada a esa puerta de enlace cuando se cree una LIF con dicha subred.
- Si asigna direcciones IP manualmente (sin una subred), es posible que deba configurar una ruta predeterminada para una puerta de enlace si hay clientes o controladores de dominio en una subred IP diferente. La `network route create` La página man contiene información sobre la creación de una ruta estática dentro de una SVM.
- Para la `-firewall-policy` opción, utilice el mismo valor predeterminado `data` Como el rol de LIF.

Si lo desea, puede crear y agregar una política de firewall personalizada más adelante.



A partir de ONTAP 9.10.1, las políticas de firewall están obsoletas y sustituidas por completo por políticas de servicios LIF. Para obtener más información, consulte ["Configurar políticas de firewall para LIF"](#).

- `-auto-revert` Permite especificar si un LIF de datos se revierte automáticamente a su nodo principal en circunstancias como el inicio, los cambios en el estado de la base de datos de gestión o el momento en que se realiza la conexión de red. El valor predeterminado es `false`, pero puede establecerlo en `false` según las políticas de administración de red del entorno.
- La `-service-policy` opción especifica la política de servicios de administración y datos que ha creado y cualquier otra política que necesite.

2. Si desea asignar una dirección IPv6 en el `-address` opción:

- Utilice la `network ndp prefix show` Comando para ver la lista de prefijos RA aprendidos en varias interfaces.

La `network ndp prefix show` el comando está disponible en el nivel de privilegio avanzado.

- Utilice el formato `prefix:id` Para construir la dirección IPv6 manualmente.

`prefix` es el prefijo aprendido en varias interfaces.

Para obtener la `id`, elija un número hexadecimal aleatorio de 64 bits.

- Compruebe que la LIF se ha creado correctamente mediante el `network interface show` comando.
- Compruebe que se pueda acceder a la dirección IP configurada:

| Para verificar una... | Usar... |
|-----------------------|----------------------------|
| Dirección IPv4 | <code>network ping</code> |
| Dirección IPv6 | <code>network ping6</code> |

Ejemplos

El siguiente comando muestra cómo crear una LIF de datos de S3 asignada con el `my-S3-policy` política de servicio:

```
network interface create -vserver svml.example.com -lif lif2 -home-node
node2 -homeport e0d -service-policy my-S3-policy -subnet-name ipspace1
```

El siguiente comando muestra todas las LIF del clúster-1. Data LIF datalif1 y datalif3 están configurados con direcciones IPv4, y datalif4 está configurado con una dirección IPv6:

```
cluster-1::> network interface show
```

| Vserver | Logical Interface | Status Admin/Oper | Network Address/Mask | Current Node | Current Is Port |
|-----------------|-------------------|-------------------|----------------------|--------------|-----------------|
| Home | | | | | |
| ----- | ----- | ----- | ----- | ----- | ----- |
| ---- | | | | | |
| cluster-1 | | | | | |
| | cluster_mgmt | up/up | 192.0.2.3/24 | node-1 | e1a |
| true | | | | | |
| node-1 | | | | | |
| | clus1 | up/up | 192.0.2.12/24 | node-1 | e0a |
| true | | | | | |
| | clus2 | up/up | 192.0.2.13/24 | node-1 | e0b |
| true | | | | | |
| | mgmt1 | up/up | 192.0.2.68/24 | node-1 | e1a |
| true | | | | | |
| node-2 | | | | | |
| | clus1 | up/up | 192.0.2.14/24 | node-2 | e0a |
| true | | | | | |
| | clus2 | up/up | 192.0.2.15/24 | node-2 | e0b |
| true | | | | | |
| | mgmt1 | up/up | 192.0.2.69/24 | node-2 | e1a |
| true | | | | | |
| vs1.example.com | | | | | |
| | datalif1 | up/down | 192.0.2.145/30 | node-1 | e1c |
| true | | | | | |
| vs3.example.com | | | | | |
| | datalif3 | up/up | 192.0.2.146/30 | node-2 | e0c |
| true | | | | | |
| | datalif4 | up/up | 2001::2/64 | node-2 | e0c |
| true | | | | | |

5 entries were displayed.

Cree LIF de interconexión de clústeres para la organización en niveles de FabricPool remota

Si va a habilitar la organización en niveles de la capacidad remota de FabricPool (cloud) mediante ONTAP S3, debe configurar las LIF entre clústeres. Las LIF de interconexión

de clústeres se pueden configurar en los puertos compartidos con la red de datos. De este modo, se reduce el número de puertos necesarios para interconectar redes.

Antes de empezar

- El puerto de red físico o lógico subyacente debe haber sido configurado para el administrador up estado.
- Debe haber la política de servicio de LIF.

Acerca de esta tarea

Las LIF de interconexión de clústeres no son necesarias para la organización en niveles de los pools de estructura local ni para servir aplicaciones S3 externas.

Pasos

1. Enumere los puertos del clúster:

```
network port show
```

En el siguiente ejemplo se muestran los puertos de red en cluster01:

```
cluster01::> network port show
```

| (Mbps) | | | | | | Speed |
|--------------|------|---------|------------------|------|------|------------|
| Node | Port | IPspace | Broadcast Domain | Link | MTU | Admin/Oper |
| ----- | | | | | | |
| ----- | | | | | | |
| cluster01-01 | | | | | | |
| | e0a | Cluster | Cluster | up | 1500 | auto/1000 |
| | e0b | Cluster | Cluster | up | 1500 | auto/1000 |
| | e0c | Default | Default | up | 1500 | auto/1000 |
| | e0d | Default | Default | up | 1500 | auto/1000 |
| cluster01-02 | | | | | | |
| | e0a | Cluster | Cluster | up | 1500 | auto/1000 |
| | e0b | Cluster | Cluster | up | 1500 | auto/1000 |
| | e0c | Default | Default | up | 1500 | auto/1000 |
| | e0d | Default | Default | up | 1500 | auto/1000 |

2. Crear LIF de interconexión de clústeres en la SVM del sistema:

```
network interface create -vserver Cluster -lif LIF_name -service-policy
default-intercluster -home-node node -home-port port -address port_IP -netmask
netmask
```

En el siguiente ejemplo se crean LIF de interconexión de clústeres cluster01_icl01 y.
cluster01_icl02:

```

cluster01::> network interface create -vserver Cluster -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver Cluster -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0

```

3. Compruebe que se han creado las LIF de interconexión de clústeres:

```
network interface show -service-policy default-intercluster
```

```

cluster01::> network interface show -service-policy default-intercluster

```

| Current Is | Logical | Status | Network | Current |
|------------|-----------------|------------|------------------|------------------|
| Vserver | Interface | Admin/Oper | Address/Mask | Node |
| Home | | | | Port |
| ----- | ----- | ----- | ----- | ----- |
| cluster01 | cluster01_icl01 | up/up | 192.168.1.201/24 | cluster01-01 e0c |
| true | cluster01_icl02 | up/up | 192.168.1.202/24 | cluster01-02 e0c |
| true | | | | |

4. Compruebe que las LIF de interconexión de clústeres son redundantes:

```
network interface show -service-policy default-intercluster -failover
```

El siguiente ejemplo muestra las LIF de interconexión de clústeres `cluster01_icl01` y `cluster01_icl02` en la `e0c` el puerto se conmuta al nodo de respaldo `e0d` puerto.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
```

| Vserver | Logical Interface | Home Node:Port | Failover Policy | Failover Group |
|-----------|----------------------|-------------------|-------------------------------------|-------------------|
| cluster01 | | | | |
| | cluster01_icl01 | cluster01-01:e0c | local-only | |
| | 192.168.1.201/24 | | | |
| | | | Failover Targets: cluster01-01:e0c, | |
| | | | cluster01-01:e0d | |
| | cluster01_icl02 | cluster01-02:e0c | local-only | |
| | 192.168.1.201/24 | | | |
| | | | Failover Targets: cluster01-02:e0c, | |
| | | | cluster01-02:e0d | |

Cree el servidor de almacenamiento de objetos S3

El servidor de almacenamiento de objetos ONTAP gestiona los datos como objetos S3, a diferencia del almacenamiento de archivos o bloques que proporcionan los servidores NAS y SAN de ONTAP.

Antes de empezar

Debe estar preparado para introducir el nombre del servidor S3 como un nombre de dominio completo (FQDN), que los clientes usarán para el acceso S3. El FQDN no debe comenzar por un nombre de bloque.

Debe tener un certificado de CA autofirmado (creado en pasos anteriores) o un certificado firmado por un proveedor de CA externo. Un certificado de CA no es necesario para un caso de uso de organización en niveles local, donde el tráfico de IP pasa únicamente por las LIF del clúster.

Acerca de esta tarea

Cuando se crea un servidor de almacenamiento de objetos, se crea un usuario raíz con UID 0. No se genera ninguna clave de acceso ni clave secreta para este usuario raíz. El administrador de ONTAP debe ejecutar el `object-store-server users regenerate-keys` comando para establecer la clave de acceso y la clave secreta de este usuario.



Como práctica recomendada por NetApp, no utilice este usuario raíz. Cualquier aplicación cliente que utilice la clave de acceso o la clave secreta del usuario raíz tiene acceso completo a todos los bloques y objetos del almacén de objetos.


Consulte `vserver object-store-server` páginas de manual para opciones de visualización y configuración adicionales.

Ejemplo 16. Pasos

System Manager

Utilice este procedimiento si va a añadir un servidor S3 a una máquina virtual de almacenamiento existente. Para añadir un servidor de S3 a una máquina virtual de almacenamiento nueva, consulte "[Cree una SVM de almacenamiento para S3](#)".

Debe estar preparado para introducir direcciones IP para los datos de roles de interfaz.

1. Habilitar S3 en una máquina virtual de almacenamiento existente.
 - a. Seleccione la VM de almacenamiento: Haga clic en **almacenamiento > Storage VMs**, seleccione una VM de almacenamiento, haga clic en **Configuración** y, a continuación, haga clic en  En **S3**.
 - b. Haga clic en **Activar S3** y, a continuación, introduzca el nombre del servidor S3.
 - c. Seleccione el tipo de certificado.

Tanto si selecciona un certificado generado por el sistema como uno propio, será necesario para el acceso de los clientes.
 - d. Introduzca las interfaces de red.
2. Si seleccionó el certificado generado por el sistema, la información del certificado se muestra cuando se confirma la creación de la máquina virtual de almacenamiento nueva. Haga clic en **Descargar** y guárdelo para acceder a los clientes.
 - La clave secreta no se volverá a mostrar.
 - Si necesita de nuevo la información del certificado: Haga clic en **almacenamiento > Storage VMs**, seleccione la VM de almacenamiento y haga clic en **Configuración**.

CLI

1. Cree el servidor S3:

```
vserver object-store-server create -vserver svm_name -object-store-server  
s3_server_fqdn -certificate-name server_certificate_name -comment text  
[additional_options]
```

Puede especificar opciones adicionales al crear el servidor S3 o en cualquier momento posterior.

- Si va a configurar la organización en niveles local, el nombre de la SVM puede ser una SVM de datos o un nombre de System SVM (clúster).
- El nombre del certificado debe ser el nombre del certificado de servidor (certificado de usuario final o de hoja), no el certificado de CA de servidor (certificado de CA intermedio o raíz).
- De forma predeterminada, HTTPS está habilitado en el puerto 443. Puede cambiar el número de puerto con el `-secure-listener-port` opción.

Cuando HTTPS está activado, se necesitan certificados de CA para una correcta integración con SSL/TLS.

- HTTP está desactivado de forma predeterminada. Cuando está activado, el servidor recibe en el puerto 80. Puede habilitarla mediante el `-is-http-enabled` o cambie el número de puerto con `-listener-port` opción.

Cuando HTTP está activado, la solicitud y las respuestas se envían a través de la red en texto sin cifrar.

2. Compruebe que S3 está configurado:

```
vserver object-store-server show
```

Ejemplo

Este comando verifica los valores de configuración de todos los servidores de almacenamiento de objetos:

```
cluster1:> vserver object-store-server show

Vserver: vs1

      Object Store Server Name: s3.example.com
      Administrative State: up
      Listener Port For HTTP: 80
      Secure Listener Port For HTTPS: 443
      HTTP Enabled: false
      HTTPS Enabled: true
      Certificate for HTTPS Connections: svml_ca
      Comment: Server comment
```

Añadir capacidad de almacenamiento a una SVM habilitada para S3

Crear un bucket

Los objetos S3 se guardan en *buckets*. No se anidan como archivos dentro de un directorio dentro de otros directorios.

Antes de empezar

Debe existir una máquina virtual de almacenamiento que contenga un servidor S3.

Acerca de esta tarea

- A partir de ONTAP 9.14.1, se habilitó el ajuste de tamaño automático en los volúmenes FlexGroup de S3 TB cuando se crean buckets en ellos. De este modo se elimina la asignación de capacidad excesiva durante la creación de bloques en volúmenes de FlexGroup nuevos y existentes. El tamaño de los volúmenes FlexGroup se cambia a un tamaño mínimo requerido según las siguientes directrices. El tamaño mínimo requerido es el tamaño total de todos los bloques de S3 KB de un volumen FlexGroup.
 - A partir de ONTAP 9.14.1, si se crea un volumen de S3 FlexGroup como parte de la creación de un bloque nuevo, el volumen de FlexGroup se creará con el tamaño mínimo requerido.
 - Si se creó un volumen FlexGroup de S3 GB antes de ONTAP 9.14.1, el primer bloque creado o eliminado posteriormente a ONTAP 9.14.1 cambia el tamaño del volumen FlexGroup al tamaño mínimo requerido.
 - Si se creó un volumen FlexGroup de S3 GB anterior a ONTAP 9.14.1 y ya tenía el tamaño mínimo requerido, la creación o eliminación de un bloque posterior a ONTAP 9.14.1 mantendrán el tamaño del

volumen de S3 FlexGroup.

- Los niveles de servicio de almacenamiento son grupos de políticas de calidad de servicio (QoS) adaptativos predefinidos, con niveles *Value*, *Performance* y *Extreme* predeterminados. En lugar de uno de los niveles de servicio de almacenamiento predeterminados, también puede definir un grupo de políticas de calidad de servicio personalizado y aplicarlo a un bloque. Para obtener más información sobre las definiciones de servicios de almacenamiento, consulte ["Definiciones de servicios de almacenamiento"](#). Para obtener más información sobre la gestión del rendimiento, consulte ["Gestión del rendimiento"](#). A partir de ONTAP 9.8, cuando se aprovisiona el almacenamiento, la calidad de servicio se habilita de forma predeterminada. Puede deshabilitar la calidad de servicio o seleccionar una política de calidad de servicio personalizada durante el proceso de aprovisionamiento o más adelante.
- Si va a configurar la organización en niveles de capacidad local, debe crear bloques y usuarios en una máquina virtual de almacenamiento de datos, no en la máquina virtual de almacenamiento del sistema donde está ubicado el servidor S3.
- Para el acceso de cliente remoto, debe configurar buckets en una máquina virtual de almacenamiento habilitada para S3. Si crea un bloque en una máquina virtual de almacenamiento que no tiene la función S3, solo estará disponible para la organización en niveles local.
- A partir de ONTAP 9.14.1, puede hacerlo ["Cree un bucket en un agregado reflejado o no reflejado en una configuración de MetroCluster"](#).
- Para la CLI, cuando crea un bloque, tiene dos opciones de aprovisionamiento:
 - Dejar a ONTAP Select los agregados subyacentes y los componentes de FlexGroup (predeterminado)
 - ONTAP crea y configura un volumen de FlexGroup para el primer bloque seleccionando automáticamente los agregados. Seleccionará automáticamente el nivel de servicio más alto disponible para su plataforma, o bien se puede especificar el nivel de servicio de almacenamiento. Todos los bloques adicionales que añada más adelante a la máquina virtual de almacenamiento tendrán el mismo volumen de FlexGroup subyacente.
 - También puede especificar si el bloque se utilizará para la organización en niveles, en cuyo caso ONTAP intentará seleccionar medios de bajo coste con un rendimiento óptimo para los datos organizados en niveles.
 - Seleccione los agregados subyacentes y los componentes de FlexGroup (requiere opciones de comandos de privilegios avanzados): Tiene la opción de seleccionar manualmente los agregados donde se debe crear el bloque y el volumen de FlexGroup, y luego especificar la cantidad de componentes en cada agregado. Al añadir cubos adicionales:
 - Si especifica agregados y componentes para un bloque nuevo, se creará una FlexGroup nueva para el bloque nuevo.
 - Si no se especifican agregados y componentes para un bloque nuevo, el nuevo bloque se añadirá a una FlexGroup existente.

Consulte [Gestión de volúmenes de FlexGroup](#) si quiere más información.

Cuando se especifican agregados y componentes al crear un bloque, no se aplican grupos de políticas de calidad de servicio, predeterminados ni personalizados. Puede hacerlo más tarde con el `vserver object-store-server bucket modify` comando.

Consulte ["modificación de bucket object-store-server de vserver"](#) si quiere más información.

Nota: Si está sirviendo cubos de Cloud Volumes ONTAP, debe utilizar el procedimiento CLI. Se recomienda seleccionar manualmente los agregados subyacentes para garantizar que solo utilicen un nodo. El uso de agregados de ambos nodos puede afectar al rendimiento, ya que los nodos se encuentran en zonas de disponibilidad separadas geográficamente y, por lo tanto, pueden estar expuestos a problemas de latencia.

Crear bloques S3 con la interfaz de línea de comandos de ONTAP

1. Si piensa seleccionar agregados y componentes de FlexGroup por su cuenta, establezca el nivel de privilegio en Advanced (de lo contrario, el nivel de privilegio de administrador es suficiente): `set -privilege advanced`

2. Crear un bloque:

```
vserver object-store-server bucket create -vserver svm_name -bucket
bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
[additional_options]
```

El nombre de la máquina virtual de almacenamiento puede ser una máquina virtual de almacenamiento de datos o `Cluster` (El nombre de VM de almacenamiento del sistema) si se va a configurar la organización en niveles local.

Si no especifica ninguna opción, ONTAP crea un bucket de 800GB con el nivel de servicio definido en el nivel más alto disponible para su sistema.

Si desea que ONTAP cree un bloque según el rendimiento o el uso, utilice una de las siguientes opciones:

- nivel de servicio

Incluya el `-storage-service-level` opción con uno de los siguientes valores: `value`, `performance`, o `extreme`.

- Organización en niveles

Incluya el `-used-as-capacity-tier true` opción.

Si desea especificar los agregados en los que se creará el volumen de FlexGroup subyacente, utilice las siguientes opciones:

- La `-aggr-list` El parámetro especifica la lista de agregados que se usarán para los componentes de volumen de FlexGroup.

Cada entrada de la lista crea un componente en el agregado especificado. Puede especificar un agregado varias veces para que se creen varios componentes en el agregado.

Para obtener un rendimiento coherente en todo el volumen FlexGroup, todos los agregados deben usar las mismas configuraciones de tipo de disco y grupo RAID.

- La `-aggr-list-multiplier` parámetro especifica la cantidad de veces que se debe iterar sobre los agregados que se enumeran con el `-aggr-list` Parámetro cuando se crea un volumen de FlexGroup.

El valor predeterminado de `-aggr-list-multiplier` el parámetro es 4.

3. Añada un grupo de políticas QoS si es necesario:

```
vserver object-store-server bucket modify -bucket bucket_name -qos-policy
-group qos_policy_group
```

4. Verificar creación de bloques:

```
vserver object-store-server bucket show [-instance]
```

Ejemplo

El siguiente ejemplo crea un bloque para la máquina virtual de almacenamiento `vs1` de tamaño 1TB y especificando el agregado:

```
cluster-1::*> vserver object-store-server bucket create -vserver  
svml.example.com -bucket testbucket -aggr-list aggr1 -size 1TB
```

Crear bloques S3 con System Manager

1. Añadir un nuevo bloque en una máquina virtual de almacenamiento habilitada para S3.
 - a. Haga clic en **almacenamiento > Cuchos** y, a continuación, haga clic en **Agregar**.
 - b. Introduzca un nombre, seleccione la máquina virtual de almacenamiento e introduzca un tamaño.
 - Si hace clic en **Guardar** en este punto, se crea un bloque con estos valores predeterminados:
 - No se concede acceso a ningún usuario al bloque a menos que ninguna política de grupo esté ya en vigor.



No se debe usar el usuario raíz de S3 para gestionar el almacenamiento de objetos ONTAP y compartir sus permisos, ya que tiene acceso ilimitado al almacén de objetos. En su lugar, cree un usuario o grupo con privilegios administrativos que asigne.

- Un nivel de calidad de servicio (rendimiento) que es el más alto disponible para su sistema.
- Haga clic en **Guardar** para crear un bucket con estos valores predeterminados.

Configurar permisos y restricciones adicionales

Puede hacer clic en **Más opciones** para configurar la configuración de bloqueo de objetos, permisos de usuario y nivel de rendimiento cuando configure el depósito, o puede modificar estos ajustes más adelante.

Si tiene la intención de utilizar el almacén de objetos S3 para la organización en niveles de FabricPool, considere la posibilidad de seleccionar **utilizar para la organización en niveles** (utilizar medios de bajo coste con un rendimiento óptimo para los datos organizados en niveles) en lugar de un nivel de servicio de rendimiento.

Si desea habilitar el control de versiones de sus objetos para su posterior recuperación, seleccione **Activar control de versiones**. El control de versiones está activado de forma predeterminada si está activando el bloqueo de objetos en el depósito. Para obtener más información sobre el control de versiones de objetos, consulte ["Uso del control de versiones en bloques de S3 para Amazon"](#).

A partir de 9.14.1, el bloqueo de objetos es compatible con bloques de S3. El bloqueo de objetos de S3 GB requiere una licencia estándar de SnapLock. Esta licencia se incluye con ["ONTAP One"](#).

Antes de ONTAP One, la licencia de SnapLock se incluía en el paquete de seguridad y cumplimiento de normativas. El paquete de seguridad y cumplimiento ya no se ofrece, pero sigue siendo válido. Aunque actualmente no es obligatorio, los clientes existentes pueden optar por hacerlo ["Actualice a ONTAP One"](#). Si está activando el bloqueo de objetos en un depósito, debe hacerlo ["Compruebe que hay instalada una licencia de SnapLock"](#). Si no hay una licencia de SnapLock instalada, debe ["instale"](#) antes de poder activar el bloqueo de objetos.

Cuando haya verificado que la licencia de SnapLock está instalada, para evitar que los objetos de su depósito se borren o sobrescriban, seleccione **Habilitar bloqueo de objetos**. El bloqueo se puede habilitar en todas las versiones de objetos o en algunas específicas, y solo cuando se inicializa el reloj de cumplimiento de normativas de SnapLock para los nodos del clúster. Siga estos pasos:

1. Si el reloj de cumplimiento de SnapLock no se inicializa en ningún nodo del clúster, aparece el botón **Inicializar reloj de cumplimiento de SnapLock**. Haga clic en **Inicializar reloj de cumplimiento de SnapLock** para inicializar el reloj de cumplimiento de SnapLock en los nodos del clúster.
2. Seleccione el modo **Gobernanza** para activar un bloqueo basado en el tiempo que permite los permisos *Escribir una vez, leer muchos (WORM)* en los objetos. Incluso en el modo *Governance*, los objetos pueden ser eliminados por los usuarios administradores con permisos específicos.
3. Seleccione el modo **Compliance** si desea asignar reglas más estrictas de eliminación y actualización en los objetos. En este modo de bloqueo de objetos, los objetos solo pueden caducarse al finalizar el período de retención especificado. A menos que se especifique un período de retención, los objetos permanecen bloqueados indefinidamente.
4. Especifique la tenencia de retención del bloqueo en días o años si desea que el bloqueo se aplique durante un período determinado.



El bloqueo se aplica a los cucharones S3 con versiones y sin versiones. El bloqueo de objetos no se aplica a los objetos NAS.

Puede configurar los ajustes de protección y permisos, así como el nivel de servicio de rendimiento del bloque.



Debe haber creado usuarios y grupos antes de configurar los permisos.

Para obtener más información, consulte ["Crear reflejo para nuevo bloque"](#).

Verifique el acceso al cucharón

En aplicaciones cliente S3 (ya sea ONTAP S3 o una aplicación externa de terceros), puede verificar el acceso al depósito recién creado introduciendo lo siguiente:

- El certificado de CA de servidor S3.
- La clave de acceso y la clave secreta del usuario.
- El nombre FQDN del servidor S3 y el nombre de bloque.

Cree un bucket en un agregado reflejado o no reflejado en una configuración de MetroCluster

A partir de ONTAP 9.14.1, puede aprovisionar un bloque en un agregado reflejado o no reflejado en las configuraciones de IP y FC de MetroCluster.

Acerca de esta tarea

- De forma predeterminada, los buckets se aprovisionan en agregados reflejados.
- Las mismas directrices de provisión descritas en la ["Crear un bucket"](#) Aplique para crear un bloque en un entorno MetroCluster.
- Las siguientes funciones de almacenamiento de objetos S3 no son compatibles con entornos MetroCluster:
 - SnapMirror S3

- Gestión del ciclo de vida de los bloques de S3
- Bloqueo de objetos S3 en el modo **Compliance**



Se admite el bloqueo de objetos S3 en el modo **Gobernanza**.

- Organización en niveles de FabricPool local

Antes de empezar

Debe haber una SVM que contenga un servidor S3.

Proceso para crear cubos

CLI

1. Si piensa seleccionar agregados y componentes de FlexGroup por su cuenta, establezca el nivel de privilegio en Advanced (de lo contrario, el nivel de privilegio de administrador es suficiente): `set -privilege advanced`
2. Crear un bloque:

```
vserver object-store-server bucket create -vserver <svm_name> -bucket  
<bucket_name> [-size integer[KB|MB|GB|TB|PB]] [-use-mirrored-aggregates  
true/false]
```

Ajuste la `-use-mirrored-aggregates` opción a. `true` o. `false` según si desea usar un agregado reflejado o no reflejado.



De forma predeterminada, la `-use-mirrored-aggregates` opción establecida en `true`.

- El nombre de la SVM debe ser una SVM de datos.
- Si no especifica ninguna opción, ONTAP crea un bucket de 800GB con el nivel de servicio definido en el nivel más alto disponible para su sistema.
- Si desea que ONTAP cree un bloque según el rendimiento o el uso, utilice una de las siguientes opciones:

- nivel de servicio

Incluya el `-storage-service-level` opción con uno de los siguientes valores: `value`, `performance`, o. `extreme`.

- Organización en niveles

Incluya el `-used-as-capacity-tier true` opción.

- Si desea especificar los agregados en los que se creará el volumen de FlexGroup subyacente, utilice las siguientes opciones:

- La `-aggr-list` El parámetro especifica la lista de agregados que se usarán para los componentes de volumen de FlexGroup.

Cada entrada de la lista crea un componente en el agregado especificado. Puede especificar un agregado varias veces para que se creen varios componentes en el agregado.

Para obtener un rendimiento coherente en todo el volumen FlexGroup, todos los agregados deben usar las mismas configuraciones de tipo de disco y grupo RAID.

- La `-aggr-list-multiplier` parámetro especifica la cantidad de veces que se debe iterar sobre los agregados que se enumeran con el `-aggr-list` Parámetro cuando se crea un volumen de FlexGroup.

El valor predeterminado de `-aggr-list-multiplier` el parámetro es 4.

3. Añada un grupo de políticas QoS si es necesario:

```
vserver object-store-server bucket modify -bucket bucket_name -qos-policy
```

```
-group qos_policy_group
```

4. Verificar creación de bloques:

```
vserver object-store-server bucket show [-instance]
```

Ejemplo

En el ejemplo siguiente se crea un bloque para SVM VS1 de tamaño 1TB en un agregado reflejado:

```
cluster-1::*> vserver object-store-server bucket create -vserver  
svm1.example.com -bucket testbucket -size 1TB -use-mirrored-aggregates  
true
```


System Manager

1. Añadir un nuevo bloque en una máquina virtual de almacenamiento habilitada para S3.
 - a. Haga clic en **almacenamiento > Cuchos** y, a continuación, haga clic en **Agregar**.
 - b. Introduzca un nombre, seleccione la máquina virtual de almacenamiento e introduzca un tamaño.

De forma predeterminada, el bloque se aprovisiona en un agregado reflejado. Si quieres crear un bucket en un agregado no reflejado, selecciona **Más opciones** y desmarca la casilla **Usar el nivel SyncMirror** bajo **Protección** como se muestra en la siguiente imagen:

Add bucket ✕

NAME

 To use this bucket from a remote cluster, configure S3 service on storage VM "vs1".

FOLDER (OPTIONAL)

Browse

Specify the folder to map to this bucket. [Know more](#)

CAPACITY

Size

GB

☐ Use tiering

If you select this option, the system will try to select low-cost media with optimal performance for the tiered data.

☐ Enable versioning

Versioning-enabled buckets allow you to recover objects that were accidentally deleted or overwritten. After versioning is enabled, it can't be disabled. However, you can suspend versioning.

PERFORMANCE SERVICE LEVEL

Value

Not sure? [Get help selecting type](#)

Permissions
☐ Copy access permissions from an existing bucket

| Principal | Effect | Actions | Resources | Conditions |
|---------------------------|--------|------------|-----------|------------|
| All users of this stor... | allow | ListBucket | * | |

+ Add

Object locking
☐ Enable object locking

Object locking utilizes the "Write Once, Read Many" (WORM) model in which objects or their versions are protected from being deleted or overwritten during the specified retention period.

Protection
☒ Use the S3x3Min protection

Save

Cancel

- Si hace clic en **Guardar** en este punto, se crea un bloque con estos valores predeterminados:
 - No se concede acceso a ningún usuario al bloque a menos que ninguna política de grupo esté ya en vigor.



No se debe usar el usuario raíz de S3 para gestionar el almacenamiento de objetos ONTAP y compartir sus permisos, ya que tiene acceso ilimitado al almacén de objetos. En su lugar, cree un usuario o grupo con privilegios administrativos que asigne.

- Un nivel de calidad de servicio (rendimiento) que es el más alto disponible para su sistema.
- Puede hacer clic en **más opciones** para configurar los permisos de usuario y el nivel de rendimiento al configurar el bloque, o puede modificar esta configuración más tarde.

- Debe haber creado usuarios y grupos antes de utilizar **más opciones** para configurar sus permisos.
 - Si tiene la intención de utilizar el almacén de objetos S3 para la organización en niveles de FabricPool, considere la posibilidad de seleccionar **utilizar para la organización en niveles** (utilizar medios de bajo coste con un rendimiento óptimo para los datos organizados en niveles) en lugar de un nivel de servicio de rendimiento.
2. En aplicaciones de cliente S3, otro sistema ONTAP o una aplicación de terceros externa, verifique el acceso al nuevo bloque introduciendo lo siguiente:
- El certificado de CA de servidor S3.
 - Clave secreta y clave de acceso del usuario.
 - El nombre FQDN del servidor S3 y el nombre de bloque.

Cree una regla de gestión del ciclo de vida del bloque

A partir de ONTAP 9.13.1, puede crear reglas de gestión del ciclo de vida para gestionar los ciclos de vida de los objetos en sus bloques S3. Puede definir reglas de supresión para objetos específicos de un depósito y, a través de estas reglas, caducar esos objetos de cubo. De este modo, se cumplen los requisitos de retención y se gestiona un almacenamiento de objetos S3 general de forma eficiente.



Si el bloqueo de objetos está activado para los objetos de depósito, las reglas de gestión del ciclo de vida para la caducidad de objetos no se aplicarán a los objetos bloqueados. Para obtener más información sobre el bloqueo de objetos, consulte ["Crear un bucket"](#).

Antes de empezar

Debe haber una SVM habilitada para S3 que contenga un servidor S3 y un bloque. Consulte ["Cree una SVM para S3"](#) si quiere más información.

Acerca de esta tarea

Al crear las reglas de gestión del ciclo de vida, puede aplicar las siguientes acciones de eliminación a los objetos del depósito:

- Supresión de versiones actuales: Esta acción vence los objetos identificados por la regla. Si el control de versiones está activado en el depósito, S3 hace que todos los objetos caducados no estén disponibles. Si el control de versiones no está activado, esta regla suprime los objetos de forma permanente. La acción de la CLI es `Expiration`.
- Eliminación de versiones no actuales: Esta acción especifica cuándo S3 puede eliminar permanentemente objetos no actuales. La acción de la CLI es `NoncurrentVersionExpiration`.
- Supresión de marcadores de supresión caducados: Esta acción suprime los marcadores de supresión de objetos caducados.
En los bloques con control de versiones activado, los objetos con marcadores de supresión se convierten en las versiones actuales de los objetos. Los objetos no se eliminan y no se puede realizar ninguna acción en ellos. Estos objetos caducan cuando no hay versiones actuales asociadas a ellos. La acción de la CLI es `Expiration`.
- Eliminación de cargas multiparte incompletas: Esta acción establece un tiempo máximo (en días) en el que desea permitir que las cargas multiparte permanezcan en curso. Después de lo cual, se eliminan. La acción de la CLI es `AbortIncompleteMultipartUpload`.

El procedimiento que siga depende de la interfaz que utilice. Con ONTAP 9.13.1, tiene que utilizar la CLI. A partir de ONTAP 9.14.1, también puede usar System Manager.

Gestione las reglas de gestión del ciclo de vida con la interfaz de línea de comandos

A partir de ONTAP 9.13.1, puede usar la interfaz de línea de comandos de ONTAP para crear reglas de gestión del ciclo de vida para caducar objetos en sus bloques S3.

Antes de empezar

Para la CLI, debe definir los campos necesarios para cada tipo de acción de caducidad al crear una regla de gestión del ciclo de vida del bloque. Estos campos se pueden modificar después de la creación inicial. En la siguiente tabla se muestran los campos únicos para cada tipo de acción.

| Tipo de acción | Campos únicos |
|--|--|
| Caducidad sin CurrentVersionexpiración | <ul style="list-style-type: none">• <code>-non-curr-days</code> - Número de días después de los cuales se eliminarán las versiones no actuales• <code>-new-non-curr-versions</code> - Número de últimas versiones no actuales que se conservarán |
| Caducidad | <ul style="list-style-type: none">• <code>-obj-age-days</code> - Número de días desde la creación, después de lo cual se puede eliminar la versión actual de los objetos• <code>-obj-exp-date</code> - Fecha específica en la que los objetos deben expirar• <code>-expired-obj-del-markers</code> - Limpiar objetos borrar marcadores |
| AbortEncompleteMultipartUpload | <ul style="list-style-type: none">• <code>-after-initiation-days</code> - Número de días de iniciación, después de los cuales la carga puede ser abortada |

Para que la regla de gestión del ciclo de vida del depósito se aplique sólo a un subconjunto específico de objetos, los administradores deben establecer cada filtro al crear la regla. Si estos filtros no se establecen al crear la regla, la regla se aplicará a todos los objetos del depósito.

Todos los filtros se pueden modificar después de la creación inicial *Excepto* para lo siguiente: +

- `-prefix`
- `-tags`
- `-obj-size-greater-than`
- `-obj-size-less-than`

Pasos

1. Utilice la `vserver object-store-server bucket lifecycle-management-rule create` comando con los campos necesarios para el tipo de acción de vencimiento para crear la regla de gestión del ciclo de vida del bloque.

Ejemplo

El siguiente comando crea una regla de gestión del ciclo de vida del bloque `NonCurrentVersionExpiration`:

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
NonCurrentVersionExpiration -index <lifecycle_rule_index_integer> -is
-enabled {true|false} -prefix <object_name> -tags <text> -obj-size-greater
-than {<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -new-non-curr-versions <integer> -non-curr
-days <integer>
```

Ejemplo

El siguiente comando crea una regla de gestión del ciclo de vida del depósito de vencimiento:

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
Expiration -index <lifecycle_rule_index_integer> -is-enabled {true|false}
-prefix <object_name> -tags <text> -obj-size-greater-than
{<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -obj-age-days <integer> -obj-exp-date
<"MM/DD/YYYY HH:MM:SS"> -expired-obj-del-marker {true|false}
```

Ejemplo


El siguiente comando crea una regla de gestión del ciclo de vida del bloque AbortIncompleteMultipartUpload:

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
AbortIncompleteMultipartUpload -index <lifecycle_rule_index_integer> -is
-enabled {true|false} -prefix <object_name> -tags <text> -obj-size-greater
-than {<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -after-initiation-days <integer>
```

Gestione las reglas de gestión del ciclo de vida con System Manager

A partir de ONTAP 9.14.1, puede caducar objetos de S3 mediante System Manager. Puede agregar, editar y eliminar reglas de gestión del ciclo de vida para los objetos S3. Además, puede importar una regla de ciclo de vida creada para un depósito y utilizarla para los objetos de otro depósito. Puede desactivar una regla activa y habilitarla más tarde.

Agregue una regla de gestión del ciclo de vida

1. Haga clic en **Almacenamiento > Buckets**.
2. Seleccione el período para el que desea especificar la regla de caducidad.
3. Haga clic en la  icono y seleccione **Administrar reglas de ciclo de vida**.
4. Haga clic en **Agregar > Regla de ciclo de vida**.
5. En la página Agregar una regla de ciclo de vida, agregue el nombre de la regla.

6. Defina el ámbito de la regla, si desea que se aplique a todos los objetos del depósito o a objetos específicos. Si desea especificar objetos, agregue al menos uno de los siguientes criterios de filtro:
 - a. **Prefijo:** Especifique un prefijo de los nombres de clave de objeto a los que se debe aplicar la regla. Normalmente, es la ruta o carpeta del objeto. Puede introducir un prefijo por regla. A menos que se proporcione un prefijo válido, la regla se aplica a todos los objetos de un depósito.
 - b. **Etiquetas:** Especifique hasta tres pares de clave y valor (etiquetas) para los objetos a los que se debe aplicar la regla. Sólo se utilizan claves válidas para el filtrado. El valor es opcional. Sin embargo, si agrega valores, asegúrese de agregar sólo valores válidos para las claves correspondientes.
 - c. **Tamaño:** Puede limitar el alcance entre los tamaños mínimo y máximo de los objetos. Puede introducir uno o ambos valores. La unidad predeterminada es MIB.
7. Especifique la acción:
 - a. **Expire la versión actual de los objetos:** Establezca una regla para que todos los objetos actuales no estén disponibles permanentemente después de un número específico de días desde su creación, o en una fecha específica. Esta opción no está disponible si se selecciona la opción **Eliminar marcadores de eliminación de objetos caducados**.
 - b. *** Eliminar permanentemente versiones no actuales*:** Especifique el número de días después de los cuales la versión se convierte en no actual, y después puede ser eliminado, y el número de versiones a retener.
 - c. **Eliminar marcadores de eliminación de objetos caducados:** Seleccione esta acción para eliminar objetos con marcadores de eliminación caducados, es decir, eliminar marcadores sin un objeto actual asociado.



Esta opción no está disponible cuando selecciona la opción **Expire la versión actual de los objetos** que elimina automáticamente todos los objetos después del período de retención. Esta opción también no está disponible cuando se utilizan etiquetas de objetos para filtrar.

- d. **Eliminar cargas multiparte incompletas:** Establece el número de días después de los cuales las cargas multiparte incompletas deben ser eliminadas. Si las cargas de varias partes que están en curso fallan dentro del período de retención especificado, puede eliminar las cargas incompletas de varias partes. Esta opción no está disponible cuando se utilizan etiquetas de objetos para filtrar.
- e. Haga clic en **Guardar**.


Importar una regla de ciclo de vida

1. Haga clic en **Almacenamiento > Buckets**.
2. Seleccione el período para el que desea importar la regla de caducidad.
3. Haga clic en la **⋮** Icono y seleccione **Administrar reglas de ciclo de vida**.
4. Haga clic en **Agregar > Importar una regla**.
5. Seleccione el depósito desde el que desea importar la regla. Aparecen las reglas de gestión del ciclo de vida definidas para el bloque seleccionado.
6. Seleccione la regla que desea importar. Tiene la opción de seleccionar una regla a la vez, siendo la selección predeterminada la primera regla.
7. Haga clic en **Importar**.

Editar, eliminar o desactivar una regla

Sólo puede editar las acciones de gestión del ciclo de vida asociadas a la regla. Si la regla se filtró con etiquetas de objeto, las opciones **Eliminar marcadores de eliminación de objetos caducados** y **Eliminar cargas incompletas de varias partes** no estarán disponibles.

Al eliminar una regla, dicha regla ya no se aplicará a los objetos asociados anteriormente.

1. Haga clic en **Almacenamiento > Buckets**.
2. Seleccione el depósito para el que desea editar, suprimir o desactivar la regla de gestión del ciclo de vida.
3. Haga clic en la  Icono y seleccione **Administrar reglas de ciclo de vida**.
4. Seleccione la regla necesaria. Puede editar y desactivar una regla a la vez. Puede eliminar varias reglas a la vez.
5. Seleccione **Editar**, **Eliminar** o **Desactivar** y complete el procedimiento.

Cree un usuario de S3

Se requiere autorización de usuario en todos los almacenes de objetos de ONTAP para restringir la conectividad a los clientes autorizados.

Antes de empezar.

Debe existir una máquina virtual de almacenamiento habilitada para S3.

Acerca de esta tarea

Se puede otorgar acceso a cualquier bloque de una máquina virtual de almacenamiento a un usuario de S3. Cuando crea un usuario S3, también se generan una clave de acceso y una clave secreta para el usuario. Se deben compartir con el usuario junto con el FQDN del almacén de objetos y el nombre del bloque. Se pueden ver las teclas de un usuario de S3 con el `vserver object-store-server user show` comando.

Puede conceder permisos de acceso específicos a usuarios de S3 en una política de bloque o una política de servidor de objetos.



Al crear un nuevo servidor de almacén de objetos, ONTAP crea un usuario raíz (UID 0), que es un usuario con privilegios con acceso a todos los depósitos. En lugar de administrar ONTAP S3 como usuario raíz, NetApp recomienda crear un rol de usuario administrador con privilegios específicos.

CLI

1. Cree un usuario de S3:

```
vserver object-store-server user create -vserver svm_name -user user_name  
-comment [-comment text] -key-time-to-live time
```


- Agregar un comentario es opcional.
- A partir de ONTAP 9.14.1, puede definir el período de tiempo durante el cual la clave será válida en el `-key-time-to-live` parámetro. Puede agregar el período de retención en este formato para indicar el período después del cual caduca la clave de acceso:
`P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W`
Por ejemplo, si desea introducir un período de retención de un día, dos horas, tres minutos y cuatro segundos, introduzca el valor como `P1DT2H3M4S`. A menos que se especifique, la clave es válida durante un período de tiempo indefinido.

El siguiente ejemplo crea un usuario con su nombre `sm_user1` En equipos virtuales de almacenamiento `vs0`, con un período de retención clave de una semana.

```
vserver object-store-server user create -vserver vs0 -user sm_user1  
-key-time-to-live P1W
```

2. Asegúrese de guardar la clave de acceso y la clave secreta. Serán necesarios para el acceso de S3 clientes.

System Manager

1. Haga clic en **almacenamiento > Storage VMs**. Seleccione la VM de almacenamiento a la que necesita agregar un usuario, seleccione **Configuración** y luego haga clic en  En S3.
2. Para agregar un usuario, haga clic en **Usuarios > Agregar**.
3. Introduzca un nombre para el usuario.
4. A partir de ONTAP 9.14.1, puede especificar el período de retención de las claves de acceso que se crean para el usuario. Puede especificar el período de retención en días, horas, minutos o segundos, después del cual las claves caducan automáticamente. De forma predeterminada, el valor se establece en 0 esto indica que la clave es válida indefinidamente.
5. Haga clic en **Guardar**. Se crea el usuario y se generan una clave de acceso y una clave secreta para el usuario.
6. Descargue o guarde la clave de acceso y la clave secreta. Serán necesarios para el acceso de S3 clientes.

Siguientes pasos

- [Cree o modifique grupos S3](#)

Cree o modifique grupos S3

Puede simplificar el acceso a bloques mediante la creación de grupos de usuarios con las autorizaciones de acceso adecuadas.

Antes de empezar

Los usuarios S3 de una SVM habilitada para S3 ya deben existir.

Acerca de esta tarea

A los usuarios de un grupo de S3 se puede conceder acceso a cualquier bloque de una SVM, pero no a varias SVM. Los permisos de acceso a grupos se pueden configurar de dos formas:


- A nivel de cucharón

Después de crear un grupo de usuarios S3, debe especificar permisos de grupo en las sentencias de política de bloque y sólo se aplican a ese bloque.

- A nivel de SVM

Después de crear un grupo de usuarios S3, debe especificar nombres de políticas de servidor de objetos en la definición del grupo. Esas políticas determinan los bloques y el acceso de los miembros del grupo.

System Manager

1. Edite el equipo virtual de almacenamiento: Haga clic en **almacenamiento > equipos virtuales de almacenamiento**, haga clic en el equipo virtual de almacenamiento, seleccione **Configuración** y, a continuación, haga clic en  En S3.
2. Agregar un grupo: Seleccione **grupos** y, a continuación, seleccione **Agregar**.
3. Introduzca un nombre de grupo y selecciónelo en una lista de usuarios.
4. Puede seleccionar una política de grupo existente o añadirla ahora, o bien agregar una política más adelante.

CLI

1. Cree un grupo de S3:

```
vserver object-store-server group create -vserver svm_name -name group_name  
-users user_name\(s\) [-policies policy_names] [-comment text\]
```

La `-policies` la opción se puede omitir en configuraciones con un solo bloque en un almacén de objetos; el nombre del grupo se puede agregar a la política de bloque.

La `-policies` la opción se puede añadir más adelante con la `vserver object-store-server group modify` comando después de crear las políticas de servidor de almacenamiento de objetos.

Regenerar claves y modificar su período de retención

Las claves de acceso y las claves secretas se generan automáticamente durante la creación del usuario para habilitar el acceso de los clientes S3. Puede volver a generar claves para un usuario si una clave ha caducado o está en peligro.

Para obtener más información sobre la generación de claves de acceso, consulte ["Cree un usuario de S3"](#).



CLI

1. Vuelva a generar las claves secretas y de acceso para un usuario ejecutando el `vserver object-store-server user regenerate-keys` comando.
2. De forma predeterminada, las claves generadas son válidas indefinidamente. A partir de 9.14.1, puede modificar su período de retención, después del cual las claves caducan automáticamente. Puede agregar el período de retención en este formato:
`P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W`
Por ejemplo, si desea introducir un período de retención de un día, dos horas, tres minutos y cuatro segundos, introduzca el valor como `P1DT2H3M4S`.

```
vserver object-store-server user regenerate-keys -vserver svm_name  
-user user -key-time-to-live 0
```

3. Guarde el acceso y las claves secretas. Serán necesarios para el acceso de S3 clientes.

System Manager

1. Haga clic en **almacenamiento > Storage VMs** y, a continuación, seleccione la VM de almacenamiento.
2. En la ficha **Configuración**, haga clic en  En el mosaico **S3**.
3. En la pestaña **Usuarios**, verifique que no haya ninguna clave de acceso o que la clave haya caducado para el usuario.
4. Si necesita volver a generar la clave, haga clic en  Junto al usuario, luego haga clic en **Regenerar clave**.
5. De forma predeterminada, las claves generadas son válidas durante un período de tiempo indefinido. A partir de 9.14.1, puede modificar su período de retención, después del cual las claves caducan automáticamente. Introduzca el período de retención en días, horas, minutos o segundos.
6. Haga clic en **Guardar**. La clave se regenera. Cualquier cambio en el período de retención de clave se aplica inmediatamente.
7. Descargue o guarde la clave de acceso y la clave secreta. Serán necesarios para el acceso de S3 clientes.

Crear o modificar sentencias de directiva de acceso

Acerca de las políticas de servidor de almacenamiento de objetos y bloques

El acceso de usuario y grupo a recursos S3 está controlado por las políticas de servidores de almacén de objetos y bloques. Si tiene un pequeño número de usuarios o grupos, es probable que sea suficiente controlar el acceso a nivel de bloque, pero si tiene muchos usuarios y grupos, es más fácil controlar el acceso a nivel de servidor del almacén de objetos.

Modificar una política de bloques

Puede agregar reglas de acceso a la política de bloque predeterminada. El ámbito de su control de acceso es el cucharón que contiene, por lo que resulta más adecuado cuando

hay un único cucharón.

Antes de empezar

Debe existir una máquina virtual de almacenamiento habilitada para S3 que contenga un servidor S3 y un bloque.

Debe haber creado usuarios o grupos antes de conceder permisos.

Acerca de esta tarea

Puede agregar nuevas sentencias para usuarios y grupos nuevos o modificar los atributos de las sentencias existentes. Para obtener más opciones, consulte `vserver object-store-server bucket policy` páginas de manual.

Los permisos de usuario y grupo se pueden otorgar cuando se crea el bloque o cuando se necesite más adelante. También puede modificar la asignación de capacidad de los bloques y del grupo de políticas de calidad de servicio.

A partir de ONTAP 9.9.1, si tiene previsto admitir la funcionalidad de etiquetado de objetos de cliente de AWS con el servidor ONTAP S3, las acciones se realizarán `GetObjectTagging`, `PutObjectTagging`, y `DeleteObjectTagging` debe permitirse el uso de las políticas de bloque o grupo.

El procedimiento que siga depende de la interfaz que utilice: System Manager o CLI:

System Manager

Pasos

1. Edite la cuchara: Haga clic en **almacenamiento > Cuchos**, haga clic en la cuchara deseada y, a continuación, haga clic en **Editar**.

Al agregar o modificar permisos, puede especificar los siguientes parámetros:

- **Principal:** El usuario o grupo al que se concede acceso.
- **Efecto:** Permite o deniega el acceso a un usuario o grupo.
- **Acciones:** Acciones permitidas en el cucharón para un usuario o grupo determinado.
- **Recursos:** Rutas y nombres de objetos dentro del bloque para los cuales se concede o deniega el acceso.

Los valores predeterminados **bucketname** y **bucketname/*** conceden acceso a todos los objetos del bloque. También puede otorgar acceso a objetos individuales; por ejemplo, **bucketname/*_readme.txt**.

- **Condiciones** (opcional): Expresiones que se evalúan cuando se intenta acceder. Por ejemplo, puede especificar una lista de direcciones IP para las que se permitirá o deniega el acceso.



A partir de ONTAP 9.14.1, puede especificar variables para la política de depósitos en el campo **Recursos**. Estas variables son marcadores de posición que se reemplazan por valores contextuales cuando se evalúa la política. Por ejemplo, `If ${aws:username}` se especifica como una variable para una política, a continuación, esta variable se sustituye por el nombre de usuario del contexto de solicitud y la acción de política se puede realizar como se ha configurado para ese usuario.

CLI

Pasos

1. Agregar una sentencia a una política de bloque:

```
vserver object-store-server bucket policy add-statement -vserver svm_name  
-bucket bucket_name -effect {allow|deny} -action object_store_actions  
-principal user_and_group_names -resource object_store_resources [-sid  
text] [-index integer]
```

Los siguientes parámetros definen los permisos de acceso:

| | |
|---------|---|
| -effect | La declaración puede permitir o denegar el acceso |
| -action | Puede especificar * para indicar todas las acciones, o una lista de una o varias de las siguientes: GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, y.. ListMultipartUploadParts. |

| | |
|------------|---|
| -principal | <p>Una lista de uno o más grupos o usuarios de S3.</p> <ul style="list-style-type: none"> • Se puede especificar un máximo de 10 usuarios o grupos. • Si se especifica un grupo de S3, debe estar en el formulario <code>group/group_name</code>. • * se puede especificar que significa acceso público; es decir, acceso sin clave de acceso y clave secreta. • Si no se especifica ningún principal, se concede acceso a todos los usuarios S3 de la máquina virtual de almacenamiento. |
| -resource | <p>El bloque y cualquier objeto que contenga. Los caracteres comodín * y.. ? se puede utilizar para formar una expresión regular para especificar un recurso. En el caso de un recurso, puede especificar variables en una política. Estas son variables de política que son marcadores de posición que se reemplazan por los valores contextuales cuando se evalúa la política.</p> |

Opcionalmente, puede especificar una cadena de texto como comentario con el `-sid` opción.

Ejemplos

En el siguiente ejemplo se crea una sentencia de política de depósito de servidor de almacén de objetos para la máquina virtual de almacenamiento `svm1.example.com` y `bucket1` que especifica el acceso permitido a una carpeta `Léame` para el usuario de servidor de almacén de objetos `user1`.

```
cluster1::> vservers object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal user1 -resource
bucket1/readme/* -sid "fullAccessToReadmeForUser1"
```

En el siguiente ejemplo se crea una sentencia de política de depósito de servidor de almacén de objetos para la máquina virtual de almacenamiento `svm1.example.com` y `bucket1` que especifica el acceso permitido a todos los objetos para el grupo de servidores de almacén de objetos `group1`.

```
cluster1::> vservers object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal group/group1
-resource bucket1/* -sid "fullAccessForGroup1"
```

A partir de ONTAP 9.14.1, puede especificar variables para una política de bloque. En el siguiente ejemplo se crea una sentencia de política de bloque de servidor para la máquina virtual de almacenamiento `svm1` y `bucket1`, y especifica `${aws:username}` como variable para un recurso de política. Cuando se evalúa la política, la variable de política se sustituye por el nombre de usuario de contexto de solicitud y la acción de política se puede realizar según se haya configurado para ese usuario. Por ejemplo, cuando se evalúa la siguiente sentencia de política, `${aws:username}` Se sustituye por el usuario que realiza la operación S3. Si es un usuario `user1` realiza la operación a la que

el usuario tiene acceso bucket1 como bucket1/user1/*.

```
cluster1::> object-store-server bucket policy statement create -vserver  
svml -bucket bucket1 -effect allow -action * -principal - -resource  
bucket1,bucket1/${aws:username}/*##
```

Cree o modifique una política de servidor de almacenes de objetos

Puede crear políticas que se puedan aplicar a uno o varios bloques de un almacén de objetos. Las políticas de servidores de almacenamiento de objetos pueden conectarse a grupos de usuarios, lo cual simplifica la gestión del acceso a los recursos en varios bloques.

Antes de empezar

Debe haber una SVM habilitada para S3 que contenga un servidor S3 y un bloque.

Acerca de esta tarea

Puede habilitar las políticas de acceso en el nivel de SVM especificando una política predeterminada o personalizada en un grupo de servidores de almacenamiento de objetos. Las directivas no surten efecto hasta que se especifiquen en la definición del grupo.



Cuando se utilizan directivas de servidor de almacenamiento de objetos, se especifican los principales (es decir, los usuarios y los grupos) en la definición de grupo, no en la propia directiva.

Hay tres políticas predeterminadas de solo lectura para el acceso a los recursos de ONTAP S3:

- Acceso completo
- NoS3Access
- ReadOnlyAccess

También puede crear nuevas directivas personalizadas y, a continuación, agregar nuevas sentencias para nuevos usuarios y grupos, o puede modificar los atributos de las sentencias existentes. Para obtener más opciones, consulte `vserver object-store-server policy` ["referencia de comandos"](#).


A partir de ONTAP 9.9.1, si tiene previsto admitir la funcionalidad de etiquetado de objetos de cliente de AWS con el servidor ONTAP S3, las acciones se realizarán `GetObjectTagging`, `PutObjectTagging`, y `DeleteObjectTagging` debe permitirse el uso de las políticas de bloque o grupo.

El procedimiento que siga depende de la interfaz que utilice: System Manager o CLI:

System Manager

Utilice System Manager para crear o modificar una directiva de servidor de almacén de objetos

Pasos

1. Edite el equipo virtual de almacenamiento: Haga clic en **almacenamiento > equipos virtuales de almacenamiento**, haga clic en el equipo virtual de almacenamiento, seleccione **Configuración** y, a continuación, haga clic en  En S3.
2. Agregar un usuario: Haga clic en **Directivas** y, a continuación, haga clic en **Agregar**.
 - a. Introduzca un nombre de política y selecciónelo de una lista de grupos.
 - b. Seleccione una política predeterminada existente o agregue una nueva.

Al agregar o modificar una política de grupo, se pueden especificar los siguientes parámetros:

- Grupo: Los grupos a los que se concede acceso.
- Efecto: Permite o deniega el acceso a uno o varios grupos.
- Acciones: Acciones permitidas en uno o más cucharones para un grupo determinado.
- Recursos: Rutas y nombres de objetos dentro de uno o más segmentos para los que se concede o deniega el acceso.

Por ejemplo:

- * Concede acceso a todos los bloques del equipo virtual de almacenamiento.
- **bucketname** y **bucketname/*** conceden acceso a todos los objetos de un bloque específico.
- **bucketname/readme.txt** otorga acceso a un objeto en un bloque específico.

- c. Si lo desea, agregue sentencias a las directivas existentes.

CLI

Utilice la CLI para crear o modificar una directiva de servidor de almacén de objetos

Pasos

1. Cree una política de servidor de almacenamiento de objetos:

```
vserver object-store-server policy create -vserver svm_name -policy policy_name [-comment text]
```

2. Crear una instrucción para la directiva:

```
vserver object-store-server policy statement create -vserver svm_name -policy policy_name -effect {allow|deny} -action object_store_actions -resource object_store_resources [-sid text]
```

Los siguientes parámetros definen los permisos de acceso:

| | |
|---------|---|
| -effect | La declaración puede permitir o denegar el acceso |
|---------|---|

| | |
|------------------------|---|
| <code>-action</code> | Puede especificar * para indicar todas las acciones, o una lista de una o varias de las siguientes: <code>GetObject</code> , <code>PutObject</code> , <code>DeleteObject</code> , <code>ListBucket</code> , <code>GetBucketAcl</code> , <code>GetObjectAcl</code> , <code>ListAllMyBuckets</code> , <code>ListBucketMultipartUploads</code> , y <code>ListMultipartUploadParts</code> . |
| <code>-resource</code> | El bloque y cualquier objeto que contenga. Los caracteres comodín * y . ? se puede utilizar para formar una expresión regular para especificar un recurso. |

Opcionalmente, puede especificar una cadena de texto como comentario con el `-sid` opción.

De forma predeterminada, las nuevas sentencias se agregan al final de la lista de sentencias, que se procesan en orden. Cuando agregue o modifique sentencias más tarde, tiene la opción de modificar las sentencias `-index` configuración para cambiar la orden de procesamiento.

Configure el acceso S3 para los servicios de directorio externos

A partir de ONTAP 9.14.1, los servicios para directorios externos se han integrado con el almacenamiento de objetos S3 de ONTAP. Esta integración simplifica la administración de usuarios y accesos a través de servicios de directorio externos.

Puede proporcionar grupos de usuarios que pertenecen a un servicio de directorio externo con acceso al entorno de almacenamiento de objetos de ONTAP. El protocolo ligero de acceso a directorios (LDAP) es una interfaz para la comunicación con servicios de directorio, como Active Directory, que proporcionan una base de datos y servicios para la gestión de identidades y accesos (IAM). Para proporcionar acceso, debe configurar los grupos LDAP en el entorno de ONTAP S3. Después de configurar el acceso, los miembros del grupo tienen permisos para los buckets de ONTAP S3. Para obtener más información sobre LDAP, consulte ["Información general sobre cómo usar LDAP"](#).

También puede configurar grupos de usuarios de Active Directory para el modo de enlace rápido, de modo que las credenciales de usuario se puedan validar y las aplicaciones S3 de terceros y de código abierto se puedan autenticar a través de conexiones LDAP.

Antes de empezar

Asegúrese de lo siguiente antes de configurar los grupos LDAP y habilitar el modo de enlace rápido para el acceso de grupos:

1. Se creó una máquina virtual de almacenamiento habilitada para S3 que contiene un servidor S3. Consulte ["Cree una SVM para S3"](#).
2. Se ha creado un bloque en esa máquina virtual de almacenamiento. Consulte ["Crear un bucket"](#).
3. DNS está configurado en la máquina virtual de almacenamiento. Consulte ["Configure los servicios DNS"](#).
4. Hay un certificado de entidad de certificación raíz (CA) autofirmado del servidor LDAP instalado en la máquina virtual de almacenamiento. Consulte ["Instale el certificado de CA raíz autofirmado en la SVM"](#).

5. Se configura un cliente LDAP con TLS habilitado en la SVM. Consulte ["Cree una configuración de cliente LDAP"](#) y.. ["Asocie la configuración del cliente LDAP con las SVM para obtener información"](#).

Configure el acceso S3 para los servicios de directorio externos

1. Especifique LDAP como la base de datos del servicio *name* de la SVM para el grupo y la contraseña a LDAP:

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

Para obtener más información acerca de este comando, consulte ["servicios de vserver servicio de nombres ns-switch modificar"](#) comando.

2. Cree una sentencia de política de cubo de almacén de objetos con principal Defina el grupo LDAP al que desea otorgar acceso:

```
object-store-server bucket policy statement create -bucket <bucket-name>
-effect allow -principal nasgroup/<ldap-group-name> -resource <bucket-
name>, <bucket-name>/*
```

Ejemplo: En el siguiente ejemplo se crea una sentencia de política de bloque para buck1. La política permite el acceso al grupo LDAP group1 al recurso (bloque y sus objetos) buck1.

```
vserver object-store-server bucket policy add-statement -bucket buck1
-effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,Li
stBucketMultipartUploads,ListMultipartUploadParts,
ListBucketVersions,GetObjectTagging,PutObjectTagging,DeleteObjectTagging
,GetBucketVersioning,PutBucketVersioning -principal nasgroup/group1
-resource buck1, buck1/*
```

3. Verifique que un usuario del grupo LDAP group1 Es capaz de realizar operaciones S3 desde el cliente S3.

Use el modo de enlace rápido LDAP para la autenticación

1. Especifique LDAP como la base de datos del servicio *name* de la SVM para el grupo y la contraseña a LDAP:

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

Para obtener más información acerca de este comando, consulte ["servicios de vserver servicio de nombres ns-switch modificar"](#) comando.

2. Asegúrese de que un usuario LDAP que acceda al bloque de S3 tenga permisos definidos en las políticas de bloque. Para obtener más información, consulte ["Modificar una política de bloques"](#).
3. Verifique que un usuario del grupo LDAP pueda realizar las siguientes operaciones:
 - a. Configure la clave de acceso en el cliente S3 en este formato:
"NTAPFASTBIND" + base64-encode(user-name:password)
Ejemplo: "NTAPFASTBIND" + base64-encode(ldapuser:password), lo que resulta en
NTAPFASTBINDbGRhcHVzZXI6cGFzc3dvcmQ=



Es posible que el cliente S3 solicite una clave secreta. En ausencia de una clave secreta, se puede introducir cualquier contraseña de al menos 16 caracteres.

- b. Realice operaciones S3 básicas desde el cliente S3 para el que el usuario tenga permisos.

Habilite LDAP o usuarios de dominio para generar sus propias claves de acceso S3

A partir de ONTAP 9.14.1, como administrador de ONTAP, puede crear roles personalizados y concederles a grupos de dominio locales o a grupos de protocolo ligero de acceso a directorios (LDAP), de modo que los usuarios que pertenecen a esos grupos puedan generar sus propias claves secretas y de acceso para el acceso de clientes S3.

Debe realizar algunos pasos de configuración en la máquina virtual de almacenamiento, de manera que el rol personalizado se pueda crear y asignar al usuario que llama a la API para la generación de claves de acceso.

Antes de empezar

Asegúrese de lo siguiente:

1. Se creó una máquina virtual de almacenamiento habilitada para S3 que contiene un servidor S3. Consulte ["Cree una SVM para S3"](#).
2. Se ha creado un bloque en esa máquina virtual de almacenamiento. Consulte ["Crear un bucket"](#).
3. DNS está configurado en la máquina virtual de almacenamiento. Consulte ["Configure los servicios DNS"](#).
4. Hay un certificado de entidad de certificación raíz (CA) autofirmado del servidor LDAP instalado en la máquina virtual de almacenamiento. Consulte ["Instale el certificado de CA raíz autofirmado en la SVM"](#).
5. Se configura un cliente LDAP con TLS habilitado en la máquina virtual de almacenamiento. Consulte ["Cree una configuración de cliente LDAP"](#) y .
6. Asocie la configuración del cliente al Vserver. Consulte ["Asocie la configuración del cliente LDAP con las SVM"](#) y.. ["creación de ldap de servicio de nombres de servicios vserver"](#).
7. Si utiliza una máquina virtual de almacenamiento de datos, cree una interfaz de red de gestión (LIF) y en la máquina virtual, así como una política de servicio para la LIF. Consulte ["se crea la interfaz de red"](#) y.. ["interfaz de red service-policy create"](#) comandos.

Configurar usuarios para la generación de claves de acceso

1. Especifique LDAP como la base de datos del servicio *name* de la máquina virtual de almacenamiento para el grupo y la contraseña a LDAP:

```
ns-switch modify -vserver <vserver-name> -database group -sources  
files,ldap  
ns-switch modify -vserver <vserver-name> -database passwd -sources  
files,ldap
```

Para obtener más información acerca de este comando, consulte ["servicios de vserver servicio de nombres ns-switch modificar"](#) comando.

2. Cree un rol personalizado con acceso al extremo de la API de REST DE S3 usuarios:

```
security login rest-role create -vserver <vserver-name> -role <custom-role-  
name> -api "/api/protocols/s3/services/*/users" -access <access-type>
```

En este ejemplo, la *s3-role* Se genera el rol para los usuarios en la máquina virtual de almacenamiento *svm-1*, a los que se otorgan todos los derechos de acceso, leer, crear y actualizar.

```
security login rest-role create -vserver svm-1 -role s3role -api  
"/api/protocols/s3/services/*/users" -access all
```

Para obtener más información acerca de este comando, consulte ["creación de rest-role de conexión de seguridad"](#) comando.

3. Cree un grupo de usuarios LDAP con el comando `security login` y añada el nuevo rol personalizado para acceder al punto final de la API DE REST DE usuarios de S3. Para obtener más información acerca de este comando, consulte ["seguridad de inicio de sesión creado"](#) comando.

```
security login create -user-or-group-name <ldap-group-name> -application  
http -authentication-method nsswitch -role <custom-role-name> -is-ns  
-switch-group yes
```

En este ejemplo, el grupo LDAP *ldap-group-1* se crea en *svm-1*, y el rol personalizado *s3role* Se ha añadido a él para acceder al punto final de la API, junto con la habilitación del acceso LDAP en el modo de enlace rápido.

```
security login create -user-or-group-name ldap-group-1 -application http  
-authentication-method nsswitch -role s3role -is-ns-switch-group yes  
-second-authentication-method none -vserver svm-1 -is-ldap-fastbind yes
```

Para obtener más información, consulte ["Utilice el enlace rápido LDAP para la autenticación nsswitch"](#).

Al agregar el rol personalizado al dominio o grupo LDAP, los usuarios de ese grupo tendrán acceso limitado a la `ONTAP /api/protocols/s3/services/{svm.uuid}/users` extremo. Al invocar la API, los usuarios del grupo de dominio o LDAP pueden generar su propio acceso y claves secretas para acceder al cliente S3.

Pueden generar las claves solo para ellos mismos y no para otros usuarios.

Como usuario S3 o LDAP, genere sus propias claves de acceso

A partir de ONTAP 9.14.1, puede generar sus propias claves de acceso y secretas para acceder a clientes S3, si su administrador le ha otorgado el rol para generar sus propias claves. Puede generar claves únicamente para usted mediante el siguiente extremo de la API REST DE ONTAP.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo. Para obtener información sobre los otros métodos de este punto final, consulte la referencia ["Documentación de API"](#).

| Método HTTP | Ruta |
|-------------|---|
| PUBLICAR | /api/protocols/s3/services/{svm.uid}/usuarios |

Ejemplo de curl

```
curl
--request POST \
--location "https://$FQDN_IP /api/protocols/s3/services/{svm.uid}/users "
\
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
--data '{"name": "_name_"}'
```

Ejemplo de resultado JSON

```
{
  "records": [
    {
      "access_key":
"Pz3SB54G2B_6dsXQPrA5HrTPcf478qoAW6_Xx6qyqZ948AgZ_7YfCf_9nO87YoZmskxx3cq41
U2JAH2M3_fs321B4rkzS3a_oC5_8u7D8j_45N8OsBCBPWGD_1d_ccfq",
      "_links": {
        "next": {
          "href": "/api/resourcelink"
        },
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "user-1",
      "secret_key":
"A20_tDhC_cux2C2BmtL45bXB_a_Q65c_96FsAcOdo14Az8V31jBKDTc0uCL62Bh559gPB8s9r
rn0868QrF38_1dsV2u1_9H2tSf3qQ5xp9NT259C6z_GiZQ883Qn63X1"
    }
  ],
  "num_records": "1"
}
```

Habilite el acceso del cliente al almacenamiento de objetos de S3

Habilite el acceso de ONTAP S3 para la organización remota en niveles de FabricPool

Para que ONTAP S3 se use como nivel de capacidad de FabricPool remota (cloud), el administrador de ONTAP S3 debe proporcionar información acerca de la configuración del servidor S3 al administrador de clústeres de ONTAP remoto.

Acerca de esta tarea

Se necesita la siguiente información del servidor S3 para configurar niveles de cloud FabricPool:

- Nombre del servidor (FQDN)
- nombre del bloque
- Certificado de CA
- clave de acceso
- contraseña (clave de acceso secreta)

Además, se requiere la siguiente configuración de red:

- Debe haber una entrada para el nombre de host del servidor ONTAP S3 remoto en el servidor DNS configurado para la SVM de administrador, incluido el nombre FQDN del servidor S3 y las direcciones IP en sus LIF.

- Las LIF de interconexión de clústeres se deben configurar en el clúster local, aunque no sea necesaria la relación de clústeres entre iguales.

Consulte la documentación de FabricPool sobre cómo configurar ONTAP S3 como nivel de cloud.

"Gestión de niveles de almacenamiento mediante FabricPool"

Habilite el acceso de ONTAP S3 para la organización local de FabricPool Tiering

Para que ONTAP S3 se pueda usar como nivel de capacidad FabricPool local, debe definir un almacén de objetos basado en el bloque que ha creado y, a continuación, adjuntar el almacén de objetos a un agregado de nivel de rendimiento para crear una FabricPool.

Antes de empezar

Debe tener el nombre del servidor ONTAP S3 y un nombre de bloque, y el servidor S3 debe haberse creado mediante las LIF del clúster (con el `-vserver Cluster` parámetro).

Acerca de esta tarea

La configuración del almacén de objetos contiene información sobre el nivel de capacidad local, incluidos los nombres de servidor S3 y bloques, y los requisitos de autenticación.

Una vez creada, la configuración de almacén de objetos no debe volver a asociarse con un almacén de objetos o un bloque diferentes. Es posible crear varios bloques para niveles locales, pero no se pueden crear varios almacenes de objetos en un solo bloque.

No se requiere una licencia de FabricPool para un nivel de capacidad local.

Pasos

1. Cree el almacén de objetos para el nivel de capacidad local:

```
storage aggregate object-store config create -object-store-name store_name
-ipospace Cluster -provider-type ONTAP_S3 -server S3_server_name -container
-name bucket_name -access-key access_key -secret-password password
```

- La `-container-name` Es el bloque de S3 que ha creado.
- La `-access-key` El parámetro autoriza las solicitudes al servidor ONTAP S3.
- La `-secret-password` El parámetro (clave de acceso secreta) autentica las solicitudes en el servidor ONTAP S3.
- Puede ajustar la `-is-certificate-validation-enabled` parámetro a `false` Para deshabilitar la comprobación de certificados para ONTAP S3.

```
cluster1::> storage aggregate object-store config create
-object-store-name MyLocalObjStore -ipospace Cluster -provider-type
ONTAP_S3 -server s3.example.com
-container-name bucket1 -access-key myS3key -secret-password myS3pass
```

2. Mostrar y verificar la información de configuración del almacén de objetos:

```
storage aggregate object-store config show
```

3. Opcional: Para ver cuántos datos de un volumen están inactivos, siga los pasos de ["Determinar cuántos datos de un volumen están inactivos mediante la generación de informes de datos inactivos"](#).

Ver cuántos datos de un volumen están inactivos puede ayudarle a decidir qué agregado usar para la organización en niveles local de FabricPool.

4. Asocie el almacén de objetos a un agregado:

```
storage aggregate object-store attach -aggregate aggr_name -object-store-name store_name
```

Puede utilizar el `allow-flexgroup` **true** Opción para conectar agregados que contienen componentes de volumen FlexGroup.

```
cluster1::> storage aggregate object-store attach  
-aggregate aggr1 -object-store-name MyLocalObjStore
```

5. Muestre la información del almacén de objetos y compruebe que el almacén de objetos asociado esté disponible:

```
storage aggregate object-store show
```

```
cluster1::> storage aggregate object-store show
```

| Aggregate | Object Store Name | Availability State |
|-----------|-------------------|--------------------|
| ----- | ----- | ----- |
| aggr1 | MyLocalObjStore | available |

Habilite el acceso del cliente desde una aplicación de S3

Para que las aplicaciones cliente S3 puedan acceder al servidor ONTAP S3, el administrador de ONTAP S3 debe proporcionar información de configuración al usuario S3.

Antes de empezar

La aplicación cliente S3 debe poder autenticarse con el servidor ONTAP S3 mediante las siguientes versiones de firma AWS:

- Firma Versión 4, ONTAP 9.8 y posterior
- Versión de la firma 2, ONTAP 9.11.1 y posterior

ONTAP S3 no admite otras versiones de firma.

El administrador de ONTAP S3 debe haber creado usuarios de S3 y haberle otorgado permisos de acceso, como usuarios individuales o como miembro de un grupo, en la política de bucket o en la de los servidores de almacenamiento de objetos.

La aplicación cliente S3 debe poder resolver el nombre del servidor ONTAP S3, lo que requiere que el administrador de ONTAP S3 proporcione el nombre del servidor S3 (FQDN) y las direcciones IP para los LIF del servidor S3.

Acerca de esta tarea

Para acceder a un bloque de ONTAP S3, un usuario de la aplicación del cliente de S3 introduce información que proporciona el administrador de ONTAP S3.

A partir de ONTAP 9.9.1, el servidor ONTAP S3 admite la siguiente funcionalidad del cliente AWS:

- metadatos de objetos definidos por el usuario

Un conjunto de pares de clave-valor se puede asignar a objetos como metadatos cuando se crean usando PUT (o POST). Cuando se realiza una operación GET/HEAD en el objeto, los metadatos definidos por el usuario se devuelven junto con los metadatos del sistema.

- etiquetado de objetos

Se puede asignar un conjunto separado de pares clave-valor como etiquetas para categorizar objetos. A diferencia de los metadatos, se crean y se leen etiquetas con las API DE REST independientemente del objeto, y se implementan cuando se crean los objetos o en cualquier momento.



Para permitir que los clientes obtengan y coloquen información sobre el etiquetado, las acciones `GetObjectTagging`, `PutObjectTagging`, y `DeleteObjectTagging` debe permitirse el uso de las políticas de bloque o grupo.

Para obtener más información, consulte la documentación de AWS S3.

Pasos

1. Autentique la aplicación cliente S3 con el servidor ONTAP S3 introduciendo el nombre del servidor S3 y el certificado de CA.
2. Para autenticar un usuario en la aplicación S3 Client, introduzca la siguiente información:
 - El nombre del servidor S3 (FQDN) y el nombre del bloque
 - clave secreta y clave de acceso del usuario

Definiciones de servicios de almacenamiento

ONTAP incluye servicios de almacenamiento predefinidos que están asignados a factores mínimos de rendimiento correspondientes.

El conjunto real de servicios de almacenamiento disponibles en un clúster o SVM está determinado por el tipo de almacenamiento que compone un agregado en la SVM.

En la siguiente tabla se muestra cómo se asignan los factores mínimos de rendimiento a los servicios de almacenamiento predefinidos:

| Servicio de almacenamiento | IOPS (SLA) esperada | Pico de IOPS (SLO) | IOPS de volumen mínimo | Latencia estimada | ¿Se espera que las IOPS se apliquen? |
|----------------------------|---------------------|--------------------|------------------------|-------------------|---|
| valor | 128 \$ por TB | 512 \$ por TB | 75 | 17 ms | En AFF: Sí En caso contrario: No |
| rendimiento | 2048 por TB | 4096 \$ por TB | 500 | 2 ms | Sí |
| extremo | 6144 \$ por TB | 12288 \$ por TB | 1000 | 1 ms | Sí |

En la siguiente tabla se define el nivel de servicio de almacenamiento disponible para cada tipo de medios o nodo:

| Medios o nodo | Nivel de servicio de almacenamiento disponible |
|--|--|
| Disco | valor |
| Disco de máquina virtual | valor |
| LUN de FlexArray | valor |
| Híbrido | valor |
| Flash con optimización de la capacidad | valor |
| Unidad de estado sólido (SSD): No AFF | valor |
| Flash optimizado para el rendimiento - SSD (AFF) | extremo, rendimiento, valor |

Proteja los bloques con SnapMirror de S3

Información general de SnapMirror de S3

A partir de ONTAP 9.10.1, puede proteger buckets en almacenes de objetos de ONTAP S3 mediante mirroring de SnapMirror y funcionalidad de backup. A diferencia de SnapMirror estándar, SnapMirror de S3 permite el mirroring y los backups en destinos que no sean de NetApp, como AWS S3.

SnapMirror de S3 admite reflejos activos y niveles de backup desde bloques de ONTAP S3 en los siguientes destinos:

| Destino | ¿Admite los reflejos activos y la toma de control? | ¿Compatible con backup y restauración? |
|--|--|--|
| ONTAP S3 <ul style="list-style-type: none"> • Bloques en la misma SVM • Los bloques de diferentes SVM en el mismo clúster • Bloques en SVM en clústeres diferentes | ✓ | ✓ |
| StorageGRID | | ✓ |
| AWS S3 | | ✓ |
| Cloud Volumes ONTAP para Azure | ✓ | ✓ |
| Cloud Volumes ONTAP para AWS | ✓ | ✓ |
| Cloud Volumes ONTAP para Google Cloud | ✓ | ✓ |

Puede proteger bloques existentes en servidores ONTAP S3 o puede crear nuevos bloques con protección de datos habilitada de inmediato.

Requisitos de SnapMirror de S3

- Versión de ONTAP
ONTAP 9.10.1 o una versión posterior debe ejecutarse en clústeres de origen y de destino.
- Licencia
Los siguientes paquetes de licencia se requieren en los sistemas de origen y de destino de ONTAP:
 - Paquete básico
Para el protocolo y el almacenamiento ONTAP S3.
 - Bundle de protección de datos
Para SnapMirror de S3 para dirigirse a otros destinos de almacenes de objetos de NetApp (ONTAP S3, StorageGRID y Cloud Volumes ONTAP).
 - Bundle de protección de datos y de cloud híbrido
Para S3 SnapMirror para apuntar a almacenes de objetos de terceros, incluido AWS S3.
- ONTAP S3
 - Los servidores ONTAP S3 deben ejecutar SVM de origen y de destino.
 - Se recomienda, pero no es obligatorio, que los certificados de CA para el acceso TLS estén instalados en sistemas que alojan servidores S3.
 - Los certificados de CA utilizados para firmar los certificados de los servidores S3 deben instalarse en la máquina virtual de almacenamiento de administrador de los clústeres que alojan servidores S3.
 - Es posible usar un certificado de CA autofirmado o un certificado firmado por un proveedor de CA externo.
 - Si las máquinas virtuales de almacenamiento de origen o de destino no escuchan con HTTPS, no es necesario instalar certificados de CA.
- Relaciones entre iguales (para destinos de ONTAP S3)

- Las LIF de interconexión de clústeres deben configurarse (para destinos de ONTAP remotos).
- Los clústeres de origen y destino tienen una relación entre iguales (para destinos de ONTAP remotos).
- Las máquinas virtuales de almacenamiento de origen y de destino tienen una relación entre iguales (para todos los destinos ONTAP).
- Política de SnapMirror
 - Se requiere una política de SnapMirror específica para S3 en todas las relaciones de SnapMirror S3, pero se puede usar la misma política para varias relaciones.
 - Puede crear su propia directiva o aceptar la predeterminada **continua**, que incluye los siguientes valores:
 - Acelerador (límite superior de rendimiento/ancho de banda): Ilimitado.
 - Tiempo objetivo de punto de recuperación: 1 hora (3600 segundos).
- Claves de usuario raíz

Se requieren claves de acceso del usuario raíz de Storage VM para las relaciones de SnapMirror de S3; ONTAP no las asigna de forma predeterminada. La primera vez que crea una relación SnapMirror de S3, debe comprobar que las claves existen tanto en los equipos virtuales de almacenamiento de origen como de destino, y volver a regenerarlas si no lo hacen. Si necesita volver a regenerarlos, debe asegurarse de que todos los clientes y todas las configuraciones del almacén de objetos de SnapMirror que utilicen el par de claves secreta y de acceso se actualicen con las nuevas claves.

Para obtener información sobre la configuración del servidor S3, consulte los temas siguientes:

- ["Habilite un servidor S3 en una máquina virtual de almacenamiento"](#)
- ["Acerca del proceso de configuración de S3"](#)

Para obtener información acerca de la relación entre iguales de clústeres y máquinas virtuales de almacenamiento, consulte el tema siguiente:

- ["Preparación del mirroring y el almacenamiento \(System Manager, pasos 1 a 6\)"](#)
- ["Relaciones entre iguales de clústeres y SVM \(CLI\)"](#)

Relaciones de SnapMirror admitidas

SnapMirror de S3 admite relaciones de distribución ramificada y en cascada. Para ver información general, consulte ["Puestas en marcha de protección de datos en cascada y distribución ramificada"](#).

S3 SnapMirror no admite puestas en marcha ramificadas (relaciones de protección de datos entre varios bloques de origen y un único bloque de destino). SnapMirror de S3 puede admitir varios duplicados de bloques de varios clústeres en un único clúster secundario, pero cada bloque de origen debe tener su propio bloque de destino en el clúster secundario.

Controle el acceso a S3 cucharones

Cuando se crean bloques nuevos, se puede controlar el acceso mediante la creación de usuarios y grupos. Para obtener más información, consulte los siguientes temas:

- ["Añadir usuarios y grupos de S3 \(System Manager\)"](#)
- ["Crear un usuario de S3 \(CLI\)"](#)
- ["Crear o modificar grupos S3 \(CLI\)"](#)

Refleje y protección de backup en un clúster remoto

Crear una relación de mirroring para un bloque nuevo (clúster remoto)

Cuando se crean nuevos bloques S3, se pueden proteger inmediatamente a un destino S3 SnapMirror en un clúster remoto.



Acerca de esta tarea


Deberá realizar tareas tanto en los sistemas de origen como de destino.

Antes de empezar


- Se han completado los requisitos para las versiones de ONTAP, las licencias y la configuración de servidores S3.
- Existe una relación de paridad entre los clústeres de origen y de destino, y existe una relación entre iguales entre las máquinas virtuales de almacenamiento de origen y de destino.
- Los certificados DE CA se necesitan para las máquinas virtuales de origen y de destino. Puede usar certificados de CA autofirmados o certificados firmados por un proveedor de CA externo.

System Manager

1. Si esta es la primera relación SnapMirror de S3 para este equipo virtual de almacenamiento, compruebe que existen claves de usuario raíz para los equipos virtuales de almacenamiento de origen y de destino, y regenlas si no:
 - a. Haga clic en **almacenamiento > Storage VMs** y, a continuación, seleccione la VM de almacenamiento.
 - b. En la ficha **Configuración**, haga clic en  En el mosaico **S3**.
 - c. En la ficha **usuarios**, compruebe que hay una clave de acceso para el usuario raíz.
 - d. Si no lo hay, haga clic en  Junto a **root**, haga clic en **regenerar clave**. No vuelva a generar la clave si ya existe.
2. Edite la máquina virtual de almacenamiento para añadir usuarios y añadir usuarios a grupos, tanto en las máquinas virtuales de almacenamiento de origen como de destino:

Haga clic en **almacenamiento > Storage VMs**, haga clic en la VM de almacenamiento, haga clic en **Configuración** y, a continuación, haga clic en  En S3.

Consulte "[Añada usuarios y grupos de S3](#)" si quiere más información.

3. En el clúster de origen, cree una política de SnapMirror de S3 si no tiene una existente y no desea usar la directiva predeterminada:
 - a. Haga clic en **Protección > Descripción general** y, a continuación, en **Configuración de directivas locales**.
 - b. Haga clic en  Junto a **Directivas de protección**, haga clic en **Agregar**.
 - Escriba el nombre de la política y una descripción.
 - Seleccione el alcance de las políticas, el clúster o la SVM
 - Seleccione **Continuous** para las relaciones de SnapMirror de S3.
 - Introduzca los valores **acelerador** y **objetivo de punto de recuperación**.
4. Crear un bloque con la protección SnapMirror:
 - a. Haga clic en **almacenamiento > Cuchos** y, a continuación, haga clic en **Agregar**. Verificar permisos es opcional pero se recomienda.
 - b. Introduzca un nombre, seleccione el equipo virtual de almacenamiento, introduzca un tamaño y, a continuación, haga clic en **más opciones**.
 - c. En **permisos**, haga clic en **Agregar**.
 - **Principal y efecto**: Seleccione los valores correspondientes a la configuración de su grupo de usuarios o acepte los valores predeterminados.
 - **Acciones**- Asegúrese de que se muestran los siguientes valores:

```
GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, ListMultipartUploadParts
```

- **Recursos**: Utilice los valores predeterminados (*bucketname*, *bucketname/**) u otros valores que necesite.

Consulte ["Gestionar el acceso del usuario a bloques"](#) para obtener más información sobre estos campos.

d. En **Protección**, compruebe **Activar SnapMirror (ONTAP o nube)**. A continuación, introduzca los siguientes valores:

- Destino
 - **OBJETIVO: Sistema ONTAP**
 - **CLUSTER:** Seleccione el cluster remoto.
 - **STORAGE VM:** Seleccione una VM de almacenamiento en el cluster remoto.
 - **Certificado de CA del SERVIDOR S3:** Copie y pegue el contenido del certificado *source*.
- Origen
 - **Certificado de CA del SERVIDOR S3:** copie y pegue el contenido del certificado *Destination*.

5. Marque **Utilice el mismo certificado en el destino** si está utilizando un certificado firmado por un proveedor de CA externo.

6. Si hace clic en **Configuración de destino**, también puede introducir sus propios valores en lugar de los valores predeterminados para el nombre del bloque, la capacidad y el nivel de servicio de rendimiento.

7. Haga clic en **Guardar**. Se crea un nuevo bucket en la máquina virtual de almacenamiento de origen que se refleja en un nuevo bucket que se crea la máquina virtual de almacenamiento de destino.

Haga retroceder los cucharones bloqueados

A partir de ONTAP 9.14.1, puede crear un backup de bloques S3 bloqueados y restaurarlos según sea necesario.

Al definir la configuración de protección para un bloque nuevo o existente, puede habilitar el bloqueo de objetos en los buckets de destino, siempre y cuando los clústeres de origen y de destino ejecuten ONTAP 9.14.1 o una versión posterior, y que el bloqueo de objetos se habilite en el bloque de origen. El modo de bloqueo de objetos y la tenencia de retención de bloqueos del bloque de origen se aplican a los objetos replicados en el bloque de destino. También puede definir un período de retención de bloqueo diferente para el depósito de destino en la sección **Configuración de destino**. Este período de retención también se aplica a cualquier objeto no bloqueado replicado desde el bloque de origen e interfaces S3.

Para obtener información sobre cómo activar el bloqueo de objetos en un depósito, consulte ["Crear un bucket"](#).

CLI

1. Si esta es la primera relación SnapMirror de S3 para esta SVM, compruebe que existen claves de usuario raíz para las SVM de origen y de destino y vuelva a regenerarlas si no:

```
vserver object-store-server user show
```

Compruebe que hay una clave de acceso para el usuario raíz. Si no lo hay, introduzca:

```
vserver object-store-server user regenerate-keys -vserver svm_name -user root
```

No vuelva a generar la clave si ya existe.

2. Cree bloques en las SVM de origen y destino:

```
vserver object-store-server bucket create -vserver svm_name -bucket
bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
[additional_options]
```

3. Añada reglas de acceso a las políticas de bloque predeterminadas tanto en las SVM de origen como de destino:

```
vserver object-store-server bucket policy add-statement -vserver svm_name
-bucket bucket_name -effect {allow|deny} -action object_store_actions
-principal user_and_group_names -resource object_store_resources [-sid
text] [-index integer]
```

Ejemplo

```
src_cluster::> vserver object-store-server bucket policy add-
statement -bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. En la SVM de origen, cree una política de SnapMirror S3 si no tiene una existente y no quiere usar la política predeterminada:

```
snapmirror policy create -vserver svm_name -policy policy_name -type
continuous [-rpo integer] [-throttle throttle_type] [-comment text]
[additional_options]
```

Parámetros:

- tipo continuous - El único tipo de política para las relaciones de SnapMirror S3 (requerido).
- -rpo - especifica el tiempo para el objetivo de punto de recuperación, en segundos (opcional).
- -throttle - especifica el límite superior de rendimiento/ancho de banda, en kilobytes/segundos (opcional).

Ejemplo

```
src_cluster::> snapmirror policy create -vserver vs0 -type
continuous -rpo 0 -policy test-policy
```

5. Instale los certificados de servidor de CA en las SVM de administrador de los clústeres de origen y destino:

a. En el clúster de origen, instale el certificado de CA que firmó el certificado de servidor *Destination* S3:

```
security certificate install -type server-ca -vserver src_admin_svm
-cert-name dest_server_certificate
```

b. En el clúster de destino, instale el certificado de CA que firmó el certificado de servidor *source* S3:

```
security certificate install -type server-ca -vserver dest_admin_svm
```

```
-cert-name src_server_certificate
```

Si utiliza un certificado firmado por un proveedor de CA externo, instale el mismo certificado en la SVM de administrador de origen y de destino.

Consulte `security certificate install manual` para más detalles.

6. En la SVM de origen, cree una relación de SnapMirror de S3:

```
snapmirror create -source-path src_svm_name:/bucket/bucket_name  
-destination-path dest_peer_svm_name:/bucket/bucket_name, ...} [-policy  
policy_name]
```

Puede usar una política que haya creado o aceptar la predeterminada.

Ejemplo

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-  
bucket -destination-path vs1-dest:bucket/test-bucket-mirror -policy  
test-policy
```

7. Compruebe que el mirroring está activo:

```
snapmirror show -policy-type continuous -fields status
```

Crear una relación de mirroring para un bloque existente (clúster remoto)

Puede comenzar a proteger bloques de S3 existentes en cualquier momento; por ejemplo, si actualizó una configuración de S3 desde una versión anterior a ONTAP 9.10.1.

Acerca de esta tarea

Debe realizar tareas en los clústeres de origen y de destino.



Antes de empezar


- Se han completado los requisitos para las versiones de ONTAP, las licencias y la configuración de servidores S3.
- Existe una relación de paridad entre los clústeres de origen y de destino, y existe una relación entre iguales entre las máquinas virtuales de almacenamiento de origen y de destino.
- Los certificados DE CA se necesitan para las máquinas virtuales de origen y de destino. Puede usar certificados de CA autofirmados o certificados firmados por un proveedor de CA externo.

Pasos



Puede crear una relación de mirroring mediante System Manager o la interfaz de línea de comandos de ONTAP.

System Manager

1. Si esta es la primera relación SnapMirror de S3 para este equipo virtual de almacenamiento, compruebe que existen claves de usuario raíz para los equipos virtuales de almacenamiento de origen y de destino, y regénalas si no:
 - a. Seleccione **Almacenamiento > Storage VMs** y, a continuación, seleccione la VM de almacenamiento.
 - b. En la ficha **Configuración**, haga clic en  En el mosaico **S3**.
 - c. En la ficha **usuarios**, compruebe que hay una clave de acceso para el usuario raíz.
 - d. Si no lo hay, haga clic en  Junto a **root**, luego haga clic en **Regenerar clave**. No vuelva a generar la clave si ya existe.

2. Compruebe que el acceso de usuario y grupo es correcto tanto en las máquinas virtuales de almacenamiento de origen como de destino:
Seleccione **Almacenamiento > VM de almacenamiento**, luego seleccione la VM de almacenamiento y luego **Configuración**. Por último, seleccione  En **S3**.

Consulte "[Añada usuarios y grupos de S3](#)" si quiere más información.

3. En el clúster de origen, cree una política de SnapMirror de S3 si no tiene una existente y no desea usar la directiva predeterminada:
 - a. Seleccione **Protección > Descripción general** y, a continuación, haga clic en **Configuración de política local**.
 - b. Seleccione  Junto a **Directivas de protección**, haga clic en **Agregar**.
 - c. Escriba el nombre de la política y una descripción.
 - d. Seleccione el alcance de las políticas, el clúster o la SVM
 - e. Seleccione **Continuous** para las relaciones de SnapMirror de S3.
 - f. Introduzca los valores **acelerador** y **objetivo de punto de recuperación**.
4. Compruebe que la política de acceso a bloques del bloque existente sigue cumpliéndose con sus necesidades:
 - a. Haga clic en **almacenamiento > Cuchos** y, a continuación, seleccione el cucharón que desea proteger.
 - b. En la ficha **permisos**, haga clic en  **Editar**, luego haz clic en **Agregar** bajo **Permisos**.
 - **Principal y efecto**: Seleccione los valores correspondientes a la configuración de su grupo de usuarios o acepte los valores predeterminados.
 - **Acciones**: Asegúrese de que se muestran los siguientes valores:

`GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, ListMultipartUploadParts`

- **Recursos**: Utilice los valores predeterminados (*bucketname*, *bucketname/**) u otros valores que necesite.

Consulte "[Gestionar el acceso del usuario a bloques](#)" para obtener más información sobre estos campos.

5. Proteja un bloque existente con la protección S3 SnapMirror:

- a. Haga clic en **almacenamiento > Cuchos** y, a continuación, seleccione la cuchara que desea proteger.
 - b. Haga clic en **proteger** e introduzca los siguientes valores:
 - Destino
 - **OBJETIVO**: Sistema ONTAP
 - **CLUSTER**: Seleccione el cluster remoto.
 - **STORAGE VM**: Seleccione una VM de almacenamiento en el cluster remoto.
 - **Certificado de CA del SERVIDOR S3**: Copie y pegue el contenido del certificado *source*.
 - Origen
 - **Certificado de CA del SERVIDOR S3**: Copie y pegue el contenido del certificado *Destination*.
6. Marque **Utilice el mismo certificado en el destino** si está utilizando un certificado firmado por un proveedor de CA externo.
7. Si hace clic en **Configuración de destino**, también puede introducir sus propios valores en lugar de los valores predeterminados para el nombre del bloque, la capacidad y el nivel de servicio de rendimiento.
8. Haga clic en **Guardar**. El bloque existente se refleja en un nuevo bloque en la máquina virtual de almacenamiento de destino.

Haga retroceder los cucharones bloqueados

A partir de ONTAP 9.14.1, puede crear un backup de bloques S3 bloqueados y restaurarlos según sea necesario.

Al definir la configuración de protección para un bloque nuevo o existente, puede habilitar el bloqueo de objetos en los buckets de destino, siempre y cuando los clústeres de origen y de destino ejecuten ONTAP 9.14.1 o una versión posterior, y que el bloqueo de objetos se habilite en el bloque de origen. El modo de bloqueo de objetos y la tenencia de retención de bloqueos del bloque de origen se aplican a los objetos replicados en el bloque de destino. También puede definir un período de retención de bloqueo diferente para el depósito de destino en la sección **Configuración de destino**. Este período de retención también se aplica a cualquier objeto no bloqueado replicado desde el bloque de origen e interfaces S3.

Para obtener información sobre cómo activar el bloqueo de objetos en un depósito, consulte "[Crear un bucket](#)".

CLI

1. Si esta es la primera relación SnapMirror de S3 para esta SVM, compruebe que existen claves de usuario raíz para las SVM de origen y de destino y vuelva a regenerarlas si no:

```
vserver object-store-server user show
```

Compruebe que hay una clave de acceso para el usuario raíz. Si no lo hay, introduzca:

```
vserver object-store-server user regenerate-keys -vserver svm_name -user root
```

No vuelva a generar la clave si ya existe.

2. Crear un bucket en la SVM de destino que sea el destino de mirroring:

```
vserver object-store-server bucket create -vserver svm_name -bucket
```



```
dest_bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
[additional_options]
```

3. Compruebe que las reglas de acceso de las políticas de bloque predeterminadas sean correctas tanto en las SVM de origen como de destino:

```
vserver object-store-server bucket policy add-statement -vserver svm_name
-bucket bucket_name -effect {allow|deny} -action object_store_actions
-principal user_and_group_names -resource object_store_resources [-sid
text] [-index integer]
```

Ejemplo

```
src_cluster::> vserver object-store-server bucket policy add-
statement -bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. En la SVM de origen, cree una política de SnapMirror de S3 si no tiene una existente y no quiere usar la directiva predeterminada:

```
snapmirror policy create -vserver svm_name -policy policy_name -type
continuous [-rpo integer] [-throttle throttle_type] [-comment text]
[additional_options]
```

Parámetros:

- `continuous` : El único tipo de política para relaciones SnapMirror de S3 (obligatorio).
- `-rpo` – especifica el tiempo para el objetivo de punto de recuperación, en segundos (opcional).
- `-throttle` – especifica el límite superior de rendimiento/ancho de banda, en kilobytes/segundos (opcional).

Ejemplo

```
src_cluster::> snapmirror policy create -vserver vs0 -type
continuous -rpo 0 -policy test-policy
```

5. Instale los certificados de CA en las SVM de administrador de los clústeres de origen y destino:
 - a. En el clúster de origen, instale el certificado de CA que firmó el certificado de servidor *Destination* S3:

```
security certificate install -type server-ca -vserver src_admin_svm
-cert-name dest_server_certificate
```
 - b. En el clúster de destino, instale el certificado de CA que firmó el certificado de servidor *source* S3:

```
security certificate install -type server-ca -vserver dest_admin_svm
-cert-name src_server_certificate
```

Si utiliza un certificado firmado por un proveedor de CA externo, instale el mismo certificado en la SVM de administrador de origen y de destino.

Consulte `security certificate install` manual para más detalles.

6. En la SVM de origen, cree una relación de SnapMirror de S3:

```
snapmirror create -source-path src_svm_name:/bucket/bucket_name  
-destination-path dest_peer_svm_name:/bucket/bucket_name, ...} [-policy  
policy_name]
```

Puede usar una política que haya creado o aceptar la predeterminada.

Ejemplo

```
src_cluster::> snapmirror create -source-path vs0:/bucket/test-  
bucket -destination-path vs1:/bucket/test-bucket-mirror -policy  
test-policy
```

7. Compruebe que el mirroring está activo:

```
snapmirror show -policy-type continuous -fields status
```

Toma de control y sirve datos desde el bloque de destino (clúster remoto)

Si los datos de un bloque de origen dejan de estar disponibles, puede romper la relación de SnapMirror para hacer que el bloque de destino sea editable y comenzar a servir datos.

Acerca de esta tarea


Cuando se realiza una operación de toma de control, el bloque de origen se convierte en bloque de destino original de solo lectura y se convierte en bloque de destino original de lectura y escritura; de este modo, se invierte la relación de SnapMirror de S3.

Una vez que el bloque de origen deshabilitado se vuelva a poner disponible, S3 SnapMirror vuelve a sincronizar automáticamente el contenido de los dos bloques. No es necesario volver a sincronizar explícitamente la relación, tal y como es necesario en puestas en funcionamiento de SnapMirror para volúmenes.

La operación de toma de control se debe iniciar desde el clúster remoto.

System Manager

Conmutación por error desde el bloque no disponible y empiece a servir datos:

1. Haga clic en **Protección > Relaciones** y seleccione **S3 SnapMirror**.
2. Haga clic en , Seleccione **Failover** y, a continuación, haga clic en **failover**.

CLI

1. Inicie una operación de conmutación al nodo de respaldo para el bloque de destino:
`snapmirror failover start -destination-path svm_name:/bucket/bucket_name`
2. Compruebe el estado de la operación de conmutación por error:
`snapmirror show -fields status`

Ejemplo

```
dest_cluster::> snapmirror failover start -destination-path  
dest_svm1:/bucket/test-bucket-mirror
```

Restaurar un bloque a partir de la máquina virtual de almacenamiento de destino (clúster remoto)

Si los datos de un depósito de origen se pierden o se dañan, puede volver a rellenar los datos restaurando objetos desde un bloque de destino.

Acerca de esta tarea

Puede restaurar el bloque de destino en un bloque existente o en un bloque nuevo. El bloque de destino para la operación de restauración debe ser mayor que el espacio utilizado lógico del bucket de destino.

Si utiliza un bloque existente, debe estar vacío al iniciar una operación de restauración. La restauración no "rollback" de un bloque en el tiempo; más bien, rellena un bloque vacío con su contenido anterior.

La operación de restauración debe iniciarse desde el clúster remoto.

System Manager

Restaurar los datos de la copia de seguridad:

1. Haga clic en **Protección > Relaciones** y seleccione **S3 SnapMirror**.
2. Haga clic en **Y**, a continuación, seleccione **Restaurar**.
3. En **Fuente**, seleccione **cucharón existente** (predeterminado) o **Nuevo cucharón**.
 - Para restaurar a un **segmento existente** (valor predeterminado), lleve a cabo las siguientes acciones:
 - Seleccione la máquina virtual de almacenamiento y clúster para buscar el bloque existente.
 - Seleccione el bloque existente.
 - Copie y pegue el contenido del certificado de CA del servidor *destination* S3.
 - Para restaurar a un **New Bucket**, introduzca los siguientes valores:
 - El equipo virtual de clúster y almacenamiento para alojar el nuevo bloque.
 - El nombre, la capacidad y el nivel de servicio de rendimiento del bloque nuevo. Consulte ["Los niveles de servicio de almacenamiento"](#) si quiere más información.
 - El contenido del certificado de CA del servidor *Destination* S3.
4. En **destino**, copie y pegue el contenido del certificado de CA del servidor *source* S3.
5. Haga clic en **Protección > Relaciones** para supervisar el progreso de la restauración.

Restaurar los cucharones bloqueados

A partir de ONTAP 9.14.1, puede realizar backups de bloques bloqueados y restaurarlos según sea necesario.

Es posible restaurar un bloque de bloqueo de objetos a un bloque nuevo o existente. Puede seleccionar un depósito bloqueado por objeto como destino en las siguientes situaciones:

- **Restaurar a un nuevo cubo:** Cuando se habilita el bloqueo de objetos, un cubo puede restaurarse creando un cubo que también tiene habilitado el bloqueo de objetos. Cuando restaura un bucket bloqueado, se replican el modo de bloqueo de objetos y el periodo de retención del bucket original. También puede definir un período de retención de bloqueo diferente para el nuevo período. Este período de retención se aplica a objetos no bloqueados de otros orígenes.
- **Restaurar a un cubo existente:** Un cubo bloqueado por objeto se puede restaurar a un cubo existente, siempre y cuando el control de versiones y un modo de bloqueo de objetos similar estén habilitados en el cubo existente. Se mantiene la tenencia de retención del cucharón original.
- **Restaurar cubo no bloqueado:** Incluso si el bloqueo de objetos no está habilitado en un cubo, puede restaurarlo en un cubo que tiene el bloqueo de objetos activado y está en el clúster de origen. Al restaurar el bloque, todos los objetos no bloqueados se bloquean, y se aplican el modo de retención y la tenencia del bloque de destino.

CLI

1. Crear el nuevo bloque de destino para la restauración. Para obtener más información, consulte ["Crear una relación de backup para un bloque nuevo \(destino cloud\)"](#).
2. Inicie una operación de restauración para el bloque de destino:

```
snapmirror restore -source-path svm_name:/bucket/bucket_name -destination-path svm_name:/bucket/bucket_name
```

Ejemplo

```
dest_cluster::> snapmirror restore -source-path src_vs1:/bucket/test-  
bucket -destination-path dest_vs1:/bucket/test-bucket-mirror
```

Protección de reflejo y backup en el clúster local




Crear una relación de mirroring para un bloque nuevo (clúster local)

Cuando crea nuevos bloques S3, puede protegerlos inmediatamente a un destino S3 SnapMirror en el mismo clúster. Puede reflejar datos en un bloque de una máquina virtual de almacenamiento diferente o en la misma máquina virtual de almacenamiento que el origen.


Antes de empezar

- Se han completado los requisitos para las versiones de ONTAP, las licencias y la configuración de servidores S3.
- Existe una relación de paridad entre las máquinas virtuales de almacenamiento de origen y de destino.
- Los certificados DE CA se necesitan para las máquinas virtuales de origen y de destino. Puede usar certificados de CA autofirmados o certificados firmados por un proveedor de CA externo.

System Manager

1. Si esta es la primera relación SnapMirror de S3 para este equipo virtual de almacenamiento, compruebe que existen claves de usuario raíz para los equipos virtuales de almacenamiento de origen y de destino, y regenlas si no:
 - a. Haga clic en **almacenamiento > Storage VMs** y, a continuación, seleccione la VM de almacenamiento.
 - b. En la ficha **Configuración**, haga clic en  En el icono S3.
 - c. En la ficha **usuarios**, compruebe que hay una clave de acceso para el usuario raíz
 - d. Si no lo hay, haga clic en  Junto a **root**, haga clic en **regenerar clave**.
No vuelva a generar la clave si ya existe.
2. Edite la máquina virtual de almacenamiento para añadir usuarios y añadir usuarios a grupos, tanto en las máquinas virtuales de almacenamiento de origen como de destino:
Haga clic en **almacenamiento > Storage VMs**, haga clic en la VM de almacenamiento, haga clic en **Configuración** y, a continuación, haga clic en  En S3.

Consulte "[Añada usuarios y grupos de S3](#)" si quiere más información.

3. Cree una política de SnapMirror de S3 si no tiene una existente y no desea usar la directiva predeterminada:
 - a. Haga clic en **Protección > Descripción general** y, a continuación, haga clic en **Configuración de política local**.
 - b. Haga clic en  Junto a **Directivas de protección**, haga clic en **Agregar**.
 - Escriba el nombre de la política y una descripción.
 - Seleccione el alcance de las políticas, el clúster o la SVM
 - Seleccione **Continuous** para las relaciones de SnapMirror de S3.
 - Introduzca los valores **acelerador** y **objetivo de punto de recuperación**.
4. Crear un bloque con la protección SnapMirror:
 - a. Haga clic en **almacenamiento > Cuchos** y, a continuación, haga clic en **Agregar**.
 - b. Introduzca un nombre, seleccione el equipo virtual de almacenamiento, introduzca un tamaño y, a continuación, haga clic en **más opciones**.
 - c. En **permisos**, haga clic en **Agregar**. Verificar permisos es opcional pero se recomienda.
 - **Principal y efecto**: Seleccione los valores correspondientes a la configuración del grupo de usuarios o acepte los valores predeterminados.
 - **Acciones** - Asegúrese de que se muestran los siguientes valores:

```
GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, ListMultipartUploadParts
```

- **Recursos**: Utilice los valores predeterminados (`bucketname`, `bucketname/*`) u otros valores que necesite

Consulte "[Gestionar el acceso del usuario a bloques](#)" para obtener más información sobre estos campos.

d. En **Protección**, compruebe **Activar SnapMirror (ONTAP o nube)**. A continuación, introduzca los siguientes valores:

- Destino
 - **OBJETIVO**: Sistema ONTAP
 - **CLUSTER**: Seleccione el cluster local.
 - **VM DE ALMACENAMIENTO**: Seleccione una VM de almacenamiento en el clúster local.
 - **Certificado de CA del SERVIDOR S3**: Copie y pegue el contenido del certificado fuente.
- Origen
 - **Certificado de CA del SERVIDOR S3**: Copie y pegue el contenido del certificado de destino.

5. Marque **Utilice el mismo certificado en el destino** si está utilizando un certificado firmado por un proveedor de CA externo.
6. Si hace clic en **Configuración de destino**, también puede introducir sus propios valores en lugar de los valores predeterminados para el nombre del bloque, la capacidad y el nivel de servicio de rendimiento.
7. Haga clic en **Guardar**. Se crea un nuevo bucket en la máquina virtual de almacenamiento de origen que se refleja en un nuevo bucket que se crea la máquina virtual de almacenamiento de destino.

Haga retroceder los cucharones bloqueados

A partir de ONTAP 9.14.1, puede crear un backup de bloques S3 bloqueados y restaurarlos según sea necesario.

Al definir la configuración de protección para un bloque nuevo o existente, puede habilitar el bloqueo de objetos en los buckets de destino, siempre y cuando los clústeres de origen y de destino ejecuten ONTAP 9.14.1 o una versión posterior, y que el bloqueo de objetos se habilite en el bloque de origen. El modo de bloqueo de objetos y la tenencia de retención de bloqueos del bloque de origen se aplican a los objetos replicados en el bloque de destino. También puede definir un período de retención de bloqueo diferente para el depósito de destino en la sección **Configuración de destino**. Este período de retención también se aplica a cualquier objeto no bloqueado replicado desde el bloque de origen e interfaces S3.

Para obtener información sobre cómo activar el bloqueo de objetos en un depósito, consulte "[Crear un bucket](#)".

CLI

1. Si esta es la primera relación SnapMirror de S3 para esta SVM, compruebe que existen claves de usuario raíz para las SVM de origen y de destino y vuelva a regenerarlas si no:

```
vserver object-store-server user show
```

Compruebe que hay una clave de acceso para el usuario raíz. Si no lo hay, introduzca:

```
vserver object-store-server user regenerate-keys -vserver svm_name -user root
```

No vuelva a generar la clave si ya existe.

2. Cree bloques en las SVM de origen y destino:

```
vserver object-store-server bucket create -vserver svm_name -bucket bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text] [additional_options]
```

3. Añada reglas de acceso a las políticas de bloque predeterminadas tanto en las SVM de origen como de destino:

```
vserver object-store-server bucket policy add-statement -vserver svm_name  
-bucket bucket_name -effect {allow|deny} -action object_store_actions  
-principal user_and_group_names -resource object_store_resources [-sid  
text] [-index integer]
```

```
src_cluster::> vserver object-store-server bucket policy add-  
statement -bucket test-bucket -effect allow -action  
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc  
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -  
-resource test-bucket, test-bucket /*
```

4. Cree una política de SnapMirror de S3 si no tiene una existente y no desea usar la directiva predeterminada:

```
snapmirror policy create -vserver svm_name -policy policy_name -type  
continuous [-rpo integer] [-throttle throttle_type] [-comment text]  
[additional_options]
```

Parámetros:

- `continuous` : El único tipo de política para relaciones SnapMirror de S3 (obligatorio).
- `-rpo` – especifica el tiempo para el objetivo de punto de recuperación, en segundos (opcional).
- `-throttle` – especifica el límite superior de rendimiento/ancho de banda, en kilobytes/segundos (opcional).

Ejemplo

```
src_cluster::> snapmirror policy create -vserver vs0 -type  
continuous -rpo 0 -policy test-policy
```

5. Instale los certificados de servidor de CA en la SVM de administrador:

- a. Instale el certificado de CA que firmó el certificado del servidor *source* S3 en la SVM de administración:

```
security certificate install -type server-ca -vserver admin_svm -cert  
-name src_server_certificate
```

- b. Instale el certificado de CA que firmó el certificado del servidor *destination* S3 en la SVM de administración:

```
security certificate install -type server-ca -vserver admin_svm -cert  
-name dest_server_certificate
```

Si utiliza un certificado firmado por un proveedor de CA externo, solo debe instalar este certificado en la SVM de administrador.

Consulte `security certificate install manual` para más detalles.

6. Cree una relación de SnapMirror de S3:


```
snapmirror create -source-path src_svm_name:/bucket/bucket_name  
-destination-path dest_peer_svm_name:/bucket/bucket_name, ...} [-policy  
policy_name]`
```

Puede usar una política que haya creado o aceptar la predeterminada.

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-  
bucket -destination-path vs1-dest:/vs1/bucket/test-bucket-mirror  
-policy test-policy
```

7. Compruebe que el mirroring está activo:

```
snapmirror show -policy-type continuous -fields status
```




Crear una relación de mirroring para un bloque existente (clúster local)

Puede empezar a proteger bloques de S3 existentes en el mismo clúster en cualquier momento; por ejemplo, si actualizó una configuración de S3 desde una versión anterior a ONTAP 9.10.1. Puede reflejar datos en un bloque de una máquina virtual de almacenamiento diferente o en la misma máquina virtual de almacenamiento que el origen.



Antes de empezar

- Se han completado los requisitos para las versiones de ONTAP, las licencias y la configuración de servidores S3.
- Existe una relación de paridad entre las máquinas virtuales de almacenamiento de origen y de destino.
- Los certificados DE CA se necesitan para las máquinas virtuales de origen y de destino. Puede usar certificados de CA autofirmados o certificados firmados por un proveedor de CA externo.

System Manager

1. Si esta es la primera relación SnapMirror de S3 para este equipo virtual de almacenamiento, compruebe que existen claves de usuario raíz para los equipos virtuales de almacenamiento de origen y de destino, y regenlas si no:
 - a. Haga clic en **almacenamiento > Storage VMs** y, a continuación, seleccione la VM de almacenamiento.
 - b. En la ficha **Configuración**, haga clic en  En el mosaico **S3**.
 - c. En la ficha **usuarios**, compruebe que hay una clave de acceso para el usuario raíz.
 - d. Si no lo hay, haga clic en  Junto a **root**, haga clic en **regenerar clave**.
No vuelva a generar la clave si ya existe
2. Compruebe que el acceso de usuario y grupo es correcto tanto en las máquinas virtuales de almacenamiento de origen como de destino:
 - Haga clic en **almacenamiento > Storage VMs**, haga clic en la VM de almacenamiento, haga clic en **Configuración** y, a continuación, haga clic en  En S3.

Consulte "[Añada usuarios y grupos de S3](#)" si quiere más información.

3. Cree una política de SnapMirror de S3 si no tiene una existente y no desea usar la directiva predeterminada:
 - a. Haga clic en **Protección > Descripción general** y, a continuación, haga clic en **Configuración de directiva local**.
 - b. Haga clic en  Junto a **Directivas de protección**, haga clic en **Agregar**.
 - Escriba el nombre de la política y una descripción.
 - Seleccione el alcance de las políticas, el clúster o la SVM
 - Seleccione **Continuous** para las relaciones de SnapMirror de S3.
 - Introduzca los valores **acelerador** y **objetivo de punto de recuperación**.
4. Compruebe que la política de acceso a bloques del bloque existente sigue cumpliendo con sus necesidades:
 - a. Haga clic en **almacenamiento > Cuchos** y, a continuación, seleccione el cucharón que desea proteger.
 - b. En la ficha **permisos**, haga clic en  **Edición** y, a continuación, haga clic en **Agregar en permisos**.
 - **Principal y efecto**: Seleccione los valores correspondientes a la configuración del grupo de usuarios o acepte los valores predeterminados.
 - **Acciones** - Asegúrese de que se muestran los siguientes valores:

`GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, ListMultipartUploadParts`

- **Recursos**: Utilice los valores predeterminados (*bucketname*, *bucketname/**) u otros valores que necesite.

Consulte "[Gestionar el acceso del usuario a bloques](#)" para obtener más información sobre

estos campos.

5. Proteja un bloque existente con SnapMirror de S3:

- a. Haga clic en **almacenamiento** > **Cuchos** y, a continuación, seleccione la cuchara que desea proteger.
 - b. Haga clic en **proteger** e introduzca los siguientes valores:
 - Destino
 - **OBJETIVO**: Sistema ONTAP
 - **CLUSTER**: Seleccione el cluster local.
 - **STORAGE VM**: Seleccione la misma máquina virtual de almacenamiento o una diferente.
 - **Certificado de CA del SERVIDOR S3**: Copie y pegue el contenido del certificado *source*.
 - Origen
 - **Certificado de CA del SERVIDOR S3**: Copie y pegue el contenido del certificado *Destination*.
6. Marque **Utilice el mismo certificado en el destino** si está utilizando un certificado firmado por un proveedor de CA externo.
7. Si hace clic en **Configuración de destino**, también puede introducir sus propios valores en lugar de los valores predeterminados para el nombre del bloque, la capacidad y el nivel de servicio de rendimiento.
8. Haga clic en **Guardar**. El bloque existente se refleja en un nuevo bloque en la máquina virtual de almacenamiento de destino.

Haga retroceder los cucharones bloqueados

A partir de ONTAP 9.14.1, puede crear un backup de bloques S3 bloqueados y restaurarlos según sea necesario.

Al definir la configuración de protección para un bloque nuevo o existente, puede habilitar el bloqueo de objetos en los buckets de destino, siempre y cuando los clústeres de origen y de destino ejecuten ONTAP 9.14.1 o una versión posterior, y que el bloqueo de objetos se habilite en el bloque de origen. El modo de bloqueo de objetos y la tenencia de retención de bloqueos del bloque de origen se aplican a los objetos replicados en el bloque de destino. También puede definir un período de retención de bloqueo diferente para el depósito de destino en la sección **Configuración de destino**. Este período de retención también se aplica a cualquier objeto no bloqueado replicado desde el bloque de origen e interfaces S3.

Para obtener información sobre cómo activar el bloqueo de objetos en un depósito, consulte "[Crear un bucket](#)".

CLI

1. Si esta es la primera relación SnapMirror de S3 para esta SVM, compruebe que existen claves de usuario raíz para las SVM de origen y de destino y vuelva a regenerarlas si no:

```
vserver object-store-server user show
```

Compruebe que hay una clave de acceso para el usuario raíz. Si no lo hay, introduzca:

```
vserver object-store-server user regenerate-keys -vserver svm_name -user root
```

No vuelva a generar la clave si ya existe.

2. Crear un bucket en la SVM de destino que sea el destino de mirroring:

```
vserver object-store-server bucket create -vserver svm_name -bucket
dest_bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
[additional_options]
```

3. Compruebe que las reglas de acceso a las políticas de bloque predeterminadas sean correctas tanto en las SVM de origen como de destino:

```
vserver object-store-server bucket policy add-statement -vserver svm_name
-bucket bucket_name -effect {allow|deny} -action object_store_actions
-principal user_and_group_names -resource object_store_resources [-sid
text] [-index integer]`
```

Ejemplo

```
clusterA::> vserver object-store-server bucket policy add-statement
-bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. Cree una política de SnapMirror de S3 si no tiene una existente y no desea usar la directiva predeterminada:

```
snapmirror policy create -vserver svm_name -policy policy_name -type
continuous [-rpo _integer] [-throttle throttle_type] [-comment text]
[additional_options]
```

Parámetros:

- `continuous` : El único tipo de política para relaciones SnapMirror de S3 (obligatorio).
- `-rpo` – especifica el tiempo para el objetivo de punto de recuperación, en segundos (opcional).
- `-throttle` – especifica el límite superior de rendimiento/ancho de banda, en kilobytes/segundos (opcional).

Ejemplo

```
clusterA::> snapmirror policy create -vserver vs0 -type
continuous -rpo 0 -policy test-policy
```

5. Instale los certificados de servidor de CA en la SVM de administrador:

- a. Instale el certificado de CA que firmó el certificado del servidor *source* S3 en la SVM de administración:

```
security certificate install -type server-ca -vserver admin_svm -cert
-name src_server_certificate
```

- b. Instale el certificado de CA que firmó el certificado del servidor *destination* S3 en la SVM de administración:

```
security certificate install -type server-ca -vserver admin_svm -cert
```

```
-name dest_server_certificate
```

Si utiliza un certificado firmado por un proveedor de CA externo, solo debe instalar este certificado en la SVM de administrador.

Consulte `security certificate install manual` para más detalles.

6. Cree una relación de SnapMirror de S3:

```
snapmirror create -source-path src_svm_name:/bucket/bucket_name  
-destination-path dest_peer_svm_name:/bucket/bucket_name, ...} [-policy  
policy_name]
```

Puede usar una política que haya creado o aceptar la predeterminada.

Ejemplo

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-  
bucket -destination-path vs1-dest:/bucket/test-bucket-mirror -policy  
test-policy
```

7. Compruebe que el mirroring está activo:

```
snapmirror show -policy-type continuous -fields status
```

Toma de control y sirve datos desde el bloque de destino (clúster local)

Si los datos de un bloque de origen dejan de estar disponibles, puede romper la relación de SnapMirror para hacer que el bloque de destino sea editable y comenzar a servir datos.

Acerca de esta tarea


Cuando se realiza una operación de toma de control, el bloque de origen se convierte en bloque de destino original de solo lectura y se convierte en bloque de destino original de lectura y escritura; de este modo, se invierte la relación de SnapMirror de S3.

Una vez que el bloque de origen deshabilitado se vuelva a poner disponible, S3 SnapMirror vuelve a sincronizar automáticamente el contenido de los dos bloques. No es necesario resincronizar explícitamente la relación, como es necesario para puestas en funcionamiento de SnapMirror para volúmenes estándar.

Si el bloque de destino se encuentra en un clúster remoto, la operación de toma de control se debe iniciar desde el clúster remoto.

System Manager

Conmutación por error desde el bloque no disponible y empiece a servir datos:

1. Haga clic en **Protección > Relaciones** y seleccione **S3 SnapMirror**.
2. Haga clic en , Seleccione **Failover** y, a continuación, haga clic en **failover**.

CLI

1. Inicie una operación de conmutación al nodo de respaldo para el bloque de destino:
`snapmirror failover start -destination-path svm_name:/bucket/bucket_name`
2. Compruebe el estado de la operación de conmutación por error:
`snapmirror show -fields status`

Ejemplo

```
clusterA::> snapmirror failover start -destination-path vs1:/bucket/test-  
bucket-mirror
```

Restaurar un bloque desde la máquina virtual de almacenamiento de destino (clúster local)

Cuando los datos de un depósito de origen se pierden o dañan, puede volver a rellenar los datos restaurando objetos desde un bloque de destino.

Acerca de esta tarea


Puede restaurar el bloque de destino en un bloque existente o en un bloque nuevo. El depósito de destino para la operación de restauración debe ser mayor que el espacio lógico utilizado del cubo de destino.

Si utiliza un bloque existente, debe estar vacío al iniciar una operación de restauración. La restauración no "rollback" de un bloque en el tiempo; más bien, rellena un bloque vacío con su contenido anterior.

La operación de restauración se debe iniciar desde el clúster local.

System Manager

Restaura los datos de backup:

1. Haga clic en **Protección > Relaciones** y, a continuación, seleccione el bloque.
2. Haga clic en  Y, a continuación, seleccione **Restaurar**.
3. En **Fuente**, seleccione **cucharón existente** (predeterminado) o **Nuevo cucharón**.
 - Para restaurar a un **segmento existente** (valor predeterminado), lleve a cabo las siguientes acciones:
 - Seleccione la máquina virtual de almacenamiento y clúster para buscar el bloque existente.
 - Seleccione el bloque existente.
4. Copie y pegue el contenido del certificado de CA del servidor S3 de destino.
 - Para restaurar a un **New Bucket**, introduzca los siguientes valores:
 - El equipo virtual de clúster y almacenamiento para alojar el nuevo bloque.
 - El nombre, la capacidad y el nivel de servicio de rendimiento del bloque nuevo. Consulte "[Los niveles de servicio de almacenamiento](#)" si quiere más información.
 - El contenido del certificado de CA de servidor S3 de destino.
5. En **destino**, copie y pegue el contenido del certificado de CA del servidor S3 de origen.
6. Haga clic en **Protección > Relaciones** para supervisar el progreso de la restauración.

Restaura los cucharones bloqueados

A partir de ONTAP 9.14.1, puede realizar backups de bloques bloqueados y restaurarlos según sea necesario.

Es posible restaurar un bloque de bloqueo de objetos a un bloque nuevo o existente. Puede seleccionar un depósito bloqueado por objeto como destino en las siguientes situaciones:

- **Restaurar a un nuevo cubo:** Cuando se habilita el bloqueo de objetos, un cubo puede restaurarse creando un cubo que también tiene habilitado el bloqueo de objetos. Cuando restaura un bucket bloqueado, se replican el modo de bloqueo de objetos y el periodo de retención del bucket original. También puede definir un período de retención de bloqueo diferente para el nuevo período. Este período de retención se aplica a objetos no bloqueados de otros orígenes.
- **Restaurar a un cubo existente:** Un cubo bloqueado por objeto se puede restaurar a un cubo existente, siempre y cuando el control de versiones y un modo de bloqueo de objetos similar estén habilitados en el cubo existente. Se mantiene la tenencia de retención del cucharón original.
- **Restaurar cubo no bloqueado:** Incluso si el bloqueo de objetos no está habilitado en un cubo, puede restaurarlo en un cubo que tiene el bloqueo de objetos activado y está en el clúster de origen. Al restaurar el bloque, todos los objetos no bloqueados se bloquean, y se aplican el modo de retención y la tenencia del bloque de destino.

CLI

1. Si va a restaurar objetos en un bloque nuevo, cree el bloque nuevo. Para obtener más información, consulte "[Crear una relación de backup para un bloque nuevo \(destino cloud\)](#)".
2. Inicie una operación de restauración para el bloque de destino:

```
snapmirror restore -source-path svm_name:/bucket/bucket_name -destination-path svm_name:/bucket/bucket_name
```

Ejemplo

```
clusterA::> snapmirror restore -source-path vs0:/bucket/test-bucket  
-destination-path vs1:/bucket/test-bucket-mirror
```

Protección de backup con destinos cloud

Requisitos para las relaciones objetivo del cloud

Asegúrese de que sus entornos de origen y objetivo cumplen los requisitos de la protección de backup de SnapMirror S3 en los destinos cloud.

Debe tener credenciales de cuenta válidas con el proveedor de almacenes de objetos para acceder al bloque de datos.

Las interfaces de red entre clústeres y un espacio IP se deben configurar en el clúster antes de que el clúster se pueda conectar a un almacén de objetos en cloud. Debe crear interfaces de red de clúster en cada nodo para transferir datos sin problemas desde el almacenamiento local al almacén de objetos en cloud.

Para los destinos StorageGRID, debe conocer la siguiente información:

- Nombre del servidor, expresado como un nombre de dominio completo (FQDN) o una dirección IP
- nombre de bloque; el bloque debe existir antes
- clave de acceso
- clave secreta

Además, el certificado de CA utilizado para firmar el certificado de servidor StorageGRID debe instalarse en la máquina virtual de almacenamiento de administración del clúster ONTAP S3 mediante el `security certificate install` command. Para obtener más información, consulte ["Instalar un certificado de CA"](#) Si utiliza StorageGRID.

Para los destinos AWS S3, debe conocer la siguiente información:

- Nombre del servidor, expresado como un nombre de dominio completo (FQDN) o una dirección IP
- nombre de bloque; el bloque debe existir antes
- clave de acceso
- clave secreta

El servidor DNS de la máquina virtual de almacenamiento de administración del clúster ONTAP debe poder resolver FQDN (si se utiliza) a direcciones IP.


Crear una relación de backup para un bloque nuevo (destino cloud)

Cuando crea nuevos buckets de S3, puede realizar backups inmediatamente en un bloque de destino de SnapMirror S3 en un proveedor de almacenamiento de objetos, que puede ser un sistema StorageGRID o una implementación de Amazon S3.


Antes de empezar

- Tiene credenciales de cuenta válidas e información de configuración para el proveedor de almacenes de objetos.
- Las interfaces de red entre clústeres y un espacio IP se han configurado en el sistema de origen.
- • La configuración de DNS para la máquina virtual de almacenamiento de origen debe ser capaz de resolver el FQDN del destino.

System Manager

1. Edite la máquina virtual de almacenamiento para añadir usuarios y añadir usuarios a los grupos:
 - a. Haga clic en **almacenamiento > Storage VMs**, haga clic en la VM de almacenamiento, haga clic en **Configuración** y, a continuación, haga clic en  En **S3**.

Consulte "[Añada usuarios y grupos de S3](#)" si quiere más información.

2. Añada un almacén de objetos cloud en el sistema de origen:
 - a. Haga clic en **Protección > Descripción general** y seleccione **almacenamiento de objetos en la nube**.
 - b. Haga clic en **Agregar** y, a continuación, seleccione **Amazon S3** o **StorageGRID**.
 - c. Introduzca los siguientes valores:
 - Nombre de almacén de objetos en cloud
 - Estilo de URL (ruta o host virtual)
 - Máquina virtual de almacenamiento (habilitada para S3)
 - Nombre del servidor de almacén de objetos (FQDN)
 - Certificado de almacén de objetos
 - Clave de acceso
 - Clave secreta
 - Nombre del contenedor (cubo)
3. Cree una política de SnapMirror de S3 si no tiene una existente y no desea usar la directiva predeterminada:
 - a. Haga clic en **Protección > Descripción general** y, a continuación, en **Configuración de directivas locales**.
 - b. Haga clic en  Junto a **Directivas de protección**, haga clic en **Agregar**.
 - Escriba el nombre de la política y una descripción.
 - Seleccione el alcance de las políticas, el clúster o la SVM
 - Seleccione **Continuous** para las relaciones de SnapMirror de S3.
 - Introduzca los valores **acelerador** y **objetivo de punto de recuperación**.
4. Crear un bloque con la protección SnapMirror:
 - a. Haga clic en **almacenamiento > Cuchos** y, a continuación, haga clic en **Agregar**.
 - b. Introduzca un nombre, seleccione el equipo virtual de almacenamiento, introduzca un tamaño y, a continuación, haga clic en **más opciones**.
 - c. En **permisos**, haga clic en **Agregar**. Verificar permisos es opcional pero se recomienda.
 - **Principal y efecto**: Seleccione los valores correspondientes a la configuración de su grupo de usuarios o acepte los valores predeterminados.
 - **Acciones** - Asegúrese de que se muestran los siguientes valores:

```
`GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts`
```

- **Recursos:** Utilice los valores predeterminados `_(bucketname, bucketname/*)` u otros valores que necesite.

Consulte "[Gestionar el acceso del usuario a bloques](#)" para obtener más información sobre estos campos.

- d. En **Protección**, marque **Activar SnapMirror (ONTAP o nube)**, seleccione **almacenamiento en nube** y, a continuación, seleccione **almacén de objetos en nube**.

Al hacer clic en **Guardar**, se crea un nuevo bloque en el equipo virtual de almacenamiento de origen y se realiza una copia de seguridad en el almacén de objetos en la nube.

CLI

1. Si esta es la primera relación SnapMirror de S3 para esta SVM, compruebe que existen claves de usuario raíz para las SVM de origen y de destino y vuelva a regenerarlas si no:

```
vserver object-store-server user show
```

Confirmar que existe una clave de acceso para el usuario raíz. Si no lo hay, introduzca:

```
vserver object-store-server user regenerate-keys -vserver svm_name -user root
```

No vuelva a generar la clave si ya existe.

2. Crear un bloque en la SVM de origen:

```
vserver object-store-server bucket create -vserver svm_name -bucket bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text] [additional_options]
```

3. Agregar reglas de acceso a la directiva de bloque predeterminada:

```
vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {allow|deny} -action object_store_actions -principal user_and_group_names -resource object_store_resources [-sid text] [-index integer]
```

Ejemplo

```
clusterA::> vserver object-store-server bucket policy add-statement -bucket test-bucket -effect allow -action GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts -principal -resource test-bucket, test-bucket /*
```

4. Cree una política de SnapMirror de S3 si no tiene una existente y no desea usar la directiva predeterminada:

```
snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]
```

Parámetros:

- * `type continuous` : El único tipo de política para relaciones SnapMirror de S3 (obligatorio).
- * `-rpo` – especifica el tiempo para el objetivo de punto de recuperación, en segundos (opcional).
- * `-throttle` – especifica el límite superior de rendimiento/ancho de banda, en kilobytes/segundos (opcional).

Ejemplo

```
clusterA::> snapmirror policy create -vserver vs0 -type continuous  
-rpo 0 -policy test-policy
```

5. Si el destino es un sistema StorageGRID, instale el certificado de servidor de CA StorageGRID en la SVM de administrador del clúster de origen:

```
security certificate install -type server-ca -vserver src_admin_svm -cert  
-name storage_grid_server_certificate
```

Consulte `security certificate install manual` para más detalles.

6. Defina el almacén de objetos de destino de SnapMirror S3:

```
snapmirror object-store config create -vserver svm_name -object-store-name  
target_store_name -usage data -provider-type {AWS_S3|SGWS} -server  
target_FQDN -container-name remote_bucket_name -is-ssl-enabled true -port  
port_number -access-key target_access_key -secret-password  
target_secret_key
```

Parámetros:

- * `-object-store-name` : El nombre del destino de almacén de objetos en el sistema ONTAP local.
- * `-usage` – uso `data` para este flujo de trabajo.
- * `-provider-type` – `AWS_S3` y.. `SGWS` Se admiten los destinos de (StorageGRID).
- * `-server` – La dirección IP o FQDN del servidor de destino.
- * `-is-ssl-enabled` –La activación de SSL es opcional pero se recomienda.

Consulte `snapmirror object-store config create manual` para más detalles.

Ejemplo

```
src_cluster::> snapmirror object-store config create -vserver vs0  
-object-store-name sgws-store -usage data -provider-type SGWS  
-server sgws.example.com -container-name target-test-bucket -is-ssl  
-enabled true -port 443 -access-key abc123 -secret-password xyz890
```

7. Cree una relación de SnapMirror de S3:

```
snapmirror create -source-path svm_name:/bucket/bucket_name -destination  
-path object_store_name:/objstore -policy policy_name
```

Parámetros:

- * `-destination-path` - el nombre del almacén de objetos que creó en el paso anterior y el valor fijo `objstore`.

Puede usar una política que haya creado o aceptar la predeterminada.

Ejemplo

```
src_cluster::> snapmirror create -source-path vs0:/bucket/test-  
bucket -destination-path sgws-store:/objstore -policy test-policy
```

8. Compruebe que el mirroring está activo:

```
snapmirror show -policy-type continuous -fields status
```


Crear una relación de backup para un bloque existente (destino cloud)

Puede empezar a realizar en cualquier momento backups de bloques de S3 existentes; por ejemplo, si actualizó una configuración de S3 desde una versión anterior a ONTAP 9.10.1.



Antes de empezar

- Tiene credenciales de cuenta válidas e información de configuración para el proveedor de almacenes de objetos.
- Las interfaces de red entre clústeres y un espacio IP se han configurado en el sistema de origen.
- La configuración de DNS para el equipo virtual de almacenamiento de origen debe poder resolver el FQDN del destino.

System Manager

1. Compruebe que los usuarios y grupos están definidos correctamente:
Haga clic en **almacenamiento > Storage VMs**, haga clic en la VM de almacenamiento, haga clic en **Configuración** y, a continuación, haga clic en  En S3.

Consulte "[Añada usuarios y grupos de S3](#)" si quiere más información.

2. Cree una política de SnapMirror de S3 si no tiene una existente y no desea usar la directiva predeterminada:
 - a. Haga clic en **Protección > Descripción general** y, a continuación, en **Configuración de directivas locales**.
 - b. Haga clic en  Junto a **Directivas de protección**, haga clic en **Agregar**.
 - c. Escriba el nombre de la política y una descripción.
 - d. Seleccione el alcance de las políticas, el clúster o la SVM
 - e. Seleccione **Continuuous** para las relaciones de SnapMirror de S3.
 - f. Introduzca los valores de los objetivos **acelerador** y **punto de recuperación**.
3. Añada un almacén de objetos cloud en el sistema de origen:
 - a. Haga clic en **Protección > Descripción general** y seleccione **Tienda de objetos en la nube**.
 - b. Haga clic en **Agregar** y, a continuación, seleccione **Amazon S3** o **otros** para StorageGRID Webscale.
 - c. Introduzca los siguientes valores:
 - Nombre de almacén de objetos en cloud
 - Estilo de URL (ruta o host virtual)
 - Máquina virtual de almacenamiento (habilitada para S3)
 - Nombre del servidor de almacén de objetos (FQDN)
 - Certificado de almacén de objetos
 - Clave de acceso
 - Clave secreta
 - Nombre del contenedor (cubo)
4. Compruebe que la política de acceso a bloques del bloque existente sigue cumpliéndose con sus necesidades:
 - a. Haga clic en **almacenamiento > Cuchos** y, a continuación, seleccione la cuchara que desea proteger.
 - b. En la ficha **permisos**, haga clic en  **Edición** y, a continuación, haga clic en **Agregar** en **permisos**.
 - **Principal y efecto**: Seleccione los valores correspondientes a la configuración de su grupo de usuarios o acepte los valores predeterminados.
 - **Acciones** - Asegúrese de que se muestran los siguientes valores:
`GetObject`, `PutObject`, `DeleteObject`, `ListBucket`, `GetBucketAcl`, `GetObjectAcl`, `ListBucketMultipartUploads`, `ListMultipartUploadParts`
 - **Recursos**: Utilice los valores predeterminados (`bucketname`, `bucketname/*`) u otros valores que necesite.

Consulte ["Gestionar el acceso del usuario a bloques"](#) para obtener más información sobre estos campos.

5. Realice un backup del bloque con S3 SnapMirror:

- Haga clic en **almacenamiento** > **Cuchos** y, a continuación, seleccione la cuchara de la que desea realizar la copia de seguridad.
- Haga clic en **proteger**, seleccione **almacenamiento en nube** en **objetivo** y, a continuación, seleccione **almacén de objetos en nube**.

Al hacer clic en **Guardar**, se realiza una copia de seguridad del bloque existente en el almacén de objetos en la nube.

CLI

1. Compruebe que las reglas de acceso de la política de bloque predeterminada son correctas:

```
vserver object-store-server bucket policy add-statement -vserver svm_name  
-bucket bucket_name -effect {allow|deny} -action object_store_actions  
-principal user_and_group_names -resource object_store_resources [-sid  
text] [-index integer]
```

Ejemplo

```
clusterA::> vserver object-store-server bucket policy add-statement  
-bucket test-bucket -effect allow -action  
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,  
ListBucketMultipartUploads,ListMultipartUploadParts -principal -  
-resource test-bucket, test-bucket /*
```

2. Cree una política de SnapMirror de S3 si no tiene una existente y no desea usar la directiva predeterminada:

```
snapmirror policy create -vserver svm_name -policy policy_name -type  
continuous [-rpo integer] [-throttle throttle_type] [-comment text]  
[additional_options]
```

Parámetros:

- * `type continuous` : El único tipo de política para relaciones SnapMirror de S3 (obligatorio).
- * `-rpo` – especifica el tiempo para el objetivo de punto de recuperación, en segundos (opcional).
- * `-throttle` – especifica el límite superior de rendimiento/ancho de banda, en kilobytes/segundos (opcional).

Ejemplo

```
clusterA::> snapmirror policy create -vserver vs0 -type continuous  
-rpo 0 -policy test-policy
```

3. Si el destino es un sistema StorageGRID, instale el certificado de CA StorageGRID en la SVM de administrador del clúster de origen:

```
security certificate install -type server-ca -vserver src_admin_svm -cert  
-name storage_grid_server_certificate
```

Consulte `security certificate install` manual para más detalles.

4. Defina el almacén de objetos de destino de SnapMirror S3:

```
snapmirror object-store config create -vserver svm_name -object-store-name  
target_store_name -usage data -provider-type {AWS_S3|SGWS} -server  
target_FQDN -container-name remote_bucket_name -is-ssl-enabled true -port  
port_number -access-key target_access_key -secret-password  
target_secret_key
```

Parámetros:

- * -object-store-name : El nombre del destino de almacén de objetos en el sistema ONTAP local.
- * -usage – uso data para este flujo de trabajo.
- * -provider-type – AWS_S3 y.. SGWS Se admiten los destinos de (StorageGRID).
- * -server – La dirección IP o FQDN del servidor de destino.
- * -is-ssl-enabled –La activación de SSL es opcional pero se recomienda.

Consulte `snapmirror object-store config create manual` para más detalles.

Ejemplo

```
src_cluster::> snapmirror object-store config create -vserver vs0  
-object-store-name sgws-store -usage data -provider-type SGWS  
-server sgws.example.com -container-name target-test-bucket -is-ssl  
-enabled true -port 443 -access-key abc123 -secret-password xyz890
```

5. Cree una relación de SnapMirror de S3:

```
snapmirror create -source-path svm_name:/bucket/bucket_name -destination  
-path object_store_name:/objstore -policy policy_name
```

Parámetros:

- * -destination-path - el nombre del almacén de objetos que creó en el paso anterior y el valor fijo objstore.

Puede usar una política que haya creado o aceptar la predeterminada.

```
src_cluster::> snapmirror create -source-path vs0:/bucket/buck-evp  
-destination-path sgws-store:/objstore -policy test-policy
```

6. Compruebe que el mirroring está activo:

```
snapmirror show -policy-type continuous -fields status
```

Restaurar un bloque a partir de un destino de cloud

Cuando los datos de un bloque de origen se pierden o dañan, puede volver a rellenar los datos mediante la restauración a partir de un bloque de destino.

Acerca de esta tarea

Puede restaurar el bloque de destino en un bloque existente o en un bloque nuevo. El bloque de destino para la operación de restauración debe ser mayor que el espacio lógico usado del cucharón de destino.

Si utiliza un bloque existente, debe estar vacío al iniciar una operación de restauración. La restauración no "rollback" de un bloque en el tiempo; más bien, rellena un bloque vacío con su contenido anterior.

System Manager

Restaurar los datos de backup:

1. Haga clic en **Protección > Relaciones** y seleccione **S3 SnapMirror**.
2. Haga clic en **Y**, a continuación, seleccione **Restaurar**.
3. En **Fuente**, seleccione **cucharón existente** (predeterminado) o **Nuevo cucharón**.
 - Para restaurar a un **segmento existente** (valor predeterminado), lleve a cabo las siguientes acciones:
 - Seleccione la máquina virtual de almacenamiento y clúster para buscar el bloque existente.
 - Seleccione el bloque existente.
 - Copie y pegue el contenido del certificado de CA del servidor *destination* S3.
 - Para restaurar a un **New Bucket**, introduzca los siguientes valores:
 - El equipo virtual de clúster y almacenamiento para alojar el nuevo bloque.
 - El nombre, la capacidad y el nivel de servicio de rendimiento del nuevo cucharón. Consulte ["Los niveles de servicio de almacenamiento"](#) si quiere más información.
 - El contenido del certificado de CA de servidor S3 de destino.
4. En **destino**, copie y pegue el contenido del certificado de CA del servidor *source* S3.
5. Haga clic en **Protección > Relaciones** para supervisar el progreso de la restauración.

Procedimiento de la CLI

1. Crear el nuevo bloque de destino para la restauración. Para obtener más información, consulte ["Crear una relación de backup para un bloque \(destino de cloud\)"](#).
2. Inicie una operación de restauración para el bloque de destino:

```
snapmirror restore -source-path object_store_name:/objstore -destination  
-path svm_name:/bucket/bucket_name
```

Ejemplo

En el ejemplo siguiente se restaura un bloque de destino a un bloque existente.


```
clusterA::> snapmirror restore -source-path sgws.store:/objstore  
-destination-path vs0:/bucket/test-bucket
```

Modificar una política de mirroring

Es posible que desee modificar una política de reflejo de S3; por ejemplo, si desea ajustar los valores de RPO y acelerador.

System Manager

Si desea ajustar estos valores, puede editar una política de protección existente.

1. Haga clic en **Protección > Relaciones** y, a continuación, seleccione la política de protección para la relación que desea modificar.
2. Haga clic en  Junto al nombre de la directiva y, a continuación, haga clic en **Editar**.

CLI

Modifique una política de SnapMirror de S3:

```
snapmirror policy modify -vserver svm_name -policy policy_name [-rpo integer]
[-throttle throttle_type] [-comment text]
```

Parámetros:

- **-rpo** – especifica el tiempo para el objetivo de punto de recuperación, en segundos.
- **-throttle** – especifica el límite superior de capacidad de procesamiento/ancho de banda, en kilobytes/segundos.

```
clusterA::> snapmirror policy modify -vserver vs0 -policy test-policy
-rpo 60
```

Auditar eventos S3

Auditar eventos S3

A partir de ONTAP 9.10.1, puede auditar eventos de datos y gestión en entornos ONTAP S3. La funcionalidad de auditoría de S3 es similar a las funcionalidades de auditoría NAS existentes, y la auditoría de S3 y NAS puede coexistir en un clúster.

Cuando se crea y se habilita una configuración de auditoría de S3 en una SVM, los eventos de S3 se registran en un archivo de registro. El puede especificar los siguientes eventos que se registrarán:

- Eventos de acceso a objetos (datos)

GetObject, PutObject y DeleteObject

- Eventos de gestión

Cubo de puta y eliminarbloque

El formato del registro es notación de objetos JavaScript (JSON).

El límite combinado para las configuraciones de auditoría de S3 y NFS es de 50 SVM por clúster.

Se requiere el siguiente paquete de licencia:

- Paquete principal, para el protocolo ONTAP S3 y el almacenamiento

Para obtener más información, consulte ["Cómo funciona el proceso de auditoría de ONTAP"](#).

Auditoría garantizada

De forma predeterminada, se garantiza la auditoría de S3 y NAS. ONTAP garantiza que se registren todos los eventos de acceso a bloques que pueden someterse a auditorías, incluso si un nodo no está disponible. No se puede completar una operación de bloque solicitada hasta que el registro de auditoría de esa operación se guarde en el volumen provisional en un almacenamiento persistente. Si los registros de auditoría no se pueden guardar en los archivos de almacenamiento provisional, ya sea por falta de espacio o por otros problemas, se deniegan las operaciones de cliente.

Requisitos de espacio para la auditoría

En el sistema de auditoría de ONTAP, los registros de auditoría se almacenan inicialmente en archivos binarios de almacenamiento provisional en nodos individuales. Periódicamente, se consolidan y convierten en registros de eventos legibles por el usuario, que se almacenan en el directorio del registro de eventos de auditoría de la SVM.

Los archivos de almacenamiento provisional se almacenan en un volumen de almacenamiento provisional dedicado, que ONTAP crea cuando se crea la configuración de auditoría. Hay un volumen de almacenamiento provisional por agregado.

Debe planificar el espacio disponible suficiente en la configuración de auditoría:

- Para los volúmenes de almacenamiento provisional en agregados que contienen bloques auditados.
- Para el volumen que contiene el directorio en el que se almacenan los registros de eventos convertidos.

Es posible controlar el número de registros de eventos y, por lo tanto, el espacio disponible en el volumen, mediante uno de los dos métodos al crear la configuración de auditoría de S3:

- Un límite numérico; el `-rotate-limit` parámetro controla la cantidad mínima de archivos de auditoría que se deben conservar.
- Un límite de tiempo; el `-retention-duration` parámetro controla el período máximo que se pueden conservar los archivos.

En ambos parámetros, una vez excedido el valor configurado, se pueden eliminar los archivos de auditoría más antiguos para dejar espacio para otros más nuevos. Para ambos parámetros, el valor es 0, lo que indica que se deben mantener todos los archivos. Para garantizar que haya espacio suficiente, se recomienda, por tanto, establecer uno de los parámetros en un valor distinto de cero.

Debido a la auditoría garantizada, si el espacio disponible para los datos de auditoría se agota antes del límite de rotación, no se pueden crear datos de auditoría más nuevos, lo que provoca errores en el acceso de los clientes a los datos. Por lo tanto, la elección de este valor y del espacio asignado a la auditoría se debe elegir cuidadosamente, y debe responder a las advertencias sobre el espacio disponible del sistema de auditoría.

Para obtener más información, consulte ["Conceptos básicos de auditoría"](#).

Planifique una configuración de auditoría de S3

Debe especificar una serie de parámetros para la configuración de auditoría de S3 o aceptar los valores predeterminados. En particular, debe considerar qué parámetros de rotación de log ayudarán a garantizar un espacio libre adecuado.

Consulte **vserver object-store-server audit create** man page para detalles de la sintaxis.

Parámetros generales

Hay dos parámetros necesarios que debe especificar al crear la configuración de auditoría. También puede especificar tres parámetros opcionales.

| Tipo de información | Opción | Obligatorio |
|--|---|-------------|
| <i>SVM name</i> Nombre de la SVM en la que se creará la configuración de auditoría. La SVM ya debe existir y estar habilitada para S3. | <code>-verserver svm_name</code> | Sí |
| <i>Ruta de destino del registro</i> Especifica dónde se almacenan los registros de auditoría convertidos. La ruta ya debe existir en la SVM. La ruta puede tener hasta 864 caracteres y debe tener permisos de lectura y escritura. Si la ruta no es válida, el comando de configuración de auditoría falla. | <code>-destination text</code> | Sí |
| <i>Categorías de eventos para auditar</i> Se pueden auditar las siguientes categorías de eventos: <ul style="list-style-type: none">• sql server Eventos GetObject, PutObject y DeleteObject• gestión Eventos PutBucket y DeleteBucket El valor predeterminado es auditar únicamente los eventos de datos. | <code>-events {data management}, ...</code> | No |

Es posible introducir uno de los siguientes parámetros para controlar la cantidad de archivos de registro de auditoría. Si no se introduce ningún valor, se conservan todos los archivos de registro.

| Tipo de información | Opción | Obligatorio |
|---------------------|--------|-------------|
|---------------------|--------|-------------|

| | | |
|---|--|-----------|
| <p><i>Límite de rotación de los archivos de registro</i></p> <p>Determina cuántos archivos de registro de auditoría se retendrán antes de rotar el archivo de registro más antiguo. Por ejemplo, si introduce un valor de 5, se conservan los cinco últimos archivos de registro.</p> <p>El valor 0 indica que se conservan todos los archivos de registro. El valor predeterminado es 0.</p> | <p><code>-rotate-limit integer</code></p> | <p>No</p> |
| <p><i>Límite de duración de los archivos de registro</i></p> <p>Determina cuánto tiempo se puede retener un archivo de registro antes de eliminarlo. Por ejemplo, si introduce un valor de 5d0h0m, se eliminarán los registros de más de 5 días de antigüedad.</p> <p>El valor 0 indica que se conservan todos los archivos de registro. El valor predeterminado es 0.</p> | <p><code>-retention duration integer_time</code></p> | <p>No</p> |

Parámetros para la rotación del registro de auditoría

Puede rotar los registros de auditoría en función del tamaño o la programación. El valor predeterminado es girar los registros de auditoría en función del tamaño.

Rotar registros según el tamaño del registro

Si desea utilizar el método de rotación de registro predeterminado y el tamaño de registro predeterminado, no necesita configurar ningún parámetro específico para la rotación de registros. El tamaño predeterminado del registro es 100 MB.

Si no desea utilizar el tamaño predeterminado del registro, puede configurar el `-rotate-size` parámetro para especificar un tamaño de registro personalizado.

Si desea restablecer la rotación basándose únicamente en un tamaño de registro, utilice el siguiente comando para anular la definición del `-rotate-schedule-minute` parámetro:

```
vserver audit modify -vserver svm_name -destination / -rotate-schedule-minute -
```

Rotar registros según un programa

Si opta por rotar los registros de auditoría según una programación, puede programar la rotación del registro utilizando los parámetros de rotación basados en tiempo en cualquier combinación.

- Si utiliza rotación basada en tiempo, el `-rotate-schedule-minute` el parámetro es obligatorio.
- Todos los demás parámetros de rotación basados en el tiempo son opcionales.
 - `-rotate-schedule-month`
 - `-rotate-schedule-dayofweek`
 - `-rotate-schedule-day`
 - `-rotate-schedule-hour`

- El programa de rotación se calcula utilizando todos los valores relacionados con el tiempo.
Por ejemplo, si especifica solo el `-rotate-schedule-minute` parámetro, los archivos de registro de auditoría se rotan en función de los minutos especificados en todos los días de la semana, durante todas las horas en todos los meses del año.
- Si especifica solo uno o dos parámetros de rotación basados en la hora (por ejemplo, `-rotate-schedule-month` y `-rotate-schedule-minutes`), los archivos de registro se rotan en función de los valores de minutos que haya especificado en todos los días de la semana, durante todas las horas, pero sólo durante los meses especificados.

Por ejemplo, puede especificar que el registro de auditoría se va a rotar durante los meses de enero, marzo y agosto todos los lunes, miércoles y sábados a las 10:30 a.m.

- Si especifica valores para ambos `-rotate-schedule-dayofweek` y `-rotate-schedule-day`, se consideran independientes.

Por ejemplo, si especifica `-rotate-schedule-dayofweek` Como viernes y `-rotate-schedule-day` Como 13, los registros de auditoría se girarían cada viernes y el día 13 del mes especificado, no sólo cada viernes 13.

- Si desea restablecer la rotación únicamente según una programación, utilice el siguiente comando para anular la definición del `-rotate-size` parameter:

```
vserver audit modify -vserver svm_name -destination / -rotate-size -
```

Rotar registros según el tamaño del registro y el programa

Puede optar por girar los archivos de registro según el tamaño del registro y una programación estableciendo tanto el parámetro `-rotate-size` como los parámetros de rotación basados en tiempo en cualquier combinación. Por ejemplo: Si `-rotate-size` Se establece en 10 MB y `-rotate-schedule-minute` Se establece en 15, los archivos de registro giran cuando el tamaño del archivo de registro alcanza 10 MB o en el 15 minuto de cada hora (el evento que ocurra primero).

Cree y habilite una configuración de auditoría de S3

Para implementar la auditoría de S3, primero se debe crear una configuración de auditoría del almacén de objetos persistente en una SVM habilitada para S3 y, luego, habilitar la configuración.

Lo que necesitará

- Una SVM habilitada para S3.
- Espacio suficiente para organizar temporalmente volúmenes en el agregado.

Acerca de esta tarea

Se requiere una configuración de auditoría para cada SVM que contenga bloques de S3 que se desee auditar. Puede habilitar la auditoría de S3 en servidores S3 nuevos o existentes. Las configuraciones de auditoría persisten en un entorno S3 hasta que se elimina mediante el comando **`vserver object-store-Server audit delete`**.

La configuración de auditoría de S3 se aplica a todos los bloques de la SVM que seleccione para auditoría. Una SVM habilitada para auditoría puede contener bloques auditados y no auditados.

Se recomienda configurar la auditoría de S3 para la rotación automática del registro, determinada por el

tamaño del registro o una programación. Si no configura la rotación automática del registro, todos los archivos de registro se conservan de forma predeterminada. También puede rotar los archivos de registro S3 manualmente mediante el comando **VServer objeto-almacén-auditoría rotate-log**.

Si la SVM es un origen de recuperación ante desastres de SVM, la ruta de destino no puede estar en el volumen raíz.

Procedimiento

- 1. Cree la configuración de auditoría para rotar los registros de auditoría según el tamaño del registro o un programa.

| Si desea rotar registros de auditoría en... | Introduzca... |
|---|---|
| Tamaño del registro | <pre>vserver object-store-server audit create -vserver svm_name -destination path [[-events] {data management}, ...] [[-rotate-limit integer] [-retention-duration [integer_d] [_integer_h][_integer_m][_integers]]] [-rotate-size {integer[KB MB GB TB PB]}]</pre> |
| Un programa | <pre>vserver object-store-server audit create -vserver svm_name -destination path [[-events] {data management}, ...] [[-rotate-limit integer] [-retention-duration [integerd][integerh] [integerm][_integers]]] [-rotate-schedule-month chron_month] [-rotate-schedule-dayofweek chron_dayofweek] [-rotate-schedule-day chron_dayofmonth] [-rotate-schedule-hour chron_hour] -rotate-schedule-minute chron_minute</pre> <p>La <code>-rotate-schedule-minute</code> el parámetro es necesario si se configura la rotación del registro de auditoría basado en tiempo.</p> |

- 2. Habilitar auditoría de S3:

```
vserver object-store-server audit enable -vserver svm_name
```

Ejemplos

En el siguiente ejemplo, se crea una configuración de auditoría que audita todos los eventos de S3 (los valores predeterminados) mediante la rotación basada en tamaño. Los registros se almacenan en el directorio `/audit_log`. El límite de tamaño del archivo de registro es de 200 MB. Los registros se rotan cuando alcanzan los 200 MB de tamaño.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -rotate -size 200MB
```

En el siguiente ejemplo, se crea una configuración de auditoría que audita todos los eventos de S3 (los valores predeterminados) mediante la rotación basada en tamaño. El límite de tamaño del archivo de registro es 100 MB (el valor predeterminado) y los registros se conservan durante 5 días antes de eliminarse.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -retention
```

```
-duration 5d0h0m
```

El siguiente ejemplo crea una configuración de auditoría que audita los eventos de gestión de S3 y eventos de configuración de políticas de acceso central mediante rotación basada en el tiempo. Los registros de auditoría se rotan mensualmente, a las 12:30 p.m. en todos los días de la semana. El límite de rotación del registro es 5.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -events  
management -rotate-schedule-month all -rotate-schedule-dayofweek all -rotate  
-schedule-hour 12 -rotate-schedule-minute 30 -rotate-limit 5
```

Seleccione bloques para auditoría de S3

Debe especificar qué bloques se van a auditar en una SVM habilitada para auditoría.

Lo que necesitará

- Una SVM habilitada para la auditoría de S3.

Acerca de esta tarea

Las configuraciones de auditoría de S3 se habilitan por SVM, pero debe seleccionar los bloques en SVM que estén habilitadas para auditoría. Si añade bloques a la SVM y desea que se auditen los nuevos bloques, debe seleccionarlos con este procedimiento. También puede tener bloques no auditados en una SVM habilitada para la auditoría de S3.

Las configuraciones de auditoría persisten en los bloques hasta que se eliminan por el `vserver object-store-server audit object-select delete` comando.

Procedimiento

Seleccione un bloque para la auditoría de S3:

```
vserver object-store-server audit event-selector create -vserver svm_name -bucket  
bucket_name [[-access] {read-only|write-only|all}] [[-permission] {allow-  
only|deny-only|all}]
```

- `-access` - especifica el tipo de acceso a eventos que se va a auditar: `read-only`, `write-only` o `all` (el valor predeterminado es `all`).
- `-permission` - especifica el tipo de permiso de evento que se va a auditar: `allow-only`, `deny-only` o `all` (el valor predeterminado es `all`).

Ejemplo

En el siguiente ejemplo se crea una configuración de auditoría de bloques que solo registra los eventos permitidos con acceso de solo lectura:

```
cluster1::> vserver object-store-server audit event-selector create -vserver vs1  
-bucket test-bucket -access read-only -permission allow-only
```

Modifique una configuración de auditoría de S3

Puede modificar los parámetros de auditoría de bloques individuales o la configuración de auditoría de todos los bloques seleccionados para la auditoría en la SVM.

| Si desea modificar la configuración de auditoría para... | Introduzca... |
|--|---|
| Cucharones individuales | <code>vserver object-store-server audit event-selector modify -vserver svm_name [-bucket bucket_name] [parameters to modify]</code> |
| Todos los bloques del SVM | <code>vserver object-store-server audit modify -vserver svm_name [parameters to modify]</code> |

Ejemplos

En el siguiente ejemplo se modifica una configuración de auditoría de bloque individual para auditar únicamente los eventos de acceso de sólo escritura:

```
cluster1::> vserver object-store-server audit event-selector modify
-vserver vs1 -bucket test-bucket -access write-only
```

En el siguiente ejemplo se modifica la configuración de auditoría de todos los bloques de la SVM para cambiar el límite de tamaño del registro a 10MB y para retener 3 archivos de registro antes de rotar.

```
cluster1::> vserver object-store-server audit modify -vserver vs1 -rotate
-size 10MB -rotate-limit 3
```

Muestra configuraciones de auditoría de S3

Después de completar la configuración de auditoría, puede comprobar que la auditoría está configurada correctamente y que está activada. También puede mostrar información sobre todas las configuraciones de auditoría del almacén de objetos en el clúster.

Acerca de esta tarea

Puede mostrar información sobre las configuraciones de auditoría de bloques y SVM.

- Cubos: Utilice la `vserver object-store-server audit event-selector show` comando

Sin parámetros, el comando muestra la siguiente información sobre los bloques de todas las SVM del clúster con configuraciones de auditoría del almacén de objetos:

- Nombre de SVM
- Nombre del bloque
- Valores de acceso y permisos

- SVM: Utilice `vserver object-store-server audit show` comando

Sin parámetros, el comando muestra la siguiente información sobre todas las SVM del clúster con configuraciones de auditoría del almacén de objetos:

- Nombre de SVM

- Estado de auditoría
- Directorio de destino

Puede especificar el `-fields` parámetro para especificar la información de configuración de auditoría que se va a mostrar.

Procedimiento

Mostrar información acerca de las configuraciones de auditoría de S3:

| Si desea modificar la configuración para... | Introduzca... |
|---|---|
| Cucharones | <code>vserver object-store-server audit event-selector show [-vserver <i>svm_name</i>] [<i>parameters</i>]</code> |
| SVM | <code>vserver object-store-server audit show [-vserver <i>svm_name</i>] [<i>parameters</i>]</code> |

Ejemplos

El siguiente ejemplo muestra información para un solo bloque:

```
cluster1::> vserver object-store-server audit event-selector show -vserver
vs1 -bucket test-bucket
```

| Vserver | Bucket | Access | Permission |
|---------|---------|-----------|------------|
| ----- | ----- | ----- | ----- |
| vs1 | bucket1 | read-only | allow-only |

El siguiente ejemplo muestra información para todos los bloques de una SVM:

```
cluster1::> vserver object-store-server audit event-selector show -vserver
vs1
```

| | |
|------------|--------------|
| Vserver | :vs1 |
| Bucket | :test-bucket |
| Access | :all |
| Permission | :all |

En el siguiente ejemplo, se muestra el nombre, el estado de auditoría, los tipos de evento, el formato de registro y el directorio objetivo de todas las SVM.

```
cluster1::> vserver object-store-server audit show
```

| Vserver | State | Event Types | Log Format | Target Directory |
|---------|-------|-------------|------------|------------------|
| ----- | ----- | ----- | ----- | ----- |
| vs1 | false | data | json | /audit_log |

En el siguiente ejemplo, se muestran los nombres de las SVM y los detalles sobre el registro de auditoría de todas las SVM.

```
cluster1::> vserver object-store-server audit show -log-save-details
```

| Vserver | Rotation | | Rotation | |
|---------|----------|-------|----------|-------|
| | File | Size | Schedule | Limit |
| ----- | ----- | ----- | ----- | ----- |
| vs1 | 100MB | - | | 0 |

El siguiente ejemplo muestra de una lista con toda la información de configuración de auditoría acerca de todas las SVM.

```
cluster1::> vserver object-store-server audit show -instance

Vserver: vs1
Auditing state: true
Log Destination Path: /audit_log
Categories of Events to Audit: data
Log Format: json
Log File Size Limit: 100MB
Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
Log Rotation Schedule: Day: -
Log Rotation Schedule: Hour: -
Log Rotation Schedule: Minute: -
Rotation Schedules: -
Log Files Rotation Limit: 0
Log Retention Time: 0s
```

Autenticación y control de acceso

Información general sobre el control de acceso y autenticación

La autenticación de clústeres ONTAP y el control de acceso a los servicios web de ONTAP se pueden gestionar.

Mediante System Manager o la CLI, puede controlar y proteger el acceso de cliente y administrador al clúster y al almacenamiento.

Si utiliza la versión clásica de System Manager (disponible solo en ONTAP 9.7 y versiones anteriores), consulte ["System Manager Classic \(ONTAP de 9.0 a 9.7\)"](#)

Autenticación y autorización de clientes

ONTAP autentica un equipo de cliente y un usuario al verificar sus identidades con un origen de confianza. ONTAP autoriza a un usuario a acceder a un archivo o directorio comparando las credenciales del usuario con los permisos configurados en el archivo o directorio.

Autenticación de administrador y RBAC

Los administradores utilizan cuentas de inicio de sesión locales o remotas para autenticarse en el clúster y en las máquinas virtuales de almacenamiento. El control de acceso basado en roles (RBAC) determina los comandos a los que tiene acceso un administrador.

Gestione la autenticación de administrador y RBAC

Autenticación de administrador y información general de RBAC con la interfaz de línea de comandos

Puede habilitar cuentas de inicio de sesión para los administradores del clúster ONTAP y los administradores de máquinas virtuales de almacenamiento (SVM). También es posible usar el control de acceso basado en roles (RBAC) para definir las funcionalidades de los administradores.

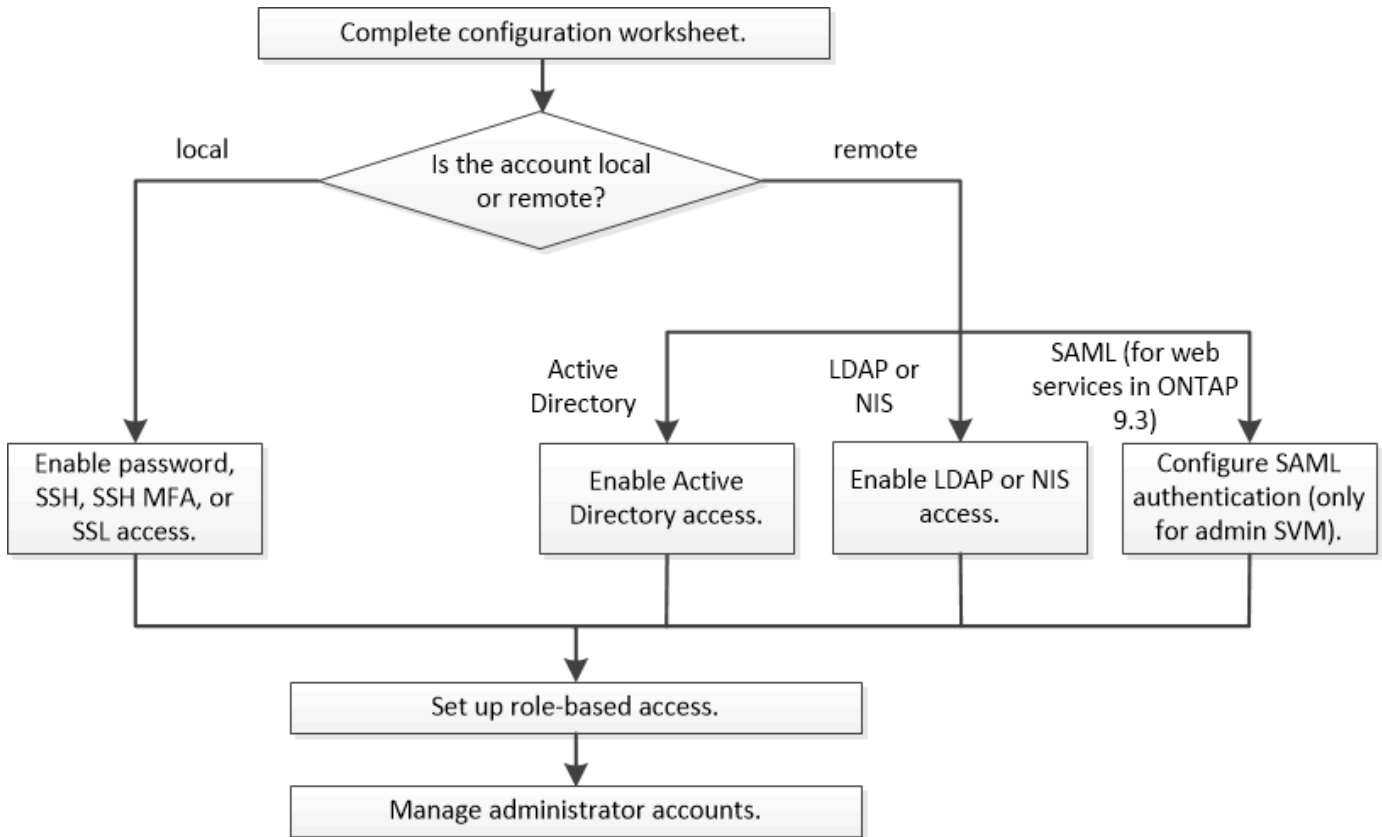
Las cuentas de inicio de sesión y RBAC se habilitan de las siguientes maneras:

- Desea usar la interfaz de línea de comandos (CLI) de ONTAP, no System Manager ni una herramienta de secuencias de comandos automatizada.
- Quiere utilizar las prácticas recomendadas, no explorar todas las opciones disponibles.
- No utiliza SNMP para recopilar información sobre el clúster.

Flujo de trabajo de autenticación de administrador y RBAC

Puede habilitar la autenticación para cuentas de administrador locales o cuentas de administrador remotas. La información de cuentas de una cuenta local reside en el sistema de almacenamiento de y la información de la cuenta de una cuenta remota se

encuentra en otro lugar. Cada cuenta puede tener una función predefinida o una función personalizada.



Es posible habilitar cuentas de administrador local para acceder a una SVM o una SVM de administrador con los siguientes tipos de autenticación:

- Contraseña
- Clave pública SSH
- Certificado SSL
- Autenticación multifactor (MFA) de SSH

A partir de ONTAP 9.3, se admite la autenticación con contraseña y clave pública.

Puede habilitar cuentas de administrador remoto para acceder a una SVM de administrador o a una SVM de datos con los siguientes tipos de autenticación:

- Active Directory
- Autenticación SAML (solo para SVM de administrador)

A partir de ONTAP 9.3, la autenticación del lenguaje de marcado de aserción de seguridad (SAML) puede usarse para acceder a la SVM de administración utilizando cualquiera de los siguientes servicios web: Infraestructura de procesador de servicio, API de ONTAP o System Manager.

- A partir de ONTAP 9.4, la MFA de SSH puede utilizarse para usuarios remotos en servidores LDAP o NIS. Se admite la autenticación con nsswitch y clave pública.

Hojas de cálculo para la autenticación del administrador y la configuración de RBAC

Antes de crear cuentas de inicio de sesión y configurar el control de acceso basado en roles (RBAC), debe recopilar información para cada elemento de las hojas de cálculo de configuración.

Crear o modificar cuentas de inicio de sesión

Se deben proporcionar estos valores con el `security login create` Comando cuando habilita las cuentas de inicio de sesión para acceder a una máquina virtual de almacenamiento. Se proporcionan los mismos valores con `security login modify` Comando al modificar la forma en que una cuenta accede a una máquina virtual de almacenamiento.

| Campo | Descripción | Su valor |
|----------------------------------|---|----------|
| <code>-vserver</code> | El nombre de la máquina virtual de almacenamiento a la que accede la cuenta. El valor predeterminado es el nombre de la máquina virtual de almacenamiento de administrador para el clúster. | |
| <code>-user-or-group-name</code> | El nombre de usuario o el nombre de grupo de la cuenta. La especificación de un nombre de grupo permite el acceso a cada usuario del grupo. Puede asociar un nombre de usuario o un nombre de grupo con varias aplicaciones. | |
| <code>-application</code> | La aplicación que se utiliza para acceder a la VM de almacenamiento: <ul style="list-style-type: none">• <code>http</code>• <code>ontapi</code>• <code>snmp</code>• <code>ssh</code> | |

| | | |
|--------------------------|---|--|
| -authmethod | <p>El método que se utiliza para autenticar la cuenta:</p> <ul style="list-style-type: none"> • <code>cert</code> Para la autenticación de certificados SSL • <code>domain</code> Para la autenticación de Active Directory • <code>nsswitch</code> Para la autenticación LDAP o NIS • <code>password</code> para autenticación de contraseña de usuario • <code>publickey</code> para la autenticación de claves públicas • <code>community</code> Para cadenas de comunidad SNMP • <code>usm</code> Para el modelo de seguridad de usuario SNMP • <code>saml</code> Para la autenticación del lenguaje de marcado de aserción de seguridad (SAML) | |
| -remote-switch-ipaddress | <p>La dirección IP del switch remoto. El conmutador remoto puede ser un conmutador de clúster supervisado por el monitor de estado del conmutador de clúster (CSHM) o un conmutador Fibre Channel (FC) supervisado por el monitor de estado MetroCluster (MCC-HM). Esta opción sólo se aplica cuando la aplicación está <code>snmp</code> y el método de autenticación es <code>usm</code>.</p> | |
| -role | <p>El rol de control de acceso que se asigna a la cuenta:</p> <ul style="list-style-type: none"> • Para el clúster (la VM de almacenamiento del administrador), el valor predeterminado es <code>admin</code>. • Para una máquina virtual de almacenamiento de datos, el valor predeterminado es <code>vsadmin</code>. | |

| | | |
|--|--|--|
| <code>-comment</code> | (Opcional) texto descriptivo para la cuenta. El texto debe escribirse entre comillas dobles ("). | |
| <code>-is-ns-switch-group</code> | Si la cuenta es una cuenta de grupo LDAP o una cuenta de grupo NIS (yes o. no). | |
| <code>-second-authentication-method</code> | <p>Segundo método de autenticación en caso de autenticación multifactor:</p> <ul style="list-style-type: none"> • <code>none</code> si no utiliza la autenticación multifactor, valor predeterminado • <code>publickey</code> para la autenticación de claves públicas cuando el <code>authmethod</code> es la contraseña o <code>nsswitch</code> • <code>password</code> para la autenticación de contraseña de usuario cuando el <code>authmethod</code> es clave pública • <code>nsswitch</code> para la autenticación de contraseña de usuario cuando <code>authmethod</code> es <code>publickey</code> <p>El orden de autenticación es siempre la clave pública seguida de la contraseña.</p> | |
| <code>-is-ldap-fastbind</code> | A partir de ONTAP 9.11.1, cuando se establece en <code>true</code> , habilita el enlace rápido LDAP para la autenticación <code>nsswitch</code> ; el valor predeterminado es <code>false</code> . Para utilizar el enlace rápido LDAP, el <code>-authentication-method</code> el valor se debe establecer en <code>nsswitch</code> . "Obtenga información acerca de ldap fastbind para la autenticación nsswitch." | |

Configurar la información de seguridad de Cisco Duo

Se deben proporcionar estos valores con el `security login duo create` Comando cuando se habilita la autenticación de dos factores Cisco Duo con inicios de sesión SSH para una máquina virtual de almacenamiento.

| Campo | Descripción | Su valor |
|------------------|---|----------|
| -vserver | El equipo virtual de almacenamiento (denominado Vserver en la CLI de ONTAP) al que se aplica la configuración de autenticación Duo. | |
| -integration-key | Su clave de integración, obtenida al registrar su aplicación SSH con Duo. | |
| -secret-key | Su clave secreta, obtenida al registrar su aplicación SSH con Duo. | |
| -api-host | <p>El nombre de host de la API, obtenido al registrar su aplicación SSH con Duo. Por ejemplo:</p> <pre>api- <HOSTNAME>.duosecurity.com</pre> | |
| -fail-mode | En los errores de servicio o configuración que impiden la autenticación Duo, se produce un error <code>safe</code> (permitir acceso) o. <code>secure</code> (denegar acceso). El valor predeterminado es <code>safe</code> , Lo que significa que la autenticación DUO se omite si falla debido a errores como el servidor Duo API no es accesible. | |
| -http-proxy | <p>Utilice el proxy HTTP especificado. Si el proxy HTTP requiere autenticación, incluya las credenciales en la URL del proxy. Por ejemplo:</p> <pre>http- proxy=http://username :password@proxy.example.org:8080</pre> | |

| | | |
|---------------------|--|--|
| <p>-autopush</p> | <p>Uno de los dos <code>true</code> o <code>false</code>. El valor predeterminado es <code>false</code>. Si <code>true</code>, Duo envía automáticamente una solicitud de inicio de sesión push al teléfono del usuario, volviendo a una llamada telefónica si no está disponible push. Tenga en cuenta que esto desactiva efectivamente la autenticación de contraseña. Si <code>false</code>, se le pide al usuario que elija un método de autenticación.</p> <p>Cuando se configura con <code>autopush = true</code>, recomendamos el ajuste <code>max-prompts = 1</code>.</p> | |
| <p>-max-prompts</p> | <p>Si un usuario no se autentica con un segundo factor, Duo solicita al usuario que se autentique de nuevo. Esta opción establece el número máximo de peticiones de datos que Duo muestra antes de denegar el acceso. Debe ser 1, 2, o 3. El valor predeterminado es 1.</p> <p>Por ejemplo, cuando <code>max-prompts = 1</code>, el usuario debe autenticarse correctamente en la primera petición de datos, mientras que si <code>max-prompts = 2</code>, si el usuario introduce información incorrecta en el prompt inicial, se le pedirá que se autentique de nuevo.</p> <p>Cuando se configura con <code>autopush = true</code>, recomendamos el ajuste <code>max-prompts = 1</code>.</p> <p>Para la mejor experiencia, un usuario con solo autenticación <code>publickey</code> siempre tendrá <code>max-prompts</code> establezca en 1.</p> | |

| | | |
|----------|--|--|
| -enabled | Active la autenticación de dos factores Duo. Establezca en <code>true</code> de forma predeterminada. Cuando está activada, la autenticación de dos factores Duo se aplica durante el inicio de sesión SSH de acuerdo con los parámetros configurados. Cuando Duo está desactivado (establecido en <code>false</code>), se ignora la autenticación Duo. | |
|----------|--|--|

Definir funciones personalizadas

Se deben proporcionar estos valores con el `security login role create` comando al definir un rol personalizado.

| Campo | Descripción | Su valor |
|-------------|---|----------|
| -vserver | (Opcional) Nombre del equipo virtual de almacenamiento (denominado Vserver en la CLI de ONTAP) asociado al rol. | |
| -role | El nombre del rol. | |
| -cmddirname | El comando o el directorio de comandos al que tiene acceso el rol. Debe escribir los nombres de subdirectorio de comandos entre comillas dobles ("). Por ejemplo: "volume snapshot". Debe entrar <code>DEFAULT</code> para especificar todos los directorios de comandos. | |

| | | |
|---------|--|--|
| -access | <p>(Opcional) el nivel de acceso del rol. Para directorios de comandos:</p> <ul style="list-style-type: none"> • none (el valor predeterminado para las funciones personalizadas) niega el acceso a los comandos del directorio de comandos • readonly concede acceso a show comandos del directorio de comandos y sus subdirectorios • all concede acceso a todos los comandos del directorio de comandos y sus subdirectorios <p>Para <i>comandos no intrínsecos</i> (comandos que no terminan en create, modify, delete, o. show):</p> <ul style="list-style-type: none"> • none (el valor predeterminado para los roles personalizados) niega el acceso al comando • readonly no es aplicable • all concede acceso al comando <p>Para conceder o denegar el acceso a comandos intrínsecos, debe especificar el directorio de comandos.</p> | |
| -query | <p>(Opcional) el objeto de consulta que se utiliza para filtrar el nivel de acceso, que se especifica en forma de una opción válida para el comando o para un comando en el directorio de comandos. El objeto de consulta debe escribirse entre comillas dobles ("). Por ejemplo, si el directorio de comandos es volume, el objeto de consulta "-aggr aggr0" habilitará el acceso para el aggr0 solo agregados.</p> | |

Asociar una clave pública a una cuenta de usuario

Se deben proporcionar estos valores con el `security login publickey create` Cuando asocia una clave pública SSH a una cuenta de usuario.

| Campo | Descripción | Su valor |
|------------|--|----------|
| -vserver | (Opcional) Nombre de la máquina virtual de almacenamiento a la que accede la cuenta. | |
| -username | El nombre de usuario de la cuenta. El valor predeterminado, <code>admin</code> , que es el nombre predeterminado del administrador del clúster. | |
| -index | El número de índice de la clave pública. El valor predeterminado es 0 si la clave es la primera clave que se crea para la cuenta; de lo contrario, el valor predeterminado es uno más que el número de índice más alto existente para la cuenta. | |
| -publickey | La clave pública de OpenSSH. La clave debe escribirse entre comillas dobles ("). | |
| -role | El rol de control de acceso que se asigna a la cuenta. | |
| -comment | (Opcional) texto descriptivo para la clave pública. El texto debe escribirse entre comillas dobles ("). | |

| | | |
|-------------------|---|--|
| -x509-certificate | <p>(Opcional) A partir de ONTAP 9.13.1, le permite gestionar la asociación de certificados X,509 con la clave pública SSH.</p> <p>Cuando asocia un certificado X,509 a la clave pública SSH, ONTAP comprueba el inicio de sesión SSH para ver si este certificado es válido. Si ha caducado o se ha revocado, el inicio de sesión no está permitido y la clave pública SSH asociada está deshabilitada. Los posibles valores son los siguientes:</p> <ul style="list-style-type: none"> • <code>install</code>: Instale el certificado X,509 codificado PEM especificado y asócielo a la clave pública SSH. Incluya el texto completo del certificado que desea instalar. • <code>modify</code>: Actualizar el certificado X,509 con codificación PEM existente con el certificado especificado y asociarlo con la clave pública SSH. Incluya el texto completo para el nuevo certificado. • <code>delete</code>: Eliminar la asociación de certificados X,509 existente con la clave pública SSH. | |
|-------------------|---|--|

Instale un certificado digital de servidor firmado por CA

Se deben proporcionar estos valores con el `security certificate generate-csr` Comando cuando se genera una solicitud de firma de certificación digital (CSR) para utilizarla en la autenticación de una máquina virtual de almacenamiento como un servidor SSL.

| Campo | Descripción | Su valor |
|--------------|---|----------|
| -common-name | El nombre del certificado, que es un nombre de dominio completo (FQDN) o un nombre común personalizado. | |

| | | |
|----------------|---|--|
| -size | El número de bits de la clave privada. Cuanto mayor sea el valor, más segura será la clave. El valor predeterminado es 2048. Los valores posibles son 512, 1024, 1536, y. 2048. | |
| -country | El país de la máquina virtual de almacenamiento, en un código de dos letras. El valor predeterminado es US. Consulte las páginas de manual para obtener una lista de códigos. | |
| -state | El estado o la provincia de la máquina virtual de almacenamiento. | |
| -locality | La localidad de la máquina virtual de almacenamiento. | |
| -organization | La organización de la máquina virtual de almacenamiento. | |
| -unit | La unidad de la organización de la máquina virtual de almacenamiento. | |
| -email-addr | La dirección de correo electrónico del administrador de contacto para la máquina virtual de almacenamiento. | |
| -hash-function | Función de hash criptográfico para firmar el certificado. El valor predeterminado es SHA256. Los valores posibles son SHA1, SHA256, y. MD5. | |

Se deben proporcionar estos valores con el `security certificate install` Comando cuando instala un certificado digital firmado por CA para utilizarlo en la autenticación del clúster o de la máquina virtual de almacenamiento como un servidor SSL. En la siguiente tabla solo se muestran las opciones relevantes para la configuración de la cuenta.

| Campo | Descripción | Su valor |
|----------|---|----------|
| -vserver | Nombre de la máquina virtual de almacenamiento en la que se va a instalar el certificado. | |

| | | |
|-------|--|--|
| -type | <p>El tipo de certificado:</p> <ul style="list-style-type: none"> • <code>server</code> para los certificados de servidor y los certificados intermedios • <code>client-ca</code> Para el certificado de clave pública de la CA raíz del cliente SSL • <code>server-ca</code> Para el certificado de clave pública de la CA raíz del servidor SSL del que ONTAP es un cliente • <code>client</code> Para un certificado digital autofirmado o firmado por CA y una clave privada para ONTAP como cliente SSL | |
|-------|--|--|

Configurar el acceso al controlador de dominio de Active Directory

Se deben proporcionar estos valores con el `security login domain-tunnel create` Comando cuando ya configuró un servidor SMB para una máquina virtual de almacenamiento de datos y desea configurar la máquina virtual de almacenamiento como una puerta de enlace o *tunnel* para el acceso de la controladora de dominio de Active Directory al clúster.

| Campo | Descripción | Su valor |
|----------|---|----------|
| -vserver | El nombre de la máquina virtual de almacenamiento para la que se configuró el servidor SMB. | |

Se deben proporcionar estos valores con el `vserver active-directory create` Comando cuando no configuró un servidor SMB y desea crear una cuenta de equipo virtual de almacenamiento en el dominio de Active Directory.

| Campo | Descripción | Su valor |
|---------------|--|----------|
| -vserver | Nombre de la máquina virtual de almacenamiento para la que desea crear una cuenta de equipo de Active Directory. | |
| -account-name | Nombre NetBIOS de la cuenta de equipo. | |
| -domain | El nombre de dominio completo (FQDN). | |

| | | |
|-----|--|--|
| -ou | La unidad organizativa del dominio. El valor predeterminado es CN=Computers. ONTAP agrega este valor al nombre de dominio para producir el nombre distintivo de Active Directory. | |
|-----|--|--|

Configurar el acceso a servidores LDAP o NIS

Se deben proporcionar estos valores con el `vserver services name-service ldap client create` Comando cuando crea una configuración de cliente LDAP para la máquina virtual de almacenamiento.

En la tabla siguiente solo se muestran las opciones relevantes para la configuración de la cuenta:

| Campo | Descripción | Su valor |
|----------------|---|----------|
| -vserver | El nombre de la máquina virtual de almacenamiento para la configuración del cliente. | |
| -client-config | El nombre de la configuración del cliente. | |
| -ldap-servers | Lista separada por comas de direcciones IP y nombres de host para los servidores LDAP a los que se conecta el cliente. | |
| -schema | Esquema que utiliza el cliente para realizar consultas LDAP. | |
| -use-start-tls | <p>Si el cliente utiliza Start TLS para cifrar la comunicación con el servidor LDAP (<code>true</code> o <code>false</code>).</p> <div>  <p>Start TLS solo es compatible para el acceso a las máquinas virtuales de almacenamiento de datos. No se admite para el acceso a las máquinas virtuales de almacenamiento de administradores.</p> </div> | |

Se deben proporcionar estos valores con el `vserver services name-service ldap create` Comando cuando se asocia una configuración de cliente LDAP a la máquina virtual de almacenamiento.

| Campo | Descripción | Su valor |
|------------------------------|--|----------|
| <code>-vserver</code> | Nombre de la máquina virtual de almacenamiento a la que se asociará la configuración del cliente. | |
| <code>-client-config</code> | El nombre de la configuración del cliente. | |
| <code>-client-enabled</code> | Si la máquina virtual de almacenamiento puede usar la configuración de clientes LDAP (<code>true</code> o <code>false</code>). | |

Se deben proporcionar estos valores con el `vserver services name-service nis-domain create` Comando cuando se crea una configuración de dominio NIS en una máquina virtual de almacenamiento.

| Campo | Descripción | Su valor |
|---------------------------|---|----------|
| <code>-vserver</code> | Nombre de la máquina virtual de almacenamiento en la que se creará la configuración del dominio. | |
| <code>-domain</code> | El nombre del dominio. | |
| <code>-active</code> | Si el dominio está activo (<code>true</code> o <code>false</code>). | |
| <code>-servers</code> | ONTAP 9.0, 9.1: Lista separada por comas de direcciones IP para los servidores NIS que se utilizan en la configuración de dominio. | |
| <code>-nis-servers</code> | Lista separada por comas de direcciones IP y nombres de host para los servidores NIS que utiliza la configuración de dominio. | |

Se deben proporcionar estos valores con el `vserver services name-service ns-switch create` al especificar el orden de búsqueda para fuentes de servicio de nombres.

| Campo | Descripción | Su valor |
|-----------------------|---|----------|
| <code>-vserver</code> | Nombre de la máquina virtual de almacenamiento en la que se va a configurar el orden de consulta del servicio de nombres. | |

| | | |
|-----------|---|--|
| -database | <p>La base de datos del servicio de nombres:</p> <ul style="list-style-type: none"> • <code>hosts</code> Para los archivos y los servicios de nombres DNS • <code>group</code> Para archivos, LDAP y servicios de nombres NIS • <code>passwd</code> Para archivos, LDAP y servicios de nombres NIS • <code>netgroup</code> Para archivos, LDAP y servicios de nombres NIS • <code>namemap</code> Para archivos y servicios de nombres LDAP | |
| -sources | <p>El orden en el que buscar fuentes de servicio de nombres (en una lista separada por comas):</p> <ul style="list-style-type: none"> • <code>files</code> • <code>dns</code> • <code>ldap</code> • <code>nis</code> | |

Configure el acceso SAML

A partir de ONTAP 9.3, se proporcionan estos valores con el `security saml-sp create` Comando para configurar la autenticación SAML.

| Campo | Descripción | Su valor |
|----------|---|----------|
| -idp-uri | La dirección FTP o la dirección HTTP del host del proveedor de identidades (IDP) desde el que se pueden descargar los metadatos de IDP. | |
| -sp-host | El nombre de host o la dirección IP del host del proveedor de servicios SAML (sistema ONTAP). De manera predeterminada, se utiliza la dirección IP de la LIF de administración del clúster. | |

| | | |
|---|--|--|
| <code>-cert-ca y. -cert-serial, o. -cert-common-name</code> | Los detalles del certificado de servidor del host del proveedor de servicios (sistema ONTAP). Puede introducir la entidad emisora de certificados (CA) del proveedor de servicios y el número de serie del certificado o el nombre común del certificado del servidor. | |
| <code>-verify-metadata-server</code> | Si la identidad del servidor de metadatos de IDP debe validarse (<code>true</code> o <code>false</code>). Lo más recomendable es establecer siempre este valor como <code>true</code> . | |

Crear cuentas de inicio de sesión

Información general de las cuentas de inicio de sesión de

Puede habilitar cuentas de administrador de SVM y de clúster local o remoto. Una cuenta local es aquella en la que reside la información de la cuenta, la clave pública o el certificado de seguridad en el sistema de almacenamiento. La información DE la cuenta DE AD se almacena en un controlador de dominio. Las cuentas LDAP y NIS residen en servidores LDAP y NIS.

Administradores de clústeres y SVM

Un administrador de *cluster* accede a la SVM de administrador del clúster. La SVM de administrador y un administrador de clúster con el nombre reservado `admin` se crean automáticamente cuando se configura el clúster.

Un administrador de clúster con los valores predeterminados `admin` el rol puede administrar todo el clúster y sus recursos. El administrador de clúster puede crear administradores de clúster adicionales con diferentes roles según sea necesario.

Un administrador de SVM accede a una SVM de datos. El administrador de clúster crea SVM de datos y administradores de SVM según sea necesario.

A los administradores de SVM se les asigna el `vsadmin` función predeterminada. El administrador de clúster puede asignar diferentes roles a los administradores de SVM según sea necesario.

Convenciones de nomenclatura

Los siguientes nombres genéricos no se pueden utilizar para cuentas de administrador de SVM o de clúster remoto:

- `adm`
- `bandeja`
- `cli`

- demonio
- ftp
- “juegos”
- detener
- lp
- correo
- «hombre»
- «naroot»
- «NetApp»
- «noticias»
- «nadie»
- operador
- «raíz»
- apagado
- sshd
- sincronizar
- sistema
- uucp
- «www»

Roles fusionados

Si habilita varias cuentas remotas para el mismo usuario, se le asigna la unión de todas las funciones especificadas para las cuentas. Es decir, si se asigna una cuenta LDAP o NIS el `vsadmin`. Asimismo, se asigna el rol y la cuenta de grupo AD del mismo usuario `vsadmin-volume`. El rol, el usuario de AD inicia sesión con más incluido `vsadmin` funcionalidades. Se dice que los roles son *fusionado*.

Habilite el acceso de cuenta local

Habilite la información general de acceso de la cuenta local

Una cuenta local es aquella en la que reside la información de la cuenta, la clave pública o el certificado de seguridad en el sistema de almacenamiento. Puede utilizar el `security login create` Comando para habilitar cuentas locales para acceder a un administrador o una SVM de datos.

Active el acceso a la cuenta de contraseña

Puede utilizar el `security login create` Comando para habilitar las cuentas de administrador para acceder a una SVM de administrador o de datos con una contraseña. Se le pedirá la contraseña después de introducir el comando.

Acerca de esta tarea

Si no está seguro de la función de control de acceso que desea asignar a la cuenta de inicio de sesión, puede

usar la `security login modify` comando para añadir el rol más adelante.

Antes de empezar

Para realizar esta tarea, debe ser un administrador de clústeres.

Paso

- 1. Habilite las cuentas de administrador local para acceder a una SVM mediante una contraseña:

```
security login create -vserver SVM_name -user-or-group-name user_or_group_name
-application application -authmethod authentication_method -role role -comment
comment
```

Para obtener una sintaxis completa del comando, consulte ["hoja de trabajo"](#).

El siguiente comando habilita la cuenta de administrador de clúster `admin1` con los predefinidos `backup` Rol para acceder a la SVM de administrador `engCluster` usar una contraseña. Se le pedirá la contraseña después de introducir el comando.

```
cluster1::>security login create -vserver engCluster -user-or-group-name
admin1 -application ssh -authmethod password -role backup
```

Habilite cuentas de clave pública de SSH

Puede utilizar el `security login create` Comando para habilitar cuentas de administrador para acceder a una SVM de administrador o de datos con una clave pública SSH.

Acerca de esta tarea

- Debe asociar la clave pública a la cuenta para que esta pueda acceder a la SVM.

[Asociación de una clave pública con una cuenta de usuario](#)

Puede realizar esta tarea antes o después de habilitar el acceso a la cuenta.

- Si no está seguro de la función de control de acceso que desea asignar a la cuenta de inicio de sesión, puede usar la `security login modify` comando para añadir el rol más adelante.

Si desea habilitar el modo FIPS en su clúster, las cuentas de claves públicas SSH existentes sin los algoritmos de clave admitidos deben volver a configurarse con un tipo de clave admitida. Las cuentas se deben volver a configurar antes de habilitar FIPS o se producirá un error en la autenticación del administrador.

La siguiente tabla indica los algoritmos de tipo de clave de host que se admiten para las conexiones SSH de ONTAP. Estos tipos de claves no se aplican a la configuración de la autenticación pública SSH.

| | | |
|------------------|---|--|
| Versión de ONTAP | Tipos de clave compatibles con el modo FIPS | Tipos de clave compatibles con el modo no FIPS |
|------------------|---|--|

| | | |
|---------------------|------------------------------------|--|
| 9.11.1 y posterior | ecdsa-sha2-nistp256 | ecdsa-sha2-nistp256 rsa-sha2-512 rsa-sha2-256 ssh-ed25519 ssh-dss ssh-rsa |
| 9.10.1 y anteriores | ecdsa-sha2-nistp256 ssh-ed25519 | ecdsa-sha2-nistp256 ssh-ed25519 ssh-dss ssh-rsa |



La compatibilidad con el algoritmo de clave de host ssh-ed25519 se elimina a partir de ONTAP 9.11.1.

Para obtener más información, consulte ["Configurar la seguridad de red con FIPS"](#).

Antes de empezar

Para realizar esta tarea, debe ser un administrador de clústeres.

Paso

1. Habilite cuentas de administrador local para acceder a una SVM mediante una clave pública de SSH:

```
security login create -vserver SVM_name -user-or-group-name user_or_group_name
-application application -authmethod authentication_method -role role -comment
comment
```

Para obtener una sintaxis completa del comando, consulte ["hoja de trabajo"](#).

El siguiente comando habilita la cuenta de administrador de SVM `svmadmin1` con los predefinidos `vsadmin-volume` Rol para acceder a la `SVMengData1` Mediante una clave pública SSH:

```
cluster1::>security login create -vserver engData1 -user-or-group-name
svmadmin1 -application ssh -authmethod publickey -role vsadmin-volume
```

Después de terminar

Si no ha asociado una clave pública a la cuenta de administrador, debe hacerlo para que la cuenta pueda acceder a la SVM.

[Asociación de una clave pública con una cuenta de usuario](#)

Habilite las cuentas de autenticación multifactor (MFA)

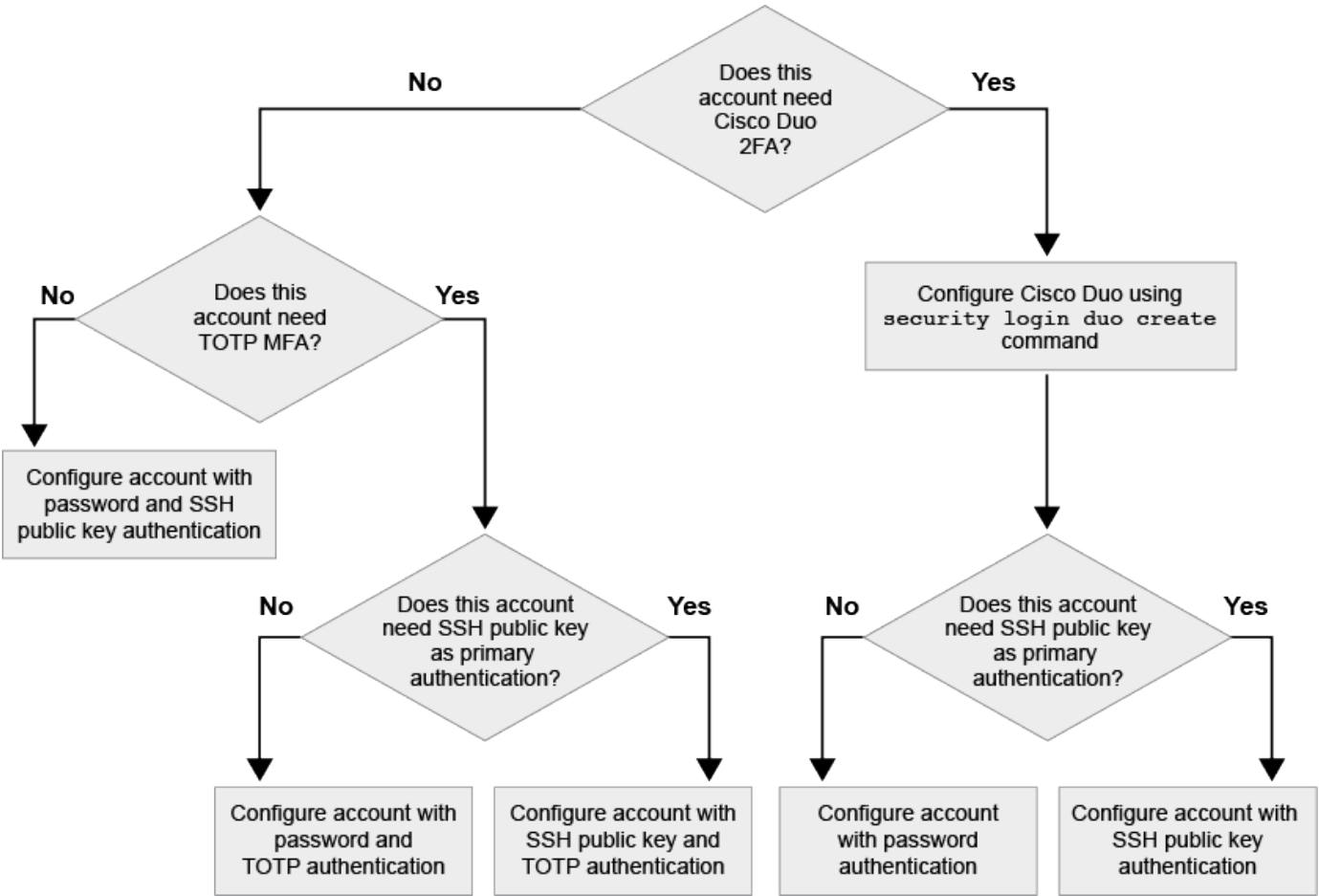
Información general de la autenticación multifactor

La autenticación multifactor (MFA) permite mejorar la seguridad al requerir que los usuarios proporcionen dos métodos de autenticación para iniciar sesión en un administrador o en un equipo virtual de almacenamiento de datos.

Dependiendo de la versión de ONTAP, puede utilizar una combinación de una clave pública SSH, una contraseña de usuario y una contraseña de un solo uso basada en el tiempo (TOTP) para la autenticación multifactor. Al habilitar y configurar Cisco Duo (ONTAP 9.14.1 y posterior), sirve como un método de autenticación adicional, que complementa los métodos existentes para todos los usuarios.

| Disponible empezando por... | Primer método de autenticación | Segundo método de autenticación |
|-----------------------------|--------------------------------|---------------------------------|
| ONTAP 9.14.1 | Clave pública SSH | TOTP |
| | Contraseña de usuario | TOTP |
| | Clave pública SSH | Cisco Duo |
| | Contraseña de usuario | Cisco Duo |
| ONTAP 9.13.1 | Clave pública SSH | TOTP |
| | Contraseña de usuario | TOTP |
| ONTAP 9,3 | Clave pública SSH | Contraseña de usuario |

Si se configura MFA, el administrador del clúster primero debe habilitar la cuenta de usuario local, entonces el usuario local debe configurar la cuenta.



Habilite la autenticación multifactor

La autenticación multifactor (MFA) permite mejorar la seguridad al requerir que los

usuarios proporcionen dos métodos de autenticación para iniciar sesión en un administrador o una SVM de datos.

Acerca de esta tarea

- Para realizar esta tarea, debe ser un administrador de clústeres.
- Si no está seguro de la función de control de acceso que desea asignar a la cuenta de inicio de sesión, puede usar la `security login modify` comando para añadir el rol más adelante.

"Modificar el rol asignado a un administrador"

- Si utiliza una clave pública para la autenticación, debe asociar la clave pública con la cuenta para que la cuenta pueda acceder a la SVM.

"Asociar una clave pública a una cuenta de usuario"

Puede realizar esta tarea antes o después de habilitar el acceso a la cuenta.

- A partir de ONTAP 9.12.1, puede usar dispositivos de autenticación de hardware Yubikey para la MFA del cliente SSH mediante los estándares de autenticación FIDO2 (Fast Identity Online) o de verificación de identidad personal (PIV).

Habilite MFA con clave pública SSH y contraseña de usuario

A partir de ONTAP 9.3, un administrador de clúster puede configurar cuentas de usuario locales para iniciar sesión con MFA mediante una clave pública SSH y una contraseña de usuario.

1. Habilite MFA en cuenta de usuario local con clave pública SSH y contraseña de usuario:

```
security login create -vserver <svm_name> -user-or-group-name  
<user_name> -application ssh -authentication-method <password|publickey>  
-role admin -second-authentication-method <password|publickey>
```

El siguiente comando requiere la cuenta de administrador de SVM `admin2` con los predefinidos `admin` Rol que desea iniciar sesión en la SVM `engData1` Con una clave pública SSH y una contraseña de usuario:

```
cluster-1::> security login create -vserver engData1 -user-or-group-name  
admin2 -application ssh -authentication-method publickey -role admin  
-second-authentication-method password
```

Please enter a password for user 'admin2':

Please enter it again:

Warning: To use public-key authentication, you must create a public key
for user "admin2".

Habilite MFA con TOTP

A partir de ONTAP 9.13.1, puede mejorar la seguridad al requerir que los usuarios locales inicien sesión en un

administrador o una SVM de datos con una clave pública SSH o una contraseña de usuario y una contraseña de un solo uso basada en un tiempo (TOTP). Después de habilitar la cuenta para MFA con TOTP, el usuario local debe iniciar sesión en ["complete la configuración"](#).

TOTP es un algoritmo informático que utiliza la hora actual para generar una contraseña de un solo uso. Si se utiliza TOTP, siempre es la segunda forma de autenticación después de la clave pública SSH o la contraseña de usuario.

Antes de empezar

Debe ser un administrador de almacenamiento para realizar estas tareas.

Pasos

Puede configurar MFA con una contraseña de usuario o una clave pública SSH como primer método de autenticación y TOTP como segundo método de autenticación.

Habilite MFA con contraseña de usuario y TOTP

1. Habilite una cuenta de usuario para la autenticación multifactor con una contraseña de usuario y TOTP.

Para nuevas cuentas de usuario

```
security login create -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
password -second-authentication-method totp -role <role> -comment  
<comment>
```

Para cuentas de usuario existentes

```
security login modify -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
password -second-authentication-method totp -role <role> -comment  
<comment>
```

2. Compruebe que MFA con TOTP está activado:

```
security login show
```

Habilite MFA con clave pública SSH y TOTP

1. Habilite una cuenta de usuario para la autenticación multifactor con una clave pública SSH y TOTP.

Para nuevas cuentas de usuario

```
security login create -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
publickey -second-authentication-method totp -role <role> -comment  
<comment>
```

Para cuentas de usuario existentes

```
security login modify -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
publickey -second-authentication-method totp -role <role> -comment  
<comment>
```

2. Compruebe que MFA con TOTP está activado:

```
security login show
```

Después de terminar

- Si no ha asociado una clave pública a la cuenta de administrador, debe hacerlo para que la cuenta pueda acceder a la SVM.

["Asociación de una clave pública con una cuenta de usuario"](#)

- El usuario local debe iniciar sesión para completar la configuración MFA con TOTP.

["Configure la cuenta de usuario local para MFA con TOTP"](#)

Información relacionada

Más información acerca de ["Autenticación multifactor en ONTAP 9 \(TR-4647\)"](#).

Configure la cuenta de usuario local para MFA con TOTP

A partir de ONTAP 9.13.1, las cuentas de usuario se pueden configurar con autenticación multifactor (MFA) con una contraseña de un solo uso basada en tiempo (TOTP).

Antes de empezar

- El administrador de almacenamiento debe ["Habilite MFA con TOTP"](#) como segundo método de autenticación para su cuenta de usuario.
- El método de autenticación de la cuenta de usuario principal debe ser una contraseña de usuario o una clave SSH pública.
- Debes configurar tu aplicación TOTP para que funcione con tu smartphone y crear tu clave secreta TOTP.

TOTP es compatible con varias aplicaciones de autenticación como Google Authenticator.

Pasos

1. Inicie sesión en su cuenta de usuario con el método de autenticación actual.

Su método de autenticación actual debe ser una contraseña de usuario o una clave pública SSH.

2. Cree la configuración de TOTP en su cuenta:

```
security login totp create -vserver "<svm_name>" -username  
"<account_username >"
```

3. Compruebe que la configuración de TOTP está activada en su cuenta:

```
security login totp show -vserver "<svm_name>" -username  
"<account_username>"
```

Restablezca la clave secreta TOTP

Para proteger la seguridad de su cuenta, si su clave secreta TOTP se ve comprometida o se pierde, debe deshabilitarla y crear una nueva.

Restablezca TOTP si su clave está comprometida

Si tu clave secreta TOTP está comprometida, pero aún tienes acceso a ella, puedes quitar la clave comprometida y crear una nueva.

1. Inicie sesión en su cuenta de usuario con su contraseña de usuario o clave pública SSH y su clave secreta TOTP comprometida.
2. Elimine la clave secreta TOTP comprometida:

```
security login totp delete -vserver <svm_name> -username  
<account_username>
```

3. Cree una nueva clave secreta de TOTP:

```
security login totp create -vserver <svm_name> -username  
<account_username>
```

4. Compruebe que la configuración de TOTP está activada en su cuenta:

```
security login totp show -vserver <svm_name> -username  
<account_username>
```

Restablezca TOTP si se pierde la clave

Si se pierde la clave secreta de TOTP, comuníquese con el administrador de almacenamiento de ["tener la clave desactivada"](#). Una vez desactivada la clave, puede utilizar el primer método de autenticación para iniciar sesión y configurar un nuevo TOTP.

Antes de empezar

La clave secreta de TOTP debe ser deshabilitada por un administrador de almacenamiento.

Si no tiene una cuenta de administrador de almacenamiento, póngase en contacto con su administrador de almacenamiento para deshabilitar la clave.

Pasos

1. Una vez que un administrador de almacenamiento haya desactivado el secreto TOTP, utilice el método de autenticación principal para iniciar sesión en su cuenta local.
2. Cree una nueva clave secreta de TOTP:

```
security login totp create -vserver <svm_name> -username  
<account_username >
```

3. Compruebe que la configuración de TOTP está activada en su cuenta:

```
security login totp show -vserver <svm_name> -username  
<account_username>
```

Desactive la clave secreta TOTP para la cuenta local

Si se pierde la clave secreta de una sola vez basada en el tiempo (TOTP) de un usuario local, el administrador de almacenamiento debe desactivar la clave perdida antes de que el usuario pueda crear una nueva clave secreta TOTP.

Acerca de esta tarea

Esta tarea solo se puede realizar desde una cuenta de administrador de clúster.

Paso

1. Desactive la clave secreta TOTP:

```
security login totp delete -vserver "<svm_name>" -username  
"<account_username>"
```

Habilite cuentas de certificado SSL

Puede utilizar el `security login create` Comando para habilitar las cuentas de administrador para acceder a una SVM de administrador o de datos con un certificado SSL.

Acerca de esta tarea

- Para que la cuenta pueda acceder a la SVM, debe instalar un certificado digital de servidor firmado por CA.

[Generar e instalar un certificado de servidor firmado por CA](#)

Puede realizar esta tarea antes o después de habilitar el acceso a la cuenta.

- Si no está seguro del rol de control de acceso que desea asignar a la cuenta de inicio de sesión, puede añadir el rol más adelante con la `security login modify` comando.

[Modificar el rol asignado a un administrador](#)



Para las cuentas de administrador de clúster, se admite la autenticación de certificados con el `http`, `ontapi`, y `rest` más grandes. Para las cuentas de administrador de SVM, la autenticación de certificados solo se admite con el `ontapi` y `rest` más grandes.

Paso

1. Habilite las cuentas de administrador local para acceder a una SVM mediante un certificado SSL:

```
security login create -vserver SVM_name -user-or-group-name user_or_group_name  
-application application -authmethod authentication_method -role role -comment  
comment
```

Para obtener una sintaxis completa del comando, consulte ["Páginas manuales de ONTAP por versión"](#).

El siguiente comando habilita la cuenta de administrador de SVM `svmadmin2` con el valor predeterminado `vsadmin` Rol para acceder a la SVM `engData2` Mediante un certificado digital SSL.

```
cluster1::>security login create -vserver engData2 -user-or-group-name  
svmadmin2 -application ontapi -authmethod cert
```

Después de terminar

Si no instaló un certificado digital de servidor firmado por CA, debe hacerlo para que la cuenta pueda acceder a la SVM.

[Generar e instalar un certificado de servidor firmado por CA](#)

Habilite el acceso de cuenta de Active Directory

Puede utilizar el `security login create` Comando para habilitar cuentas de usuarios o grupos de Active Directory (AD) para acceder a un administrador o a la SVM de datos. Cualquier usuario del grupo de AD puede acceder a la SVM con el rol asignado al grupo.

Acerca de esta tarea

- Para poder acceder a la SVM, es necesario configurar el acceso de la controladora de dominio de AD al clúster o a la SVM.

[Configuración del acceso al controlador de dominio de Active Directory](#)

Puede realizar esta tarea antes o después de habilitar el acceso a la cuenta.

- A partir de ONTAP 9.13.1, puede usar una clave pública SSH como método de autenticación principal o secundario con una contraseña de usuario de AD.

Si elige usar una clave pública SSH como autenticación principal, no se realiza ninguna autenticación de AD.

- A partir de ONTAP 9.11.1, se puede utilizar ["Enlace rápido LDAP para la autenticación nsswitch"](#) Si es compatible con el servidor LDAP de AD.
- Si no está seguro de la función de control de acceso que desea asignar a la cuenta de inicio de sesión,

puede usar la `security login modify` comando para añadir el rol más adelante.

Modificar el rol asignado a un administrador



El acceso a la cuenta DE grupo DE AD solo se admite con SSH, `ontapi`, y. rest más grandes. Los grupos de AD no se admiten con la autenticación de clave pública SSH, que se utiliza comúnmente para la autenticación multifactor.

Antes de empezar

- La hora del clúster debe sincronizarse con un plazo de cinco minutos desde la hora del controlador de dominio de AD.
- Para realizar esta tarea, debe ser un administrador de clústeres.

Paso

1. Habilite las cuentas de administrador de usuario o de grupo de AD para acceder a una SVM:

Para usuarios de AD:

| Versión de ONTAP | Autenticación principal | Autenticación secundaria | Comando |
|--------------------|-------------------------|--------------------------|---|
| 9.13.1 y posterior | Clave pública | Ninguno | <pre>security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method publickey -role <role></pre> |

| Versión de ONTAP | Autenticación principal | Autenticación secundaria | Comando |
|--------------------|-------------------------|--------------------------|---|
| 9.13.1 y posterior | Dominio | Clave pública | <p>Para un nuevo usuario</p> <pre>security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role></pre> <p>Para un usuario existente</p> <pre>security login modify -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role></pre> |
| 9,0 y posterior | Dominio | Ninguno | <pre>security login create -vserver <svm_name> -user-or-group-name <user_name> -application <application> -authentication-method domain -role <role> -comment <comment> [-is-ldap- fastbind true]</pre> |

Para grupos AD:

| Versión de ONTAP | Autenticación principal | Autenticación secundaria | Comando |
|------------------|-------------------------|--------------------------|---|
| 9,0 y posterior | Dominio | Ninguno | <pre>security login create -vserver <svm_name> -user-or-group-name <user_name> -application <application> -authentication-method domain -role <role> -comment <comment> [-is-ldap- fastbind true]</pre> |

Para obtener una sintaxis completa del comando, consulte ["Hojas de trabajo para la autenticación de](#)

Después de terminar

Si no configuró el acceso de la controladora de dominio de AD al clúster o a la SVM, debe hacerlo antes de que la cuenta pueda acceder a la SVM.

Configuración del acceso al controlador de dominio de Active Directory

Habilite el acceso a cuenta de LDAP o NIS

Puede utilizar el `security login create` Comando para habilitar cuentas de usuario LDAP o NIS para acceder a un administrador o una SVM de datos. Si no ha configurado el acceso del servidor LDAP o NIS a la SVM, debe hacerlo antes de que la cuenta pueda acceder a la SVM.

Acerca de esta tarea

- Las cuentas de grupo no son compatibles.
- Para que la cuenta pueda acceder a la SVM, debe configurar el acceso del servidor LDAP o NIS con la SVM.

Configurar el acceso a servidores LDAP o NIS

Puede realizar esta tarea antes o después de habilitar el acceso a la cuenta.

- Si no está seguro de la función de control de acceso que desea asignar a la cuenta de inicio de sesión, puede usar la `security login modify` comando para añadir el rol más adelante.

Modificar el rol asignado a un administrador

- A partir de ONTAP 9.4, la autenticación multifactor (MFA) es compatible para usuarios remotos a través de servidores LDAP o NIS.
- A partir de ONTAP 9.11.1, se puede utilizar "[Enlace rápido LDAP para la autenticación nsswitch](#)" Si es compatible con el servidor LDAP.
- Debido a un problema LDAP conocido, no debe utilizar el ' : ' (Dos puntos) carácter en cualquier campo de la información de la cuenta de usuario LDAP (por ejemplo, `gecos`, `userPassword`, y así sucesivamente). De lo contrario, la operación de búsqueda fallará para ese usuario.

Antes de empezar

Para realizar esta tarea, debe ser un administrador de clústeres.

Pasos

1. Habilite las cuentas de usuario o grupo de LDAP o NIS para acceder a una SVM:

```
security login create -vserver SVM_name -user-or-group-name user_name
-application application -authmethod nsswitch -role role -comment comment -is
-ns-switch-group yes|no [-is-ldap-fastbind true]
```

Para obtener una sintaxis completa del comando, consulte "[hoja de trabajo](#)".

"Crear o modificar cuentas de inicio de sesión"

El siguiente comando habilita la cuenta de administrador de clúster LDAP o NIS `guest2` con los predefinidos `backup` Rol para acceder a la SVM de `administradorengCluster`.

```
cluster1::>security login create -vserver engCluster -user-or-group-name
guest2 -application ssh -authmethod nsswitch -role backup
```

2. Habilitar el inicio de sesión MFA para usuarios de LDAP o NIS:

```
security login modify -user-or-group-name rem_usr1 -application ssh
-authentication-method nsswitch -role admin -is-ns-switch-group no -second
-authentication-method publickey
```

El método de autenticación se puede especificar como `publickey` y el segundo método de autenticación como `nsswitch`.

En el siguiente ejemplo, se muestra la autenticación MFA que está habilitada:

```
cluster-1::*> security login modify -user-or-group-name rem_usr2
-application ssh -authentication-method nsswitch -vserver
cluster-1 -second-authentication-method publickey"
```

Después de terminar

Si no ha configurado el acceso del servidor LDAP o NIS a la SVM, debe hacerlo antes de que la cuenta pueda acceder a la SVM.

[Configurar el acceso a servidores LDAP o NIS](#)

Gestione los roles de control de acceso

Información general sobre los roles de gestión de control de acceso

El rol asignado a un administrador determina los comandos a los que el administrador tiene acceso. La función se asigna al crear la cuenta para el administrador. Puede asignar un rol diferente o definir roles personalizados según sea necesario.

Modifique la función asignada a un administrador

Puede utilizar el `security login modify` Comando para cambiar la función de una cuenta de administrador de clúster o SVM. Puede asignar un rol predefinido o personalizado.

Antes de empezar

Para realizar esta tarea, debe ser un administrador de clústeres.

Paso

1. Cambie la función de un administrador de clúster o SVM:

```
security login modify -vserver SVM_name -user-or-group-name user_or_group_name  
-application application -authmethod authentication_method -role role -comment  
comment
```

Para obtener una sintaxis completa del comando, consulte ["hoja de trabajo"](#).

"Crear o modificar cuentas de inicio de sesión"

El siguiente comando cambia el rol de la cuenta de administrador de clúster de AD DOMAIN1\guest1 a los predefinidos readonly función.

```
cluster1::>security login modify -vserver engCluster -user-or-group-name  
DOMAIN1\guest1 -application ssh -authmethod domain -role readonly
```

El siguiente comando cambia el rol de las cuentas de administrador de SVM en la cuenta de grupo AD DOMAIN1\adgroup al personalizado vol_role función.

```
cluster1::>security login modify -vserver engData -user-or-group-name  
DOMAIN1\adgroup -application ssh -authmethod domain -role vol_role
```

Definir funciones personalizadas

Puede utilizar el `security login role create` comando para definir un rol personalizado. Puede ejecutar el comando tantas veces como sea necesario para obtener la combinación exacta de funcionalidades que desea asociar al rol.

Acerca de esta tarea

- Un rol, ya sea predefinido o personalizado, concede o deniega el acceso a los comandos o directorios de comandos de ONTAP.

Un directorio de comandos (`volume`, por ejemplo) es un grupo de comandos y subdirectorios de comandos relacionados. Excepto como se describe en este procedimiento, la concesión o denegación del acceso a un directorio de comandos otorga o deniega el acceso a cada comando del directorio y sus subdirectorios.

- El acceso a comandos específicos o al subdirectorio anula el acceso al directorio principal.

Si se define un rol con un directorio de comandos y se define de nuevo con un nivel de acceso diferente para un comando específico o para un subdirectorio del directorio principal, el nivel de acceso especificado para el comando o subdirectorio anula el nivel del primario.



No puede asignar un administrador de SVM un rol que otorga acceso a un comando o un directorio de comandos que solo esté disponible para el `admin` administrador de clúster: por ejemplo, el `security` directorio de comandos.

Antes de empezar

Para realizar esta tarea, debe ser un administrador de clústeres.

Paso

- 1. Defina un rol personalizado:

```
security login role create -vserver SVM_name -role role -cmddirname
command_or_directory_name -access access_level -query query
```

Para obtener una sintaxis completa del comando, consulte ["hoja de trabajo"](#).

Los siguientes comandos conceden el `vol_role` rol de acceso completo a los comandos de la `volume` el directorio de comandos y el acceso de sólo lectura a los comandos de la `volume snapshot` subdirectorio.

```
cluster1::>security login role create -role vol_role -cmddirname
"volume" -access all

cluster1::>security login role create -role vol_role -cmddirname "volume
snapshot" -access readonly
```

Los siguientes comandos conceden el `SVM_storage` el acceso de solo lectura de roles a los comandos de la `storage` directorio de comandos, sin acceso a los comandos de la `storage encryption` y acceso completo al subdirectorio `storage aggregate plex offline` comando no intrínseco.

```
cluster1::>security login role create -role SVM_storage -cmddirname
"storage" -access readonly

cluster1::>security login role create -role SVM_storage -cmddirname
"storage encryption" -access none

cluster1::>security login role create -role SVM_storage -cmddirname
"storage aggregate plex offline" -access all
```

Roles predefinidos para administradores de clúster

Los roles predefinidos para administradores de clúster deben cumplir con la mayoría de las necesidades. Puede crear roles personalizados según sea necesario. De manera predeterminada, un administrador de clúster asigna las opciones predefinidas `admin` función.

En la siguiente tabla, se enumeran los roles predefinidos para los administradores de clúster:

| Este rol... | Tiene este nivel de acceso... | A los siguientes comandos o directorios de comandos |
|-------------|-------------------------------|---|
| admin | todo | Todos los directorios de comandos (DEFAULT) |

| | | |
|--|--|--|
| Admin-no-fsa (disponible a partir de ONTAP 9.12.1) | Lectura/Escritura | <ul style="list-style-type: none"> • Todos los directorios de comandos (DEFAULT) • security login rest-role • security login role |
| Solo lectura | <ul style="list-style-type: none"> • security login rest-role create • security login rest-role delete • security login rest-role modify • security login rest-role show • security login role create • security login role create • security login role delete • security login role modify • security login role show • volume activity-tracking • volume analytics | Ninguno |
| volume file show-disk-usage | AutoSupport | todo |
| <ul style="list-style-type: none"> • set • system node autosupport | ninguno | Todos los demás directorios de comandos (DEFAULT) |
| Backup | todo | vserver services ndmp |
| sólo lectura | volume | ninguno |
| Todos los demás directorios de comandos (DEFAULT) | sólo lectura | todo |

| | | |
|--|---|----------|
| <ul style="list-style-type: none"> • security login password <p>Sólo para gestionar la contraseña local y la información de claves de la cuenta de usuario propia</p> <ul style="list-style-type: none"> • set | ninguno | security |
| sólo lectura | Todos los demás directorios de comandos (DEFAULT) | ninguno |



La autosupport el rol se asigna a los predefinidos autosupport Cuenta, que utiliza AutoSupport OnDemand. ONTAP le impide modificar o eliminar el autosupport cuenta. ONTAP también le impide asignar el autosupport función para otras cuentas de usuario.

Roles predefinidos para administradores de SVM

Los roles predefinidos para administradores de SVM deben cumplir con la mayoría de las necesidades. Puede crear roles personalizados según sea necesario. De manera predeterminada, un administrador de SVM asigna el valor predefinido `vsadmin` función.

En la siguiente tabla, se enumeran los roles predefinidos para los administradores de SVM:

| Nombre del rol | Funcionalidades |
|----------------|---|
| vsadmin | <ul style="list-style-type: none"> • Administrar la información de clave y la contraseña local de la cuenta de usuario propia • Gestión de volúmenes, excepto movimientos de volúmenes • Gestión de cuotas, qtrees, copias Snapshot y archivos • Gestionar las LUN • Realizar operaciones de SnapLock, excepto la eliminación con privilegios • Configuración de protocolos: NFS, SMB, iSCSI, FC, FCoE y NVMe/FC y NVMe/TCP • Servicios de configuración: DNS, LDAP y NIS • Supervisar trabajos de • Supervisar las conexiones de red y la interfaz de red • Supervisar el estado del SVM |

| | |
|-------------------|---|
| vsadmin-volumen | <ul style="list-style-type: none"> • Administrar la información de clave y la contraseña local de la cuenta de usuario propia • Gestión de volúmenes, incluidos los movimientos de volúmenes • Gestión de cuotas, qtrees, copias Snapshot y archivos • Gestionar las LUN • Configuración de protocolos: NFS, SMB, iSCSI, FC, FCoE y NVMe/FC y NVMe/TCP • Servicios de configuración: DNS, LDAP y NIS • Supervisar la interfaz de red • Supervisar el estado del SVM |
| protocolo vsadmin | <ul style="list-style-type: none"> • Administrar la información de clave y la contraseña local de la cuenta de usuario propia • Configuración de protocolos: NFS, SMB, iSCSI, FC, FCoE y NVMe/FC y NVMe/TCP • Servicios de configuración: DNS, LDAP y NIS • Gestionar las LUN • Supervisar la interfaz de red • Supervisar el estado del SVM |
| vsadmin-backup | <ul style="list-style-type: none"> • Administrar la información de clave y la contraseña local de la cuenta de usuario propia • Gestión de operaciones de NDMP • Hacer que un volumen restaurado sea de lectura/escritura • Gestionar las relaciones de SnapMirror y las copias de Snapshot • Visualización de información de volúmenes y de red |

| | |
|------------------|--|
| vsadmin-snaplock | <ul style="list-style-type: none"> • Administrar la información de clave y la contraseña local de la cuenta de usuario propia • Gestión de volúmenes, excepto movimientos de volúmenes • Gestión de cuotas, qtrees, copias Snapshot y archivos • Realizar operaciones de SnapLock, incluida la eliminación con privilegios • Configurar protocolos: NFS y SMB • Servicios de configuración: DNS, LDAP y NIS • Supervisar trabajos de • Supervisar las conexiones de red y la interfaz de red |
| vsadmin-readonly | <ul style="list-style-type: none"> • Administrar la información de clave y la contraseña local de la cuenta de usuario propia • Supervisar el estado del SVM • Supervisar la interfaz de red • Ver volúmenes y LUN • Servicios y protocolos de visualización |

Control del acceso de administradores

El rol asignado a un administrador determina qué funciones puede realizar el administrador con System Manager. Los roles predefinidos para los administradores de clúster y los administradores de máquinas virtuales de almacenamiento son provistos por System Manager. Puede asignar la función al crear la cuenta del administrador o asignar una función diferente más adelante.

En función de cómo haya habilitado el acceso a cuentas, es posible que deba realizar cualquiera de las siguientes acciones:


- Asociar una clave pública a una cuenta local.
- Instale un certificado digital de servidor firmado por CA.
- Configure el acceso AD, LDAP o NIS.

Puede ejecutar estas tareas antes o después de habilitar el acceso a la cuenta.

Asignación de un rol a un administrador

Asigne un rol a un administrador, como se indica a continuación:

Pasos

1. Seleccione **Cluster > Settings**.
2. Seleccione  Junto a **usuarios y roles**.

3. Seleccione **+ Add** En **usuarios**.
4. Especifique un nombre de usuario y seleccione un rol en el menú desplegable **rol**.
5. Especifique un método de inicio de sesión y una contraseña para el usuario.

Cambiar el rol de un administrador

Cambie el rol de un administrador, como se indica a continuación:

Pasos

1. Haga clic en **clúster > Configuración**.
2. Seleccione el nombre de usuario cuyo rol desea cambiar y haga clic en el **:** que aparece junto al nombre de usuario.
3. Haga clic en **Editar**.
4. Seleccione un rol en el menú desplegable para **rol**.

Administrar cuentas de administrador

Información general sobre las cuentas de administrador

En función de cómo haya habilitado el acceso a una cuenta, puede que deba asociar una clave pública a una cuenta local, instalar un certificado digital de servidor firmado por CA o configurar AD, LDAP o NIS. Es posible realizar todas estas tareas antes o después de habilitar el acceso a la cuenta.

Asociar una clave pública a una cuenta de administrador

Para la autenticación de clave pública SSH, debe asociar la clave pública a una cuenta de administrador para que la cuenta pueda acceder a la SVM. Puede utilizar el `security login publickey create` comando para asociar una clave a una cuenta de administrador.

Acerca de esta tarea

Si autentica una cuenta a través de SSH tanto con una contraseña como con una clave pública SSH, la cuenta se autentica primero con la clave pública.

Antes de empezar

- Debe haber generado la clave SSH.
- Debe ser un administrador de clúster o de SVM para ejecutar esta tarea.

Pasos

1. Asociar una clave pública a una cuenta de administrador:

```
security login publickey create -vserver SVM_name -username user_name -index  
index -publickey certificate -comment comment
```

Para obtener una sintaxis completa del comando, consulte la referencia de la hoja de datos de ["Asociación de una clave pública con una cuenta de usuario"](#).

2. Verifique el cambio visualizando la clave pública:

```
security login publickey show -vserver SVM_name -username user_name -index index
```

Ejemplo

El siguiente comando asocia una clave pública con la cuenta de administrador de SVM `svmin1` Para la SVM `engData1`. A la clave pública se le asigna el número de índice 5.

```
cluster1::> security login publickey create -vserver engData1 -username svmin1 -index 5 -publickey "<key text>"
```

Gestione claves públicas SSH y certificados X,509 para una cuenta de administrador

Para una mayor seguridad de autenticación SSH con cuentas de administrador, puede utilizar el `security login publickey` Conjunto de comandos para administrar la clave pública SSH y su asociación con certificados X,509.

Asocie una clave pública y un certificado X,509 a una cuenta de administrador

A partir de ONTAP 9.13.1, puede asociar un certificado X,509 a la clave pública asociada a la cuenta de administrador. Esto le proporciona la seguridad añadida de las comprobaciones de caducidad o revocación de certificados al iniciar sesión SSH para esa cuenta.

Acerca de esta tarea

Si autentica una cuenta a través de SSH con una clave pública SSH y un certificado X,509, ONTAP comprueba la validez del certificado X,509 antes de autenticarse con la clave pública SSH. El inicio de sesión SSH se rechazará si ese certificado caduca o se revoca y la clave pública se deshabilitará automáticamente.

Antes de empezar

- Debe ser un administrador de clúster o de SVM para ejecutar esta tarea.
- Debe haber generado la clave SSH.
- Si solo necesita que el certificado X,509 sea verificado para su vencimiento, puede usar un certificado autofirmado.
- Si necesita que el certificado X,509 sea comprobado para su vencimiento y revocación:
 - Debe haber recibido el certificado de una CA.
 - Debe instalar la cadena de certificados (certificados de CA intermedios y raíz) mediante `security certificate install` comandos.
 - Debe habilitar OCSP para SSH. Consulte ["Verifique que los certificados digitales sean válidos mediante OCSP"](#) si desea obtener instrucciones.

Pasos

1. Asocie una clave pública y un certificado X,509 a una cuenta de administrador:

```
security login publickey create -vserver SVM_name -username user_name -index index -publickey certificate -x509-certificate install
```

Para obtener una sintaxis completa del comando, consulte la referencia de la hoja de datos de ["Asociación de una clave pública con una cuenta de usuario"](#).

2. Verifique el cambio visualizando la clave pública:

```
security login publickey show -vserver SVM_name -username user_name -index index
```

Ejemplo

El siguiente comando asocia una clave pública y un certificado X,509 con la cuenta de administrador de SVM svmin2 Para la SVM engData2. A la clave pública se le asigna el número de índice 6.

```
cluster1::> security login publickey create -vserver engData2 -username svmin2 -index 6 -publickey "<key text>" -x509-certificate install
Please enter Certificate: Press <Enter> when done
<certificate text>
```

Elimine la asociación de certificados de la clave pública SSH para una cuenta de administrador

Puede eliminar la asociación de certificados actual de la clave pública SSH de la cuenta, mientras conserva la clave pública.

Antes de empezar

Debe ser un administrador de clúster o de SVM para ejecutar esta tarea.

Pasos

1. Elimine la asociación de certificados X,509 de una cuenta de administrador y conserve la clave pública SSH existente:

```
security login publickey modify -vserver SVM_name -username user_name -index index -x509-certificate delete
```

2. Verifique el cambio visualizando la clave pública:

```
security login publickey show -vserver SVM_name -username user_name -index index
```

Ejemplo

El siguiente comando quita la asociación de certificados X,509 de la cuenta de administrador de SVM svmin2 Para la SVM engData2 en el índice número 6.

```
cluster1::> security login publickey modify -vserver engData2 -username svmin2 -index 6 -x509-certificate delete
```

Elimine la asociación de clave pública y certificado de una cuenta de administrador

Puede eliminar la configuración de clave pública y certificado actual de una cuenta.

Antes de empezar

Debe ser un administrador de clúster o de SVM para ejecutar esta tarea.

Pasos

1. Elimine la clave pública y una asociación de certificados X,509 de una cuenta de administrador:

```
security login publickey delete -vserver SVM_name -username user_name -index index
```

2. Verifique el cambio visualizando la clave pública:

```
security login publickey show -vserver SVM_name -username user_name -index index
```

Ejemplo

El siguiente comando quita una clave pública y un certificado X,509 de la cuenta de administrador de SVM svmadmin3 Para la SVM engData3 en el índice número 7.

```
cluster1::> security login publickey delete -vserver engData3 -username svmadmin3 -index 7
```

Configurar Cisco Duo 2FA para inicios de sesión SSH

A partir de ONTAP 9.14.1, puede configurar ONTAP para que use Cisco Duo para la autenticación de dos factores (2FA) durante los inicios de sesión SSH. Se configura Duo a nivel de clúster y se aplica a todas las cuentas de usuario de forma predeterminada. También puede configurar Duo a nivel del equipo virtual de almacenamiento (anteriormente denominado Vserver), en cuyo caso sólo se aplica a los usuarios para dicho equipo virtual de almacenamiento. Si habilita y configura DUO, sirve como un método de autenticación adicional, que complementa los métodos existentes para todos los usuarios.

Si habilita la autenticación Duo para los inicios de sesión SSH, los usuarios tendrán que inscribir un dispositivo la próxima vez que inicien sesión con SSH. Para obtener información sobre la inscripción, consulte el Cisco Duo ["documentación de inscripción"](#).

Puede utilizar la interfaz de línea de comandos de ONTAP para realizar las siguientes tareas con Cisco Duo:

- [Configurar Cisco Duo](#)
- [Cambie la configuración de Cisco Duo](#)
- [Elimine la configuración de Cisco Duo](#)
- [Vea la configuración de Cisco Duo](#)
- [Eliminar un grupo Duo](#)

- [Ver grupos Duo](#)
- [Omitir autenticación Duo para usuarios](#)

Configurar Cisco Duo

Puede crear una configuración de Cisco Duo para todo el clúster o para un equipo virtual de almacenamiento específico (denominado Vserver en la CLI de ONTAP) mediante el `security login duo create` comando. Cuando hace esto, Cisco Duo se habilita para inicios de sesión SSH para este clúster o máquina virtual de almacenamiento.

Pasos

1. Inicie sesión en el panel de administración de Cisco Duo.
2. Vaya a **Aplicaciones > Aplicación UNIX**.
3. Registre la clave de integración, la clave secreta y el nombre de host de la API.
4. Inicie sesión en su cuenta de ONTAP con SSH.
5. Habilite la autenticación de Cisco Duo para esta VM de almacenamiento, sustituyendo la información de su entorno por los valores entre paréntesis:

```
security login duo create \  
-vserver <STORAGE_VM_NAME> \  
-integration-key <INTEGRATION_KEY> \  
-secret-key <SECRET_KEY> \  
-apihost <API_HOSTNAME>
```

Para obtener más información sobre los parámetros necesarios y opcionales para este comando, consulte ["Hojas de cálculo para la autenticación del administrador y la configuración de RBAC"](#).

Cambie la configuración de Cisco Duo

Puede cambiar la forma en que Cisco Duo autentica a los usuarios (por ejemplo, cuántas peticiones de datos de autenticación se dan o qué proxy HTTP se utiliza). Si necesita cambiar la configuración de Cisco Duo para un equipo virtual de almacenamiento (conocido como Vserver en la CLI de ONTAP), puede utilizar el `security login duo modify` comando.

Pasos

1. Inicie sesión en el panel de administración de Cisco Duo.
2. Vaya a **Aplicaciones > Aplicación UNIX**.
3. Registre la clave de integración, la clave secreta y el nombre de host de la API.
4. Inicie sesión en su cuenta de ONTAP con SSH.
5. Cambie la configuración de Cisco Duo para esta máquina virtual de almacenamiento, sustituyendo la información actualizada de su entorno por los valores entre paréntesis:

```
security login duo modify \  
-vserver <STORAGE_VM_NAME> \  
-integration-key <INTEGRATION_KEY> \  
-secret-key <SECRET_KEY> \  
-apihost <API_HOSTNAME> \  
-pushinfo true|false \  
-http-proxy <HTTP_PROXY_URL> \  
-autopush true|false \  
-prompts 1|2|3 \  
-max-unenrolled-logins <NUM_LOGINS> \  
-is-enabled true|false \  
-fail-mode safe|secure
```

Elimine la configuración de Cisco Duo

Puede eliminar la configuración de Cisco Duo, que eliminará la necesidad de que los usuarios de SSH se autenticquen mediante Duo al iniciar sesión. Para eliminar la configuración de Cisco Duo para un equipo virtual de almacenamiento (denominado Vserver en la CLI de ONTAP), puede utilizar el `security login duo delete` comando.

Pasos

1. Inicie sesión en su cuenta de ONTAP con SSH.
2. Elimine la configuración de Cisco Duo para esta máquina virtual de almacenamiento y sustituya el nombre de máquina virtual de almacenamiento para `<STORAGE_VM_NAME>`:

```
security login duo delete -vserver <STORAGE_VM_NAME>
```

De este modo se elimina de forma permanente la configuración de Cisco Duo para este equipo virtual de almacenamiento.

Vea la configuración de Cisco Duo

Puede ver la configuración existente de Cisco Duo para un equipo virtual de almacenamiento (denominado Vserver en la CLI de ONTAP) mediante el `security login duo show` comando.

Pasos

1. Inicie sesión en su cuenta de ONTAP con SSH.
2. Muestre la configuración de Cisco Duo para esta máquina virtual de almacenamiento. Opcionalmente, puede utilizar la `vserver` Parámetro para especificar una máquina virtual de almacenamiento, en lugar del nombre de la máquina virtual de almacenamiento para `<STORAGE_VM_NAME>`:

```
security login duo show -vserver <STORAGE_VM_NAME>
```

Debería ver una salida similar a la siguiente:

```
Vserver: testcluster
Enabled: true

Status: ok
INTEGRATION-KEY: DI89811J9JWMJCCO7IOH
SKEY SHA Fingerprint:
b79ffa4b1c50b1c747fbacdb34g671d4814
API Host: api-host.duosecurity.com
Autopush: true
Push info: true
Failmode: safe
Http-proxy: 192.168.0.1:3128
Prompts: 1
Comments: -
```

Cree un grupo Duo

Puede indicar a Cisco Duo que incluya solo los usuarios de un determinado Active Directory, LDAP o grupo de usuarios local en el proceso de autenticación Duo. Si crea un grupo Duo, sólo se solicita la autenticación Duo a los usuarios de ese grupo. Puede crear un grupo Duo mediante `security login duo group create` comando. Al crear un grupo, opcionalmente puede excluir usuarios específicos de ese grupo del proceso de autenticación Duo.

Pasos

1. Inicie sesión en su cuenta de ONTAP con SSH.
2. Cree el grupo DUO, sustituyendo la información del entorno por los valores entre paréntesis. Si omite `-vserver` parámetro, el grupo se crea en el nivel de clúster:

```
security login duo group create -vserver <STORAGE_VM_NAME> -group-name
<GROUP_NAME> -exclude-users <USER1, USER2>
```

El nombre del grupo Duo debe coincidir con un directorio activo, LDAP o grupo local. Usuarios que especifique con el opcional `-exclude-users` El parámetro no se incluirá en el proceso de autenticación Duo.

Ver grupos Duo

Puede ver las entradas de grupo Cisco Duo existentes mediante el `security login duo group show` comando.

Pasos

1. Inicie sesión en su cuenta de ONTAP con SSH.
2. Muestra las entradas del grupo Duo, sustituyendo la información del entorno por los valores entre paréntesis. Si omite `-vserver` parámetro, el grupo se muestra en el nivel de clúster:


```
security login duo group show -vserver <STORAGE_VM_NAME> -group-name  
<GROUP_NAME> -exclude-users <USER1, USER2>
```

El nombre del grupo Duo debe coincidir con un directorio activo, LDAP o grupo local. Usuarios que especifique con el opcional `-exclude-users` no se mostrará el parámetro.

Eliminar un grupo Duo

Puede eliminar una entrada de grupo Duo mediante `security login duo group delete` comando. Si elimina un grupo, los usuarios de ese grupo ya no se incluirán en el proceso de autenticación Duo.

Pasos

1. Inicie sesión en su cuenta de ONTAP con SSH.
2. Elimine la entrada de grupo Duo, sustituyendo la información de su entorno por los valores entre paréntesis. Si omite `-vserver` parámetro, el grupo se elimina en el nivel de clúster:

```
security login duo group delete -vserver <STORAGE_VM_NAME> -group-name  
<GROUP_NAME>
```

El nombre del grupo Duo debe coincidir con un directorio activo, LDAP o grupo local.

Omitir autenticación Duo para usuarios

Puede excluir a todos los usuarios o usuarios específicos del proceso de autenticación Duo SSH.

Excluir todos los usuarios de DUO

Puede deshabilitar la autenticación SSH de Cisco Duo para todos los usuarios.

Pasos

1. Inicie sesión en su cuenta de ONTAP con SSH.
2. Desactive la autenticación de Cisco Duo para usuarios SSH, sustituyendo el nombre de Vserver por `<STORAGE_VM_NAME>`:

```
security login duo -vserver <STORAGE_VM_NAME> -is-duo-enabled=false
```

Excluir usuarios del grupo DUO

Puede excluir ciertos usuarios que forman parte de un grupo Duo del proceso de autenticación Duo SSH.

Pasos

1. Inicie sesión en su cuenta de ONTAP con SSH.
2. Desactive la autenticación de Cisco Duo para usuarios específicos de un grupo. Sustituya el nombre de grupo y la lista de usuarios para excluir los valores entre paréntesis:

```
security login group modify -group-name <GROUP_NAME> -exclude-users
<USER1, USER2>
```

El nombre del grupo Duo debe coincidir con un directorio activo, LDAP o grupo local. Usuarios que especifique con `-exclude-users` El parámetro no se incluirá en el proceso de autenticación Duo.

Excluir usuarios locales de DUO

Puede excluir a usuarios locales específicos del uso de la autenticación Duo mediante el panel de administración de Cisco Duo. Para obtener instrucciones, consulte "[Documentación de Cisco Duo](#)".

Genere e instale una información general de certificados de servidor firmados por CA

En los sistemas de producción, se recomienda instalar un certificado digital firmado por CA para usarlo en la autenticación del clúster o SVM como servidor SSL. Puede utilizar el `security certificate generate-csr` Para generar una solicitud de firma de certificación (CSR) y la `security certificate install` comando para instalar el certificado que recibe de la autoridad de certificación.

Genere una solicitud de firma de certificación

Puede utilizar el `security certificate generate-csr` Comando para generar una solicitud de firma de certificación (CSR). Después de procesar la solicitud, la entidad de certificación (CA) envía el certificado digital firmado.

Antes de empezar

Debe ser un administrador de clúster o de SVM para ejecutar esta tarea.

Pasos

1. Genere una CSR:

```
security certificate generate-csr -common-name FQDN_or_common_name -size
512|1024|1536|2048 -country country -state state -locality locality
-organization organization -unit unit -email-addr email_of_contact -hash
-function SHA1|SHA256|MD5
```

El siguiente comando crea un CSR con una clave privada de 2048 bits generada por la función de hash «SHA256» para su uso por el grupo «Software» en el departamento «IT» de una empresa cuyo nombre común personalizado es «`server1.companyname.com``», ubicada en Sunnyvale, California, EE.UU. La dirección de correo electrónico del administrador de contacto de SVM es «`web@example.com`». El sistema muestra la CSR y la clave privada en la salida.

Ejemplo de creación de una CSR

```
cluster1::>security certificate generate-csr -common-name  
server1.companyname.com -size 2048 -country US -state California  
-locality Sunnyvale -organization IT -unit Software -email-addr  
web@example.com -hash-function SHA256
```

Certificate Signing Request :

-----BEGIN CERTIFICATE REQUEST-----

```
MIIBGjCBxQIBADBgMRQWEgYDVQQDEwtleGFtcGxlLmNvbTELMakGA1UEBhMCVVMx  
CTAHBgNVBAgTADAEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBgNVBAStADEPMA0G  
CSqGSIB3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApTlnzS  
xOcxixqImRRGZCR7tVmTYyqPSuTvfVtWdJbmXuj6U3alwoUsb13wfEvQnHVFNCi  
2ninsJ8CAwEAAaAAMA0GCSqGSIB3DQEBChUAA0EA6EagLfso5+4g+ejiRKKTUPQO  
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==  
-----END CERTIFICATE REQUEST-----
```

Private Key :

-----BEGIN RSA PRIVATE KEY-----

```
MIIBOwIBAAJBAPXFanNoJApTlnzSxOcxixqImRRGZCR7tVmTYyqPSuTvfVtWdJb  
mXuj6U3alwoUsb13wfEvQnHVFNCi2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQlu  
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgPv+p5kaZTTM  
gQIhAPsp+j1hrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehAiEA+oDbOooWlVvu  
xj4aitxVBu6ByVckYU8LbsfeRNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NCtEYxd0Q5  
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsKO077itF+h9FGFNHbtuNTrVq4vPW3nAiAA  
peMBQgEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==  
-----END RSA PRIVATE KEY-----
```

Note: Please keep a copy of your certificate request and private key for future reference.

2. Copie la solicitud de certificado de la salida CSR y envíela en formato electrónico (por ejemplo, correo electrónico) a una CA de terceros de confianza para su firma.

Después de procesar la solicitud, la CA envía el certificado digital firmado. Debe conservar una copia de la clave privada y el certificado digital firmado por la CA.

Instale un certificado de servidor firmado por CA

Puede utilizar el `security certificate install` Comando para instalar un certificado de servidor firmado por CA en una SVM. ONTAP solicita los certificados raíz y intermedios de la entidad de certificación (CA) que forman la cadena de certificados del certificado de servidor.

Antes de empezar

Debe ser un administrador de clúster o de SVM para ejecutar esta tarea.

Paso

1. Instale un certificado de servidor firmado por CA:

```
security certificate install -vserver SVM_name -type certificate_type
```

Para obtener una sintaxis completa del comando, consulte ["hoja de trabajo"](#).



ONTAP solicita los certificados intermedios y de raíz de CA que forman la cadena de certificados del certificado de servidor. La cadena comienza con el certificado de la CA que emitió el certificado de servidor y puede llegar hasta el certificado raíz de la CA. Cualquier certificado intermedio que falte provocará el error en la instalación del certificado de servidor.

El siguiente comando instala el certificado de servidor firmado por CA y los certificados intermedios en SVM 'engData2'.

Ejemplo de instalación de certificados intermedios de certificado de servidor firmados por CA

```
cluster1::>security certificate install -vserver engData2 -type
server
Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIB8TCCA ZugAwIBAwIBADANBgkqhkiG9w0BAQQFADBfMRMwEQYDVQQDEwpuZXRh
cHAuY29tMQswCQYDVQQGEwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNV
BAoTADAEJMAcGA1UECXMAMQ8wDQYJKoZIhvcNAQkBFgAwHhcNMTAwNDI2MTk0OTI4
WhcNMTAwNTI2MTk0OTI4WjBfMRMwEQYDVQQDEwpuZXRhcHAuY29tMQswCQYDVQQG
EwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNVBAoTADAEJMAcGA1UECXM
AMQ8wDQYJKoZIhvcNAQkBFgAwXDANBgkqhkiG9w0BAQEFAANLADBIaKEAyXrK2sry
-----END CERTIFICATE-----
```

```
Please enter Private Key: Press <Enter> when done
-----BEGIN RSA PRIVATE KEY-----
MIIBPAIBAAJBAMl6ytrK8nQj82UsWeHOeT8gk0BPX+Y5MLyCsUdXA7hXhumHNpvF
C6lX2G32Sx8VEalth94tx+vOEzq+UaqHlt0CAwEAAQJBAMZjDWlgmlm3qIr/n8VT
PFnnZnbVcXVM70tbUsgPKw+QCCh9dF1jmuQKeDr+wUMWkn1DeGrfhILpzfJGHRlJ
z7UCIQDr8d3gOG7lUyX+BbFmo/N0uAKjS2cvUU+Y8a8pDxGLLwIhANqa99SuS18U
DiPvdaKTj6+EcGuXfCXz+G0rfgTZK8uzAiEArlmnrfYC8KwE9k7A0ylRzBLdUwK9
AvuJDn+/z+H1Bd0CIQDD93P/xpaJETNz53Au49VE5Jba/Jugckrbosd/lSd7nQIG
aEMAzt6qHHT4mndi8Bo8sDGedG2SKx6Qbn2IpuNZ7rc=
-----END RSA PRIVATE KEY-----
```

Do you want to continue entering root and/or intermediate
certificates {y|n}: y

```
Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIE+zCCBGSGAwIBAgICAQ0wDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBACGTG1Zh
bGlDZXJ0IFZhbGlkYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIElu
Yy4xNTAzBgNVBAsTTFZhbGlDZXJ0IENsYXNzIDIGUG9saWN5IFZhbGlkYXRpb24g
QXV0aG9yaXR5MSEwHwYDVQQDExhodHRwOi8vd3d3LnZhbGljZXJ0LmNvbS8xIDAe
BgkqhkiG9w0BCQEWEluZm9AdmFsaWNlcnQuY29tMB4XDTA0MDYyOTE3MDYyMFoX
DTI0MDYyOTE3MDYyMFowYzELMAkGA1UEBhMCVVMxITAfBgNVBAoTGFROZSBHbyBE
YWRkeSBHcm91cCwgSW5jLjExMC8GA1UECXMOR28gRGFkZkhkgQ2xhc3MgMiBDZXJ0
-----END CERTIFICATE-----
```

Do you want to continue entering root and/or intermediate
certificates {y|n}: y

```
Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
```

```
MIIC5zCCAlACAQEwDQYJKoZIhvcNAQEFBQAwbgsxJDAiBgNVBACzG1ZhbGlDZXJ0
IFZhbGlkYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAz
BgNVBAsTTFZhbGlDZXJ0IENsYXNzIDIGUG9saWN5IFZhbGlkYXRpb24gQXV0aG9y
aXR5MSEwHwYDVQQDEzhodHRwOi8vd3d3LnZhbGljZXJ0LmNvbS8xIDAeBgkqhkiG
9w0BCQEWEluZm9AdmFsaWNlcnQuY29tMB4XDTE5MDYyNjAwMTk1NFoXDTE5MDYy
NjAwMTk1NFowgbsxJDAiBgNVBACzG1ZhbGlDZXJ0IFZhbGlkYXRpb24gTmV0d29y
azEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAzBgNVBAsTTFZhbGlDZXJ0IENs
YXNzIDIGUG9saWN5IFZhbGlkYXRpb24gQXV0aG9yaXR5MSEwHwYDVQQDEzhodHRw
-----END CERTIFICATE-----
```

Do you want to continue entering root and/or intermediate
certificates {y|n}: n

You should keep a copy of the private key and the CA-signed digital
certificate for future reference.

Gestione los certificados con System Manager

A partir de ONTAP 9.10.1, se puede utilizar System Manager para gestionar autoridades de certificados de confianza, certificados de cliente/servidor y autoridades de certificados locales (integradas).

Con System Manager, puede gestionar los certificados recibidos de otras aplicaciones para que pueda autenticar las comunicaciones de dichas aplicaciones. También puede administrar sus propios certificados que identifican su sistema a otras aplicaciones.

Ver información del certificado

Con System Manager, es posible ver las autoridades de certificados de confianza, los certificados de cliente/servidor y las autoridades de certificados locales almacenadas en el clúster.

Pasos

1. En System Manager, seleccione **Cluster > Settings**.
2. Desplácese hasta el área **Seguridad**.
En la sección **certificados**, se muestran los siguientes detalles:
 - El número de autoridades de certificados de confianza almacenadas.
 - El número de certificados de cliente/servidor almacenados.
 - El número de autoridades de certificados locales almacenadas.
3. Seleccione cualquier número para ver los detalles de una categoría de certificados o seleccione → Para abrir la página **Certificados**, que contiene información sobre todas las categorías.
La lista muestra la información del clúster completo. Si desea mostrar información solo de una máquina virtual de almacenamiento específica, realice los pasos siguientes:
 - a. Seleccione **Almacenamiento > Storage VMs**.
 - b. Seleccione la máquina virtual de almacenamiento.

- c. Cambie a la pestaña **Settings**.
- d. Seleccione un número que se muestra en la sección **Certificado**.

Qué hacer a continuación

- Desde la página **certificados**, puede [Genere una solicitud de firma de certificación](#).
- La información del certificado se divide en tres fichas, una para cada categoría. Es posible realizar las siguientes tareas desde cada pestaña:

| En esta pestaña... | Puede ejecutar estos procedimientos... |
|---|---|
| Autoridades de certificados de confianza | <ul style="list-style-type: none"> • [install-trusted-cert] • Elimine una entidad de certificación de confianza • Renueve una entidad de certificación de confianza |
| Certificados cliente/servidor | <ul style="list-style-type: none"> • [install-cs-cert] • [gen-cs-cert] • [delete-cs-cert] • [renew-cs-cert] |
| Autoridades de certificados locales | <ul style="list-style-type: none"> • Cree una nueva entidad de certificación local • Firme un certificado mediante una entidad de certificación local • Elimine una entidad de certificación local • Renueve una autoridad de certificación local |

Genere una solicitud de firma de certificación

Puede generar una solicitud de firma de certificación (CSR) con System Manager desde cualquier pestaña de la página **certificados**. Se genera una clave privada y una CSR correspondiente, que se pueden firmar mediante una autoridad de certificación para generar un certificado público.


Pasos

1. Abra la página **certificados**. Consulte [Ver información del certificado](#).
2. Seleccione **+Generar CSR**.
3. Complete la información del nombre del asunto:
 - a. Introduzca un **nombre común**.
 - b. Seleccione un **país**.
 - c. Introduzca una **organización**.
 - d. Introduzca una **unidad organizativa**.
4. Si desea anular los valores predeterminados, seleccione **más opciones** y proporcione información adicional.

Instale (añada) una entidad de certificación de confianza

Puede instalar autoridades de certificado de confianza adicionales en System Manager.

Pasos

1. Abra la pestaña **autoridades de certificados de confianza**. Consulte [Ver información del certificado](#).
2. Seleccione  .
3. En el panel **Agregar autoridad de certificado de confianza**, realice lo siguiente:
 - Introduzca un **nombre**.
 - Para **Scope**, seleccione un equipo virtual de almacenamiento.
 - Introduzca un **nombre común**.
 - Seleccione un **tipo**.
 - Introduzca o importe **detalles del certificado**.


Elimine una entidad de certificación de confianza

Con System Manager, es posible eliminar una entidad de certificación de confianza.



No puede eliminar las autoridades de certificación de confianza preinstaladas con ONTAP.


Pasos

1. Abra la pestaña **autoridades de certificados de confianza**. Consulte [Ver información del certificado](#).
2. Seleccione el nombre de la entidad de certificación de confianza.
3. Seleccione  Junto al nombre, luego selecciona **Eliminar**.

Renueve una entidad de certificación de confianza

Con System Manager, puede renovar una entidad de certificación de confianza que ha caducado o está a punto de expirar.

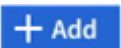
Pasos

1. Abra la pestaña **autoridades de certificados de confianza**. Consulte [Ver información del certificado](#).
2. Seleccione el nombre de la entidad de certificación de confianza.
3. Seleccione  Junto al nombre del certificado, luego **Renew**.

Instale (agregue) un certificado de cliente/servidor

Con System Manager, puede instalar certificados de cliente/servidor adicionales.

Pasos

1. Abra la ficha **certificados cliente/servidor**. Consulte [Ver información del certificado](#).
2. Seleccione  .
3. En el panel **Agregar certificado de cliente/servidor**, realice lo siguiente:
 - Introduzca un **nombre de certificado**.
 - Para **Scope**, seleccione un equipo virtual de almacenamiento.
 - Introduzca un **nombre común**.
 - Seleccione un **tipo**.
 - Introduzca o importe **detalles del certificado**.

Puede escribir o copiar y pegar los detalles del certificado desde un archivo de texto o puede importar el texto desde un archivo de certificado haciendo clic en **Importar**.

- Introduzca la **clave privada**.

Puede escribir o copiar y pegar en la clave privada desde un archivo de texto o puede importar el texto desde un archivo de claves privadas haciendo clic en **Importar**.

Genere (agregue) un certificado de cliente/servidor autofirmado

Con System Manager, puede generar otros certificados de cliente/servidor autofirmados.


Pasos

1. Abra la ficha **certificados cliente/servidor**. Consulte [Ver información del certificado](#).
2. Seleccione **+Generar certificado autofirmado**.
3. En el panel **generar certificado autofirmado**, realice lo siguiente:
 - Introduzca un **nombre de certificado**.
 - Para **Scope**, seleccione un equipo virtual de almacenamiento.
 - Introduzca un **nombre común**.
 - Seleccione un **tipo**.
 - Seleccione una función **hash**.
 - Seleccione un **tamaño de clave**.
 - Seleccione una **VM de almacenamiento**.

Eliminar un certificado de cliente/servidor

Con System Manager, puede eliminar certificados de cliente/servidor.


Pasos

1. Abra la ficha **certificados cliente/servidor**. Consulte [Ver información del certificado](#).
2. Seleccione el nombre del certificado de cliente/servidor.
3. Seleccione  Junto al nombre, haga clic en **Eliminar**.

Renueve un certificado de cliente/servidor

Con System Manager, puede renovar un certificado de cliente/servidor que ha caducado o está a punto de expirar.

Pasos


1. Abra la ficha **certificados cliente/servidor**. Consulte [Ver información del certificado](#).
2. Seleccione el nombre del certificado de cliente/servidor.
3. Seleccione  Junto al nombre, haga clic en **renovar**.

Cree una nueva entidad de certificación local

Con System Manager, es posible crear una nueva entidad de certificación local.

Pasos


1. Abra la ficha **autoridades de certificado local**. Consulte [Ver información del certificado](#).

2. Seleccione  .
3. En el panel **Agregar autoridad de certificación local**, realice lo siguiente:
 - Introduzca un **nombre**.
 - Para **Scope**, seleccione un equipo virtual de almacenamiento.
 - Introduzca un **nombre común**.
4. Si desea anular los valores predeterminados, seleccione **más opciones** y proporcione información adicional.

Firme un certificado mediante una entidad de certificación local

En System Manager, es posible usar una entidad de certificación local para firmar un certificado.


Pasos

1. Abra la ficha **autoridades de certificado local**. Consulte [Ver información del certificado](#).
2. Seleccione el nombre de la autoridad de certificación local.
3. Seleccione  Junto al nombre luego **Firma un certificado**.
4. Complete el formulario **firmar una solicitud de firma de certificado**.
 - Puede pegar el contenido de firma de certificados o importar un archivo de solicitud de firma de certificados haciendo clic en **Importar**.
 - Especifique el número de días para los que será válido el certificado.

Elimine una entidad de certificación local

Con System Manager, es posible eliminar una entidad de certificación local.


Pasos

1. Abra la ficha **Autoridad de certificado local**. Consulte [Ver información del certificado](#).
2. Seleccione el nombre de la autoridad de certificación local.
3. Seleccione  Junto al nombre luego **Eliminar**.

Renueve una autoridad de certificación local

Con System Manager, puede renovar una autoridad de certificado local que ha caducado o está a punto de expirar.

Pasos

1. Abra la ficha **Autoridad de certificado local**. Consulte [Ver información del certificado](#).
2. Seleccione el nombre de la autoridad de certificación local.
3. Seleccione  Junto al nombre, haga clic en **renovar**.

Configurar la información general de acceso al controlador de dominio de Active Directory

Para poder acceder a la SVM, es necesario configurar el acceso de la controladora de dominio de AD al clúster o a la SVM. Si ya ha configurado un servidor SMB para una SVM de datos, puede configurar la SVM como puerta de enlace, o *tunnel*, para el acceso de AD al clúster. Si no configuró un servidor SMB, puede crear una cuenta de equipo

para la SVM en el dominio de AD.

ONTAP admite los siguientes servicios de autenticación de controladores de dominio:

- Kerberos
- LDAP
- Netlogon
- Autoridad de seguridad local (LSA)

ONTAP admite los siguientes algoritmos de clave de sesión para conexiones seguras de Netlogon:

| Algoritmo de clave de sesión | Disponible empezando por... |
|---|--------------------------------|
| HMAC-SHA256, basado en el estándar de cifrado avanzado (AES) Si el clúster ejecuta ONTAP 9.9.1 o una versión anterior y el controlador de dominio aplica AES para los servicios seguros de Netlogon, la conexión falla. En este caso, debe reconfigurar el controlador de dominio para aceptar conexiones de clave fuerte con ONTAP. | ONTAP 9.10.1 |
| DES y HMAC-MD5 (cuando se establece la clave fuerte) | Todas las versiones de ONTAP 9 |

Si desea utilizar claves de sesión AES durante la creación de canal seguro Netlogon, debe verificar que AES esté habilitado en su SVM.

- A partir de ONTAP 9.14.1, AES se habilita de forma predeterminada cuando crea una SVM y no necesita modificar la configuración de seguridad de su SVM para utilizar las claves de sesión AES durante la establecimiento de canal seguro Netlogon.
- En ONTAP 9.10.1 a 9.13.1, AES se deshabilita de forma predeterminada al crear una SVM. Debe habilitar AES mediante el siguiente comando:

```
cifs security modify -vserver vs1 -aes-enabled-for-netlogon-channel true
```



Cuando se actualice a ONTAP 9.14.1 o una versión posterior, la configuración de AES para las SVM existentes creadas con versiones de ONTAP anteriores no cambiará automáticamente. Aún debe actualizar el valor de esta configuración para habilitar AES en esas SVM.

Configure un túnel de autenticación

Si ya ha configurado un servidor SMB para una SVM de datos, puede usar el `security login domain-tunnel create` Comando para configurar la SVM como puerta de enlace, o *tunnel*, para obtener acceso AD al clúster.

Antes de empezar

- Debe haber configurado un servidor SMB para una SVM de datos.

- Debe haber habilitado una cuenta de usuario de dominio de AD para acceder a la SVM de administrador para el clúster.
- Para realizar esta tarea, debe ser un administrador de clústeres.

A partir de ONTAP 9.10.1, si tiene una puerta de enlace SVM (túnel de dominio) para acceso AD, puede usar Kerberos para autenticación de administrador si ha deshabilitado NTLM en el dominio de AD. En versiones anteriores, Kerberos no era compatible con la autenticación de administrador para puertas de enlace de SVM. Esta funcionalidad está disponible de forma predeterminada; no se requiere configuración.



La autenticación Kerberos siempre se intenta primero. En caso de error, se intenta la autenticación NTLM.

Paso

1. Configure una SVM de datos habilitada para SMB como túnel de autenticación para el acceso de la controladora de dominio AD al clúster:

```
security login domain-tunnel create -vserver svm_name
```

Para obtener una sintaxis completa del comando, consulte ["hoja de trabajo"](#).



La SVM debe estar en ejecución para que el usuario se autentique.

El siguiente comando configura la SVM de datos habilitada para SMB como túnel de autenticación.

```
cluster1::>security login domain-tunnel create -vserver engData
```

Cree una cuenta de equipo SVM en el dominio

Si no ha configurado un servidor SMB para una SVM de datos, puede usar el `vserver active-directory create` Comando para crear una cuenta de equipo para la SVM en el dominio.

Acerca de esta tarea

Después de introducir el `vserver active-directory create` Se le pedirá que proporcione las credenciales de una cuenta de usuario de AD con privilegios suficientes para agregar equipos a la unidad organizativa especificada en el dominio. La contraseña de la cuenta no puede estar vacía.

Antes de empezar

Debe ser un administrador de clúster o de SVM para ejecutar esta tarea.

Paso

1. Cree una cuenta de equipo para una SVM en el dominio de AD:

```
vserver active-directory create -vserver SVM_name -account-name  
NetBIOS_account_name -domain domain -ou organizational_unit
```

Para obtener una sintaxis completa del comando, consulte ["hoja de trabajo"](#).

El siguiente comando crea una cuenta de computadora llamada 'ADSERVER1' en el dominio 'example.com' para SVM 'engData'. Se le pedirá que introduzca las credenciales de cuenta de usuario de AD después de introducir el comando.

```
cluster1::>vserver active-directory create -vserver engData -account  
-name ADSERVER1 -domain example.com
```

In order to create an Active Directory machine account, you must supply the name and password of a Windows account with sufficient privileges to add computers to the "CN=Computers" container within the "example.com" domain.

Enter the user name: Administrator

Enter the password:

Configure la información general sobre el acceso a servidores LDAP o NIS

Debe configurar el acceso del servidor LDAP o NIS a una SVM para que las cuentas LDAP o NIS puedan acceder a la SVM. La función de conmutador le permite utilizar LDAP o NIS como fuentes alternativas de servicio de nombres.

Configure el acceso al servidor LDAP

Para que las cuentas LDAP puedan acceder a la SVM, debe configurar el acceso del servidor LDAP a una SVM. Puede utilizar el `vserver services name-service ldap client create` Comando para crear una configuración de cliente LDAP en la SVM. A continuación, puede utilizar la `vserver services name-service ldap create` Comando para asociar la configuración del cliente LDAP con la SVM.

Acerca de esta tarea

La mayoría de los servidores LDAP pueden utilizar los esquemas predeterminados proporcionados por ONTAP:

- MS-AD-BIS (el esquema preferido para la mayoría de los servidores AD de Windows 2012 y posteriores)
- AD-IDMU (Windows 2008, Windows 2016 y servidores AD posteriores)
- AD-SFU (servidores Windows 2003 y anteriores de AD)
- RFC-2307 (SERVIDORES UNIX LDAP)

Es mejor utilizar los esquemas predeterminados a menos que haya un requisito para hacer lo contrario. Si es así, puede crear su propio esquema copiando un esquema predeterminado y modificando la copia. Para obtener más información, consulte:

- ["Configuración de NFS"](#)
- ["Informe técnico de NetApp 4835: Cómo configurar LDAP en ONTAP"](#)

Antes de empezar

- Debe haber instalado un ["Certificado digital de servidor firmado por CA"](#) En la SVM.
- Debe ser un administrador de clúster o de SVM para ejecutar esta tarea.

Pasos

1. Cree una configuración de cliente LDAP en una SVM:

```
vserver services name-service ldap client create -vserver SVM_name -client
-config client_configuration -servers LDAP_server_IPs -schema schema -use
-start-tls true|false
```



Start TLS es compatible únicamente para acceder a las SVM de datos. No admite el acceso a las SVM de administración.

Para obtener una sintaxis completa del comando, consulte ["hoja de trabajo"](#).

El siguiente comando crea una configuración de cliente LDAP llamada «corp» en SVM «engData». El cliente hace enlaces anónimos a los servidores LDAP con las direcciones IP 172.160.0.100 y 172.16.0.101. El cliente utiliza el esquema RFC-2307 para realizar consultas LDAP. La comunicación entre el cliente y el servidor se cifra mediante Start TLS.

```
cluster1::> vserver services name-service ldap client create
-vserver engData -client-config corp -servers 172.16.0.100,172.16.0.101
-schema RFC-2307 -use-start-tls true
```



A partir de ONTAP 9.2, el campo `-ldap-servers` reemplaza el campo `-servers`. Este nuevo campo puede tomar un nombre de host o una dirección IP para el servidor LDAP.

2. Asocie la configuración del cliente LDAP con la SVM: `vserver services name-service ldap create -vserver SVM_name -client-config client_configuration -client-enabled true|false`

Para obtener una sintaxis completa del comando, consulte ["hoja de trabajo"](#).

El siguiente comando asocia la configuración del cliente LDAP corp Con la SVM engData, Y habilita el cliente LDAP en la SVM.

```
cluster1::>vserver services name-service ldap create -vserver engData
-client-config corp -client-enabled true
```



A partir de ONTAP 9.2, el `vserver services name-service ldap create` El comando realiza una validación automática de la configuración e informa de un mensaje de error si ONTAP no puede comunicarse con el servidor de nombres.

3. Validar el estado de los servidores de nombres mediante el comando `vserver Services NAME-service ldap check`.

El siguiente comando valida los servidores LDAP en la SVM vs0.

```
cluster1::> vserver services name-service ldap check -vserver vs0

| Vserver: vs0 |
| Client Configuration Name: c1 |
| LDAP Status: up |
| LDAP Status Details: Successfully connected to LDAP server |
| "10.11.12.13". |
```

El comando `name service check` está disponible a partir de ONTAP 9.2.

Configurar el acceso al servidor NIS

Debe configurar el acceso del servidor NIS a una SVM antes de que las cuentas NIS puedan acceder a la SVM. Puede utilizar el `vserver services name-service nis-domain create` Comando para crear una configuración de dominio NIS en una SVM.

Acerca de esta tarea

Puede crear varios dominios NIS. Sólo se puede establecer un dominio NIS en `active` a la vez.

Antes de empezar

- Todos los servidores configurados deben estar disponibles y accesibles antes de configurar el dominio NIS en la SVM.
- Debe ser un administrador de clúster o de SVM para ejecutar esta tarea.

Paso

1. Cree una configuración de dominio NIS en una SVM:

```
vserver services name-service nis-domain create -vserver SVM_name -domain
client_configuration -active true|false -nis-servers NIS_server_IPs
```

Para obtener una sintaxis completa del comando, consulte ["hoja de trabajo"](#).



A partir de ONTAP 9.2, el campo `-nis-servers` reemplaza el campo `-servers`. Este nuevo campo puede tomar un nombre de host o una dirección IP para el servidor NIS.

El siguiente comando crea una configuración de dominio NIS en 'engData' de SVM. El dominio NIS `nisdomain` Está activo durante la creación y se comunica con un servidor NIS con la dirección IP `192.0.2.180`.

```
cluster1::>vserver services name-service nis-domain create
-vserver engData -domain nisdomain -active true -nis-servers 192.0.2.180
```

Crear un conmutador de servicio de nombres

La función de conmutador de servicio de nombres le permite utilizar LDAP o NIS como fuentes alternativas de servicio de nombres. Puede utilizar el `vserver services name-service ns-switch modify` para especificar el orden de búsqueda de fuentes de servicio de nombres.

Antes de empezar

- Debe haber configurado el acceso a los servidores LDAP y NIS.
- Debe ser un administrador de clúster o un administrador de SVM para ejecutar esta tarea.

Paso

1. Especifique el orden de búsqueda para los orígenes de servicios de nombres:

```
vserver services name-service ns-switch modify -vserver SVM_name -database  
name_service_switch_database -sources name_service_source_order
```

Para obtener una sintaxis completa del comando, consulte ["hoja de trabajo"](#).

El siguiente comando especifica el orden de búsqueda de los orígenes de servicios de nombres LDAP y NIS para la base de datos «passwd» en SVM «engData».

```
cluster1::>vserver services name-service ns-switch  
modify -vserver engData -database passwd -source files ldap,nis
```

Cambiar una contraseña de administrador

Debe cambiar la contraseña inicial inmediatamente después de iniciar sesión en el sistema por primera vez. Si es un administrador de SVM, puede usar el `security login password` para cambiar su propia contraseña. Si es un administrador de clúster, puede utilizar el `security login password` para cambiar la contraseña de cualquier administrador.

Acerca de esta tarea

La nueva contraseña debe respetar las siguientes reglas:

- No puede contener el nombre de usuario
- Debe tener al menos 8 caracteres
- Debe contener al menos una letra y un número
- No puede ser igual que las últimas seis contraseñas



Puede utilizar el `security login role config modify` comando para modificar las reglas de contraseña de las cuentas de asociadas con un rol determinado. Para obtener más información, consulte ["referencia de comandos"](#).

Antes de empezar

- Debe ser un administrador de clústeres o SVM para cambiar su propia contraseña.
- Para cambiar la contraseña de otro administrador, debe ser un administrador de clústeres.

Paso

1. Cambiar una contraseña de administrador: `security login password -vserver svm_name -username user_name`

El siguiente comando cambia la contraseña del administrador `admin1` Para la SVM `vs1.example.com`. Se le pedirá que introduzca la contraseña actual, a continuación, introduzca y vuelva a introducir la nueva contraseña.

```
vs1.example.com::>security login password -vserver engData -username  
admin1  
Please enter your current password:  
Please enter a new password:  
Please enter it again:
```

Bloquear y desbloquear una cuenta de administrador

Puede utilizar el `security login lock` para bloquear una cuenta de administrador y la `security login unlock` comando para desbloquear la cuenta.

Antes de empezar

Para poder realizar estas tareas, debe ser un administrador de clústeres.

Pasos

1. Bloquear una cuenta de administrador:

```
security login lock -vserver SVM_name -username user_name
```

El siguiente comando bloquea la cuenta de administrador `admin1` Para la SVM `vs1.example.com`:

```
cluster1::>security login lock -vserver engData -username admin1
```

2. Desbloquear una cuenta de administrador:

```
security login unlock -vserver SVM_name -username user_name
```

El siguiente comando desbloquea la cuenta de administrador `admin1` Para la SVM `vs1.example.com`:

```
cluster1::>security login unlock -vserver engData -username admin1
```

Gestionar intentos fallidos de inicio de sesión

Los intentos repetidos de inicio de sesión fallidos a veces indican que un intruso está intentando acceder al sistema de almacenamiento. Puede tomar una serie de pasos para asegurarse de que no se produzca una intrusión.

Cómo sabrá que los intentos de inicio de sesión han fallado

El sistema de gestión de eventos (EMS) notifica los intentos de inicio de sesión con errores cada hora. Puede encontrar un registro de intentos fallidos de inicio de sesión en `audit.log` archivo.

Qué hacer si fallan los intentos repetidos de inicio de sesión

A corto plazo, puede tomar una serie de pasos para evitar una intrusión:

- Requerir que las contraseñas estén compuestas por un número mínimo de caracteres en mayúscula, caracteres en minúscula, caracteres especiales y/o dígitos
- Imponer un retraso tras un intento de inicio de sesión fallido
- Limite el número de intentos fallidos permitidos y bloquee los usuarios después del número especificado de intentos fallidos
- Caducar y bloquee cuentas que estén inactivas durante un número determinado de días

Puede utilizar el `security login role config modify` comando para ejecutar estas tareas.

A largo plazo, puede realizar estos pasos adicionales:

- Utilice la `security ssh modify` Comando para limitar el número de intentos de inicio de sesión con errores de todas las SVM recién creadas.
- Migre las cuentas de algoritmo MD5 existentes al algoritmo SHA-512 más seguro al requerir que los usuarios cambien sus contraseñas.

Aplicar SHA-2 en contraseñas de cuenta de administrador

Las cuentas de administrador creadas antes de ONTAP 9.0 siguen utilizando contraseñas MD5 después de la actualización, hasta que las contraseñas se modifican manualmente. MD5 es menos seguro que SHA-2. Por lo tanto, después de la actualización, debería pedir a los usuarios de cuentas MD5 que cambien sus contraseñas para utilizar la función hash SHA-512 predeterminada.

Acerca de esta tarea

La funcionalidad hash de contraseña le permite hacer lo siguiente:

- Muestra las cuentas de usuario que coinciden con la función hash especificada.
- Caducar cuentas que utilizan una función hash especificada (por ejemplo, MD5), obligando a los usuarios a cambiar sus contraseñas en su siguiente inicio de sesión.
- Bloquear cuentas cuyas contraseñas utilizan la función hash especificada.
- Al volver a una versión anterior a ONTAP 9, restablezca la contraseña propia del administrador del clúster para que sea compatible con la función hash (MD5) admitida por la versión anterior.

ONTAP solo acepta contraseñas SHA-2 predefinidas mediante el SDK de capacidad de gestión de NetApp (`security-login-create` y `security-login-modify-password`).

Pasos

1. Migrar las cuentas de administrador MD5 a la función hash de contraseña SHA-512:

- a. Caducar todas las cuentas de administrador de MD5: `security login expire-password -vserver * -username * -hash-function md5`

Al hacerlo, se obliga a los usuarios de cuentas MD5 a cambiar sus contraseñas al siguiente inicio de sesión.

- b. Pida a los usuarios de cuentas MD5 que inicien sesión a través de una consola o una sesión SSH.

El sistema detecta que las cuentas han caducado y solicita a los usuarios que cambien sus contraseñas. SHA-512 se utiliza de forma predeterminada para las contraseñas modificadas.

2. Para las cuentas MD5 cuyos usuarios no inician sesión para cambiar sus contraseñas en un período de tiempo, fuerce la migración de la cuenta:

- a. Cuentas de bloqueo que todavía utilizan la función hash MD5 (nivel de privilegio avanzado):

```
security login expire-password -vserver * -username * -hash-function md5  
-lock-after integer
```

Después del número de días especificado por `-lock-after`, Los usuarios no pueden acceder a sus cuentas MD5.

- b. Desbloquee las cuentas cuando los usuarios estén preparados para cambiar sus contraseñas:

```
security login unlock -vserver svm_name -username user_name
```

- c. Hacer que los usuarios inicien sesión en sus cuentas mediante una sesión SSH o de consola y cambien sus contraseñas cuando el sistema les solicite que lo hagan.

Diagnosticar y corregir problemas de acceso a archivos

Pasos

1. En System Manager, seleccione **almacenamiento > Storage VMs**.
2. Seleccione la máquina virtual de almacenamiento a la que desee realizar un seguimiento.
3. Haga clic en **Más**.
4. Haga clic en **acceso a archivos de rastreo**.
5. Proporcione el nombre de usuario y la dirección IP del cliente y, a continuación, haga clic en **Iniciar rastreo**.

Los resultados del seguimiento se muestran en una tabla. La columna **razones** proporciona la razón por la que no se pudo acceder a un archivo.

6. Haga clic en  en la columna izquierda de la tabla de resultados para ver los permisos de acceso a archivos.

Gestione la verificación de varias administradores

Información general de verificación de varios administradores

A partir de ONTAP 9.11.1, puede utilizar la verificación multiprotocolo (MAV) para garantizar que determinadas operaciones, como la eliminación de volúmenes o copias snapshot, solo se puedan ejecutar tras las aprobaciones de administradores designados. De este modo, se evita que administradores comprometidos, malintencionados o inexpertos realicen cambios no deseados o eliminen datos.

La configuración de la verificación multi-admin consta de:

- ["Crear uno o varios grupos de aprobación de administrador."](#)
- ["Habilitar la funcionalidad de verificación multi-administrador."](#)

- ["Adición o modificación de reglas."](#)

Tras la configuración inicial, estos elementos sólo los pueden modificar los administradores de un grupo de aprobación MAV (administradores MAV).

Cuando la verificación multi-administrador está habilitada, la finalización de cada operación protegida requiere tres pasos:

- Cuando un usuario inicia la operación, un ["se genera la solicitud."](#)
- Antes de que pueda ejecutarse, al menos uno ["El administrador de MAV debe aprobar."](#)
- Tras la aprobación, el usuario completa la operación.

La verificación de varios administradores no está pensada para utilizarse con volúmenes o flujos de trabajo que implican una fuerte automatización, ya que cada tarea automatizada requeriría la aprobación antes de poder completar la operación. Si desea utilizar la automatización y MAV conjuntamente, se recomienda utilizar consultas para operaciones MAV específicas. Por ejemplo, puede aplicar `volume delete` MAV sólo rige para volúmenes en los que la automatización no está involucrada, y puede designar dichos volúmenes con un esquema de nomenclatura en particular.



Si necesita deshabilitar la funcionalidad de verificación multi-admin sin la aprobación del administrador de MAV, póngase en contacto con el soporte de NetApp y mencione el siguiente artículo de la base de conocimientos: ["Cómo deshabilitar la verificación de administrador múltiple si el administrador de MAV no está disponible"](#).

Cómo funciona la verificación multi-administrador

La verificación multi-admin consta de:

- Grupo de uno o más administradores con facultades de aprobación y veto.
- Conjunto de operaciones o comandos protegidos en una *rules table*.
- Un *motor de reglas* para identificar y controlar la ejecución de operaciones protegidas.

Las reglas de MAV se evalúan después de las reglas de control de acceso basado en funciones (RBAC). Por lo tanto, los administradores que ejecutan o aprueban operaciones protegidas ya deben disponer de privilegios mínimos de RBAC para esas operaciones. ["Más información acerca de RBAC."](#)

Reglas definidas por el sistema

Cuando se activa la verificación de varios administradores, las reglas definidas por el sistema (también conocidas como reglas *Guard-Rail*) establecen un conjunto de operaciones MAV para contener el riesgo de eludir el propio proceso MAV. Estas operaciones no se pueden quitar de la tabla de reglas. Una vez activado MAV, las operaciones designadas por un asterisco (*) requieren la aprobación de uno o más administradores antes de la ejecución, excepto los comandos **show**.

- `security multi-admin-verify modify` operación*

Controla la configuración de la funcionalidad de verificación multi-administrador.

- `security multi-admin-verify approval-group` operaciones*

Controlar la pertenencia al conjunto de administradores con credenciales de verificación de varios administradores.

- `security multi-admin-verify rule operaciones*`

Controle el conjunto de comandos que requieren verificación multiadministrador.

- `security multi-admin-verify request operaciones`

Controle el proceso de aprobación.

Comandos protegidos por reglas

Además de los comandos definidos por el sistema, los siguientes comandos están protegidos de forma predeterminada cuando se habilita la verificación multi-administrador, pero se pueden modificar las reglas para quitar la protección de estos comandos.

- `security login password`
- `security login unlock`
- `set`

Los siguientes comandos pueden protegerse en ONTAP 9.11.1 y versiones posteriores.

| | |
|--------------------------------------|---|
| <code>cluster peer delete</code> | <code>volume snapshot autodelete modify</code> |
| <code>event config modify</code> | <code>volume snapshot delete</code> |
| <code>security login create</code> | <code>volume snapshot policy add-schedule</code> |
| <code>security login delete</code> | <code>volume snapshot policy create</code> |
| <code>security login modify</code> | <code>volume snapshot policy delete</code> |
| <code>system node run</code> | <code>volume snapshot policy modify</code> |
| <code>system node systemshell</code> | <code>volume snapshot policy modify-schedule</code> |
| <code>volume delete</code> | <code>volume snapshot policy remove-schedule</code> |
| <code>volume flexcache delete</code> | <code>volume snapshot restore</code> |
| | <code>vserver peer delete</code> |

Los siguientes comandos se pueden proteger a partir de ONTAP 9.13.1:

- `volume snaplock modify`
- `security anti-ransomware volume attack clear-suspect`
- `security anti-ransomware volume disable`
- `security anti-ransomware volume pause`

Los siguientes comandos se pueden proteger a partir de ONTAP 9.14.1:

- `volume recovery-queue modify`
- `volume recovery-queue purge`
- `volume recovery-queue purge-all`
- `vserver modify`

Cómo funciona la aprobación multi-admin

Cada vez que se introduce una operación protegida en un cluster protegido MAV, se envía una solicitud de ejecución de operación al grupo de administradores de MAV designado.

Puede configurar:

- Los nombres, la información de contacto y el número de administradores del grupo MAV.

Un administrador de MAV debe tener una función RBAC con privilegios de administrador de clúster.

- El número de grupos de administradores de MAV.
 - Se asigna un grupo MAV para cada regla de operación protegida.
 - Para varios grupos MAV, puede configurar qué grupo MAV aprueba una regla determinada.
- El número de aprobaciones MAV necesarias para ejecutar una operación protegida.
- Período *de caducidad de aprobación* dentro del cual un administrador MAV debe responder a una solicitud de aprobación.
- Un período *expiration* de ejecución dentro del cual el administrador solicitante debe completar la operación.

Una vez configurados estos parámetros, se requiere la aprobación MAV para modificarlos.

Los administradores de MAV no pueden aprobar sus propias solicitudes para ejecutar operaciones protegidas. Por lo tanto:

- MAV no debe habilitarse en clústeres con un solo administrador.
- Si sólo hay una persona en el grupo MAV, ese administrador de MAV no puede introducir operaciones protegidas; los administradores regulares deben introducirlas y el administrador de MAV sólo puede aprobarlas.
- Si desea que los administradores de MAV puedan ejecutar operaciones protegidas, el número de administradores de MAV debe ser uno mayor que el número de aprobaciones necesarias. Por ejemplo, si se necesitan dos aprobaciones para una operación protegida y desea que los administradores de MAV las ejecuten, debe haber tres personas en el grupo de administradores de MAV.

Los administradores de MAV pueden recibir solicitudes de aprobación en alertas de correo electrónico (mediante EMS) o pueden consultar la cola de solicitudes. Cuando reciben una solicitud, pueden realizar una de estas tres acciones:

- Aprobar
- Rechazar (veto)
- Ignorar (sin acción)

Las notificaciones de correo electrónico se envían a todos los aprobadores asociados a una regla MAV cuando:

- Se crea una solicitud.
- Se ha aprobado o vetado una solicitud.
- Se ejecuta una solicitud aprobada.

Si el solicitante se encuentra en el mismo grupo de aprobación para la operación, recibirá un correo electrónico cuando se apruebe su solicitud.

Nota: Un solicitante no puede aprobar sus propias solicitudes, incluso si están en el grupo de aprobación. Pero pueden recibir las notificaciones por correo electrónico. Los solicitantes que no se encuentren en grupos de aprobación (es decir, que no sean administradores de MAV) no recibirán notificaciones por correo electrónico.

Cómo funciona la ejecución de operaciones protegidas

Si se aprueba la ejecución para una operación protegida, el usuario solicitante continúa con la operación cuando se le solicita. Si la operación es vetada, el usuario solicitante debe eliminar la solicitud antes de continuar.

Las reglas de MAV se evalúan después de los permisos de RBAC. Como resultado, un usuario sin suficientes permisos de RBAC para la ejecución de la operación no puede iniciar el proceso de solicitud de MAV.

Administrar grupos de aprobación de administradores

Antes de habilitar la verificación multi-admin (MAV), debe crear un grupo de aprobación de administrador que contenga a uno o más administradores a los que se les conceda la autorización de aprobación o de veto. Una vez que haya habilitado la verificación de varios administradores, cualquier modificación de la pertenencia al grupo de aprobación requiere la aprobación de uno de los administradores cualificados existentes.

Acerca de esta tarea

Puede agregar administradores existentes a un grupo MAV o crear nuevos administradores.


La funcionalidad MAV cumple la configuración de control de acceso basado en funciones (RBAC) existente. Los administradores potenciales de MAV deben tener privilegios suficientes para ejecutar operaciones protegidas antes de agregarlas a los grupos de administradores de MAV. ["Más información acerca de RBAC."](#)

Puede configurar MAV para avisar a los administradores de MAV de que las solicitudes de aprobación están pendientes. Para ello, debe configurar las notificaciones por correo electrónico, en concreto, el Mail From y Mail Server parámetros—o puede borrar estos parámetros para deshabilitar la notificación. Sin alertas de correo electrónico, los administradores de MAV deben comprobar manualmente la cola de aprobación.

Procedimiento de System Manager


Si desea crear un grupo de aprobación MAV por primera vez, consulte el procedimiento de System Manager a. ["habilite la verificación multi-admin."](#)

Para modificar un grupo de aprobación existente o crear un grupo de aprobación adicional:

1. Identifique a los administradores para que reciban una verificación de varios administradores.
 - a. Haga clic en **clúster > Configuración**.
 - b. Haga clic en  Junto a **usuarios y roles**.

- c. Haga clic en [+ Add](#) En **usuarios**.
- d. Modifique la planilla según sea necesario.

Para obtener más información, consulte ["Control del acceso de administradores."](#)

2. Crear o modificar el grupo de aprobación MAV:
 - a. Haga clic en **clúster > Configuración**.
 - b. Haga clic en [→](#) Junto a **aprobación Multi-Admin** en la sección **Seguridad**.
(Verá la  Icono si MAV aún no está configurado.)
 - Nombre: Introduzca un nombre de grupo.
 - Autorizadores: Seleccione autorizadores de una lista de usuarios.
 - Dirección de correo electrónico: Introduzca las direcciones de correo electrónico.
 - Grupo predeterminado: Seleccione un grupo.

Se requiere aprobación MAV para editar una configuración existente una vez que MAV está activado.

Procedimiento de la CLI

1. Compruebe que se han establecido valores para Mail From y Mail Server parámetros. Introduzca:

```
event config show
```

La pantalla debe ser similar a la siguiente:

```
cluster01::> event config show
                        Mail From:  admin@localhost
                        Mail Server: localhost
                        Proxy URL:   -
                        Proxy User:  -
                        Publish/Subscribe Messaging Enabled: true
```

Para configurar estos parámetros, introduzca:

```
event config modify -mail-from email_address -mail-server server_name
```

2. Identifique a los administradores para que reciban una verificación de varios administradores

| Si desea... | Introduzca este comando |
|--|--|
| Mostrar los administradores actuales | <code>security login show</code> |
| Modifique las credenciales de los administradores actuales | <code>security login modify <parameters></code> |
| Crear nuevas cuentas de administrador | <code>security login create -user-or-group -name <i>admin_name</i> -application ssh -authentication-method password</code> |

3. Cree el grupo de aprobación MAV:

```
security multi-admin-verify approval-group create [ -vserver svm_name] -name group_name -approvers approver1[,approver2...] [[-email address1], address1...]
```

- -vserver - Solo se admite la SVM de administrador en esta versión.
- -name - El nombre del grupo MAV, hasta 64 caracteres.
- -approvers - La lista de uno o más aprobadores.
- -email - Una o varias direcciones de correo electrónico que se notifican cuando se crea, aprueba, vetó o ejecuta una solicitud.

Ejemplo: el siguiente comando crea un grupo MAV con dos miembros y direcciones de correo electrónico asociadas.

```
cluster-1::> security multi-admin-verify approval-group create -name mav-grp1 -approvers pavan,julia -email pavan@myfirm.com,julia@myfirm.com
```

4. Verificar la creación y pertenencia a grupos:

```
security multi-admin-verify approval-group show
```

Ejemplo:

```
cluster-1::> security multi-admin-verify approval-group show
Vserver  Name      Approvers      Email
-----  -
svm-1    mav-grp1  pavan,julia    email
pavan@myfirm.com,julia@myfirm.com
```

Utilice estos comandos para modificar la configuración inicial del grupo MAV.

Nota: todos requieren la aprobación del administrador de MAV antes de la ejecución.

| Si desea... | Introduzca este comando |
|---|--|
| Modifique las características del grupo o modifique la información de miembro existente | security multi-admin-verify approval-group modify [parameters] |
| Agregar o quitar miembros | security multi-admin-verify approval-group replace [-vserver svm_name] -name group_name [-approvers-to-add approver1[,approver2...]] [-approvers-to-remove approver1[,approver2...]] |

| Si desea... | Introduzca este comando |
|-------------------|---|
| Eliminar un grupo | <code>security multi-admin-verify approval-group delete [-vserver svm_name] -name group_name</code> |

Habilitar y deshabilitar la verificación de varios administradores

La verificación de varios administradores (MAV) se debe habilitar explícitamente. Una vez activada la verificación de varios administradores, se requiere la aprobación de un grupo de aprobación MAV (administradores MAV) para eliminarlo.

Acerca de esta tarea

Una vez que MAV está activado, la modificación o desactivación de MAV requiere la aprobación del administrador de MAV.



Si necesita deshabilitar la funcionalidad de verificación multi-admin sin la aprobación del administrador de MAV, póngase en contacto con el soporte de NetApp y mencione el siguiente artículo de la base de conocimientos: ["Cómo deshabilitar la verificación de administrador múltiple si el administrador de MAV no está disponible"](#).

Al activar MAV, puede especificar los siguientes parámetros globalmente.

Grupos de aprobación

Lista de grupos de aprobación globales. Se necesita al menos un grupo para activar la funcionalidad MAV.



Si utiliza MAV con protección autónoma contra ransomware (ARP), defina un grupo de aprobación nuevo o existente que sea responsable de aprobar la pausa de ARP, deshabilitar y borrar solicitudes sospechosas.

Autorizadores requeridos

Número de autorizadores necesarios para ejecutar una operación protegida. El número predeterminado y el número mínimo son 1.



El Núm. Necesario de aprobadores debe ser menor que el Núm. Total de aprobadores únicos en los grupos de aprobación por defecto.

Caducidad de la aprobación (horas, minutos, segundos)



El período dentro del cual un administrador MAV debe responder a una solicitud de aprobación. El valor predeterminado es una hora (1h), el valor mínimo soportado es un segundo (1s) y el valor máximo soportado es 14 días (14d).

Caducidad de la ejecución (horas, minutos, segundos)



El período dentro del cual el administrador solicitante debe completar la operación. El valor predeterminado es una hora (1h), el valor mínimo soportado es un segundo (1s) y el valor máximo soportado es 14 días (14d).

También puede anular cualquiera de estos parámetros para un parámetro específico ["reglas de funcionamiento"](#).

Procedimiento de System Manager

1. Identifique a los administradores para que reciban una verificación de varios administradores.
 - a. Haga clic en **clúster > Configuración**.
 - b. Haga clic en  Junto a **usuarios y roles**.
 - c. Haga clic en  **Add** En **usuarios**.
 - d. Modifique la planilla según sea necesario.

Para obtener más información, consulte "[Control del acceso de administradores](#)."

2. Active la verificación de varios administradores creando al menos un grupo de aprobación y agregando al menos una regla.
 - a. Haga clic en **clúster > Configuración**.
 - b. Haga clic en  Junto a **aprobación Multi-Admin** en la sección **Seguridad**.
 - c. Haga clic en  **Add** para agregar al menos un grupo de aprobación.
 - Nombre: Introduzca un nombre de grupo.
 - Autorizadores: Seleccione autorizadores de una lista de usuarios.
 - Dirección de correo electrónico: Introduzca las direcciones de correo electrónico.
 - Grupo predeterminado: Seleccione un grupo.
 - d. Agregue al menos una regla.
 - Operación: Seleccione un comando admitido de la lista.
 - Query: Introduzca los valores y las opciones de comandos que desee.
 - Parámetros opcionales; déjelo en blanco para aplicar la configuración global o asigne un valor diferente para reglas específicas para anular la configuración global.
 - Número requerido de aprobadores
 - Grupos de aprobación
 - e. Haga clic en **Configuración avanzada** para ver o modificar los valores predeterminados.
 - Número requerido de autorizadores (valor predeterminado: 1)
 - Caducidad de la solicitud de ejecución (valor predeterminado: 1 hora)
 - Caducidad de la solicitud de aprobación (valor predeterminado: 1 hora)
 - Servidor de correo*
 - Desde la dirección de correo electrónico*

*Estos actualizan la configuración de correo electrónico administrada en "Notification Management". Se le pedirá que los configure si aún no se han configurado.
 - f. Haga clic en **Activar** para completar la configuración inicial de MAV.


Después de la configuración inicial, el estado actual de MAV se muestra en el mosaico **Multi-Admin Approval**.

- Estado (habilitado o no)
- Operaciones activas para las que se necesitan aprobaciones

- Número de solicitudes abiertas en estado pendiente

Puede mostrar una configuración existente haciendo clic en ➔. Se requiere aprobación MAV para editar una configuración existente.

Para deshabilitar la verificación multi-admin:

1. Haga clic en **clúster > Configuración**.
2. Haga clic en  Junto a **aprobación Multi-Admin** en la sección **Seguridad**.
3. Haga clic en el botón de alternar habilitado.

Se requiere la aprobación MAV para completar esta operación.

Procedimiento de la CLI

Antes de activar la funcionalidad MAV en la CLI, al menos una "Grupo de administradores MAV" debe haber sido creado.

| Si desea... | Introduzca este comando |
|---|--|
| Active la funcionalidad de MAV | <pre>security multi-admin-verify modify -approval-groups group1[,group2...] [- required-approvers nn] -enabled true [-execution-expiry [nnh][nmm][nns]] [-approval-expiry [nnh][nmm][nns]]</pre> <p>Ejemplo : el siguiente comando habilita MAV con 1 grupo de aprobación, 2 aprobadores requeridos y períodos de caducidad predeterminados.</p> <div> <pre>cluster-1::> security multi-admin- verify modify -approval-groups mav-grp1 -required-approvers 2 -enabled true</pre> </div> <p>Complete la configuración inicial agregando al menos una "regla de operación."</p> |
| Modificar una configuración de MAV (requiere aprobación de MAV) | <pre>security multi-admin-verify approval- group modify [-approval-groups group1 [,group2...]] [-required-approvers nn] [-execution-expiry [nnh][nmm][nns]] [-approval-expiry [nnh][nmm][nns]]</pre> |

| Si desea... | Introduzca este comando |
|--|--|
| Verifique la funcionalidad de MAV | <pre>security multi-admin-verify show</pre> <p>Ejemplo:</p> <pre>cluster-1::> security multi-admin-verify show Is Required Execution Approval Approval Enabled Approvers Expiry Expiry Groups ----- true 2 1h 1h mav-grp1</pre> |
| Desactivar la función MAV (requiere la aprobación MAV) | <pre>security multi-admin-verify modify -enabled false</pre> |

Gestione reglas de operaciones protegidas

Se crean reglas de verificación de varios administradores (MAV) para designar operaciones que requieren aprobación. Siempre que se inicia una operación, las operaciones protegidas se interceptan y se genera una solicitud de aprobación.

Las reglas se pueden crear antes de habilitar MAV por cualquier administrador con las capacidades RBAC adecuadas, pero una vez que MAV está activado, cualquier modificación del conjunto de reglas requiere la aprobación de MAV.

Sólo se puede crear una regla MAV por operación; por ejemplo, no se pueden crear varias `volume-snapshot-delete` reglas. Cualquier restricción de regla deseada debe estar contenida dentro de una regla.

Comandos protegidos por reglas

Puede crear reglas para proteger los siguientes comandos que comienzan con ONTAP 9.11.1.

| | |
|-------------------------|--|
| cluster peer delete | volume snapshot autodelete modify |
| event config modify | volume snapshot delete |
| security login create | volume snapshot policy add-schedule |
| security login delete | volume snapshot policy create |
| security login modify | volume snapshot policy delete |
| system node run | volume snapshot policy modify |
| system node systemshell | volume snapshot policy modify-schedule |
| volume delete | volume snapshot policy remove-schedule |
| volume flexcache delete | volume snapshot restore |
| | vserver peer delete |

Puede crear reglas para proteger los siguientes comandos que comienzan con ONTAP 9.13.1:

- volume snaplock modify
- security anti-ransomware volume attack clear-suspect
- security anti-ransomware volume disable
- security anti-ransomware volume pause

Puede crear reglas para proteger los siguientes comandos que comienzan con ONTAP 9.14.1:

- volume recovery-queue modify
- volume recovery-queue purge
- volume recovery-queue purge-all
- vserver modify

Las reglas para los comandos MAV system-default, el security multi-admin-verify "comandos", no se puede modificar.

Además de los comandos definidos por el sistema, los siguientes comandos están protegidos de forma predeterminada cuando se habilita la verificación multi-administrador, pero se pueden modificar las reglas para quitar la protección de estos comandos.

- security login password
- security login unlock
- set

Restricciones de regla

Al crear una regla, puede especificar opcionalmente la `-query` opción para limitar la solicitud a un subconjunto de la funcionalidad del comando. La `-query` La opción también se puede usar para limitar elementos de configuración, como los nombres de la SVM, del volumen y de las snapshots.

Por ejemplo, en la `volume snapshot delete` comando, `-query` se puede establecer en `-snapshot !hourly*,!daily*,!weekly*`, Lo que significa que las instantáneas de volumen con el prefijo de atributos por hora, diario o semanal se excluyen de las protecciones MAV.

```
smci-vs1m20::> security multi-admin-verify rule show
```

| Vserver | Operation | Required Approvers | Approval Groups |
|---------|--|-----------------------|--------------------|
| vs01 | volume snapshot delete Query: -snapshot !hourly*,!daily*,!weekly* | - | - |



MAV no protegería ningún elemento de configuración excluido y cualquier administrador podría suprimirlos o cambiarles el nombre.

De forma predeterminada, las reglas especifican que corresponde `security multi-admin-verify request create "protected_operation"` el comando se genera automáticamente cuando se introduce una operación protegida. Puede modificar este valor predeterminado para requerir que el `request create` el comando se introduce por separado.

De forma predeterminada, las reglas heredan la siguiente configuración global de MAV, aunque se pueden especificar excepciones específicas de reglas:

- Número de aprobadores requerido
- Grupos de aprobación
- Período de caducidad de la aprobación
- Periodo de caducidad de ejecución

Procedimiento de System Manager

Si desea añadir una regla de operación protegida por primera vez, consulte el procedimiento de System Manager a. "[habilite la verificación multi-admin.](#)"

Para modificar el conjunto de reglas existente:

1. Seleccione **Cluster > Settings**.
2. Seleccione Junto a **aprobación Multi-Admin** en la sección **Seguridad**.
3. Seleccione **Add** para agregar al menos una regla, también puede modificar o eliminar reglas existentes.
 - Operación: Seleccione un comando admitido de la lista.
 - Query: Introduzca los valores y las opciones de comandos que desee.
 - Parámetros opcionales: Dejar en blanco para aplicar la configuración global o asignar un valor diferente para reglas específicas para anular la configuración global.

- Número requerido de aprobadores
- Grupos de aprobación

Procedimiento de la CLI



Todo `security multi-admin-verify rule` Los comandos requieren la aprobación del administrador de MAV antes de la ejecución excepto `security multi-admin-verify rule show`.

| Si desea... | Introduzca este comando |
|--|---|
| Cree una regla | <code>security multi-admin-verify rule create -operation "protected_operation" [-query operation_subset] [parameters]</code> |
| Modifique las credenciales de los administradores actuales | <code>security login modify <parameters></code> Ejemplo: La siguiente regla requiere aprobación para eliminar el volumen raíz. <code>security multi-admin-verify rule create -operation "volume delete" -query "-vserver vs0"</code> |
| Modificar una regla | <code>security multi-admin-verify rule modify -operation "protected_operation" [parameters]</code> |
| Eliminar una regla | <code>security multi-admin-verify rule delete -operation "protected_operation"</code> |
| Muestra las reglas | <code>security multi-admin-verify rule show</code> |

Para obtener detalles de sintaxis de comandos, consulte `security multi-admin-verify rule` páginas de manual.

Solicite la ejecución de operaciones protegidas

Cuando inicia una operación o comando protegido en un clúster habilitado para la verificación de varios administradores (MAV), ONTAP intercepta automáticamente la operación y solicita generar una solicitud, que debe ser aprobada por uno o más administradores de un grupo de aprobación de MAV (administradores de MAV). También puede crear una solicitud MAV sin el diálogo.

Si se aprueba, deberá responder a la consulta para completar la operación dentro del período de caducidad de la solicitud. Si se ha vetado o si se han superado los períodos de solicitud o caducidad, debe eliminar la solicitud y volver a enviarla.

La funcionalidad MAV cumple la configuración de RBAC existente. Es decir, la función de administrador debe

tener privilegios suficientes para ejecutar una operación protegida sin tener en cuenta la configuración de MAV. "[Más información acerca de RBAC](#)".

Si es administrador de MAV, sus solicitudes de ejecución de operaciones protegidas también deben ser aprobadas por un administrador de MAV.

Procedimiento de System Manager

Cuando un usuario hace clic en un elemento de menú para iniciar una operación y la operación está protegida, se genera una solicitud de aprobación y el usuario recibe una notificación similar a la siguiente:

```
Approval request to delete the volume was sent.  
Track the request ID 356 from Events & Jobs > Multi-Admin Requests.
```

La ventana **solicitudes de administrador múltiple** está disponible cuando MAV está activado, mostrando solicitudes pendientes basadas en el ID de inicio de sesión del usuario y la función MAV (aprobador o no). Para cada solicitud pendiente, se muestran los siguientes campos:

- Funcionamiento
- Índice (número)
- Estado (pendiente, aprobado, rechazado, ejecutado o caducado)

Si un aprobador rechaza una solicitud, no es posible realizar ninguna otra acción.

- Consulta (cualquier parámetro o valor para la operación solicitada)
- Usuario solicitante
- La solicitud caduca el
- (Número de) aprobadores pendientes
- (Número de) posibles aprobadores

Una vez aprobada la solicitud, el usuario solicitante puede volver a intentar la operación dentro del período de caducidad.

Si el usuario vuelve a intentar la operación sin aprobación, se muestra una notificación similar a la siguiente:

```
Request to perform delete operation is pending approval.  
Retry the operation after request is approved.
```

Procedimiento de la CLI

1. Introduzca la operación protegida directamente o mediante el comando MAV Request.

Ejemplos: Para eliminar un volumen, introduzca uno de los siguientes comandos:

```
° volume delete
```

```
cluster-1::*> volume delete -volume voll -vserver vs0
```

```
Warning: This operation requires multi-admin verification. To create  
a
```

```
    verification request use "security multi-admin-verify  
request  
    create".
```

```
    Would you like to create a request for this operation?  
    {y|n}: y
```

```
Error: command failed: The security multi-admin-verify request (index  
3) is  
    auto-generated and requires approval.
```

```
° security multi-admin-verify request create "volume delete"
```

```
Error: command failed: The security multi-admin-verify request (index  
3)  
    requires approval.
```

2. Compruebe el estado de la solicitud y responda al aviso de MAV.

a. Si se aprueba la solicitud, responda al mensaje de la CLI para completar la operación.

Ejemplo:

```
cluster-1::> security multi-admin-verify request show 3
```

```
    Request Index: 3
      Operation: volume delete
        Query: -vserver vs0 -volume voll
        State: approved
Required Approvers: 1
Pending Approvers: 0
  Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
    Approvals: admin2
    User Vetoed: -
      Vserver: cluster-1
  User Requested: admin
    Time Created: 2/25/2022 13:32:03
    Time Approved: 2/25/2022 13:35:36
      Comment: -
  Users Permitted: -
```

```
cluster-1::*> volume delete -volume voll -vserver vs0
```

Info: Volume "voll" in Vserver "vs0" will be marked as deleted and placed in the volume recovery queue. The space used by the volume will be recovered only after the retention period of 12 hours has completed. To recover the space immediately, get the volume name using (privilege:advanced) "volume recovery-queue show voll_*" and then "volume recovery-queue purge -vserver vs0 -volume <volume_name>" command. To recover the volume use the (privilege:advanced) "volume recovery-queue recover -vserver vs0 -volume <volume_name>" command.

Warning: Are you sure you want to delete volume "voll" in Vserver "vs0" ?
{y|n}: y

- b. Si se vetó la solicitud o el período de caducidad ha pasado, elimine la solicitud y vuelva a enviarla o póngase en contacto con el administrador de MAV.

Ejemplo:

```
cluster-1::> security multi-admin-verify request show 3
```

```
Request Index: 3
  Operation: volume delete
    Query: -vserver vs0 -volume voll1
    State: vetoed
Required Approvers: 1
Pending Approvers: 1
  Approval Expiry: 2/25/2022 14:38:47
Execution Expiry: -
  Approvals: -
  User Vetoed: admin2
    Vserver: cluster-1
User Requested: admin
  Time Created: 2/25/2022 13:38:47
Time Approved: -
  Comment: -
Users Permitted: -
```

```
cluster-1::*> volume delete -volume voll1 -vserver vs0
```

```
Error: command failed: The security multi-admin-verify request (index 3)
hasbeen vetoed. You must delete it and create a new verification
request.
To delete, run "security multi-admin-verify request delete 3".
```

Gestione solicitudes de operaciones protegidas

Cuando se notifica a los administradores de un grupo de aprobación MAV (administradores MAV) de una solicitud de ejecución de operación pendiente, deben responder con un mensaje de aprobación o de veto dentro de un período de tiempo fijo (caducidad de la aprobación). Si no se recibe un número suficiente de aprobaciones, el solicitante debe eliminar la solicitud y realizar otra.

Acerca de esta tarea

Las solicitudes de aprobación se identifican con números de índice, que se incluyen en los mensajes de correo electrónico y se muestran en la cola de solicitudes.

Se puede mostrar la siguiente información de la cola de solicitudes:

Funcionamiento

La operación protegida para la que se crea la solicitud.

Consulta

El objeto (u objetos) sobre el que el usuario desea aplicar la operación.

Estado

El estado actual de la solicitud; pendiente, aprobado, rechazado, caducado, ejecutado. Si un aprobador rechaza una solicitud, no es posible realizar ninguna otra acción.

Autorizadores requeridos

El número de administradores de MAV que se necesitan para aprobar la solicitud. Un usuario puede establecer el parámetro aprobadores requeridos para la regla de operación. Si un usuario no establece los aprobadores requeridos en la regla, se aplican los autorizadores requeridos de la configuración global.

Aprobadores pendientes

El número de administradores de MAV que todavía deben aprobar la solicitud para que se marque como aprobada.

Caducidad de la aprobación

El período dentro del cual un administrador MAV debe responder a una solicitud de aprobación. Cualquier usuario autorizado puede definir la fecha de caducidad de la aprobación de una regla de operación. Si no se ha establecido la fecha de caducidad de la regla, se aplicará la fecha de caducidad de la aprobación del valor global.

Caducidad de la ejecución

El período en el que el administrador solicitante debe completar la operación. Cualquier usuario autorizado puede establecer la caducidad de la ejecución de una regla de operación. Si no se ha definido la caducidad de la ejecución para la regla, se aplicará la caducidad de la ejecución desde el valor global.

Usuarios aprobados

Los administradores de MAV que han aprobado la solicitud.

El usuario ha vetado

Los administradores de MAV que han vetado la solicitud.

VM de almacenamiento (Vserver)

La SVM con la que se asocia la solicitud. Solo esta versión admite la SVM de administrador.

Usuario solicitado

Nombre de usuario del usuario que creó la solicitud.

Hora de creación

Hora a la que se crea la solicitud.

Tiempo aprobado

Hora a la que el estado de la solicitud cambió a aprobado.

Comentar

Cualquier comentario asociado a la solicitud.

Se permiten usuarios

Lista de usuarios autorizados para realizar la operación protegida para la que se aprueba la solicitud. Si `users-permitted` está vacío y, a continuación, cualquier usuario con los permisos adecuados puede realizar la operación.

Todas las solicitudes vencidas o ejecutadas se eliminan cuando se alcanza un límite de 1000 solicitudes o cuando el tiempo de vencimiento es superior a 8 horas para las solicitudes caducadas. Las solicitudes de

vetoed se eliminan una vez marcadas como caducadas.

Procedimiento de System Manager

Los administradores de MAV reciben mensajes de correo electrónico con detalles sobre la solicitud de aprobación, el período de caducidad de la solicitud y un vínculo para aprobar o rechazar la solicitud. Pueden acceder a un diálogo de aprobación haciendo clic en el enlace del correo electrónico o navegue hasta **Eventos y trabajos>solicitudes** en System Manager.

La ventana **Requests** está disponible cuando está habilitada la verificación de varios administradores, mostrando solicitudes pendientes basadas en el ID de inicio de sesión del usuario y la función MAV (aprobador o no).

- Funcionamiento
- Índice (número)
- Estado (pendiente, aprobado, rechazado, ejecutado o caducado)

Si un aprobador rechaza una solicitud, no es posible realizar ninguna otra acción.

- Consulta (cualquier parámetro o valor para la operación solicitada)
- Usuario solicitante
- La solicitud caduca el
- (Número de) aprobadores pendientes
- (Número de) posibles aprobadores

Los administradores de MAV tienen controles adicionales en esta ventana; pueden aprobar, rechazar o eliminar operaciones individuales o grupos de operaciones seleccionados. Sin embargo, si el administrador MAV es el usuario solicitante, no puede aprobar, rechazar o eliminar sus propias solicitudes.

Procedimiento de la CLI

1. Cuando se le notifique por correo electrónico acerca de las solicitudes pendientes, anote el número de índice y el período de caducidad de la aprobación de la solicitud. El número de índice también se puede mostrar utilizando las opciones **show** o **show-anPending** que se mencionan a continuación.
2. Aprobar o vetar la solicitud.

| Si desea... | Introduzca este comando |
|--|---|
| Aprobar una solicitud | <code>security multi-admin-verify request approve nn</code> |
| Vetar una solicitud | <code>security multi-admin-verify request veto nn</code> |
| Mostrar todas las solicitudes, solicitudes pendientes o una sola solicitud | <code>`security multi-admin-verify request { show</code> |

| Si desea... | Introduzca este comando |
|--|--|
| show-pending } [nn] { -fields <i>field1</i> [, <i>field2</i> ...] | [-instance] }` Puede mostrar todas las solicitudes de la cola o sólo las solicitudes pendientes. Si introduce el número de índice, solo se mostrará la información correspondiente. Puede mostrar información sobre campos específicos (mediante la <code>-fields</code> parámetro) o todos los campos (mediante el <code>-instance</code> parámetro). |
| Eliminar una solicitud | security multi-admin-verify request delete nn |

Ejemplo:

La siguiente secuencia aprueba una solicitud después de que el administrador de MAV haya recibido el correo electrónico de solicitud con el número de índice 3, que ya tiene una aprobación.

```
cluster1::> security multi-admin-verify request show-pending
                                Pending
Index Operation      Query State  Approvers Requestor
-----
3 volume delete -    pending 1      julia

cluster-1::> security multi-admin-verify request approve 3

cluster-1::> security multi-admin-verify request show 3

Request Index: 3
  Operation: volume delete
    Query: -
    State: approved
Required Approvers: 2
Pending Approvers: 0
  Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
    Approvals: mav-admin2
    User Vetoed: -
      Vserver: cluster-1
User Requested: julia
  Time Created: 2/25/2022 13:32:03
  Time Approved: 2/25/2022 13:35:36
    Comment: -
Users Permitted: -
```

Ejemplo:

En la siguiente secuencia se vetará una solicitud después de que el administrador MAV haya recibido el correo electrónico de solicitud con el número de índice 3, que ya tiene una aprobación.

```
cluster1::> security multi-admin-verify request show-pending
Pending
Index Operation      Query State  Approvers Requestor
-----
3 volume delete -    pending 1      pavan

cluster-1::> security multi-admin-verify request veto 3

cluster-1::> security multi-admin-verify request show 3

Request Index: 3
Operation: volume delete
Query: -
State: vetoed
Required Approvers: 2
Pending Approvers: 0
Approval Expiry: 2/25/2022 14:32:03
Execution Expiry: 2/25/2022 14:35:36
Approvals: mav-admin1
User Vetoed: mav-admin2
Vserver: cluster-1
User Requested: pavan
Time Created: 2/25/2022 13:32:03
Time Approved: 2/25/2022 13:35:36
Comment: -
Users Permitted: -
```

Autenticación y autorización mediante OAuth 2,0

Descripción general de la implementación de ONTAP OAuth 2,0

A partir de ONTAP 9,14, tiene la opción de controlar el acceso a sus clústeres de ONTAP mediante el marco de autorización abierta (OAuth 2,0). Es posible configurar esta función mediante cualquiera de las interfaces administrativas de ONTAP, incluida la interfaz de línea de comandos de ONTAP, System Manager y la API de REST. Sin embargo, las decisiones de autorización y control de acceso de OAuth 2,0 solo se pueden aplicar cuando un cliente accede a ONTAP mediante la API REST.



La compatibilidad con OAuth 2,0 se introdujo por primera vez con ONTAP 9.14.0, por lo que su disponibilidad depende de la versión de ONTAP que esté utilizando. Consulte "[Notas de la versión de ONTAP](#)" si quiere más información.

Funciones y beneficios

A continuación se describen las principales características y ventajas del uso de OAuth 2,0 con ONTAP.

Compatibilidad con el estándar OAuth 2,0

OAuth 2,0 es el marco de autorización estándar de la industria. Se utiliza para restringir y controlar el acceso a recursos protegidos mediante tokens de acceso firmados. Hay varios beneficios al usar OAuth 2,0:

- Muchas opciones para la configuración de autorización
- Nunca reveles las credenciales del cliente, incluidas las contraseñas
- Los tokens se pueden definir para que caduquen según la configuración
- Ideal para su uso con API DE REST

Probado con varios servidores de autorización populares

La implementación de ONTAP está diseñada para ser compatible con cualquier servidor de autorización compatible con OAuth 2,0. Se ha probado con los siguientes servidores o servicios populares, incluyendo:

- Auth0
- Servicio de federación de Active Directory (ADFS)
- Keycloak

Compatibilidad con varios servidores de autorización simultáneos

Puede definir hasta ocho servidores de autorización para un solo clúster de ONTAP. Esto le da la flexibilidad para satisfacer las necesidades de su diverso entorno de seguridad.

Integración con los roles REST

Las decisiones de autorización de ONTAP se basan en última instancia en los roles REST asignados a usuarios o grupos. Estos roles se incluyen en el token de acceso como ámbitos independientes o se basan en definiciones de ONTAP locales junto con grupos de Active Directory o LDAP.

Opción para utilizar tokens de acceso restringido por remitente

Puede configurar ONTAP y los servidores de autorización para utilizar la seguridad de la capa de transporte mutuo (MTLS), lo que refuerza la autenticación del cliente. Garantiza que los tokens de acceso OAuth 2,0 solo son utilizados por los clientes a los que fueron emitidos originalmente. Esta característica admite y se alinea con varias recomendaciones de seguridad populares, incluidas las establecidas por FAPI y MITER.

Implementación y configuración

En un nivel alto, hay varios aspectos de una implementación y configuración de OAuth 2,0 que debe tener en cuenta al comenzar.

OAuth 2,0 entidades dentro de ONTAP

El marco de autorización OAuth 2,0 define varias entidades que se pueden asignar a elementos reales o virtuales dentro de su centro de datos o red. Las entidades OAuth 2,0 y su adaptación a ONTAP se presentan en la tabla siguiente.

| Entidad OAuth 2,0 | Descripción |
|--------------------------|---|
| Recurso | Los extremos de la API de REST que proporcionan acceso a los recursos de la ONTAP mediante comandos internos de la ONTAP. |
| Propietario del recurso | El usuario de clúster de ONTAP que creó el recurso protegido o lo posee de forma predeterminada. |
| Servidor de recursos | El host de los recursos protegidos que es el clúster de ONTAP. |
| Cliente | Una aplicación que solicita acceso a un extremo de API DE REST en nombre o con permiso del propietario del recurso. |
| Servidor de autorización | Por lo general, un servidor dedicado responsable de emitir tokens de acceso y aplicar políticas administrativas. |

Configuración principal de ONTAP

Debe configurar el clúster de ONTAP para habilitar y utilizar OAuth 2,0. Esto incluye establecer una conexión con el servidor de autorización y definir la configuración de autorización ONTAP necesaria. Esta configuración se puede realizar mediante cualquiera de las interfaces administrativas, incluidas las siguientes:

- Interfaz de línea de comandos de ONTAP
- System Manager
- API REST de ONTAP

Medio ambiente y servicios de apoyo

Además de las definiciones de ONTAP, también debe configurar los servidores de autorización. Si usa la asignación de grupo a rol, también es necesario configurar los grupos de Active Directory o el equivalente de LDAP.

Clientes ONTAP compatibles

A partir de ONTAP 9,14, un cliente API DE REST puede acceder a ONTAP con OAuth 2,0. Antes de emitir una llamada a la API de REST, debe obtener un token de acceso del servidor de autorización. A continuación, el cliente pasa este token al cluster de ONTAP como *bearer token* mediante el encabezado de solicitud de autorización HTTP. Dependiendo del nivel de seguridad necesario, también puede crear e instalar un certificado en el cliente para utilizar tokens restringidos por remitente basados en MTLS.

Terminología seleccionada

A medida que comience a explorar una implementación de OAuth 2,0 con ONTAP, es útil familiarizarse con algunos de los términos. Consulte ["Recursos adicionales"](#) Para enlaces a más información sobre OAuth 2,0.

Token de acceso

Token emitido por un servidor de autorización y utilizado por una aplicación cliente OAuth 2,0 para realizar solicitudes de acceso a los recursos protegidos.

Token web JSON

Estándar utilizado para formatear los tokens de acceso. JSON se utiliza para representar las reclamaciones OAuth 2,0 en un formato compacto con las reclamaciones dispuestas en tres secciones principales.

Token de acceso restringido por el remitente

Función opcional basada en el protocolo de seguridad de la capa de transporte mutuo (MTLS). Mediante el uso de una reclamación de confirmación adicional en el token, esto garantiza que el token de acceso solo

sea utilizado por el cliente para el que se emitió originalmente.

Juego de claves web JSON

Un JWKS es una colección de claves públicas utilizadas por ONTAP para verificar los tokens JWT presentados por los clientes. Los conjuntos de claves suelen estar disponibles en el servidor de autorización a través de un URI dedicado.

Ámbito

Los ámbitos proporcionan una forma de limitar o controlar el acceso de una aplicación a recursos protegidos como la API REST DE ONTAP. Se representan como cadenas en el token de acceso.

RoI DE REST de ONTAP

Los roles de REST se introdujeron con ONTAP 9,6 y son una parte principal del marco de control de acceso basado en roles de ONTAP. Estos roles son diferentes a los roles tradicionales anteriores que todavía son compatibles con ONTAP. La implementación de OAuth 2,0 en ONTAP solo admite roles REST.

Cabecera de autorización HTTP

Un encabezado incluido en la solicitud HTTP para identificar el cliente y los permisos asociados como parte de realizar una llamada a la API REST. Hay varios tipos o implementaciones disponibles dependiendo de cómo se realice la autenticación y la autorización. Al presentar un token de acceso OAuth 2,0 a ONTAP, el token se identifica como un token *bearer*.

Autenticación básica HTTP

Una técnica de autenticación HTTP temprana aún soportada por ONTAP. Las credenciales de texto sin formato (nombre de usuario y contraseña) se concatenan con dos puntos y se codifican en base64. La cadena se coloca en la cabecera de solicitud de autorización y se envía al servidor.

FAPI

Un grupo de trabajo de la Fundación OpenID que proporciona protocolos, esquemas de datos y recomendaciones de seguridad para el sector financiero. La API se conocía originalmente como la API de grado financiero.

INGLETE

Una compañía privada sin fines de lucro que proporciona orientación técnica y de seguridad a la Fuerza Aérea de los Estados Unidos y al gobierno de los Estados Unidos.

Recursos adicionales

A continuación se proporcionan varios recursos adicionales. Usted debe revisar estos sitios para obtener más información sobre OAuth 2,0 y los estándares relacionados.

Protocolos y estándares

- ["RFC 6749: Marco de Autorización de OAuth 2,0"](#)
- ["RFC 7519: Tokens web JSON \(JWT\)"](#)
- ["RFC 7523: Perfil JSON Web Token \(JWT\) para la autenticación y autorización de cliente OAuth 2,0"](#)
- ["RFC 7662: Introspección del token OAuth 2,0"](#)
- ["RFC 7800: Clave de prueba de posesión para JWT"](#)
- ["RFC 8705: Autenticación de cliente Mutual-TLS de OAuth 2,0 y tokens de acceso vinculados a certificados"](#)

Organizaciones

- ["Fundación OpenID"](#)
- ["Grupo de trabajo de FAPI"](#)
- ["INGLETE"](#)
- ["IANA - JWT"](#)

Productos y servicios

- ["Auth0"](#)
- ["Descripción general de ADFS"](#)
- ["Keycloak"](#)

Herramientas y utilidades adicionales

- ["JWT por Auth0"](#)
- ["OpenSSL"](#)

Documentación y recursos de NetApp

- ["Automatización de ONTAP"](#) documentación

Conceptos

Servidores de autorización y tokens de acceso

Los servidores de autorización realizan varias funciones importantes como componente central dentro del marco de autorización de OAuth 2,0.

Servidores de autorización OAuth 2,0

Los servidores de autorización son los principales responsables de crear y firmar tokens de acceso. Estos tokens contienen información de identidad y autorización que permite a una aplicación cliente acceder selectivamente a los recursos protegidos. Los servidores generalmente están aislados entre sí y se pueden implementar de varias maneras diferentes, incluyendo como un servidor dedicado independiente o como parte de un producto de gestión de identidad y acceso más grande.



En ocasiones, se puede utilizar una terminología diferente para un servidor de autorización, especialmente cuando la funcionalidad OAuth 2,0 está empaquetada dentro de un producto o solución de gestión de acceso e identidad más grande. Por ejemplo, el término **proveedor de identidad (IDP)** se utiliza con frecuencia indistintamente con **servidor de autorización**.

Administración

Además de emitir tokens de acceso, los servidores de autorización también proporcionan servicios administrativos relacionados, normalmente a través de una interfaz de usuario web. Por ejemplo, puede definir y administrar:

- Autenticación de usuarios y usuarios
- Ámbitos
- Segregación administrativa a través de inquilinos y dominios
- Aplicación de políticas
- Conexión a varios servicios externos

- Compatibilidad con otros protocolos de identidad (como SAML)

ONTAP es compatible con los servidores de autorización que cumplen con el estándar OAuth 2,0.

Definición a ONTAP

Debe definir uno o varios servidores de autorización para ONTAP. ONTAP se comunica de forma segura con cada servidor para verificar tokens y realizar otras tareas relacionadas en soporte de las aplicaciones cliente.

A continuación se presentan los principales aspectos de la configuración de ONTAP. Consulte también ["Escenarios de despliegue de OAuth 2,0"](#) si quiere más información.

Cómo y dónde se validan los tokens de acceso

Hay dos opciones para validar tokens de acceso.

- Validación local

ONTAP puede validar los tokens de acceso localmente en función de la información proporcionada por el servidor de autorización que emitió el token. ONTAP almacena en caché la información recuperada del servidor de autorización y se actualiza periódicamente.

- Introspección remota

También puede utilizar la introspección remota para validar tokens en el servidor de autorización. La introspección es un protocolo que permite a las partes autorizadas consultar un servidor de autorización sobre un token de acceso. Proporciona a ONTAP una forma de extraer ciertos metadatos de un token de acceso y validar el token. ONTAP almacena en la caché algunos datos por razones de rendimiento.

Ubicación de red

ONTAP puede estar detrás de un firewall. En este caso, debe identificar un proxy como parte de la configuración.

Cómo se definen los servidores de autorización

Puede definir un servidor de autorización para ONTAP mediante cualquiera de las interfaces de administración, incluida la CLI, System Manager o la API DE REST. Por ejemplo, con la CLI utiliza el comando `security oauth2 client create`.

Número de servidores de autorización

Puede definir hasta ocho servidores de autorización en un solo clúster de ONTAP. El mismo servidor de autorización se puede definir más de una vez en el mismo clúster de ONTAP, siempre y cuando las reclamaciones del emisor o del emisor/público sean únicas. Por ejemplo, con Keycloak esto siempre será el caso cuando se utilizan diferentes dominios.

Uso de tokens de acceso OAuth 2,0

Los tokens de acceso OAuth 2,0 emitidos por los servidores de autorización son verificados por ONTAP y utilizados para tomar decisiones de acceso basadas en roles para las solicitudes del cliente API REST.

Adquiriendo un token de acceso

Es necesario adquirir un token de acceso de un servidor de autorización definido en el clúster de ONTAP donde se utiliza la API DE REST. Para adquirir un token, debe ponerse en contacto directamente con el servidor de autorización.



ONTAP no emite tokens de acceso ni redirige las solicitudes de los clientes a los servidores de autorización.

La forma en que se solicita un token depende de varios factores, entre ellos:

- Servidor de autorización y sus opciones de configuración
- Tipo de concesión OAuth 2,0
- Cliente o herramienta de software utilizada para emitir la solicitud

Tipos de concesión

Un *grant* es un proceso bien definido, que incluye un conjunto de flujos de red, utilizado para solicitar y recibir un token de acceso OAuth 2,0. Se pueden utilizar varios tipos de concesión diferentes en función del cliente, el entorno y los requisitos de seguridad. En la tabla siguiente se presenta una lista de los tipos de subvención más populares.

| Tipo de concesión | Descripción |
|-------------------------|--|
| Credenciales de cliente | Tipo de concesión popular basado en el uso de solo credenciales (como un ID y un secreto compartido). Se supone que el cliente tiene una relación de confianza cercana con el propietario del recurso. |
| Contraseña | El tipo de concesión de credenciales de contraseña de propietario del recurso se puede utilizar en los casos en que el propietario del recurso tenga una relación de confianza establecida con el cliente. También puede ser útil al migrar clientes HTTP heredados a OAuth 2,0. |
| Código de autorización | Este es un tipo de concesión ideal para clientes confidenciales y se basa en un flujo basado en redirección. Se puede utilizar para obtener un token de acceso y un token de refrescamiento. |

Contenido de JWT

Un token de acceso OAuth 2,0 se formatea como JWT. El contenido es creado por el servidor de autorización en función de su configuración. Sin embargo, los tokens son opacos para las aplicaciones cliente. Un cliente no tiene ninguna razón para inspeccionar un token o para ser consciente de su contenido.

Cada token de acceso JWT contiene un juego de reclamaciones. Las reclamaciones describen las características del emisor y la autorización en función de las definiciones administrativas del servidor de autorización. Algunas de las reclamaciones registradas con el estándar se describen en la siguiente tabla. Todas las cadenas distinguen mayúsculas de minúsculas.

| Reclamación | Palabra clave | Descripción |
|---------------|---------------|---|
| Emisor | iss | Identifica el principal que emitió el token. El procesamiento de la reclamación es específico de la aplicación. |
| Asunto | secundario | Asunto o usuario del token. El ámbito del nombre es global o localmente único. |
| Destinatarios | aud | Destinatarios para los que está destinado el token. Implementado como una matriz de cadenas. |
| Caducidad | exp | Hora después de la cual el token caduca y debe rechazarse. |

Consulte ["RFC 7519: Tokens web JSON"](#) si quiere más información.

Opciones para la autorización de cliente de ONTAP

Hay varias opciones disponibles para personalizar la autorización de cliente de ONTAP. Las decisiones de autorización se basan, en última instancia, en los roles REST DE ONTAP contenidos en o derivados de los tokens de acceso.



Solo puede utilizar ["Roles DE REST de ONTAP"](#) Al configurar la autorización para OAuth 2,0. No se admiten los roles tradicionales de ONTAP anteriores.

Introducción

La implementación de OAuth 2,0 en ONTAP está diseñada para ser flexible y robusta, proporcionando las opciones que necesita para proteger el entorno ONTAP. En un nivel superior, hay tres categorías de configuración principales para definir la autorización de cliente de ONTAP. Estas opciones de configuración son mutuamente excluyentes.

ONTAP aplica la opción más adecuada en función de su configuración. Consulte ["Cómo ONTAP determina el acceso"](#) Para obtener más información sobre cómo ONTAP procesa sus definiciones de configuración para tomar decisiones de acceso.

OAuth 2,0 ámbitos independientes

Estos ámbitos contienen uno o más roles REST personalizados, cada uno encapsulado en una sola cadena. Son independientes de las definiciones de roles de ONTAP. Debe definir estas cadenas de ámbito en el servidor de autorización.

Roles y usuarios de REST locales específicos de ONTAP

Según su configuración, las definiciones de identidad ONTAP locales se pueden utilizar para tomar decisiones de acceso. Las opciones incluyen:

- Rol REST con nombre único
- La coincidencia del nombre de usuario con un usuario de ONTAP local

La sintaxis del ámbito para un rol con nombre es **ontap-role-`<URL-encoded-ONTAP-role-name>`**. Por ejemplo, si el rol es «admin», la cadena de alcance será «ontap-role-admin».

Grupos de Active Directory o LDAP

Si se examinan las definiciones de ONTAP locales pero no se puede tomar ninguna decisión de acceso, se utilizan los grupos de Active Directory («dominio») o LDAP («nsswitch»). La información del grupo se puede especificar de dos formas:

- Cadena de ámbito de OAuth 2,0

Admite aplicaciones confidenciales mediante el flujo de credenciales de cliente donde no hay ningún usuario con una pertenencia a grupo. El ámbito debe denominarse **ontap-group-`<URL-encoded-ONTAP-group-name>`**. Por ejemplo, si el grupo está en «desarrollo», la cadena de alcance será «ontap-group-development».

- En el reclamo de "grupo"

Esto está destinado a los tokens de acceso emitidos por ADFS mediante el flujo de propietario de recursos (concesión de contraseña).

Alcances OAuth 2,0 autónomos

Los ámbitos autónomos son cadenas que se llevan en el token de acceso. Cada una de ellas es una definición de función personalizada completa e incluye todo lo que ONTAP necesita para tomar una decisión de acceso. El ámbito está separado y distinto de cualquiera de los roles de REST definidos en el propio ONTAP.

Formato de la cadena de ámbito

En un nivel base, el ámbito se representa como una cadena contigua y se compone de seis valores separados por dos puntos. Los parámetros utilizados en la cadena de ámbito se describen a continuación.

ONTAP literal

El ámbito debe comenzar con el valor literal `ontap` en minúscula. Identifica el ámbito como específico de ONTAP.

Clúster

Esto define al cluster de ONTAP al que se aplica el ámbito. Los valores pueden incluir:

- UUID de clúster

Identifica un único clúster.

- Asterisco (*)

Indica que el ámbito se aplica a todos los clusters.

Puede usar el comando de la CLI de ONTAP `cluster identity show` Para mostrar el UUID del clúster. Si no se especifica, el ámbito se aplica a todos los clusters.

Función

Nombre del rol REST contenido en el ámbito autónomo. ONTAP no examina este valor ni se relaciona con ningún rol de REST existente definido con ONTAP. El nombre se utiliza para el registro.

Nivel de acceso

Este valor indica el nivel de acceso aplicado a la aplicación cliente cuando se utiliza el punto final de API en el ámbito. Hay seis valores posibles, como se describe en la tabla siguiente.

| Nivel de acceso | Descripción |
|--------------------|--|
| ninguno | Deniega todo el acceso al punto final especificado. |
| sólo lectura | Permite solo el acceso de lectura mediante GET. |
| read_create | Permite el acceso de lectura, así como la creación de nuevas instancias de recursos mediante POST. |
| read_modify | Permite el acceso de lectura, así como la capacidad de actualizar los recursos existentes MEDIANTE PARCHE. |
| read_create_modify | Permite todos los accesos excepto eliminar. Las operaciones permitidas incluyen GET (READ), POST (CREATE) y PARCHE (UPDATE). |

| Nivel de acceso | Descripción |
|-----------------|-----------------------------|
| todo | Permite un acceso completo. |

SVM

El nombre de la SVM dentro del clúster al que se aplica el ámbito. Utilice el valor * (asterisco) para indicar todas las SVM.



Esta función no es totalmente compatible con ONTAP 9.14.1. Puede ignorar el parámetro SVM y usar un asterisco como marcador de posición. Revise la ["Notas de la versión de ONTAP"](#) Para comprobar si hay compatibilidad futura con SVM.

URI DE LA API DE REST

Ruta de acceso completa o parcial a un recurso o juego de recursos relacionados. La cadena debe comenzar por `/api`. Si no especifica un valor, el alcance se aplica a todos los extremos de API en el clúster de ONTAP.

Ejemplos de ámbito

A continuación se presentan algunos ejemplos de ámbitos autónomos.

ontap:*:joes-role:read_create_modify:*/api/cluster

Proporciona al usuario asignado a este rol acceso de lectura, creación y modificación al `/cluster` extremo.

Herramienta administrativa de la CLI

Para que la administración de los ámbitos autónomos sea más sencilla y menos propensa a errores, ONTAP proporciona el comando de la CLI `security oauth2 scope` para generar cadenas de alcance basadas en los parámetros de entrada.

El comando `security oauth2 scope` tiene dos casos de uso basados en su información:

- Parámetros de CLI para la cadena de ámbito

Puede utilizar esta versión del comando para generar una cadena de ámbito basada en los parámetros de entrada.

- Cadena de ámbito para parámetros de CLI

Puede utilizar esta versión del comando para generar los parámetros del comando basados en la cadena de ámbito de entrada.

Ejemplo

El siguiente ejemplo genera una cadena de ámbito con la salida incluida después del siguiente ejemplo de comando. La definición se aplica a todos los clusters.

```
security oauth2 scope cli-to-scope -role joes-role -access readonly -api
/api/cluster
```

```
ontap:*:joes-role:readonly:*:/api/cluster
```

Cómo ONTAP determina el acceso

Para diseñar e implementar correctamente OAuth 2,0, es necesario comprender cómo ONTAP utiliza su configuración de autorización para tomar decisiones de acceso para los clientes.

Paso 1: Ámbitos autónomos

Si el token de acceso contiene cualquier ámbito autónomo, ONTAP examina esos ámbitos primero. Si no hay ámbitos autónomos, vaya al paso 2.

Con uno o más ámbitos independientes presentes, ONTAP aplica cada ámbito hasta que se pueda tomar una decisión explícita de **PERMITIR** o **NEGAR**. Si se toma una decisión explícita, el procesamiento finaliza.

Si ONTAP no puede tomar una decisión de acceso explícita, continúe con el paso 2.

Paso 2: Compruebe el indicador de roles locales

ONTAP examina el valor de la bandera `use-local-roles-if-present`. El valor de este indicador se define por separado para cada servidor de autorización definido en ONTAP.

- Si el valor es `true` continúe con el paso 3.
- Si el valor es `false` el procesamiento finaliza y se deniega el acceso.

Paso 3: Se denomina rol REST ONTAP

Si el token de acceso contiene un rol REST con nombre, ONTAP utiliza el rol para tomar la decisión de acceso. Esto siempre da como resultado una decisión **ALLOW** o **DENY** y el procesamiento termina.

Si no hay ningún rol REST con nombre o no se encuentra el rol, continúe con el paso 4.

Paso 4: Usuarios locales de ONTAP

Extraiga el nombre de usuario del token de acceso e intente relacionarlo con un usuario local de ONTAP.

Si un usuario local de ONTAP coincide, ONTAP utiliza el rol definido para que el usuario tome una decisión de acceso. Esto siempre resulta en una decisión **ALLOW** o **DENY** y el procesamiento termina.

Si un usuario local de ONTAP no coincide o si no hay nombre de usuario en el token de acceso, continúe con el paso 5.

Paso 5: Asignación de grupos a roles

Extraiga el grupo del token de acceso e intente relacionarlo con un grupo. Los grupos se definen mediante Active Directory o un servidor LDAP equivalente.

Si hay una coincidencia de grupo, ONTAP utiliza el rol definido para el grupo para tomar una decisión de acceso. Esto siempre resulta en una decisión **ALLOW** o **DENY** y el procesamiento termina.

Si no hay ninguna coincidencia de grupo o si no hay ningún grupo en el token de acceso, el acceso se deniega y el procesamiento finaliza.

Escenarios de despliegue de OAuth 2,0

Hay varias opciones de configuración disponibles al definir un servidor de autorización en ONTAP. Basándose en estas opciones, puede crear un servidor de autorización adecuado para su entorno de despliegue.

Resumen de los parámetros de configuración

Hay varios parámetros de configuración disponibles al definir un servidor de autorización en ONTAP. Estos parámetros se admiten generalmente en todas las interfaces administrativas.

Los nombres de los parámetros pueden variar levemente dependiendo de la interfaz administrativa de ONTAP. Por ejemplo, al configurar la introspección remota, el punto final se identifica mediante el parámetro de comando CLI `-introspection-endpoint`. Pero con System Manager, el campo equivalente es *Authorization server token introspection URI*. Para acomodar todas las interfaces administrativas de ONTAP, se proporciona una descripción general de los parámetros. El parámetro o campo exacto debe ser obvio en función del contexto.

| Parámetro | Descripción |
|--|--|
| Nombre | Nombre del servidor de autorización tal y como lo conoce ONTAP. |
| Ciente más | Aplicación interna de ONTAP a la que se aplica la definición. Debe ser http . |
| URI del emisor | El FQDN con ruta que identifica el sitio u organización que emite los tokens. |
| URI de JWKS de Proveedor | El FQDN con ruta y nombre de archivo donde ONTAP obtiene los conjuntos de claves web JSON utilizados para validar los tokens de acceso. |
| Intervalo de refrescamiento de JWKS | Intervalo de tiempo que determina la frecuencia con la que ONTAP refresca la información de certificado del URI JWKS del proveedor. El valor se especifica en formato ISO-8601. |
| Punto final de introspección | El FQDN con ruta que ONTAP utiliza para realizar la validación remota de tokens mediante introspección. |
| ID del cliente | El nombre del cliente tal y como se define en el servidor de autorización. Cuando se incluye este valor, también debe proporcionar el secreto de cliente asociado basado en la interfaz. |
| Proxy saliente | Esto es para proporcionar acceso al servidor de autorización cuando ONTAP está detrás de un firewall. El URI debe tener el formato cURL. |
| Utilice roles locales si están presentes | Un indicador booleano que determina si se usan las definiciones de ONTAP locales, incluido un rol REST con nombre y los usuarios locales. |
| Eliminar reclamación de usuario | Nombre alternativo que utiliza ONTAP para coincidir con los usuarios locales. Utilice la <code>sub</code> del token de acceso para que coincida con el nombre de usuario local. |

Escenarios de puesta en marcha

A continuación se presentan varios escenarios de implementación comunes. Se organizan en función de si ONTAP realiza la validación de tokens de forma local o remota mediante el servidor de autorización. Cada escenario incluye una lista de las opciones de configuración necesarias. Consulte "[Desplegar OAuth 2.0 en ONTAP](#)" para ver ejemplos de los comandos de configuración.



Después de definir un servidor de autorización, puede mostrar su configuración a través de la interfaz administrativa de ONTAP. Por ejemplo, utilice el comando `security oauth2 client show` Con la CLI de ONTAP.

Validación local

Los siguientes escenarios de implementación se basan en que ONTAP realiza la validación de tokens localmente.

Utilice ámbitos autónomos sin proxy

Esta es la implementación más sencilla utilizando solo los ámbitos autónomos de OAuth 2,0. No se utiliza ninguna definición de identidad ONTAP local. Debe incluir los siguientes parámetros:

- Nombre
- Aplicación (http)
- URI de JWKS de Proveedor
- URI del emisor

También debe añadir los ámbitos en el servidor de autorización.

Utilice ámbitos autónomos con un proxy

Este escenario de despliegue utiliza los ámbitos autónomos de OAuth 2,0. No se utiliza ninguna definición de identidad ONTAP local. Pero el servidor de autorización está detrás de un firewall y, por lo tanto, debe configurar un proxy. Debe incluir los siguientes parámetros:

- Nombre
- Aplicación (http)
- URI de JWKS de Proveedor
- Proxy saliente
- URI del emisor
- Destinatarios

También debe añadir los ámbitos en el servidor de autorización.

Use los roles de usuario local y la asignación predeterminada del nombre de usuario con un proxy

Este escenario de despliegue utiliza roles de usuario local con asignación de nombres por defecto. La reclamación de usuario remoto utiliza el valor predeterminado de `sub` por lo tanto, este campo en el token de acceso se utiliza para coincidir con el nombre de usuario local. El nombre de usuario debe tener 40 caracteres o menos. El servidor de autorización está detrás de un firewall, por lo que también debe configurar un proxy. Debe incluir los siguientes parámetros:

- Nombre
- Aplicación (http)
- URI de JWKS de Proveedor
- Utilice roles locales si están presentes (`true`)
- Proxy saliente
- Emisor

Debe asegurarse de que el usuario local esté definido en ONTAP.

Use roles de usuario local y una asignación de nombre de usuario alternativa con un proxy

Este escenario de despliegue utiliza roles de usuario local con un nombre de usuario alternativo que se utiliza

para que coincida con un usuario local de ONTAP. El servidor de autorización está detrás de un firewall, por lo que debe configurar un proxy. Debe incluir los siguientes parámetros:

- Nombre
- Aplicación (http)
- URI de JWKS de Proveedor
- Utilice roles locales si están presentes (`true`)
- Reclamación de usuario remoto
- Proxy saliente
- URI del emisor
- Destinatarios

Debe asegurarse de que el usuario local esté definido en ONTAP.

Introspección remota

Las siguientes configuraciones de implementación se basan en que ONTAP realiza la validación de tokens de forma remota a través de introspección.

Utilice ámbitos autónomos sin proxy

Esta es una implementación sencilla basada en el uso de los ámbitos autónomos OAuth 2.0. No se utiliza ninguna definición de identidad de ONTAP. Debe incluir los siguientes parámetros:

- Nombre
- Aplicación (http)
- Punto final de introspección
- ID del cliente
- URI del emisor

Debe definir los ámbitos, así como el secreto de cliente y cliente en el servidor de autorización.

Autenticación de clientes mediante TLS mutuo

Dependiendo de sus necesidades de seguridad, puede configurar opcionalmente TLS mutuo (MTLS) para implementar una autenticación de cliente fuerte. Cuando se utiliza con ONTAP como parte de una implementación de OAuth 2.0, MTLS garantiza que los tokens de acceso solo son utilizados por los clientes a los que se emitieron originalmente.

TLS Mutuo con OAuth 2.0

La seguridad de la capa de transporte (TLS) se utiliza para establecer un canal de comunicación seguro entre dos aplicaciones, normalmente un explorador de cliente y un servidor web. El TLS Mutuo amplía esto proporcionando una identificación sólida del cliente a través de un certificado de cliente. Cuando se utiliza en un clúster de ONTAP con OAuth 2.0, la funcionalidad MTLS base se amplía mediante la creación y el uso de tokens de acceso restringidos por el remitente.

Un token de acceso restringido por remitente solo puede ser utilizado por el cliente para el que se emitió

originalmente. Para admitir esta función, una nueva reclamación de confirmación (`cnf`) se inserta en el token. El campo contiene propiedad `x5t#S256` contiene un resumen del certificado de cliente utilizado al solicitar el token de acceso. ONTAP verifica este valor como parte de la validación del token. Los tokens de acceso emitidos por los servidores de autorización que no están restringidos por el remitente no incluyen la reclamación de confirmación adicional.

Debe configurar ONTAP para que utilice MTLS por separado para cada servidor de autorización. Por ejemplo, el comando de la CLI `security oauth2 client` incluye el parámetro `use-mutual-tls`. Para controlar el procesamiento MTLS basado en tres valores como se muestra en la tabla siguiente.



En cada configuración, el resultado y la acción de ONTAP dependen del valor del parámetro de configuración, así como del contenido del token de acceso y del certificado del cliente. Los parámetros de la tabla se organizan desde el más mínimo hasta el más restrictivo.

| Parámetro | Descripción |
|-------------|---|
| ninguno | La autenticación TLS mutua OAuth 2,0 está completamente desactivada para el servidor de autorización. ONTAP no realizará la autenticación del certificado de cliente MTLS incluso si la reclamación de confirmación está presente en el token o si se proporciona un certificado de cliente con la conexión TLS. |
| petición | OAuth 2,0 La autenticación TLS mutua se aplica si el cliente presenta un token de acceso restringido por el remitente. Es decir, MTLS se aplica solo si la reclamación de confirmación (con propiedad <code>x5t#S256</code>) está presente en el token de acceso. Esta es la configuración predeterminada. |
| obligatorio | La autenticación TLS mutua OAuth 2,0 se aplica a todos los tokens de acceso emitidos por el servidor de autorización. Por lo tanto, todos los tokens de acceso deben estar restringidos por el remitente. Se producen errores en la autenticación y la solicitud de API de REST si la reclamación de confirmación no está presente en el token de acceso o si existe un certificado de cliente no válido. |

Flujo de implantación de alto nivel

A continuación se presentan los pasos típicos que implica el uso de MTLS con OAuth 2,0 en un entorno ONTAP. Consulte ["RFC 8705: Autenticación de cliente Mutual-TLS de OAuth 2,0 y tokens de acceso vinculados a certificados"](#) para obtener más detalles.

Paso 1: Crear e instalar un certificado de cliente

El establecimiento de la identidad del cliente se basa en demostrar el conocimiento de una clave privada del cliente. La clave pública correspondiente se coloca en un certificado X,509 firmado presentado por el cliente. En un nivel alto, los pasos involucrados en la creación del certificado de cliente incluyen:

1. Generar un par de claves públicas y privadas
2. Cree una solicitud de firma de certificación
3. Envíe el archivo CSR a una CA conocida
4. CA verifica la solicitud y emite el certificado firmado

Normalmente, puede instalar el certificado de cliente en su sistema operativo local o usarlo directamente con una utilidad común, como `cURL`.

Paso 2: Configure ONTAP para usar MTLS

Debe configurar ONTAP para que utilice MTLS. Esta configuración se realiza por separado para cada servidor

de autorización. Por ejemplo, con la CLI el comando `security oauth2 client` se utiliza con el parámetro opcional `use-mutual-tls`. Consulte ["Desplegar OAuth 2,0 en ONTAP"](#) si quiere más información.

Paso 3: El cliente solicita un token de acceso

El cliente necesita solicitar un token de acceso desde el servidor de autorización configurado en ONTAP. La aplicación cliente debe utilizar MTLS con el certificado creado e instalado en el paso 1.

Paso 4: El servidor de autorización genera el token de acceso

El servidor de autorización verifica la solicitud del cliente y genera un token de acceso. Como parte de esto, crea un resumen de mensaje del certificado de cliente que se incluye en el token como una reclamación de confirmación (campo `cnf`).

Paso 5: La aplicación cliente presenta el token de acceso a ONTAP

La aplicación cliente realiza una llamada a la API REST al clúster de ONTAP e incluye el token de acceso en el encabezado de solicitud de autorización como un token **portador**. El cliente debe utilizar MTLS con el mismo certificado utilizado para solicitar el token de acceso.

Paso 6: ONTAP verifica el cliente y el token.

ONTAP recibe el token de acceso en una solicitud HTTP, así como el certificado de cliente utilizado como parte del procesamiento MTLS. ONTAP valida primero la firma en el token de acceso. En función de la configuración, ONTAP genera un resumen de mensaje del certificado de cliente y lo compara con la reclamación de confirmación `cnf` en el token. Si los dos valores coinciden, ONTAP ha confirmado que el cliente que hace la solicitud API es el mismo cliente al que se emitió originalmente el token de acceso.

Configurar e implementar

Prepárese para implementar OAuth 2,0 con ONTAP

Antes de configurar OAuth 2,0 en un entorno ONTAP, debe prepararse para el despliegue. A continuación se incluye un resumen de las principales tareas y decisiones. La disposición de las secciones generalmente está alineada con el orden que debe seguir. Sin embargo, si bien es aplicable a la mayoría de las implementaciones, debe adaptarlo a su entorno según sea necesario. También debe considerar la creación de un plan de despliegue formal.



En función del entorno, puede seleccionar la configuración de los servidores de autorización definidos en ONTAP. Esto incluye los valores de parámetros que necesita especificar para cada tipo de despliegue. Consulte ["Escenarios de despliegue de OAuth 2,0"](#) si quiere más información.

Recursos protegidos y aplicaciones cliente

OAuth 2,0 es un marco de autorización para controlar el acceso a los recursos protegidos. Dado esto, un primer paso importante en cualquier implementación es determinar cuáles son los recursos disponibles y qué clientes necesitan acceder a ellos.

Identificar aplicaciones cliente

Debe decidir qué clientes utilizarán OAuth 2,0 al emitir llamadas a la API REST y a qué puntos finales API necesitan acceso.

Revisar los roles DE REST DE ONTAP y los usuarios locales existentes

Debe revisar las definiciones de identidad ONTAP existentes, incluidos los roles REST y los usuarios locales. Dependiendo de cómo configure OAuth 2,0, estas definiciones se pueden utilizar para tomar decisiones de acceso.

Transición global a OAuth 2,0

Aunque puede implementar la autorización OAuth 2,0 gradualmente, también puede mover todos los clientes de la API REST a OAuth 2,0 inmediatamente estableciendo un indicador global para cada servidor de autorización. Esto permite tomar decisiones de acceso según la configuración de ONTAP existente sin necesidad de crear ámbitos independientes.

Servidores de autorización

Los servidores de autorización desempeñan un papel importante en su implementación de OAuth 2,0 mediante la emisión de tokens de acceso y la aplicación de la política administrativa.

Seleccione e instale el servidor de autorización

Debe seleccionar e instalar uno o más servidores de autorización. Es importante familiarizarse con las opciones de configuración y los procedimientos de sus proveedores de identidad, incluido cómo definir ámbitos.

Determine si es necesario instalar el certificado de CA raíz de autorización

ONTAP utiliza el certificado del servidor de autorización para validar los tokens de acceso firmados presentados por los clientes. Para hacerlo, ONTAP necesita el certificado de CA raíz y todos los certificados intermedios. Estos pueden preinstalarse con ONTAP. Si no es así, debe instalarlos.

Evalúe la ubicación y la configuración de la red

Si el servidor de autorización está detrás de un firewall, ONTAP debe configurarse para utilizar un servidor proxy.

Autenticación y autorización de clientes

Hay varios aspectos de la autenticación y autorización del cliente que debe considerar.

Ámbitos autónomos o definiciones de identidad locales de ONTAP

En un nivel superior, puede definir ámbitos independientes definidos en el servidor de autorización o basarse en las definiciones de identidad de ONTAP local existentes, incluidos los roles y los usuarios.

Opciones con procesamiento ONTAP local

Si utiliza las definiciones de identidad de ONTAP, debe decidir cuáles aplicar, entre ellas:

- Rol REST con nombre
- Coincide con los usuarios locales
- Grupos de Active Directory o LDAP

Validación local o introspección remota

Debe decidir si los tokens de acceso serán validados localmente por ONTAP o en el servidor de autorización mediante introspección. También hay varios valores relacionados que se deben tener en cuenta, como el intervalo de refrescamiento.

Tokens de acceso restringidos por el remitente

Para entornos que requieren un alto nivel de seguridad, puede utilizar tokens de acceso con restricciones de envío basados en MTLS. Esto requiere un certificado para cada cliente.

Interfaz administrativa

Puede realizar la administración de OAuth 2,0 a través de cualquiera de las interfaces ONTAP, incluyendo:

- Interfaz de línea de comandos
- System Manager
- API REST

Cómo solicitan los clientes tokens de acceso

Las aplicaciones cliente deben solicitar tokens de acceso directamente desde el servidor de autorización. Debe decidir cómo se hará esto, incluido el tipo de subvención.

Configure ONTAP

Debe realizar varias tareas de configuración de ONTAP.

Defina los roles REST y los usuarios locales

En función de la configuración de autorización, se puede utilizar el procesamiento de identificación de ONTAP local. En este caso, debe revisar y definir los roles REST y las definiciones de usuario.

Configuración central

Hay tres pasos principales necesarios para llevar a cabo la configuración principal de ONTAP, incluyendo los siguientes:

- Opcionalmente, instale el certificado raíz (y cualquier certificado intermedio) para la CA que firmó el certificado del servidor de autorización.
- Defina el servidor de autorización.
- Habilite el procesamiento de OAuth 2,0 para el clúster.

Desplegar OAuth 2,0 en ONTAP

La implementación de la funcionalidad principal de OAuth 2,0 implica tres pasos principales.

Antes de empezar

Debe prepararse para el despliegue de OAuth 2,0 antes de configurar ONTAP. Por ejemplo, debe evaluar el servidor de autorización, incluido cómo se firmó su certificado y si está detrás de un firewall. Consulte ["Prepárese para implementar OAuth 2,0 con ONTAP"](#) si quiere más información.

Paso 1: Instale el certificado del servidor de autenticación

ONTAP incluye un gran número de certificados de CA raíz preinstalados. Por lo tanto, en muchos casos, el certificado para su servidor de autorización será reconocido inmediatamente por ONTAP sin configuración adicional. Pero dependiendo de cómo se haya firmado el certificado del servidor de autorización, es posible que necesite instalar un certificado de CA raíz y cualquier certificado intermedio.

Siga las instrucciones proporcionadas a continuación para instalar el certificado si es necesario. Debe instalar todos los certificados necesarios en el nivel de clúster.

Elija el procedimiento correcto en función de cómo acceda a ONTAP.

Ejemplo 17. Pasos

System Manager

1. En System Manager, selecciona **Clúster > Configuración**.
2. Desplácese hacia abajo hasta la sección **Seguridad**.
3. Haga clic en → junto a **Certificados**.
4. En la pestaña **Autoridades de certificación de confianza**, haga clic en **Agregar**.
5. Haga clic en **Importar** y seleccione el archivo de certificado.
6. Complete los parámetros de configuración del entorno.
7. Haga clic en **Agregar**.

CLI

1. Comience la instalación:

```
security certificate install -type server-ca
```

2. Busque el siguiente mensaje de la consola:

```
Please enter Certificate: Press <Enter> when done
```

3. Abra el archivo de certificado con un editor de texto.
4. Copie todo el certificado, incluidas las siguientes líneas:

```
-----BEGIN CERTIFICATE-----  
  
-----END CERTIFICATE-----
```

5. Pegue el certificado en el terminal después del símbolo del sistema.
6. Presione **Enter** para completar la instalación.
7. Confirme la instalación del certificado mediante uno de los siguientes métodos:

```
security certificate show-user-installed  
  
security certificate show
```

Paso 2: Configure el servidor de autorización

Debe definir al menos un servidor de autorización para ONTAP. Debe elegir los valores de los parámetros en función de su plan de configuración e implementación. Revisar ["Situaciones de puesta en marcha de OAuth2"](#) para determinar los parámetros exactos necesarios para la configuración.



Para modificar una definición de servidor de autorización, puede suprimir la definición existente y crear una nueva.

El ejemplo que se proporciona a continuación se basa en el primer escenario de implementación simple en ["Validación local"](#). Los ámbitos autónomos se utilizan sin un proxy.

Elija el procedimiento correcto en función de cómo acceda a ONTAP. El procedimiento de la CLI utiliza

variables simbólicas que hay que reemplazar antes de emitir el comando.

Ejemplo 18. Pasos

System Manager

1. En System Manager, selecciona **Clúster > Configuración**.
2. Desplácese hacia abajo hasta la sección **Seguridad**.
3. Haga clic en **+** junto a **Autorización OAuth 2,0**.
4. Selecciona **Más opciones**.
5. Proporcione los valores necesarios para el despliegue, como:
 - Nombre
 - Aplicación (http)
 - URI de JWKS de Proveedor
 - URI del emisor
6. Haga clic en **Agregar**.

CLI

1. Vuelva a crear la definición:

```
security oauth2 client create -config-name <NAME> -provider-jwks-uri  
<URI_JWKS> -application http -issuer <URI_ISSUER>
```

Por ejemplo:

```
security oauth2 client create \  
-config-name auth0 \  
-provider-jwks-uri https://superzap.dev.netapp.com:8443/realms/my-  
realm/protocol/openid-connect/certs \  
-application http \  
-issuer https://superzap.dev.netapp.com:8443/realms/my-realm
```

Paso 3: Habilite OAuth 2,0

El paso final es habilitar OAuth 2,0. Se trata de una configuración global para el clúster de ONTAP.



No habilite el procesamiento de OAuth 2,0 hasta que confirme que ONTAP, los servidores de autorización y los servicios de soporte se han configurado correctamente.

Elija el procedimiento correcto en función de cómo acceda a ONTAP.

Ejemplo 19. Pasos

System Manager

1. En System Manager, selecciona **Clúster > Configuración**.
2. Desplácese hacia abajo hasta la sección **Seguridad**.
3. Haga clic en → junto a **OAuth 2,0 AUTORIZATION**.
4. Habilita **OAuth 2,0 autorización**.

CLI

1. Activar OAuth 2,0:

```
security oauth2 modify -enabled true
```

2. Confirme que OAuth 2,0 está activado:

```
security oauth2 show  
Is OAuth 2.0 Enabled: true
```

Emita una llamada a la API REST mediante OAuth 2,0

La implementación de OAuth 2,0 en ONTAP es compatible con las aplicaciones del cliente API de REST. Puede emitir una llamada a la API de REST simple usando cURL para comenzar a usar OAuth 2,0. El ejemplo que se presenta a continuación recupera la versión del cluster de ONTAP.

Antes de empezar

Tiene que configurar y habilitar la función OAuth 2,0 para el clúster de ONTAP. Esto incluye la definición de un servidor de autorización.

Paso 1: Adquiera un token de acceso

Debe adquirir un token de acceso para utilizarlo con la llamada de la API de REST. La solicitud de token se realiza fuera de ONTAP y el procedimiento exacto depende del servidor de autorización y de su configuración. Puede solicitar el token a través de un navegador web, con un comando curl o utilizando un lenguaje de programación.

Para fines ilustrativos, a continuación se presenta un ejemplo de cómo se puede solicitar un token de acceso desde Keycloak usando curl.

Ejemplo de Keycloak

```
curl --request POST \  
--location  
'https://superzap.dev.netapp.com:8443/realms/peterson/protocol/openid-  
connect/token' \  
--header 'Content-Type: application/x-www-form-urlencoded' \  
--data-urlencode 'client_id=dp-client-1' \  
--data-urlencode 'grant_type=client_credentials' \  
--data-urlencode 'client_secret=5iTUf9QKLGxAoYaliR33v1D5A2xq09V7'
```

Debe copiar y guardar el token devuelto.

Paso 2: Emita la llamada a la API de REST

Una vez que tenga un token de acceso válido, puede usar un comando cURL con el token de acceso para emitir una llamada a la API de REST.

Parámetros y variables

Las dos variables del ejemplo de curl se describen en la tabla siguiente.

| Variable | Descripción |
|----------------|--|
| \$FQDN_IP | El nombre de dominio completo o la dirección IP de la LIF de gestión de ONTAP. |
| \$ACCESS_TOKEN | El token de acceso OAuth 2,0 emitido por el servidor de autorización. |

Primero debe definir estas variables en el entorno de shell de Bash antes de emitir el ejemplo de cURL. Por ejemplo, en la CLI de Linux escriba el siguiente comando para establecer y mostrar la variable FQDN:

```
FQDN_IP=172.14.31.224  
echo $FQDN_IP  
172.14.31.224
```

Después de definir ambas variables en el shell Bash local, puede copiar el comando cURL y pegarlo en la CLI. Presione **Enter** para sustituir las variables y emitir el comando.

Ejemplo de curl

```
curl --request GET \  
--location "https://$FQDN_IP/api/cluster?fields=version" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Bearer $ACCESS_TOKEN"
```

Configurar la autenticación SAML

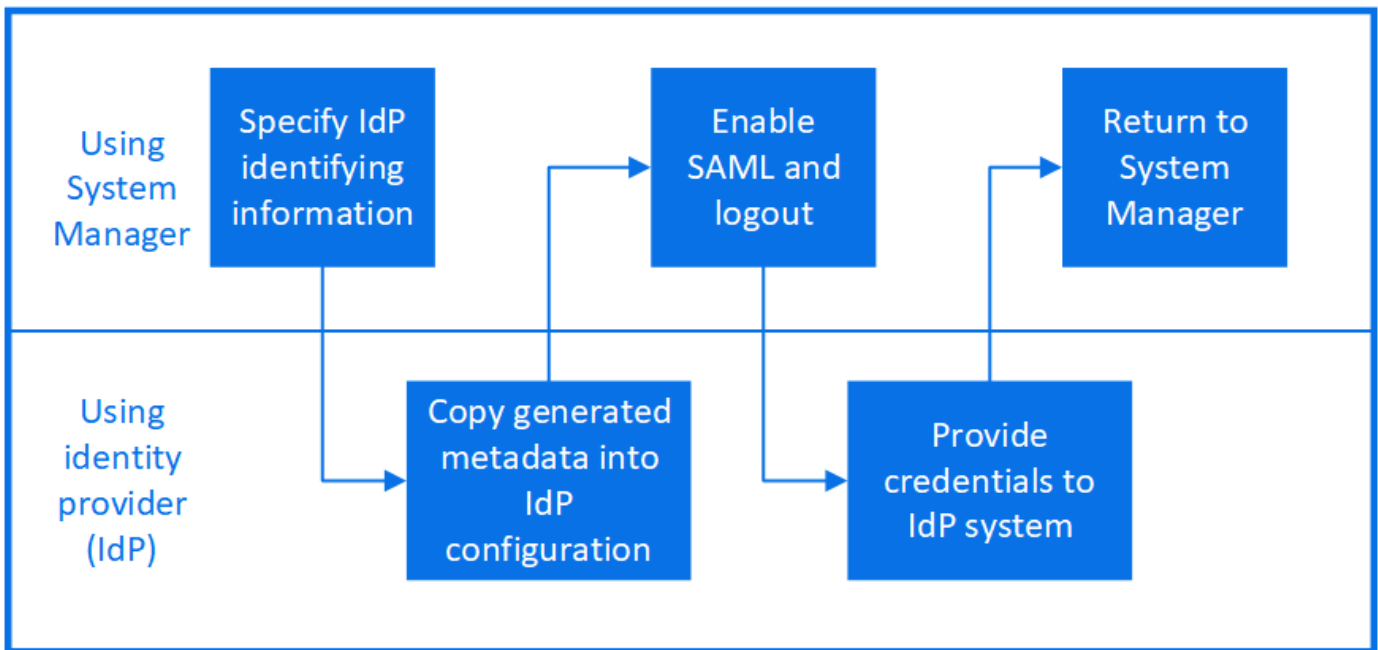
A partir de ONTAP 9.3, puede configurar la autenticación del lenguaje de marcado de aserción de seguridad (SAML) para los servicios web. Cuando se configura y se habilita la autenticación SAML, los usuarios se autentican mediante un proveedor de identidades (IDP) externo en lugar de los proveedores de servicio de directorio, como Active Directory y LDAP.

Habilite la autenticación SAML

Para habilitar la autenticación SAML con System Manager o con la CLI, realice los siguientes pasos. Si el clúster ejecuta ONTAP 9,7 o una versión anterior, los pasos que debe seguir son diferentes. Consulte la ayuda en línea de System Manager disponible en su sistema.



Después de habilitar la autenticación SAML, solo los usuarios remotos pueden acceder a la interfaz gráfica de usuario de System Manager. Los usuarios locales no pueden acceder a la interfaz gráfica de usuario de System Manager después de habilitar la autenticación de SAML.



Antes de empezar

- Se debe configurar el IDP que se planea usar para la autenticación remota.



Consulte la documentación proporcionada por el IDP que se configuró.

- Debe tener el URI del IDP.

Acerca de esta tarea

- La autenticación SAML solo se aplica a `http y.. ontapi` más grandes.

La `http y.. ontapi` Las aplicaciones se utilizan en los siguientes servicios web: Infraestructura de procesador de servicio, API de ONTAP o System Manager.

- La autenticación SAML solo se aplica para acceder a la SVM de administrador.


Los siguientes IDP se han validado con System Manager:

- Servicios de federación de Active Directory
- Cisco DUO (validado con las siguientes versiones de ONTAP:)
 - 9.7P21 y versiones posteriores de 9,7 (consulte la ["Documentación de System Manager Classic"](#))
 - 9.8P17 y versiones posteriores de 9,8
 - 9,9.1P13 y versiones posteriores de 9,9
 - 9.10.1P9 y versiones posteriores de 9,10
 - 9.11.1P4 y versiones posteriores de 9,11
 - 9.12.1 y versiones posteriores
- Shibboleth

Siga estos pasos en función de su entorno:

Ejemplo 20. Pasos

System Manager

1. Haga clic en **clúster > Configuración**.
2. Junto a **autenticación SAML**, haga clic en .
3. Asegúrese de que haya una Marca en la casilla de verificación **Habilitar autenticación SAML**.
4. Introduzca la URL del URI del IDP (incluido "https://").
5. Modifique la dirección del sistema host, si es necesario.
6. Asegúrese de utilizar el certificado correcto:
 - Si su sistema sólo se ha asignado con un certificado con el tipo "servidor", ese certificado se considera el predeterminado y no se muestra.
 - Si su sistema estaba asignado con varios certificados como tipo "servidor", se muestra uno de los certificados. Para seleccionar un certificado diferente, haga clic en **Cambiar**.
7. Haga clic en **Guardar**. Una ventana de confirmación muestra la información de metadatos, que se ha copiado automáticamente en el portapapeles.
8. Vaya al sistema IDP especificado y copie los metadatos del portapapeles para actualizar los metadatos del sistema.
9. Vuelva a la ventana de confirmación (en System Manager) y marque la casilla de verificación **he configurado el IDP con el URI de host o metadatos**.
10. Haga clic en **Cerrar sesión** para activar la autenticación basada en SAML. El sistema IDP mostrará una pantalla de autenticación.
11. En el sistema IDP, introduzca las credenciales basadas en SAML. Una vez verificadas las credenciales, se le dirigirá a la página de inicio de System Manager.

CLI

1. Cree una configuración de SAML para que ONTAP pueda acceder a los metadatos de IDP:

```
security saml-sp create -idp-uri idp_uri -sp-host ontap_host_name
```

`idp_uri` Es la dirección FTP o HTTP del host IDP desde el que se pueden descargar los metadatos de IDP.

`ontap_host_name` Es el nombre de host o la dirección IP del host del proveedor de servicios SAML que, en este caso, es el sistema ONTAP. De manera predeterminada, se utiliza la dirección IP de la LIF de administración del clúster.

Opcionalmente, puede proporcionar la información de certificado del servidor ONTAP. De manera predeterminada, se utiliza la información de certificado de servidor web ONTAP.


```
cluster_12::> security saml-sp create -idp-uri  
https://example.url.net/idp/shibboleth
```

Warning: This restarts the web server. Any HTTP/S connections that are active

will be disrupted.

Do you want to continue? {y|n}: y

[Job 179] Job succeeded: Access the SAML SP metadata using the URL:
https://10.0.0.1/saml-sp/Metadata

Configure the IdP and Data ONTAP users for the same directory server domain to ensure that users are the same for different authentication methods. See the "security login show" command for the Data ONTAP user configuration.

Se muestra la URL para acceder a los metadatos del host ONTAP.

2. Desde el host IDP, configure el IDP con los metadatos del host ONTAP.

Para obtener más información sobre cómo configurar el IDP, consulte la documentación de IDP.

3. Habilitar la configuración de SAML:

```
security saml-sp modify -is-enabled true
```

Cualquier usuario existente que acceda a `http o. ontapi` La aplicación se configura automáticamente para la autenticación SAML.

4. Si desea crear usuarios para `http o. ontapi` Aplicación después de configurar SAML, especifique SAML como método de autenticación de los nuevos usuarios.

- a. Cree un método de inicio de sesión para usuarios nuevos con autenticación SAML:

```
security login create -user-or-group-name user_name -application [http |  
ontapi] -authentication-method saml -vserver svm_name
```

```
cluster_12::> security login create -user-or-group-name admin1  
-application http -authentication-method saml -vserver  
cluster_12
```

- b. Compruebe que se ha creado la entrada de usuario:

```
security login show
```

```
cluster_12::> security login show
```

```
Vserver: cluster_12
```

```
Second
```

| User/Group | Authentication | | Acct |
|----------------|-------------------|----------|-----------|
| Authentication | | | |
| Name | Application | Method | Role Name |
| Method | | | Locked |
| ----- | ----- | ----- | ----- |
| admin | console | password | admin |
| none | | | |
| admin | http | password | admin |
| none | | | |
| admin | http | saml | admin |
| none | | | - |
| admin | ontapi | password | admin |
| none | | | |
| admin | ontapi | saml | admin |
| none | | | - |
| admin | service-processor | | |
| | | password | admin |
| none | | | |
| admin | ssh | password | admin |
| none | | | |
| admin1 | http | password | backup |
| none | | | |
| **admin1 | http | saml | backup |
| none** | | | - |


Deshabilite la autenticación SAML

Es posible deshabilitar la autenticación SAML cuando se desea detener la autenticación de usuarios web mediante un proveedor de identidades (IDP) externo. Cuando se deshabilita la autenticación SAML, los proveedores de servicios de directorio configurados, como Active Directory y LDAP, se usan para la autenticación.

Siga estos pasos en función de su entorno:

Ejemplo 21. Pasos

System Manager

1. Haga clic en **clúster > Configuración**.
2. En **autenticación SAML**, haga clic en el botón de alternar **Activado**.
3. *Opcional:* También puede hacer clic en  Junto a **autenticación SAML** y, a continuación, desactive la casilla de verificación **Activar autenticación SAML**.

CLI

1. Deshabilitar la autenticación SAML:

```
security saml-sp modify -is-enabled false
```

2. Si ya no desea usar autenticación SAML o si desea modificar el IDP, elimine la configuración de SAML:

```
security saml-sp delete
```

Solucione problemas de la configuración de SAML

Si se produce un error al configurar la autenticación del lenguaje de marcado de aserción de seguridad (SAML), puede reparar manualmente cada nodo en el que falló la configuración de SAML y recuperarse del error. Durante el proceso de reparación, se reinicia el servidor web y se interrumpen todas las conexiones HTTP o HTTPS activas.

Acerca de esta tarea

Cuando se configura la autenticación SAML, ONTAP aplica la configuración de SAML por nodo. Cuando habilita la autenticación SAML, ONTAP intenta reparar automáticamente cada nodo si existen problemas de configuración. Si hay problemas con la configuración de SAML en cualquier nodo, puede deshabilitar la autenticación SAML y luego volver a habilitar la autenticación SAML. Puede haber situaciones en las que la configuración de SAML no pueda aplicarse en uno o varios nodos incluso después de volver a habilitar la autenticación SAML. Puede identificar el nodo en el que falló la configuración de SAML y reparar manualmente ese nodo.

Pasos

1. Inicie sesión en el nivel de privilegio avanzado:

```
set -privilege advanced
```

2. Identifique el nodo en el que no pudo realizarse la configuración de SAML:

```
security saml-sp status show -instance
```

```
cluster_12::*> security saml-sp status show -instance

Node: node1
Update Status: config-success
Database Epoch: 9
Database Transaction Count: 997
Error Text:
SAML Service Provider Enabled: false
ID of SAML Config Job: 179

Node: node2
Update Status: config-failed
Database Epoch: 9
Database Transaction Count: 997
Error Text: SAML job failed, Reason: Internal error.
Failed to receive the SAML IDP Metadata file.
SAML Service Provider Enabled: false
ID of SAML Config Job: 180
2 entries were displayed.
```

3. Repare la configuración de SAML en el nodo con errores:

security saml-sp repair -node *node_name*

```
cluster_12::*> security saml-sp repair -node node2

Warning: This restarts the web server. Any HTTP/S connections that are
active
    will be disrupted.
Do you want to continue? {y|n}: y
[Job 181] Job is running.
[Job 181] Job success.
```

Se reinicia el servidor web y se interrumpen las conexiones HTTP o HTTPS activas.

4. Compruebe que SAML se haya configurado correctamente en todos los nodos:

security saml-sp status show -instance

```
cluster_12::*> security saml-sp status show -instance
```

```

                Node: node1
            Update Status: config-success
        Database Epoch: 9
    Database Transaction Count: 997
        Error Text:
SAML Service Provider Enabled: false
        ID of SAML Config Job: 179

                Node: node2
            Update Status: **config-success**
        Database Epoch: 9
    Database Transaction Count: 997
        Error Text:
SAML Service Provider Enabled: false
        ID of SAML Config Job: 180
2 entries were displayed.
```

Información relacionada

["Comandos de ONTAP 9"](#)

Gestionar servicios web

Información general sobre los servicios web de Manage

Puede habilitar o deshabilitar un servicio web para el clúster o una máquina virtual de almacenamiento (SVM), mostrar la configuración de los servicios web y controlar si los usuarios de un rol pueden acceder a un servicio web.

Puede gestionar los servicios web para el clúster o una SVM de las siguientes formas:

- Activación o desactivación de un servicio Web específico
- Especificar si el acceso a un servicio Web está restringido a sólo HTTP (SSL) cifrado
- Mostrar la disponibilidad de los servicios web
- Permitir o rechazar a los usuarios de una función acceder a un servicio web
- Mostrar los roles que pueden tener acceso a un servicio Web

Para que un usuario pueda acceder a un servicio web, se deben cumplir todas las siguientes condiciones:

- Se debe autenticar al usuario.

Por ejemplo, un servicio Web puede solicitar un nombre de usuario y una contraseña. La respuesta del usuario debe coincidir con una cuenta válida.

- Debe configurarse el usuario con el método de acceso correcto.

La autenticación sólo se realiza correctamente para los usuarios con el método de acceso correcto para el servicio web dado. Para el servicio web de la API de ONTAP (`ontapi`), los usuarios deben tener el `ontapi` método de acceso. Para todos los demás servicios web, los usuarios deben tener `http` método de acceso.



Utilice la `security login` comandos para gestionar los métodos de acceso y los métodos de autenticación de los usuarios.

- El servicio web debe estar configurado para permitir la función de control de acceso del usuario.



Utilice la `vserver services web access` comandos para controlar el acceso de un rol a un servicio web.

Si hay un firewall habilitado, la política de firewall para el LIF que se utilizará para los servicios web debe configurarse para permitir HTTP o HTTPS.

Si utiliza HTTPS para el acceso a servicios web, debe habilitar SSL para el clúster o la SVM que ofrece el servicio web, y debe proporcionar un certificado digital para el clúster o la SVM.

Administrar el acceso a los servicios web

Un servicio web es una aplicación a la que los usuarios pueden acceder mediante HTTP o HTTPS. El administrador de clúster puede configurar el motor de protocolo web, configurar SSL, habilitar un servicio web y permitir que los usuarios de un rol accedan a un servicio web.

A partir de ONTAP 9.6, se admiten los siguientes servicios web:

- Infraestructura del procesador de servicios (`spi`)

Este servicio hace que los archivos de registro, volcado de memoria y MIB de un nodo estén disponibles para el acceso HTTP o HTTPS a través de la LIF de gestión de clústeres o de una LIF de gestión de nodos. El valor predeterminado es `enabled`.

Cuando se solicita acceso a los archivos de registro de un nodo o a los archivos de volcado principales, el `spi` el servicio web crea automáticamente un punto de montaje de un nodo al volumen raíz de otro nodo, en el que residen los archivos. No es necesario crear manualmente el punto de montaje. "

- API de ONTAP (`ontapi`)

Este servicio le permite ejecutar API de ONTAP para ejecutar funciones administrativas con un programa remoto. El valor predeterminado es `enabled`.

Es posible que este servicio sea necesario para algunas herramientas de administración externas. Por ejemplo, si utiliza System Manager, debe dejar este servicio habilitado.

- Identificación de Data ONTAP (`disco`)

Este servicio permite que las aplicaciones de administración externas puedan detectar el clúster en la red.

El valor predeterminado es `enabled`.

- Diagnóstico de soporte (`supdiag`)

Este servicio controla el acceso a un entorno privilegiado en el sistema para ayudar al análisis y resolución de problemas. El valor predeterminado es `disabled`. Debe habilitar este servicio solo cuando lo indique el soporte técnico.

- System Manager (`sysmgr`)

Este servicio controla la disponibilidad de System Manager, que se incluye con ONTAP. El valor predeterminado es `enabled`. Este servicio solo es compatible en el clúster.

- Actualización de la controladora de gestión de placa base de firmware (BMC) (`FW_BMC`)

Este servicio le permite descargar archivos de firmware de BMC. El valor predeterminado es `enabled`.

- Documentación de ONTAP (`docs`)

Este servicio proporciona acceso a la documentación de ONTAP. El valor predeterminado es `enabled`.

- API RESTful de ONTAP (`docs_api`)

Este servicio proporciona acceso a la documentación de la API RESTful de ONTAP. El valor predeterminado es `enabled`.

- Carga y descarga de archivos (`fud`)

Este servicio ofrece carga y descarga de archivos. El valor predeterminado es `enabled`.

- Mensajes de ONTAP (`ontapmsg`)

Este servicio admite una interfaz de publicación y suscripción que le permite suscribirse a eventos. El valor predeterminado es `enabled`.

- Portal de ONTAP (`portal`)

Este servicio implementa la puerta de enlace en un servidor virtual. El valor predeterminado es `enabled`.

- Interfaz ONTAP RESTful (`rest`)

Este servicio es compatible con una interfaz RESTful que se utiliza para gestionar de forma remota todos los elementos de la infraestructura de clúster. El valor predeterminado es `enabled`.

- Soporte del proveedor de servicios de lenguaje de marcado de aserción de seguridad (SAML) (`saml`)

Este servicio proporciona recursos para admitir el proveedor de servicios SAML. El valor predeterminado es `enabled`.

- Proveedor de servicios SAML (`saml-sp`)

Este servicio ofrece servicios como metadatos del SP y el servicio de consumidor de aserción al proveedor de servicios. El valor predeterminado es `enabled`.

A partir de ONTAP 9.7, se admiten los siguientes servicios adicionales:

- Archivos de copia de seguridad de configuración (backups)

Este servicio permite descargar archivos de copia de seguridad de configuración. El valor predeterminado es `enabled`.

- Seguridad ONTAP (`security`)

Este servicio admite la gestión de token de CSRF para una autenticación mejorada. El valor predeterminado es `enabled`.

Administrar el motor de protocolo web

Puede configurar el motor de protocolo web en el clúster para controlar si se permite el acceso web y qué versiones SSL se pueden utilizar. También puede mostrar los ajustes de configuración del motor de protocolo web.

Puede gestionar el motor de protocolo web en el nivel de clúster de las siguientes formas:

- Puede especificar si los clientes remotos pueden utilizar HTTP o HTTPS para acceder al contenido del servicio web mediante el `system services web modify` con el `-external` parámetro.
- Puede especificar si SSLv3 debe utilizarse para el acceso seguro a la Web mediante `security config modify` con el `-supported-protocol` parámetro.
De forma predeterminada, SSLv3 está deshabilitado. La seguridad de la capa de transporte 1.0 (TLSv1.0) está habilitada y se puede desactivar si es necesario.
- Puede habilitar el modo de cumplimiento del estándar de procesamiento de información federal (FIPS) 140-2 para las interfaces de servicio web del plano de control de todo el clúster.



De manera predeterminada, el modo de cumplimiento de FIPS 140-2 está deshabilitado.

- **Cuando el modo de cumplimiento FIPS 140-2 está desactivado**

Puede habilitar el modo de cumplimiento de FIPS 140-2 mediante el `is-fips-enabled` parámetro a `true` para la `security config modify` y, a continuación, utilice el `security config show` comando para confirmar el estado en línea.

- **Cuando el modo de cumplimiento FIPS 140-2 está activado**

- A partir de ONTAP 9.11.1, TLSv1, TLSv1.1 y SSLv3 están deshabilitados y sólo TLSv1.2 y TLSv1.3 permanecen habilitados. Afecta a otros sistemas y comunicaciones internos y externos a ONTAP 9. Si habilita el modo de cumplimiento FIPS 140-2 y, a continuación, se deshabilita TLSv1, TLSv1.1 y SSLv3. En función de la configuración anterior, las opciones TLSv1.1 o TLSv1.3 permanecerán habilitadas.
- Para las versiones de ONTAP anteriores a 9.11.1, tanto TLSv1 como SSLv3 están deshabilitados y sólo TLSv1.1 y TLSv1.2 permanecen habilitados. ONTAP evita que habilite TLSv1 y SSLv3 cuando el modo de cumplimiento FIPS 140-2 está habilitado. Si activa el modo de cumplimiento FIPS 140-2 y lo deshabilita posteriormente, TLSv1 y SSLv3 permanecen deshabilitados, pero TLSv1.2 o TLSv1.1 y TLSv1.2 se habilitan en función de la configuración anterior.

- Puede mostrar la configuración de la seguridad en todo el clúster mediante la `system security config show` comando.

Si el firewall está habilitado, debe configurarse la política de firewall de la interfaz lógica (LIF) que se utilizará para los servicios web para permitir el acceso HTTP o HTTPS.

Si utiliza HTTPS para acceder a servicios web, debe habilitar también SSL para el clúster o la máquina virtual de almacenamiento (SVM) que ofrezca el servicio web, y debe proporcionar un certificado digital para el clúster o la SVM.

En las configuraciones de MetroCluster, los cambios de configuración que realice para el motor de protocolo web de un clúster no se replican en el clúster de partners.

Comandos para gestionar el motor de protocolo web

Utilice la `system services web` comandos para gestionar el motor de protocolo web.

Utilice la `system services firewall policy create y.. network interface modify` comandos para permitir que las solicitudes de acceso web atraviese el firewall.

| Si desea... | Se usa este comando... |
|--|---|
| Configure el motor de protocolo web en el nivel de clúster: <ul style="list-style-type: none">• Habilite o deshabilite el motor de protocolo web del clúster• Habilite o deshabilite SSLv3 para el clúster• Habilitar o deshabilitar el cumplimiento de la normativa FIPS 140-2 para servicios web seguros (HTTPS) | <code>system services web modify</code> |
| Muestre la configuración del motor de protocolo web en el nivel del clúster, determine si los protocolos web son funcionales en todo el clúster y muestre si el cumplimiento con FIPS 140-2 está habilitado y en línea | <code>system services web show</code> |
| Muestre la configuración del motor de protocolo web en el nivel del nodo y la actividad de la manipulación del servicio web de los nodos del clúster | <code>system services web node show</code> |
| Cree una política de firewall o agregue un servicio de protocolo HTTP o HTTPS a una política de firewall existente para permitir que las solicitudes de acceso web se atraviese por el firewall | <code>system services firewall policy create</code> Ajuste de <code>-service</code> parámetro a <code>http</code> o <code>https</code> permite que las solicitudes de acceso a la web vayan a través del firewall. |
| Asociar una política de firewall a una LIF | <code>network interface modify</code> Puede utilizar el <code>-firewall-policy</code> Parámetro para modificar la política de firewall de una LIF. |

Configure el acceso a los servicios web

Al configurar el acceso a los servicios web, los usuarios autorizados pueden usar HTTP o HTTPS para acceder al contenido del servicio en el clúster o una máquina virtual de almacenamiento (SVM).

Pasos

1. Si hay un firewall habilitado, asegúrese de que el acceso HTTP o HTTPS esté configurado en la política de firewall para la LIF que se utilizará para los servicios web:



Puede comprobar si un firewall está activado mediante el `system services firewall show` comando.

- a. Para verificar que HTTP o HTTPS está configurado en la directiva de firewall, utilice `system services firewall policy show` comando.

Establezca la `-service` parámetro de `system services firewall policy create` comando a. `http` o `https` para habilitar la directiva para admitir el acceso web.

- b. Para verificar que la política de firewall que admite HTTP o HTTPS está asociada con la LIF que proporciona servicios web, utilice `network interface show` con el `-firewall-policy` parámetro.

Utilice la `network interface modify` con el `-firewall-policy` Parámetro para poner en práctica la política de firewall en una LIF.

2. Para configurar el motor de protocolo web a nivel de clúster y hacer que el contenido de los servicios web esté accesible, utilice `system services web modify` comando.
3. Si planea utilizar servicios web seguros (HTTPS), habilite SSL y proporcione información de certificado digital para el clúster o la SVM mediante el `security ssl modify` comando.
4. Para habilitar un servicio web para el clúster o la SVM, use el `vserver services web modify` comando.

Debe repetir este paso para cada servicio que desee habilitar para el clúster o la SVM.

5. Para autorizar a un rol para acceder a los servicios web en el clúster o la SVM, use el `vserver services web access create` comando.

La función que concede acceso ya debe existir. Puede mostrar los roles existentes mediante la `security login role show` utilice el para crear roles nuevos `security login role create` comando.

6. Para un rol autorizado a acceder a un servicio web, asegúrese de que sus usuarios también están configurados con el método de acceso correcto comprobando la salida de `security login show` comando.

Para acceder al servicio web de la API de ONTAP (`ontapi`), un usuario debe estar configurado con `ontapi` método de acceso. Para acceder a todos los demás servicios web, se debe configurar un usuario con `http` método de acceso.



Utilice la `security login create` comando para añadir un método de acceso para un usuario.

Comandos para gestionar servicios web

Utilice la `vserver services web` Comandos para gestionar la disponibilidad de servicios web para el clúster o una máquina virtual de almacenamiento (SVM). Utilice la `vserver services web access` comandos para controlar el acceso de un rol a un servicio web.

| Si desea... | Se usa este comando... |
|--|---|
| Configure un servicio web para el clúster o ANSVM: <ul style="list-style-type: none">• Activar o desactivar un servicio Web• Especifique si sólo se puede utilizar HTTPS para acceder a un servicio web | <code>vserver services web modify</code> |
| Muestre la configuración y la disponibilidad de servicios web del clúster o ANSVM | <code>vserver services web show</code> |
| Autorice a un rol para acceder a un servicio web en el clúster o anSVM | <code>vserver services web access create</code> |
| Muestre los roles que están autorizados a acceder a los servicios web en el clúster o anSVM | <code>vserver services web access show</code> |
| Evite que un rol acceda a un servicio web en el clúster o anSVM | <code>vserver services web access delete</code> |

Información relacionada

["Comandos de ONTAP 9"](#)

Comandos para gestionar los puntos de montaje en los nodos

La `spi` el servicio web crea automáticamente un punto de montaje de un nodo a otro en el volumen raíz de otro nodo tras una solicitud para acceder a los archivos de registro del nodo o a los archivos de núcleo. Aunque no es necesario gestionar manualmente los puntos de montaje, puede hacerlo mediante el `system node root-mount` comandos.

| Si desea... | Se usa este comando... |
|--|--|
| Crear manualmente un punto de montaje desde un nodo al volumen raíz de otro nodo | <code>system node root-mount create</code> Solo puede haber un punto de montaje único de un nodo a otro. |

| Si desea... | Se usa este comando... |
|--|--|
| Muestra los puntos de montaje existentes en los nodos del clúster, incluida la hora en la que se creó un punto de montaje y su estado actual | <code>system node root-mount show</code> |
| Elimine un punto de montaje de un nodo a el volumen raíz de otro nodo y obligue las conexiones al punto de montaje a cerrarse | <code>system node root-mount delete</code> |

Información relacionada

["Comandos de ONTAP 9"](#)

Administrar SSL

El protocolo SSL mejora la seguridad del acceso web mediante el uso de un certificado digital para establecer una conexión cifrada entre un servidor Web y un navegador.

Puede gestionar SSL para el clúster o una máquina virtual de almacenamiento (SVM) de las siguientes maneras:

- Habilitar SSL
- Generar e instalar un certificado digital y asociarlo con el clúster o SVM
- Mostrar la configuración SSL para ver si SSL se ha habilitado y, si está disponible, el nombre del certificado SSL
- Configurar políticas de firewall para el clúster o SVM para que las solicitudes de acceso web puedan atravesarse
- Definición de las versiones SSL que se pueden utilizar
- Restringir el acceso sólo a solicitudes HTTPS para un servicio Web

Comandos para gestionar SSL

Utilice la `security ssl` Comandos para gestionar el protocolo SSL para la máquina virtual de almacenamiento (SVM) de clúster ora.



| Si desea... | Se usa este comando... |
|---|----------------------------------|
| Habilite SSL para la Naranja del clúster y asocie un certificado digital con él | <code>security ssl modify</code> |
| Muestre la configuración de SSL y el nombre de certificado del orasVM del clúster | <code>security ssl show</code> |



Solucionar problemas de acceso al servicio web

Los errores de configuración provocan problemas de acceso al servicio web. Puede resolver los errores garantizando que la LIF, la política de firewall, el motor de protocolo

web, los servicios web, los certificados digitales, y la autorización de acceso del usuario está configurada correctamente.

La tabla siguiente le ayuda a identificar y solucionar errores de configuración del servicio web:

| Este problema de acceso... | Se produce debido a este error de configuración... | Para solucionar el error... |
|---|--|---|
| <p>Su explorador Web devuelve un <code>unable to connect</code> o <code>failure to establish a connection</code> error al intentar acceder a un servicio web.</p> | <p>Es posible que el LIF se haya configurado incorrectamente.</p> | <p>Asegúrese de que puede hacer ping al LIF que proporciona el servicio web.</p> <div data-bbox="1076 640 1133 693">  </div> <p>Utilice la <code>network ping</code> Comando para hacer ping a una LIF. Para obtener información acerca de la configuración de red, consulte la <i>Network Management Guide</i>.</p> |
| <p>Es posible que el firewall esté configurado incorrectamente.</p> | <p>Asegúrese de que se haya configurado una política de firewall para que sea compatible con HTTP o HTTPS y de que la política esté asignada a la LIF que proporciona el servicio web.</p> <div data-bbox="621 1333 678 1386">  </div> <p>Utilice la <code>system services firewall policy</code> comandos para administrar las directivas de firewall. Utilice la <code>network interface modify</code> con el <code>-firewall -policy</code> Parámetro para asociar una política a una LIF.</p> | <p>Es posible que el motor de protocolo web esté desactivado.</p> |

| Este problema de acceso... | Se produce debido a este error de configuración... | Para solucionar el error... |
|--|--|---|
| <p>Asegúrese de que el motor de protocolo web está activado para que los servicios web estén accesibles.</p> <div data-bbox="167 451 220 506">  </div> <div data-bbox="277 378 542 577"> <p>Utilice la <code>system services web</code> comandos para gestionar el motor de protocolo web del clúster.</p> </div> | <p>Su explorador Web devuelve un <code>not found</code> error al intentar acceder a un servicio web.</p> | <p>Es posible que el servicio web esté desactivado.</p> |
| <p>Asegúrese de que todos los servicios web a los que desea permitir el acceso están habilitados individualmente.</p> <div data-bbox="167 898 220 953">  </div> <div data-bbox="277 825 531 1024"> <p>Utilice la <code>vserver services web modify</code> comando para habilitar un servicio web para el acceso.</p> </div> | <p>El explorador Web no puede iniciar sesión en un servicio Web con el nombre de cuenta y la contraseña de un usuario.</p> | <p>El usuario no se puede autenticar, el método de acceso no es correcto o el usuario no está autorizado a acceder al servicio web.</p> |

| Este problema de acceso... | Se produce debido a este error de configuración... | Para solucionar el error... |
|---|--|--|
| <p>Asegúrese de que la cuenta de usuario exista y esté configurada con el método de acceso y el método de autenticación correctos. Asimismo, asegúrese de que la función del usuario está autorizada para acceder al servicio web.</p> <div data-bbox="167 846 220 898">  </div> <div data-bbox="280 478 542 1266"> <p>Utilice la <code>security login</code> comandos para gestionar cuentas de usuario y sus métodos de acceso y métodos de autenticación. Para acceder al servicio web de API de ONTAP se requiere el <code>ontapi</code> método de acceso. El acceso a todos los demás servicios Web requiere el <code>http</code> método de acceso. Utilice la <code>vserver services web access</code> comandos para gestionar el acceso de un rol a un servicio web.</p> </div> | <p>Se conecta al servicio web con HTTPS y el explorador web indica que la conexión se ha interrumpido.</p> | <p>Es posible que no tenga habilitado SSL en el clúster ni la SVM que proporciona el servicio web.</p> |
| <p>Compruebe que el clúster o la SVM tengan habilitada SSL y que el certificado digital sea válido.</p> <div data-bbox="167 1654 220 1707">  </div> <div data-bbox="280 1476 542 1896"> <p>Utilice la <code>security ssl</code> Comandos para administrar la configuración SSL para los servidores HTTP y el <code>security certificate show</code> comando para mostrar información de certificados digitales.</p> </div> | <p>Se conecta al servicio web mediante HTTPS y el navegador web indica que la conexión no es de confianza.</p> | <p>Es posible que utilice un certificado digital autofirmado.</p> |

Compruebe la identidad de los servidores remotos mediante certificados

Compruebe la identidad de los servidores remotos mediante la introducción de certificados

ONTAP admite características de certificado de seguridad para verificar la identidad de los servidores remotos.

El software ONTAP permite conexiones seguras utilizando las siguientes funciones y protocolos de certificados digitales:

- El protocolo de estado de certificados en línea (OCSP) valida el estado de las solicitudes de certificados digitales de los servicios de ONTAP mediante conexiones SSL y de seguridad de la capa de transporte (TLS). Esta función está deshabilitada de forma predeterminada.
- Con el software ONTAP se incluye un conjunto predeterminado de certificados raíz de confianza.
- Los certificados de protocolo de interoperabilidad de gestión de claves (KMIP) permiten la autenticación mutua de un clúster y de un servidor KMIP.

Verifique que los certificados digitales sean válidos mediante OCSP

A partir de ONTAP 9.2, el protocolo de estado de certificado en línea (OCSP) habilita las aplicaciones ONTAP que utilizan comunicaciones de seguridad de capa de transporte (TLS) para recibir el estado de certificado digital cuando OCSP está habilitado. Es posible habilitar o deshabilitar las comprobaciones de estado de certificados de OCSP para aplicaciones específicas en cualquier momento. De manera predeterminada, la comprobación del estado de los certificados OCSP está deshabilitada.

Lo que necesitará

Necesita acceso de nivel de privilegio avanzado para realizar esta tarea.

Acerca de esta tarea

OCSP admite las siguientes aplicaciones:

- AutoSupport
- Sistema de gestión de eventos (EMS)
- LDAP sobre TLS
- Protocolo de interoperabilidad de gestión de claves (KMIP)
- Registro de auditoría
- FabricPool
- SSH (a partir de ONTAP 9.13.1)

Pasos

1. Configure el nivel de privilegio en Advanced: `set -privilege advanced`.
2. Para habilitar o deshabilitar las comprobaciones de estado de certificados de OCSP para aplicaciones de ONTAP específicas, utilice el comando correspondiente.

| Si desea que las comprobaciones del estado del certificado OCSP para que algunas aplicaciones sean... | Usar el comando... |
|---|---|
| Activado | <code>security config ocsp enable -app app name</code> |
| Deshabilitado | <code>security config ocsp disable -app app name</code> |

El siguiente comando habilita la compatibilidad de OCSP para AutoSupport y EMS.

```
cluster::*> security config ocsp enable -app asup,ems
```

Cuando OCSP está habilitado, la aplicación recibe una de las siguientes respuestas:

- Correcto: El certificado es válido y la comunicación continúa.
 - Revocado: La autoridad emisora de certificados considera permanentemente que el certificado no es de confianza y la comunicación no continúa.
 - Unknown: El servidor no tiene ninguna información de estado sobre el certificado y la comunicación no continúa.
 - Falta información del servidor OCSP en el certificado: El servidor actúa como si OCSP está deshabilitado y continúa con la comunicación TLS, pero no se produce ninguna comprobación de estado.
 - Sin respuesta del servidor OCSP: La aplicación no puede continuar.
3. Para habilitar o deshabilitar las comprobaciones de estado de certificados OCSP para todas las aplicaciones que utilizan comunicaciones TLS, utilice el comando correspondiente.

| Si desea que las comprobaciones del estado del certificado OCSP para que todas las aplicaciones sean... | Usar el comando... |
|---|--|
| Activado | <code>security config ocsp enable</code> <code>-app all</code> |
| Deshabilitado | <code>security config ocsp disable</code> <code>-app all</code> |

Cuando se habilita, todas las aplicaciones reciben una respuesta firmada que significa que el certificado especificado es correcto, revocado o desconocido. En el caso de un certificado revocado, la solicitud no continuará. Si la aplicación no recibe una respuesta del servidor OCSP o si no se puede acceder al servidor, la aplicación no podrá continuar.

4. Utilice la `security config ocsp show` Comando para mostrar todas las aplicaciones compatibles con OCSP y su estado de soporte.

```
cluster::*> security config ocsf show
Application                                OCSF Enabled?
-----
autosupport                               false
audit_log                                 false
fabricpool                                false
ems                                        false
kmip                                       false
ldap_ad                                   true
ldap_nis_namemap                          true
ssh                                        true

8 entries were displayed.
```

Ver certificados predeterminados para aplicaciones basadas en TLS

A partir de ONTAP 9.2, ONTAP proporciona un conjunto predeterminado de certificados raíz de confianza para aplicaciones ONTAP que utilizan Seguridad de la capa de transporte (TLS).

Lo que necesitará

Los certificados predeterminados solo se instalan en la SVM de administrador durante su creación o durante una actualización a ONTAP 9.2.

Acerca de esta tarea

Las aplicaciones actuales que funcionan como cliente y requieren validación de certificados son AutoSupport, EMS, LDAP, Registro de auditoría, FabricPool, Y KMIP.

Cuando los certificados caducan, se invoca un mensaje EMS que solicita al usuario que elimine los certificados. Los certificados predeterminados solo se pueden eliminar en el nivel de privilegios avanzados.



La eliminación de los certificados predeterminados puede provocar que algunas aplicaciones ONTAP no funcionen como se esperaba (por ejemplo, AutoSupport y Registro de auditoría).

Paso

1. Puede ver los certificados predeterminados que se instalan en la SVM de administrador mediante el comando `Security certificate show`:

```
security certificate show -vserver -type server-ca
```

```
fas2552-2n-abc-3::*> security certificate show -vserver fas2552-2n-abc-3
-type server-ca
Vserver      Serial Number  Common Name                                     Type
-----
fas2552-2n-abc-3
              01                      AAACertificateServices
server-ca
Certificate Authority: AAA Certificate Services
Expiration Date: Sun Dec 31 18:59:59 2028
```

Autentique mutuamente el clúster y un servidor KMIP

Autenticar mutuamente el clúster y una información general del servidor KMIP

Al autenticar mutuamente el clúster y un gestor de claves externo, como un servidor de protocolo de interoperabilidad de gestión de claves (KMIP), el administrador de claves puede comunicarse con el clúster mediante KMIP a través de SSL. Esto se hace cuando una aplicación o determinada funcionalidad (por ejemplo, la funcionalidad de cifrado del almacenamiento) requieren claves seguras para ofrecer un acceso seguro a los datos.

Genere una solicitud de firma de certificación para el clúster de

Puede utilizar el certificado de seguridad `generate-csr` Comando para generar una solicitud de firma de certificación (CSR). Después de procesar la solicitud, la entidad de certificación (CA) envía el certificado digital firmado.

Lo que necesitará

Debe ser un administrador de clúster o un administrador de SVM para ejecutar esta tarea.

Pasos

1. Genere una CSR:

```
security certificate generate-csr -common-name FQDN_or_common_name -size
512|1024|1536|2048 -country country -state state -locality locality
-organization organization -unit unit -email-addr email_of_contact -hash
-function SHA1|SHA256|MD5
```

Para obtener una sintaxis de comando completa, consulte las páginas man.

El siguiente comando crea una CSR con una clave privada de 2,048 bits generada por la función de hashing SHA256 para que la utilice el grupo Software del departamento DE TI de una empresa cuyo nombre común personalizado es server1.companyname.com, ubicado en Sunnyvale, California, EE. UU. La dirección de correo electrónico del administrador de contacto de la SVM es web@example.com. El sistema muestra la CSR y la clave privada en la salida.

```

cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California -
locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256
Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
MIIBGjCBxQIBADBgMRQwEgYDVQQDEwtleGFtcGxlLmNvbTELMakGA1UEBhMCVVMx
CTAHBgNVBAgtADEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCtAHBgNVBAStADEPMA0G
CSqGSIB3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApTlnzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJbmXuj6U3alwoUsb13wfEvQnHVFNCi
2ninsJ8CAwEAAaAAMA0GCSqGSIB3DQEBCwUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----
Private Key :
24 | Administrator Authentication and RBAC
-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAPXFanNoJApTlnzSxOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJb
mXuj6U3alwoUsb13wfEvQnHVFNCi2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQlu
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgPv+p5kaZTTM
gQIhAPsp+j1hrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehAiEA+oDbOooWlVvu
xj4aitxVBu6ByVckYU8LbsfeRNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NCtEYxd0Q5
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsKO077itF+h9FGFNHbtuNTrVq4vPW3nAiAA
peMBQgEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==
-----END RSA PRIVATE KEY-----
Note: Please keep a copy of your certificate request and private key
for future reference.

```

2. Copie la solicitud de certificado de la salida CSR y envíela en formato electrónico (por ejemplo, correo electrónico) a una CA de terceros de confianza para su firma.

Después de procesar la solicitud, la CA envía el certificado digital firmado. Debe conservar una copia de la clave privada y el certificado digital firmado por la CA.

Instale un certificado de servidor firmado por CA para el clúster

Para habilitar un servidor SSL que autentique el clúster o la máquina virtual de almacenamiento (SVM) como cliente SSL, se instala un certificado digital con el tipo de cliente en el clúster o la SVM. A continuación, proporcionará el certificado de CA de cliente al administrador del servidor SSL para su instalación en el servidor.

Lo que necesitará

Ya debe haber instalado el certificado raíz del servidor SSL en el clúster o la SVM con el `server-ca` tipo de certificado.

Pasos

1. Para usar un certificado digital autofirmado para la autenticación de clientes, use `security`

`certificate create` con el `type client` parámetro.

2. Para utilizar un certificado digital firmado por CA para la autenticación de clientes, complete los siguientes pasos:

- a. Genere una solicitud de firma de certificación (CSR) digital mediante el certificado de seguridad `generate-csr` comando.

ONTAP muestra el resultado de CSR, que incluye una solicitud de certificado y una clave privada, y le recuerda que debe copiar el resultado en un archivo para futura referencia.

- b. Envíe la solicitud de certificado de la salida de CSR en un formulario electrónico (como por ejemplo, correo electrónico) a una CA de confianza para su firma.

Debe conservar una copia de la clave privada y el certificado firmado por CA para referencia futura.

Después de procesar la solicitud, la CA envía el certificado digital firmado.

- a. Instale el certificado firmado por la CA con el `security certificate install` con el `-type client` parámetro.
- b. Introduzca el certificado y la clave privada cuando se le solicite y, a continuación, pulse **Intro**.
- c. Introduzca cualquier certificado raíz o intermedio adicional cuando se le solicite y, a continuación, pulse **Intro**.

Puede instalar un certificado intermedio en el clúster o la SVM si a una cadena de certificados que comienza en la CA raíz de confianza y finaliza con el certificado SSL emitido para usted, le faltan los certificados intermedios. Un certificado intermedio es un certificado subordinado emitido por el raíz de confianza específicamente para emitir certificados de servidor de entidades finales. El resultado es una cadena de certificados que comienza en la CA raíz de confianza, atraviesa el certificado intermedio y termina con el certificado SSL que se le emitió.

3. Proporcione el `client-ca` Certificado del clúster o SVM al administrador del servidor SSL para su instalación en el servidor.

El comando `Security certificate show` con el `-instance y.. -type client-ca` los parámetros muestran la `client-ca` información del certificado.

Instale un certificado de cliente firmado por CA para el servidor KMIP

El subtipo de certificado del protocolo de interoperabilidad de gestión de claves (KMIP) (el parámetro `-subtipo kmip-cert`), junto con los tipos de CA del cliente y del servidor, especifica que el certificado se utiliza para autenticar mutuamente el clúster y un gestor de claves externo, como un servidor KMIP.

Acerca de esta tarea

Instale un certificado KMIP para autenticar un servidor KMIP como servidor SSL en el clúster.

Pasos

1. Utilice la `security certificate install` con el `-type server-ca y.. -subtype kmip-cert` Parámetros para instalar un certificado KMIP en el servidor KMIP.
2. Cuando se le solicite, introduzca el certificado y pulse **Intro**.

ONTAP le recuerda que debe conservar una copia del certificado para futuras consultas.

```
cluster1::> security certificate install -type server-ca -subtype kmip-  
cert  
-vserver cluster1
```

Please enter Certificate: Press <Enter> when done

-----BEGIN CERTIFICATE-----

```
MIICPDCCAaUCEDyRMcsf9tAbDpq40ES/Er4wDQYJKoZIhvcNAQEFBQAwwXzELMAkG  
2JhucwNhkcV8sEVAbkSdjbCxlRhLQ2pRdKkkirWmnWXbj9T/UWZYB2oK0z5XqcJ  
2HUw19JlYDln1khVdWk/kfVIC0dpImmClr7JyDiGSnoscxlIaU5rfGW/D/xwzoiQ
```

...

-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for future reference.

```
cluster1::>
```

Seguridad y cifrado de datos

Información general sobre la gestión de seguridad con System Manager

A partir de ONTAP 9.7, puede gestionar la seguridad del clúster con System Manager.

Con System Manager, se utilizan métodos estándar de ONTAP para proteger el acceso del administrador y de cliente al almacenamiento frente a virus. Existen tecnologías avanzadas para el cifrado de datos en reposo y para el almacenamiento WORM.

Si utiliza la versión clásica de System Manager (disponible solo en ONTAP 9.7 y versiones anteriores), consulte "[System Manager Classic \(ONTAP de 9.0 a 9.7\)](#)".

Detección de virus

Puede utilizar la funcionalidad antivirus integrada en el sistema de almacenamiento para proteger los datos frente a amenazas de virus u otro código malintencionado. El análisis de virus de ONTAP, denominado *Vscan*, combina el mejor software antivirus de terceros con funciones de ONTAP que le proporcionan la flexibilidad que necesita para controlar qué archivos se analizan y cuándo.

Cifrado

ONTAP ofrece tecnologías de cifrado basadas en software y hardware para garantizar que los datos en reposo no se puedan leer en caso de reasignación, devolución, pérdida o robo del medio de almacenamiento.

Almacenamiento WORM

SnapLock es una solución de cumplimiento de alto rendimiento para organizaciones que utilizan almacenamiento *Write Once, Read Many (WORM)* para retener archivos críticos en forma no modificada con fines normativos y de gobernanza.

Protéjase contra el ransomware

Información general sobre la protección de ransomware autónoma

A partir de ONTAP 9.10.1, la función de protección de ransomware autónoma (ARP) utiliza análisis de cargas de trabajo en entornos NAS (NFS y SMB) para detectar de forma proactiva y advertir sobre una actividad anormal que puede indicar un ataque de ransomware.

Cuando se sospecha una presencia de un ataque, ARP también crea nuevas copias Snapshot, además de la protección existente frente a copias Snapshot programadas.

Licencias y habilitación

ARP requiere una licencia. ARP está disponible con el "[Licencia ONTAP ONE](#)". Si no tiene la licencia ONTAP One, hay otras licencias disponibles para usar ARP, que varían en función de la versión de ONTAP.

| Lanzamientos de ONTAP | Licencia |
|--------------------------------------|---|
| ONTAP 9.11.1 y versiones posteriores | Antiransomware |
| ONTAP 9.10.1 | MT_EK_MGMT (gestión de claves multi-tenant) |

- Si actualiza a ONTAP 9.11.1 o una versión posterior y ARP ya está configurado en el sistema, no necesita adquirir la nueva licencia contra ransomware. Para las nuevas configuraciones ARP, se requiere la nueva licencia.
- Si va a revertir de ONTAP 9.11.1 o posterior a ONTAP 9.10.1 y habilitó ARP con la licencia Anti-ransomware, verá un mensaje de advertencia y es posible que deba volver a configurar ARP. ["Aprenda sobre cómo revertir ARP"](#).

Puede configurar ARP por volumen mediante System Manager o la CLI de ONTAP.

Estrategia de protección contra ransomware ONTAP

Una estrategia efectiva de detección de ransomware debe incluir más que una única capa de protección.

Una analogía sería las características de seguridad de un vehículo. No dependes de una sola característica, como un cinturón de seguridad, para protegerte por completo en caso de accidente. Las bolsas de aire, los frenos antibloqueo y la advertencia de colisión frontal son características de seguridad adicionales que conducirán a un resultado mucho mejor. La protección contra ransomware debe verse de la misma manera.

Aunque ONTAP incluye funciones como FPolicy, copias Snapshot, SnapLock y el asesor digital de Active IQ para ayudarle a protegerse del ransomware, la siguiente información se centra en la función ARP integrada con funcionalidades de aprendizaje automático.

Para obtener más información sobre otras funciones contra el ransomware de ONTAP, consulte ["TR-4572: Solución de NetApp para ransomware."](#)

Lo que ARP detecta

ARP está diseñado para proteger contra ataques de denegación de servicio en los que el atacante retiene datos hasta que se pague un rescate. ARP ofrece detección contra ransomware basada en:

- Identificación de los datos entrantes como texto cifrado o sin formato.
- Análisis, que detecta
 - **Entropía:** Una evaluación de la aleatoriedad de los datos en un archivo
 - **Tipos de extensión de archivo:** Una extensión que no se ajusta al tipo de extensión normal
 - **IOPS de archivo:** Un aumento en la actividad de volumen anormal con cifrado de datos (a partir de ONTAP 9.11.1)

ARP puede detectar la propagación de la mayoría de ataques de ransomware solo una pequeña cantidad de archivos se cifran, toman medidas automáticamente para proteger los datos y avisan de que se está produciendo un ataque sospechoso.



Ningún sistema de detección o prevención de ransomware puede garantizar completamente la seguridad de un ataque de ransomware. Aunque es posible que un ataque no se detecte, ARP actúa como una capa adicional importante de defensa si el software antivirus no ha podido detectar una intrusión.

Modos de aprendizaje y activos

ARP tiene dos modos:

- **Aprendizaje** (o modo “dry run”)
- **Activo** (o modo “habilitado”)

Cuando habilita ARP, se ejecuta en *modo de aprendizaje*. En el modo de aprendizaje, el sistema ONTAP desarrolla un perfil de alerta basado en las áreas de análisis: Entropía, tipos de extensiones de archivos e IOPS de archivos. Después de ejecutar ARP en el modo de aprendizaje durante el tiempo suficiente para evaluar las características de la carga de trabajo, puede cambiar al modo activo y empezar a proteger los datos. Una vez que ARP ha cambiado al modo activo, ONTAP crea copias snapshot de ARP para proteger los datos en caso de que se detecte una amenaza.

Se recomienda dejar ARP en modo de aprendizaje durante 30 días. A partir de ONTAP 9.13.1, ARP determina automáticamente el intervalo óptimo del período de aprendizaje y automatiza el switch, que puede ocurrir antes de 30 días.

En el modo activo, si una extensión de archivo se marca como anormal, debe evaluar la alerta. Puede actuar en la alerta para proteger sus datos o puede marcar la alerta como un falso positivo. Al marcar una alerta como falso positivo, se actualiza el perfil de alerta. Por ejemplo, si la alerta se activa con una nueva extensión de archivo y marca la alerta como un falso positivo, no recibirá una alerta la próxima vez que se observe la extensión de archivo. El comando `security anti-ransomware volume workload-behavior show` muestra las extensiones de archivo que se han detectado en el volumen. (Si ejecuta este comando al principio del modo de aprendizaje y muestra una representación precisa de los tipos de archivo, no debe utilizar esos datos como base para pasar al modo activo, ya que ONTAP sigue recopilando otras métricas).

A partir de ONTAP 9.11.1, se pueden personalizar los parámetros de detección para ARP. Para obtener más información, consulte [Administrar los parámetros de detección de ataques ARP](#).

Evaluación de amenazas y copias Snapshot de ARP

En el modo activo, ARP evalúa la probabilidad de amenaza en función de los datos entrantes medidos con respecto a los análisis aprendidos. Se asigna una medición cuando ARP detecta una amenaza:

- **Bajo:** La detección más temprana de una anomalía en el volumen (por ejemplo, se observa una nueva extensión de archivo en el volumen).
- **Moderado:** Se observan múltiples archivos con la misma extensión de archivo Never-seen-before.
 - En ONTAP 9.10.1, el umbral para escalar a moderado es de 100 archivos o más. A partir de ONTAP 9.11.1, la cantidad de archivo es modificable; su valor predeterminado es 20.

En un caso de amenaza baja, ONTAP detecta una anomalía y crea una copia Snapshot del volumen para crear el mejor punto de recuperación. ONTAP antepone el nombre de la copia Snapshot de ARP con `Anti-ransomware-backup` para que sea fácilmente identificable, por ejemplo `Anti_ransomware_backup.2022-12-20_1248`.

La amenaza se escala a moderada después de que ONTAP ejecuta un informe de análisis para determinar si la anomalía coincide con un perfil de ransomware. Las amenazas que permanecen en el nivel bajo se registran y son visibles en la sección **Eventos** de System Manager. Cuando la probabilidad de ataque es moderada, ONTAP genera una notificación EMS que le solicita que evalúe la amenaza. ONTAP no envía alertas sobre amenazas bajas, sin embargo, a partir de ONTAP 9.14.1, usted puede [modificar la configuración de alertas](#). Para obtener más información, consulte [Responda a actividades anormales](#).

Puede ver información sobre una amenaza, independientemente del nivel, en la sección **Eventos** de System

Manager o con la `security anti-ransomware volume show` comando.

Las copias Snapshot de ARP se conservan durante un mínimo de dos días. A partir de ONTAP 9.11.1, puede modificar la configuración de retención. Para obtener más información, consulte [Modifique las opciones para las copias Snapshot](#).

Cómo recuperar los datos en ONTAP después de un ataque de ransomware

Cuando se sospecha la existencia de un ataque, el sistema toma una copia snapshot para el volumen en ese momento específico y bloquea esa copia. Si más tarde se confirma el ataque, el volumen se puede restaurar mediante la copia snapshot de ARP.

Las copias snapshot bloqueadas no se pueden eliminar de forma normal. Sin embargo, si más tarde decide marcar el ataque como un falso positivo, la copia bloqueada se eliminará.

Con el conocimiento de los ficheros afectados y el tiempo del ataque, es posible recuperar de forma selectiva los ficheros afectados de varias copias snapshot, en lugar de simplemente revertir el volumen completo a una de las copias snapshot.

De este modo, ARP se basa en la protección de datos ONTAP y la tecnología de recuperación ante desastres demostradas para responder a ataques de ransomware. Consulte los siguientes temas para obtener más información sobre cómo recuperar datos.

- ["Recuperar desde copias Snapshot \(System Manager\)"](#)
- ["Restaurar archivos desde copias Snapshot \(CLI\)"](#)
- ["Recuperación inteligente de ransomware"](#)

Casos de uso y consideraciones sobre la protección de Ransomware autónoma

La protección autónoma de Ransomware (ARP) está disponible para cargas de trabajo NAS que comiencen con ONTAP 9.10.1. Antes de implementar ARP, debe tener en cuenta los usos recomendados y las configuraciones compatibles, así como las implicaciones de rendimiento.

Configuraciones admitidas y no admitidas

Al decidir usar ARP, es importante asegurarse de que la carga de trabajo de su volumen sea adecuada para ARP y que cumpla con las configuraciones del sistema requeridas.

Cargas de trabajo adecuadas

ARP es adecuado para:

- En almacenamiento NFS
- Directorios iniciales Windows o Linux

Debido a que los usuarios podían crear archivos con extensiones que no se detectaron en el período de aprendizaje, existe una mayor posibilidad de falsos positivos en esta carga de trabajo.

- Imágenes y vídeo

Por ejemplo, historiales médicos y datos de automatización de diseño electrónico (EDA)

Cargas de trabajo poco adecuadas

ARP no es adecuado para:

- Cargas de trabajo con una gran frecuencia de creación o eliminación de archivos (cientos de miles de archivos en pocos segundos, por ejemplo, cargas de trabajo de prueba/desarrollo).
- La detección de amenazas de ARP depende de su capacidad para reconocer un aumento inusual en la actividad de creación, cambio de nombre o eliminación de archivos. Si la aplicación en sí es el origen de la actividad de archivos, no se puede distinguir eficazmente de la actividad de ransomware.
- Cargas de trabajo en las que la aplicación o el host cifran datos.
ARP depende de distinguir los datos entrantes como cifrados o no cifrados. Si la propia aplicación está cifrando los datos, se reduce la eficacia de la función. Sin embargo, la característica puede seguir funcionando según la actividad del archivo (eliminar, sobrescribir o crear, o crear o cambiar el nombre con una nueva extensión de archivo) y el tipo de archivo.

Configuraciones admitidas

ARP está disponible para volúmenes NFS y SMB en sistemas ONTAP on-premises que empiezan por ONTAP 9.10.1.

La compatibilidad con otras configuraciones y tipos de volúmenes está disponible en las siguientes versiones de ONTAP:

| | ONTAP 9.14.1 | ONTAP 9.13.1 | ONTAP 9.12.1 | ONTAP 9.11.1 | ONTAP 9.10.1 |
|---|--------------|--------------|--------------|--------------|--------------|
| Volúmenes protegidos con SnapMirror asíncrono | ✓ | ✓ | ✓ | | |
| SVM protegido con SnapMirror asíncrono (recuperación ante desastres de SVM) | ✓ | ✓ | ✓ | | |
| Movilidad de datos de SVM (vserver migrate) | ✓ | ✓ | ✓ | | |
| Volúmenes de FlexGroup | ✓ | ✓ | | | |
| Verificación de varios administradores | ✓ | ✓ | | | |

Interoperabilidad de SnapMirror y ARP

A partir de ONTAP 9.12.1, ARP es compatible con volúmenes de destino asíncronos de SnapMirror. ARP no es ** compatible con SnapMirror Synchronous.

Si un volumen de origen de SnapMirror tiene la función ARP habilitada, el volumen de destino de SnapMirror adquiere automáticamente el estado de configuración ARP (aprendizaje, habilitado, etc.), datos de

entrenamiento ARP y Snapshot creadas con ARP del volumen de origen. No se requiere habilitación explícita.

Mientras que el volumen de destino consta de copias Snapshot de solo lectura (RO), no se realiza el procesamiento ARP en sus datos. Sin embargo, cuando el volumen de destino de SnapMirror se convierte en Read-write (RW), ARP se habilita automáticamente en el volumen de destino que se convierte en RW. El volumen de destino no requiere ningún procedimiento de aprendizaje adicional además de lo que ya se ha registrado en el volumen de origen.

En ONTAP 9.10.1 y 9.11.1, SnapMirror no transfiere el estado de configuración de ARP, los datos de formación y las copias Snapshot de los volúmenes de origen a destino. Por ello, cuando el volumen de destino de SnapMirror se convierte en RW, ARP en el volumen de destino debe habilitarse explícitamente en el modo de aprendizaje después de la conversión.

ARP y máquinas virtuales

ARP es compatible con máquinas virtuales (VM). La detección de ARP se comporta de manera diferente para los cambios dentro y fuera de la VM. No se recomienda ARP para cargas de trabajo con archivos de alta entropía dentro del equipo virtual.

Realizar cambios fuera de la máquina virtual

ARP puede detectar cambios de extensión de archivo en un volumen NFS fuera de la VM si una nueva extensión entra en el volumen cifrado o cambia una extensión de archivo. Los cambios detectables en la extensión de archivo son:

- .vmx
- .vmxf
- .vmdk
- -flat.vmdk
- .nvram
- .vmem
- .vmsd
- .vmsn
- .vswp
- .vmss
- .log
- -\#.log

Cambios dentro de la VM

Si el ataque de ransomware se dirige a la máquina virtual y los archivos dentro de la máquina virtual se alteran sin hacer cambios fuera de la máquina virtual, ARP detecta la amenaza si la entropía predeterminada de la máquina virtual es baja (por ejemplo, archivos .txt, .docx o .mp4). Aunque ARP crea una instantánea de protección en este escenario, no genera una alerta de amenaza porque las extensiones de archivo fuera de la VM no se han manipulado.

Si, por defecto, los archivos son de alta entropía (por ejemplo, archivos .gzip o protegidos con contraseña), las capacidades de detección de ARP son limitadas. ARP todavía puede tomar Snapshots proactivos en este caso, sin embargo, no se activarán alertas si las extensiones de archivo no se han manipulado externamente.

Configuraciones no admitidas

ARP no es compatible con las siguientes configuraciones del sistema:

- Entornos ONTAP S3
- Entornos SAN

ARP no admite las siguientes configuraciones de volumen:

- FlexGroup Volumes (en ONTAP 9.10.1 a 9.12.1. A partir de ONTAP 9.13.1, los volúmenes de FlexGroup son compatibles)
- Volúmenes FlexCache (ARP es compatible con los volúmenes FlexVol de origen, pero no con los volúmenes de caché)
- Volúmenes sin conexión
- Volúmenes solo DE SAN
- Volúmenes de SnapLock
- SnapMirror síncrono
- SnapMirror asíncrono (solo no se admite en ONTAP 9.10.1 y 9.11.1). Se admite SnapMirror asíncrono a partir de ONTAP 9.12.1. Para obtener más información, consulte [\[snapmirror\]](#).)
- Volúmenes restringidos
- Volúmenes raíz de equipos virtuales de almacenamiento
- Volúmenes de máquinas virtuales de almacenamiento detenidas

Consideraciones de rendimiento y frecuencia de ARP

ARP puede tener un impacto mínimo en el rendimiento del sistema, ya que se mide el rendimiento y los picos de IOPS. El impacto de la función ARP depende de las cargas de trabajo de volumen específicas. Para cargas de trabajo comunes, se recomiendan los siguientes límites de configuración:

| Características de las cargas de trabajo | Límite de volúmenes recomendado por nodo | Degradación del rendimiento cuando se supera el límite de volumen por nodo pasada:[*] |
|--|--|---|
| Con una gran cantidad de lecturas o se pueden comprimir los datos. | 150 | 4 % del valor máximo de IOPS |
| Gran cantidad de escrituras y los datos no se pueden comprimir. | 60 | 10 % de IOPS máximo |

Aprobado:[*] el rendimiento del sistema no se degrada más allá de estos porcentajes, independientemente del número de volúmenes añadidos por encima de los límites recomendados.

Dado que la analítica ARP se ejecuta en una secuencia priorizada, a medida que aumenta el número de volúmenes protegidos, la analítica se ejecuta en cada volumen con menos frecuencia.

Verificación multi-admin con volúmenes protegidos con ARP

A partir de ONTAP 9.13.1, puede habilitar la verificación multiadministrador (MAV) para obtener seguridad adicional con ARP. MAV garantiza que al menos dos o más administradores autenticados deben desactivar ARP, pausar ARP o marcar un ataque sospechoso como falso positivo en un volumen protegido. Aprenda cómo ["Habilite MAV para volúmenes protegidos por ARP"](#).

Debe definir administradores para un grupo MAV y crear reglas MAV para el `security anti-ransomware volume disable`, `security anti-ransomware volume pause`, y `security anti-ransomware volume attack clear-suspect` Comandos ARP que desea proteger. Cada administrador del grupo MAV debe aprobar cada nueva solicitud de regla y. ["Vuelva a agregar la regla MAV"](#) Dentro de los ajustes de MAV.

A partir de ONTAP 9.14.1, ARP ofrece alertas para la creación de una instantánea ARP y para la observación de una nueva extensión de archivo. De forma predeterminada, las alertas correspondientes a estos eventos están deshabilitadas. Las alertas pueden establecerse en el nivel del volumen o SVM. Puede crear reglas MAV en el nivel de la SVM mediante `security anti-ransomware vserver event-log modify` o a nivel de volumen con `security anti-ransomware volume event-log modify`.

Siguientes pasos

- ["Habilite la protección de ransomware autónoma"](#)
- ["Habilite MAV para volúmenes protegidos por ARP"](#)

Habilite la protección de ransomware autónoma

A partir de ONTAP 9.10.1, la protección de ransomware autónoma (ARP) puede habilitarse en volúmenes nuevos o existentes. Primero debe habilitar ARP en el modo de aprendizaje, en el cual el sistema analiza la carga de trabajo para caracterizar el comportamiento normal. Puede habilitar ARP en un volumen existente, o bien crear un volumen nuevo y habilitar ARP desde el principio.

Acerca de esta tarea

Siempre debe habilitar ARP inicialmente en modo de aprendizaje (o ejecución en seco). Si se inicia en modo activo, se pueden producir demasiados informes de falsos positivos.

Se recomienda que deje que ARP se ejecute en modo de aprendizaje durante un mínimo de 30 días. A partir de ONTAP 9.13.1, ARP determina automáticamente el intervalo óptimo del período de aprendizaje y automatiza el switch, que puede ocurrir antes de 30 días. Para obtener más información, consulte ["Modos de aprendizaje y activos"](#).



En los volúmenes existentes, los modos de aprendizaje y activos solo se aplican a los datos recién escritos, no a los datos ya existentes en el volumen. Los datos existentes no se analizan y analizan, ya que se asumen las características del tráfico de datos normal anterior según los nuevos datos una vez habilitado para ARP el volumen.

Antes de empezar

- Debe tener una máquina virtual de almacenamiento (SVM) habilitada para NFS o SMB (o ambos).
- La [licencia correcta](#) Debe estar instalado para la versión de ONTAP.
- Debe tener carga de trabajo NAS con clientes configurados.
- El volumen que desea establecer ARP debe estar protegido y debe tener un activo ["ruta de unión"](#).
- El volumen debe estar lleno por debajo del 100%.
- Se recomienda configurar el sistema EMS para enviar notificaciones por correo electrónico, que incluirán avisos de actividad ARP. Para obtener más información, consulte ["Configure eventos de EMS para que envíen notificaciones por correo electrónico"](#).
- A partir de ONTAP 9.13.1, se recomienda habilitar la verificación multiadministrador (MAV) para que se necesiten dos o más administradores de usuarios autenticados para la configuración de protección

autónoma contra ransomware (ARP). Para obtener más información, consulte ["Habilite la verificación multiadministradora"](#).

Active ARP

Puede habilitar ARP mediante System Manager o la interfaz de línea de comandos de ONTAP.

System Manager

Pasos

1. Seleccione **Almacenamiento > Volúmenes** y, a continuación, seleccione el volumen que desea proteger.
2. En la pestaña **Seguridad** de la vista general **Volúmenes**, selecciona **Estado** para cambiar de Desactivado a Activado en el modo de aprendizaje en la casilla **Anti-ransomware**.
3. Cuando finalice el período de aprendizaje, cambie ARP al modo activo.



A partir de ONTAP 9.13.1, ARP determina automáticamente el intervalo óptimo del período de aprendizaje y automatiza el switch. Puede hacerlo ["Deshabilite este ajuste en la máquina virtual de almacenamiento asociada"](#) si desea controlar el modo de aprendizaje al modo activo, cambie manualmente.

- a. Selecciona **Almacenamiento > Volúmenes** y, a continuación, selecciona el volumen que esté listo para el modo activo.
 - b. En la pestaña **Seguridad** del resumen **Volúmenes**, selecciona **Cambiar** al modo activo en el cuadro Anti-ransomware.
4. Puede verificar el estado ARP del volumen en la casilla **Anti-ransomware**.

Para mostrar el estado ARP para todos los volúmenes: En el panel **Volúmenes**, seleccione **Mostrar/Ocultar** y, a continuación, asegúrese de que el estado **Anti-ransomware** esté marcado.

CLI

El proceso para habilitar ARP con la CLI es diferente si la habilita en un volumen existente en lugar de en un volumen nuevo.

Habilite ARP en un volumen existente

1. Modifique un volumen existente para habilitar la protección contra ransomware en el modo de aprendizaje:

```
security anti-ransomware volume dry-run -volume vol_name -vserver svm_name
```

Si ejecuta ONTAP 9.13.1 o posterior, el aprendizaje adaptativo se activa para que el cambio al estado activo se realice automáticamente. Si no desea que este comportamiento se habilite automáticamente, cambie la configuración en el nivel de SVM en todos los volúmenes asociados:

```
vserver modify svm_name -anti-ransomware-auto-switch-from-learning-to-enabled false
```

2. Cuando el periodo de aprendizaje haya terminado, modifique el volumen protegido para cambiar al modo activo si no se ha realizado automáticamente:

```
security anti-ransomware volume enable -volume vol_name -vserver svm_name
```

También se puede cambiar al modo activo con el comando modify volume:

```
volume modify -volume vol_name -vserver svm_name -anti-ransomware-state active
```


3. Verifique el estado ARP del volumen.

```
security anti-ransomware volume show
```

Habilite ARP en un nuevo volumen

1. Crea un nuevo volumen con la protección antiransomware habilitada antes de aprovisionar los datos.

```
volume create -volume vol_name -vserver svm_name -aggregate aggr_name -size nn -anti-ransomware-state dry-run -junction-path /path_name
```

Si ejecuta ONTAP 9.13.1 o posterior, el aprendizaje adaptativo se activa para que el cambio al estado activo se realice automáticamente. Si no desea que este comportamiento se habilite automáticamente, cambie la configuración en el nivel de SVM en todos los volúmenes asociados:

```
vserver modify svm_name -anti-ransomware-auto-switch-from-learning-to-enabled false
```

2. Cuando el periodo de aprendizaje haya terminado, modifique el volumen protegido para cambiar al modo activo si no se ha realizado automáticamente:

```
security anti-ransomware volume enable -volume vol_name -vserver svm_name
```

También se puede cambiar al modo activo con el comando modify volume:

```
volume modify -volume vol_name -vserver svm_name -anti-ransomware-state active
```

3. Verifique el estado ARP del volumen.

```
security anti-ransomware volume show
```

Habilite la protección de ransomware autónoma de forma predeterminada en nuevos volúmenes

A partir de ONTAP 9.10.1, puede configurar máquinas virtuales de almacenamiento (SVM) de modo que los nuevos volúmenes estén habilitados por defecto para protección de ransomware autónoma (ARP) en el modo de aprendizaje.

Acerca de esta tarea

De manera predeterminada, se crean nuevos volúmenes con ARP en el modo deshabilitado. Puede modificar este ajuste en System Manager y con la CLI. Los volúmenes que están habilitados de forma predeterminada se establecen en ARP en modo de aprendizaje (o ejecución seca).

ARP solo se habilitará en los volúmenes creados en la SVM después de modificar la configuración. ARP no estará habilitado en los volúmenes existentes. Aprenda cómo ["Habilite ARP en un volumen existente"](#).

A partir de ONTAP 9.13.1, el aprendizaje adaptativo se ha agregado a la analítica ARP, y el cambio del modo de aprendizaje al modo activo se realiza automáticamente. Para obtener más información, consulte ["Modos de aprendizaje y activos"](#).

Antes de empezar

- La [licencia correcta](#) Debe estar instalado para la versión de ONTAP.
- El volumen debe estar lleno por debajo del 100%.
- Las rutas de unión deben estar activas.
- A partir de ONTAP 9.13.1, se recomienda habilitar la verificación multiadministrador (MAV) para que se necesiten dos o más administradores de usuarios autenticados para las operaciones anti-ransomware. ["Leer más"](#).

Cambie ARP del modo de aprendizaje al modo activo

A partir de ONTAP 9.13.1, el aprendizaje adaptativo se ha añadido a la analítica ARP. El cambio del modo de aprendizaje al modo activo se realiza automáticamente. La decisión autónoma de ARP de cambiar automáticamente del modo de aprendizaje al modo activo se basa en los ajustes de configuración de las siguientes opciones:

```
-anti-ransomware-auto-switch-minimum-incoming-data-percent  
-anti-ransomware-auto-switch-duration-without-new-file-extension  
-anti-ransomware-auto-switch-minimum-learning-period  
-anti-ransomware-auto-switch-minimum-file-count  
-anti-ransomware-auto-switch-minimum-file-extension
```


Después de 30 días de aprendizaje, un volumen se cambia automáticamente al modo activo incluso si una o más de estas condiciones no se cumplen. Es decir, si el cambio automático está activado, el volumen cambia al modo activo después de un máximo de 30 días. El valor máximo de 30 días es fijo y no modificable.

Para obtener más información sobre las opciones de configuración de ARP, incluidos los valores predeterminados, consulte la ["Referencia de comandos de la ONTAP"](#).

Pasos

Puede usar System Manager o la interfaz de línea de comandos de ONTAP para habilitar ARP de manera predeterminada.

System Manager

1. Seleccione **Almacenamiento > Storage VMs** y, a continuación, seleccione la VM de almacenamiento que contiene los volúmenes que desea proteger con ARP.
2. Navega a la pestaña **Settings**. En **Seguridad**, localice el mosaico **Anti-ransomware** y luego seleccione .
3. Marque la casilla para habilitar ARP para volúmenes NAS. Marque la casilla adicional para habilitar ARP en todos los volúmenes NAS elegibles en la máquina virtual de almacenamiento.



Si ha actualizado a ONTAP 9.13.1, el ajuste **Cambie automáticamente del modo de aprendizaje al modo activo después de suficiente aprendizaje** se habilita automáticamente. Esto permite a ARP determinar el intervalo óptimo del período de aprendizaje y automatizar el cambio al modo activo. Desactive el ajuste si desea realizar la transición manual al modo activo.

CLI

1. Modifique una SVM existente para habilitar ARP de forma predeterminada en volúmenes nuevos:

```
vserver modify -vserver svm_name -anti-ransomware-default-volume-state dry-run
```

En la CLI, también puede crear una SVM nueva con ARP habilitada de forma predeterminada para volúmenes nuevos.

```
vserver create -vserver svm_name -anti-ransomware-default-volume-state dry-run [other parameters as needed]
```

Si ha actualizado a ONTAP 9.13.1 o posterior, el aprendizaje adaptativo se activa para que el cambio al estado activo se realice automáticamente. Si no desea que este comportamiento se habilite automáticamente, utilice el siguiente comando:

```
vserver modify svm_name -anti-ransomware-auto-switch-from-learning-to-enabled false
```

Detenga la protección de ransomware autónoma para excluir eventos de carga de trabajo del análisis

Si espera eventos de carga de trabajo inusuales, puede suspender temporalmente y reanudar el análisis de la protección de ransomware autónoma (ARP) en cualquier momento.

A partir de ONTAP 9.13.1, puede habilitar la verificación multiadministrador (MAV) para que se requieran dos o más administradores de usuarios autenticados para pausar ARP. ["Leer más"](#).

Acerca de esta tarea

Durante una pausa de ARP, no se registran eventos ni se realiza ninguna acción para las nuevas escrituras. No obstante, la operación de análisis continúa para registros anteriores en segundo plano.



No utilice la función de desactivación ARP para pausar el análisis. Al hacerlo, se deshabilita ARP en el volumen y se pierde toda la información existente acerca del comportamiento de la carga de trabajo adquirida. Esto requeriría un reinicio del período de aprendizaje.

Pasos

Puede usar System Manager o la interfaz de línea de comandos de ONTAP para pausar ARP.

System Manager

1. Seleccione **Almacenamiento > Volúmenes** y, a continuación, seleccione el volumen donde desea pausar ARP.
2. En la pestaña **Seguridad** de la vista general de volúmenes, selecciona **Pausa anti-ransomware** en la casilla **Anti-ransomware**.



A partir de ONTAP 9.13.1, si utiliza MAV para proteger la configuración ARP, la operación de pausa le solicita la aprobación de uno o más administradores adicionales. ["La aprobación debe recibirse de todos los administradores"](#) Asociado al grupo de aprobación MAV o la operación fallará.

CLI

1. Poner en pausa ARP en un volumen:

```
security anti-ransomware volume pause -vserver svm_name -volume vol_name
```

2. Para reanudar el procesamiento, utilice `resume` parámetro.

```
security anti-ransomware volume resume -vserver svm_name -volume vol_name
```

3. **Si está utilizando MAV (disponible con ARP a partir de ONTAP 9.13.1) para proteger su configuración ARP**, la operación de pausa le pedirá que obtenga la aprobación de uno o más administradores adicionales. Se debe recibir la aprobación de todos los administradores asociados al grupo de aprobación MAV o la operación fallará.

Si utiliza MAV y una operación de pausa esperada necesita aprobaciones adicionales, cada aprobador de grupo MAV realiza lo siguiente:

- a. Mostrar la solicitud:

```
security multi-admin-verify request show
```

- b. Apruebe la solicitud:

```
security multi-admin-verify request approve -index[number returned from show request]
```

La respuesta del último aprobador de grupo indica que el volumen se ha modificado y que el estado de ARP está en pausa.

Si utiliza MAV y es un aprobador de grupo MAV, puede rechazar una solicitud de operación de pausa:

```
security multi-admin-verify request veto -index[number returned from show request]
```

Gestiona los parámetros de detección de ataques de protección autónoma frente a ransomware

A partir de ONTAP 9.11.1, se pueden modificar los parámetros de detección de ransomware en un volumen específico habilitado para la protección autónoma contra ransomware e informar un aumento conocido como actividad normal de los archivos. El ajuste de los parámetros de detección ayuda a mejorar la precisión de los informes según la carga de trabajo del volumen específico.

Cómo funciona la detección de ataques

Cuando la protección autónoma contra ransomware (ARP) está en modo de aprendizaje, desarrolla valores básicos para los comportamientos de volumen. Son entropía, extensiones de archivos y, a partir de ONTAP 9.11.1, IOPS. Estas líneas de base se utilizan para evaluar las amenazas de ransomware. Para obtener más información sobre estos criterios, consulte [Lo que ARP detecta](#).

En ONTAP 9.10.1, ARP emite una advertencia si detecta las dos condiciones siguientes:

- más de 20 archivos con extensiones de archivo no observadas anteriormente en el volumen
- alta entropía de datos

A partir de ONTAP 9.11.1, ARP emite una advertencia de amenaza si se cumple *only* una condición. Por ejemplo, si se observan más de 20 archivos con extensiones de archivo que no se han observado previamente en el volumen en un período de 24 horas, ARP lo clasificará como una amenaza *independientemente* de la entropía observada. (Los valores de archivo de 24 hora y 20 son los valores predeterminados, que se pueden modificar).

A partir de ONTAP 9.14.1, se pueden configurar alertas cuando ARP observa una nueva extensión de archivo y cuando ARP crea una instantánea. Para obtener más información, consulte [\[modify-alerts\]](#)

Ciertos volúmenes y cargas de trabajo requieren parámetros de detección diferentes. Por ejemplo, el volumen compatible con ARP puede alojar numerosos tipos de extensiones de archivo, en cuyo caso es posible que desee modificar el recuento de umbrales para extensiones de archivo nunca vistas hasta un número mayor que el predeterminado de 20 o deshabilitar las advertencias basadas en extensiones de archivo nunca vistas. A partir de ONTAP 9.11.1, puedes modificar los parámetros de detección de ataques para que se adapten mejor a tus cargas de trabajo específicas.

Modificar los parámetros de detección de ataques

Dependiendo de los comportamientos esperados de su volumen con ARP habilitado, es posible que desee modificar los parámetros de detección de ataques.

Pasos

1. Ver los parámetros de detección de ataques existentes:

```
security anti-ransomware volume attack-detection-parameters show -vserver  
svm_name -volume volume_name
```

```
security anti-ransomware volume attack-detection-parameters show
-vserver vs1 -volume voll
```

```

Vserver Name : vs1
Volume Name : voll
Is Detection Based on High Entropy Data Rate? : true
Is Detection Based on Never Seen before File Extension? : true
Is Detection Based on File Create Rate? : true
Is Detection Based on File Rename Rate? : true
Is Detection Based on File Delete Rate? : true
Is Detection Relaxing Popular File Extensions? : true
High Entropy Data Surge Notify Percentage : 100
File Create Rate Surge Notify Percentage : 100
File Rename Rate Surge Notify Percentage : 100
File Delete Rate Surge Notify Percentage : 100
Never Seen before File Extensions Count Notify Threshold : 20
Never Seen before File Extensions Duration in Hour : 24

```

2. Todos los campos mostrados se pueden modificar con valores booleanos o enteros. Para modificar un campo, utilice la `security anti-ransomware volume attack-detection-parameters modify` comando.

Para obtener una lista completa de parámetros, consulte ["Referencia de comandos de la ONTAP"](#).

Informe de sobretensiones conocidas

ARP continúa modificando los valores de línea base para los parámetros de detección, incluso en modo activo. Si conoce aumentos en su actividad de volumen, ya sea un aumento puntual o un aumento característico de una nueva normalidad, debe informar de ello como seguro. Informar manualmente de estas subidas como seguras ayuda a mejorar la precisión de las evaluaciones de amenazas de ARP.

Informe de un aumento puntual

1. Si se produce un aumento puntual en circunstancias conocidas y desea que ARP informe de un aumento similar en circunstancias futuras, borre el aumento del comportamiento de la carga de trabajo:

```
security anti-ransomware volume workload-behavior clear-surge -vserver
svm_name -volume volume_name
```

Modificar sobretensiones de línea base

1. Si una sobretensión informada debe considerarse un comportamiento normal de la aplicación, notifique la sobretensión como tal para modificar el valor de sobretensión de línea base.

```
security anti-ransomware volume workload-behavior update-baseline-from-surge
-vserver svm_name -volume volume_name
```

Configurar alertas ARP

A partir de ONTAP 9.14.1, ARP permite especificar alertas para dos eventos ARP:

- Observación de la nueva extensión de archivo en un volumen
- Creación de una instantánea ARP

Es posible establecer alertas para estos dos eventos en volúmenes individuales o para toda la SVM. Si se habilitan alertas para la SVM, las configuraciones de alerta solo heredan los volúmenes creados después de habilitar la alerta. De manera predeterminada, las alertas no están habilitadas en ningún volumen.


Las alertas de eventos se pueden controlar con verificación multiadministrador. Para obtener más información, consulte [Verificación multi-admin con volúmenes protegidos con ARP](#).

System Manager

Configure alertas para un volumen

1. Navega a **volúmenes**. Seleccione el volumen individual para el cual desea modificar la configuración.
2. Seleccione la pestaña **Seguridad** y luego **Configuración de seguridad de eventos**.
3. Para recibir alertas de **Nueva extensión de archivo detectada** y **Instantánea de ransomware creada**, seleccione el menú desplegable bajo el encabezado **Gravedad**. Modifique la configuración de **No generar evento** a **Aviso**.
4. Seleccione **Guardar**.

Configure alertas para una SVM

1. Desplácese hasta **Storage VM** y seleccione la SVM para la que desea habilitar la configuración.
2. Bajo el encabezado **Seguridad**, localiza la tarjeta **Anti-ransomware**. Seleccione  Luego **Editar gravedad de evento de ransomware**.
3. Para recibir alertas de **Nueva extensión de archivo detectada** y **Instantánea de ransomware creada**, seleccione el menú desplegable bajo el encabezado **Gravedad**. Modifique la configuración de **No generar evento** a **Aviso**.
4. Seleccione **Guardar**.

CLI

Configure alertas para un volumen

- Para configurar alertas para una nueva extensión de archivo:

```
security anti-ransomware volume event-log modify -vserver svm_name -is  
-enabled-on-new-file-extension-seen true
```

- Para configurar alertas para la creación de una instantánea ARP:

```
security anti-ransomware volume event-log modify -vserver svm_name -is  
-enabled-on-snapshot-copy-creation true
```

- Confirme la configuración con el `anti-ransomware volume event-log show` comando.

Configure alertas para una SVM

- Para configurar alertas para una nueva extensión de archivo:

```
security anti-ransomware vserver event-log modify -vserver svm_name -is  
-enabled-on-new-file-extension-seen true
```

- Para configurar alertas para la creación de una instantánea ARP:

```
security anti-ransomware vserver event-log modify -vserver svm_name -is  
-enabled-on-snapshot-copy-creation true
```

- Confirme la configuración con el `security anti-ransomware vserver event-log show` comando.

Más información

- ["Comprende los ataques autónomos de protección frente a ransomware y el snapshot autónomo de protección frente a ransomware"](#)

Responda a actividades anormales

Cuando la protección de ransomware autónoma (ARP) detecta actividad anormal en un volumen protegido, emite una advertencia. Debe evaluar la notificación para determinar si la actividad es aceptable (falso positivo) o si un ataque parece malicioso.

Acerca de esta tarea

ARP muestra una lista de archivos sospechosos cuando detecta cualquier combinación de alta entropía de datos, actividad de volumen anormal con cifrado de datos y extensiones de archivo inusuales.

Cuando se emite la advertencia, puede responder marcando la actividad de archivo de dos maneras:

- **Falso positivo**

Se espera el tipo de archivo identificado en la carga de trabajo y se puede ignorar.

- **Potencial ataque de ransomware**

El tipo de archivo identificado no es esperado en su carga de trabajo y debe tratarse como un ataque potencial.

En ambos casos, la monitorización normal se reanuda después de actualizar y borrar los avisos. ARP registra su evaluación en el perfil de evaluación de amenazas, utilizando su elección para supervisar las actividades de archivo posteriores.

En caso de sospecha de un ataque, debes determinar si se trata de un ataque, responder a él si es así y restaurar los datos protegidos antes de borrar los avisos. ["Obtenga más información sobre cómo recuperarse de un ataque de ransomware"](#).



Si restaura un volumen completo, no hay avisos que borrar.

Antes de empezar

ARP debe estar ejecutándose en modo activo.

Pasos

Puede usar System Manager o la interfaz de línea de comandos de ONTAP para responder a una tarea anormal.

System Manager


1. Cuando recibas una notificación de “actividad anormal”, sigue el enlace o navega a la pestaña **Seguridad** de la descripción general de **Volúmenes**.

Las advertencias se muestran en el panel **Overview** del menú **Events**.

2. Cuando aparezca un mensaje de “actividad de volumen anormal detectada”, consulte los archivos sospechosos.

En la pestaña **Seguridad**, selecciona **Ver tipos de archivos sospechosos**.

3. En el cuadro de diálogo **tipos de archivo sospechosos**, examine cada tipo de archivo y márkelo como “falso positivo” o “ataque potencial de ransomware”.

| Si seleccionó este valor... | Realice esta acción... |
|------------------------------|---|
| Falso positivo | <div><div>Seleccione Actualizar y Borrar tipos de archivos sospechosos para registrar su decisión y reanudar el monitoreo normal de ARP.</div><div><div>A partir de ONTAP 9.13.1, si está utilizando MAV para proteger su configuración ARP, la operación claramente sospechosa le solicita que obtenga la aprobación de uno o más administradores adicionales. "La aprobación debe recibirse de todos los administradores" Asociado al grupo de aprobación MAV o la operación fallará.</div></div></div> |
| Posible ataque de ransomware | <div>Responda al ataque y restaure datos protegidos. A continuación, seleccione Actualizar y Borrar tipos de archivos sospechosos para registrar su decisión y reanudar el monitoreo ARP normal.</div> <div>No hay ningún tipo de archivo sospechoso que borrar si se restaura un volumen completo.</div> |

CLI

1. Cuando reciba una notificación de un ataque de ransomware sospechoso, compruebe la hora y la gravedad del ataque:

```
security anti-ransomware volume show -vserver svm_name -volume vol_name
```

Salida de muestra:

```
Vserver Name: vs0
Volume Name: vol1
State: enabled
Attack Probability: moderate
Attack Timeline: 9/14/2021 01:03:23
Number of Attacks: 1
```

También puede comprobar los mensajes de EMS:

```
event log show -message-name callhome.arw.activity.seen
```

2. Generar un informe de ataque y anotar la ubicación de salida:

```
security anti-ransomware volume attack generate-report -volume vol_name  
-dest-path file_location/
```

Salida de muestra:

```
Report "report_file_vs0_vol1_14-09-2021_01-21-08" available at path  
"vs0:vol1/"
```

3. Ver el informe en un sistema cliente de administración. Por ejemplo:

```
[root@rhel8 mnt]# cat report_file_vs0_vol1_14-09-2021_01-21-08  
  
19  "9/14/2021 01:03:23"    test_dir_1/test_file_1.jpg.lckd  
20  "9/14/2021 01:03:46"    test_dir_2/test_file_2.jpg.lckd  
21  "9/14/2021 01:03:46"    test_dir_3/test_file_3.png.lckd`
```

4. Realice una de las siguientes acciones en función de su evaluación de las extensiones de archivo:

◦ Falso positivo

Introduzca el siguiente comando para registrar su decisión, agregando la nueva extensión a la lista de los permitidos y reanudar la supervisión anti-ransomware normal:

```
anti-ransomware volume attack clear-suspect -vserver svm_name -volume  
vol_name [extension identifiers] -false-positive true
```

Utilice uno de los siguientes parámetros para identificar las extensiones:

`[-seq-no integer]` Número de secuencia del archivo en la lista de sospechosos.

`[-extension text, ...]` Extensiones de archivo

`[-start-time date_time -end-time date_time]` Horas de inicio y finalización del intervalo de archivos que se van a borrar, con el formato "MM/DD/AAAA HH:MM:SS".

◦ Ataque potencial de ransomware

Responda al ataque y. ["Recupere los datos de la instantánea de backup creada por ARP"](#).

Después de recuperar los datos, introduzca el siguiente comando para registrar su decisión y reanudar la supervisión normal de ARP:

```
anti-ransomware volume attack clear-suspect -vserver svm_name -volume  
vol_name [extension identifiers] -false-positive false
```

Utilice uno de los siguientes parámetros para identificar las extensiones:

`[-seq-no integer]` Número de secuencia del archivo en la lista de sospechosos

`[-extension text, ...]` Extensión de archivo

`[-start-time date_time -end-time date_time]` Horas de inicio y finalización del intervalo de archivos que se van a borrar, con el formato "MM/DD/AAAA HH:MM:SS".

No hay ningún tipo de archivo sospechoso que borrar si se restaura un volumen completo. Se eliminará la instantánea de copia de seguridad creada por ARP y se borrará el informe de ataque.

5. Si está utilizando MAV y se espera `clear-suspect` La operación necesita aprobaciones adicionales, cada aprobador del grupo MAV hace lo siguiente:

- a. Mostrar la solicitud:

```
security multi-admin-verify request show
```

- b. Apruebe la solicitud para reanudar la supervisión normal antiransomware:

```
security multi-admin-verify request approve -index[number returned from show request]
```

La respuesta del último aprobador de grupo indica que el volumen se ha modificado y se registra un falso positivo.

6. Si está utilizando MAV y es un aprobador de grupo MAV, también puede rechazar una solicitud clara sospechosa:

```
security multi-admin-verify request veto -index[number returned from show request]
```

Más información

- ["KB: Comprender los ataques autónomos de protección frente a ransomware y la instantánea de protección autónoma frente a ransomware"](#).

Restaura los datos después de un ataque de ransomware

Autonomous Ransomware Protection (ARP) crea copias Snapshot denominadas `Anti_ransomware_backup` cuando detecta una posible amenaza de ransomware. Puede usar una de estas copias Snapshot de ARP u otra copia Snapshot del volumen para restaurar los datos.

Acerca de esta tarea

Si el volumen tiene relaciones de SnapMirror, replique manualmente todas las copias de reflejo del volumen inmediatamente después de restaurar desde una copia de Snapshot. Si no lo hace, puede provocar copias reflejadas inutilizables que se deban eliminar y volver a crear.

Para restaurar desde una copia Snapshot que no sea la `Anti_ransomware_backup` Snapshot Después de identificar un ataque del sistema, primero debe liberar la instantánea ARP.

Si no se ha informado de ningún ataque al sistema, primero debe restaurar desde el `Anti_ransomware_backup` Y luego complete una restauración posterior del volumen de la copia Snapshot que elija.

Pasos

Puede usar System Manager o la interfaz de línea de comandos de ONTAP para restaurar los datos.

System Manager

Restaurar después de un ataque al sistema

1. Para restaurar desde la instantánea ARP, vaya al paso dos. Para restaurar desde una copia snapshot anterior, primero debe liberar el bloqueo en la instantánea ARP.
 - a. Seleccione **almacenamiento > volúmenes**.
 - b. Seleccione **Seguridad** y luego **Ver tipos de archivos sospechosos**
 - c. Marque los archivos como "False positive" .
 - d. Seleccione **Actualizar y Borrar tipos de archivos sospechosos**
2. Mostrar las copias Snapshot en los volúmenes:


Selecciona **Almacenamiento > Volúmenes** y, a continuación, selecciona el volumen y **Copias instantáneas**.

3. Seleccione  Junto a la copia Snapshot que desea restaurar, luego **Restaurar**.

Restaurar si no se identificó un ataque del sistema

1. Mostrar las copias Snapshot en los volúmenes:

Selecciona **Almacenamiento > Volúmenes** y, a continuación, selecciona el volumen y **Copias instantáneas**.

2. Seleccione  ellos eligen el `Anti_ransomware_backup` Snapshot.
3. Seleccione **Restaurar**.
4. Vuelva al menú **Copias de instantánea** y, a continuación, elija la copia de instantánea que desee utilizar. Seleccione **Restaurar**.

CLI

Restaurar después de un ataque al sistema

1. Para restaurar desde la copia snapshot de ARP, vaya al paso dos. Para restaurar datos de copias snapshot anteriores, debe liberar el bloqueo de la instantánea ARP.



Solo es necesario liberar la SnapLock antiransomware antes de restaurar desde copias de Snapshot anteriores si utiliza el `volume snap restore` comando como se describe a continuación. Si va a restaurar datos utilizando Flex Clone, Single File Snap Restore u otros métodos, esto no es necesario.

Marcar el ataque como «falso positivo» y «claro sospechoso»:

```
anti-ransomware volume attack clear-suspect -vserver svm_name -volume vol_name [extension identifiers] -false-positive true
```

Utilice uno de los siguientes parámetros para identificar las extensiones:

`[-seq-no integer]` Número de secuencia del archivo en la lista de sospechosos.

`[-extension text, ...]` Extensiones de archivo

`[-start-time date_time -end-time date_time]` Horas de inicio y finalización del intervalo de archivos que se van a borrar, con el formato "MM/DD/AAAA HH:MM:SS".

2. Enumere las copias Snapshot en un volumen:

```
volume snapshot show -vserver SVM -volume volume
```

El ejemplo siguiente muestra las copias Snapshot en vol1:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1
```

| Vserver | Volume | Snapshot | State | Size | Total% | Used% |
|---------|--------|------------------------|-------|-------|--------|-------|
| vs1 | vol1 | hourly.2013-01-25_0005 | valid | 224KB | 0% | 0% |
| | | daily.2013-01-25_0010 | valid | 92KB | 0% | 0% |
| | | hourly.2013-01-25_0105 | valid | 228KB | 0% | 0% |
| | | hourly.2013-01-25_0205 | valid | 236KB | 0% | 0% |
| | | hourly.2013-01-25_0305 | valid | 244KB | 0% | 0% |
| | | hourly.2013-01-25_0405 | valid | 244KB | 0% | 0% |
| | | hourly.2013-01-25_0505 | valid | 244KB | 0% | 0% |

7 entries were displayed.

3. Restaure el contenido de un volumen de una copia Snapshot:

```
volume snapshot restore -vserver SVM -volume volume -snapshot snapshot
```

En el ejemplo siguiente se restaura el contenido de vol1:

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1  
-snapshot daily.2013-01-25_0010
```

Restaurar si no se identificó un ataque del sistema

1. Enumere las copias Snapshot en un volumen:

```
volume snapshot show -vserver SVM -volume volume
```

El ejemplo siguiente muestra las copias Snapshot en vol1:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1
```

| Vserver | Volume | Snapshot | State | Size | Total% | Used% |
|---------|--------|------------------------|-------|-------|--------|-------|
| vs1 | vol1 | hourly.2013-01-25_0005 | valid | 224KB | 0% | 0% |
| | | daily.2013-01-25_0010 | valid | 92KB | 0% | 0% |
| | | hourly.2013-01-25_0105 | valid | 228KB | 0% | 0% |
| | | hourly.2013-01-25_0205 | valid | 236KB | 0% | 0% |
| | | hourly.2013-01-25_0305 | valid | 244KB | 0% | 0% |
| | | hourly.2013-01-25_0405 | valid | 244KB | 0% | 0% |
| | | hourly.2013-01-25_0505 | valid | 244KB | 0% | 0% |

7 entries were displayed.

2. Restaure el contenido de un volumen de una copia Snapshot:

```
volume snapshot restore -vserver SVM -volume volume -snapshot snapshot
```

En el ejemplo siguiente se restaura el contenido de vol1:

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1  
-snapshot daily.2013-01-25_0010
```

3. Repita los pasos 1 y 2 para restaurar el volumen con la copia Snapshot que desee.

Más información

- ["KB: Prevención y recuperación de ransomware en ONTAP"](#)

Modifique las opciones de las copias automáticas Snapshot

A partir de ONTAP 9.11.1, puede utilizar la interfaz de línea de comandos para controlar la configuración de retención de copias de Snapshot de protección autónoma frente a ransomware (ARP) que se generan automáticamente en respuesta a ataques de ransomware sospechosos.

Antes de empezar

Solo puede modificar las opciones de ARP Snapshots en una SVM de nodo.

Pasos

1. Para mostrar todas las opciones actuales de copias de Snapshot de ARP, introduzca:

```
vserver options -vserver svm_name arw*
```




La `vserver options` es un comando oculto. Para ver la página man, introduzca `man vserver options` En la CLI de ONTAP.

2. Para mostrar la configuración de copia de Snapshot de ARP actual seleccionada, introduzca:

```
vserver options -vserver svm_name -option-name arw_setting_name
```
3. Para modificar la configuración de una copia Snapshot de ARP, introduzca:

```
vserver options -vserver svm_name -option-name arw_setting_name -option-value arw_setting_value
```

Se pueden modificar los siguientes ajustes:

| Ajuste ARW | Descripción |
|--|--|
| arw.snap.max.count | Especifica la cantidad máxima de copias de Snapshot ARP que pueden existir en un volumen en un momento determinado. Las copias más antiguas se eliminan para garantizar que la cantidad total de copias de Snapshot ARP se encuentre dentro del límite especificado. |
| arw.snap.create.interval.hours | Especifica el intervalo <i>in hours</i> entre las copias snapshot ARP. Se crea una nueva copia snapshot cuando se sospecha de un ataque, y la copia creada anteriormente es más antigua que este intervalo especificado. |
| arw.snap.normal.retain.interval.hours | Especifica la duración <i>en horas</i> durante el cual se conserva una copia Snapshot ARP. Cuando una copia Snapshot de ARP se convierte en este antigua, se elimina cualquier otra copia Snapshot de ARP creada antes de la copia más reciente para alcanzar esta antigüedad. Ninguna copia Snapshot ARP puede tener una duración anterior a esta. |
| arw.snap.max.retain.interval.days | <p>Especifica la duración máxima <i>en días</i> durante el cual se puede conservar una copia Snapshot ARP. Cualquier copia de Snapshot ARP anterior a esta duración se eliminará si no se informa de ningún ataque en el volumen.</p> <p>+</p> <div style="display: flex; align-items: center;">  <p>El intervalo de retención máximo para las copias snapshot ARP se ignora si se detecta una amenaza moderada. La copia snapshot de ARP creada en respuesta a la amenaza se retiene hasta que haya respondido a la amenaza. Marcar una amenaza como falso positivo Elimina las copias snapshot de ARP en el volumen.</p> </div> |
| arw.snap.create.interval.hours.post.max.count | Especifica el intervalo <i>en horas</i> entre las copias Snapshot de ARP cuando el volumen ya contiene el número máximo de copias Snapshot de ARP. Cuando se alcanza el número máximo, se elimina una copia snapshot ARP para dar espacio a una nueva copia. La nueva velocidad de creación de copias Snapshot ARP puede reducirse para conservar la copia más antigua con esta opción. Si el volumen ya contiene el número máximo de copias Snapshot ARP, este intervalo especificado en esta opción se utiliza para la próxima creación de copias Snapshot ARP, en lugar de <code>arw.snap.create.interval.hours</code> . |
| arw.surge.snap.interval.days | Especifica el intervalo <i>en días</i> entre las copias Snapshot de sobrecarga de ARP. ONTAP crea una copia de exceso de Snapshot de ARP cuando hay un aumento en el tráfico de I/O y la última copia Snapshot de ARP creada es más antigua que este intervalo especificado. Esta opción también especifica el período de retención <i>in day</i> para una instantánea de sobrecarga ARP. |

Protéjase contra virus

Información general de la configuración de antivirus

VSCAN es una solución de análisis antivirus desarrollada por NetApp que permite a los clientes proteger sus datos para evitar que se vean comprometidos por virus u otro código malicioso.

VSCAN realiza análisis de virus cuando los clientes acceden a los archivos a través de SMB. Puede configurar Vscan para que escanee bajo demanda o según una programación. Puede interactuar con Vscan mediante la interfaz de línea de comandos (CLI) de ONTAP o las interfaces de programación de aplicaciones (API) de ONTAP.

Información relacionada

["Soluciones de partners de VSCAN"](#)

Acerca de la protección antivirus de NetApp

Acerca de la detección de virus de NetApp

VSCAN es una solución de análisis antivirus desarrollada por NetApp que permite a los clientes proteger sus datos para evitar que se vean comprometidos por virus u otro código malicioso. Combina el software antivirus proporcionado por los partners con las funciones de ONTAP para ofrecer a los clientes la flexibilidad que necesitan para gestionar los análisis de archivos.

Cómo funciona el análisis de virus

Los sistemas de almacenamiento descargan las operaciones de análisis en servidores externos que alojan software antivirus de otros proveedores.

Basado en el modo de análisis activo, ONTAP envía solicitudes de análisis cuando los clientes acceden a los archivos a través de SMB (en acceso) o acceden a archivos en ubicaciones específicas, en un horario o inmediatamente (bajo demanda).

- Puede utilizar *análisis en tiempo real* para comprobar si hay virus cuando los clientes abren, leen, renombran o cierran archivos en SMB. Las operaciones de archivos se suspenden hasta que el servidor externo informe del estado de análisis del archivo. Si el archivo ya se ha analizado, ONTAP permite la operación de archivo. De lo contrario, solicita un análisis desde el servidor.

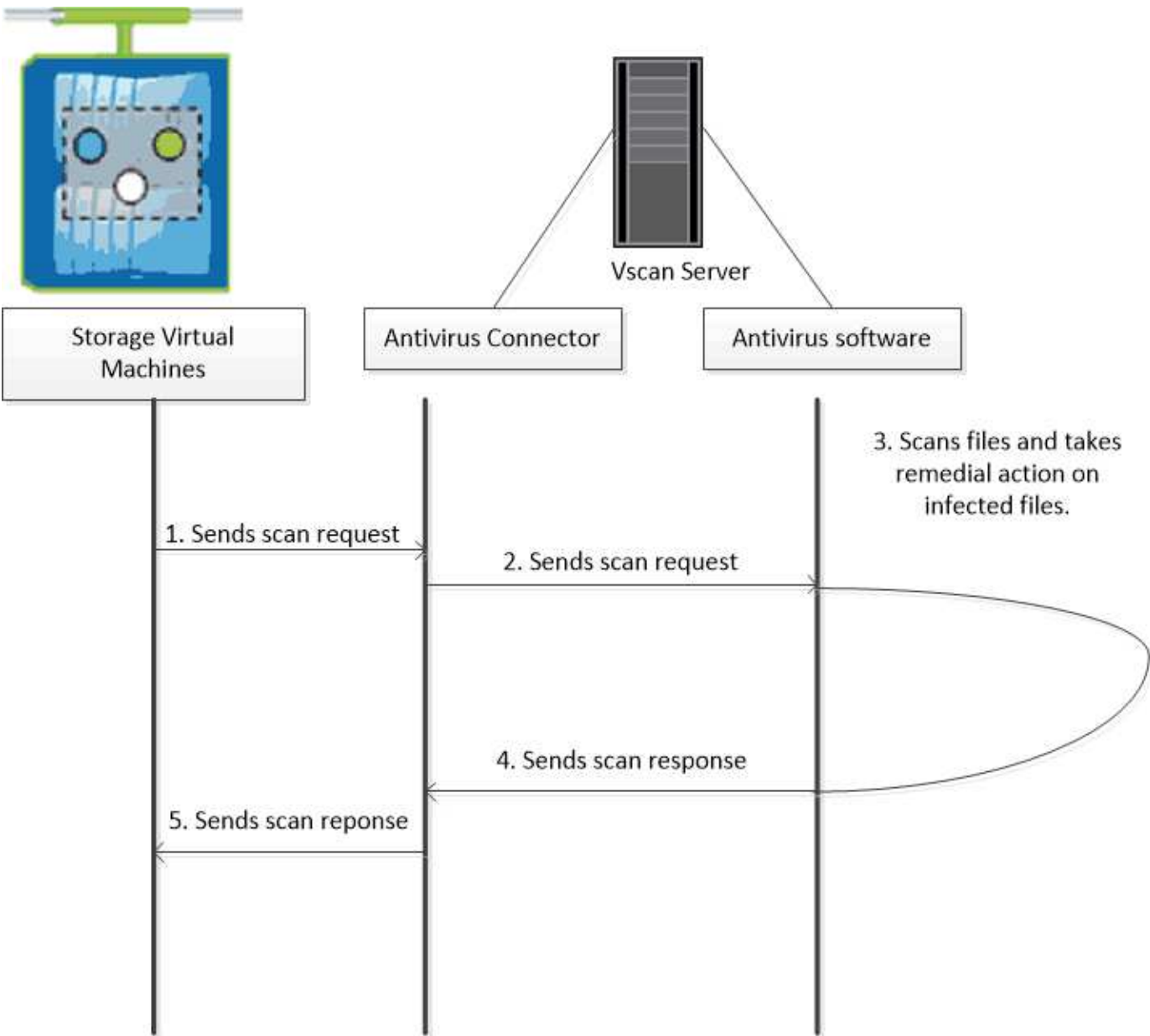
El análisis en tiempo real no es compatible con NFS.

- Puede utilizar *análisis bajo demanda* para comprobar los archivos en busca de virus inmediatamente o en una programación. Recomendamos que los análisis bajo demanda se ejecuten solo en horas de menor actividad para evitar sobrecargar la infraestructura de antivirus existente, que normalmente está dimensionada para el análisis de acceso. El servidor externo actualiza el estado de escaneo de los archivos comprobados, de modo que la latencia de acceso a archivos se reduce con SMB. Si hubo modificaciones de archivos o actualizaciones de la versión de software, solicita un nuevo análisis de archivos desde el servidor externo.

Puede utilizar el análisis bajo demanda para cualquier ruta del espacio de nombres de SVM, incluso para los volúmenes que solo se exportan mediante NFS.

Habitualmente, habilita los modos de análisis bajo acceso y bajo demanda en una SVM. En cualquiera de los dos modos, el software antivirus realiza una acción correctiva sobre los archivos infectados en función de la configuración del software.

El conector antivirus ONTAP, proporcionado por NetApp e instalado en el servidor externo, gestiona la comunicación entre el sistema de almacenamiento y el software antivirus.

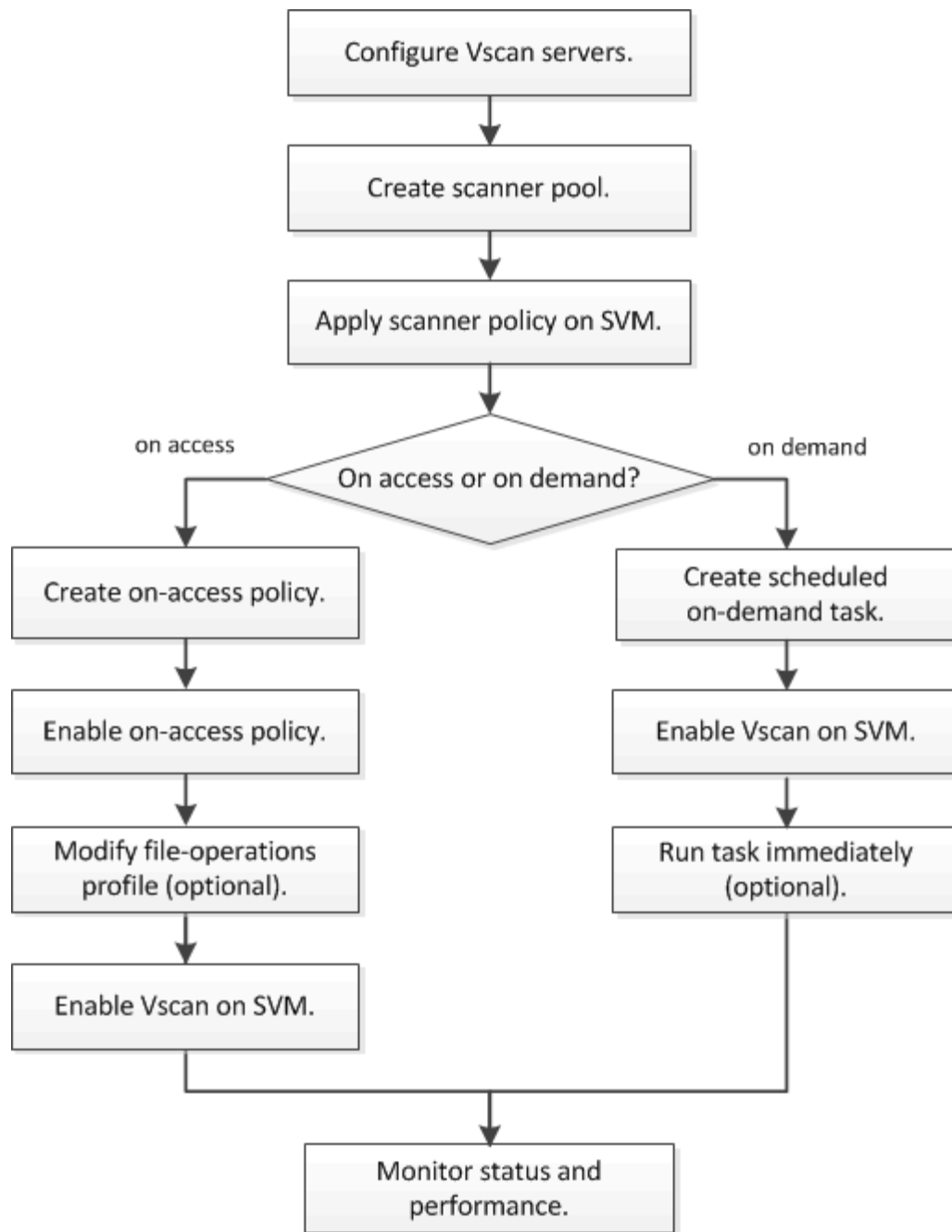


Flujo de trabajo de detección de virus

Debe crear un grupo de escáneres y aplicar una directiva de escáner antes de poder activar el análisis. Habitualmente, habilita los modos de análisis bajo acceso y bajo demanda en una SVM.



Debe haber completado la configuración de CIFS.



Siguientes pasos

- [Cree un pool de escáneres en un único clúster](#)
- [Aplicar una política de escáner en un único clúster](#)
- [Crear una política de acceso](#)

Arquitectura de antivirus

La arquitectura antivirus de NetApp consiste en el software del servidor Vscan y la configuración asociada.

Software de servidor VSCAN

Debe instalar este software en el servidor Vscan.

- **Conector antivirus ONTAP**

Se trata de un software proporcionado por NetApp que gestiona la comunicación de solicitudes de análisis y respuestas entre las SVM y el software antivirus. Puede ejecutarse en una máquina virtual, pero para obtener el mejor rendimiento, utilice una máquina física. Puede descargar este software desde el sitio de soporte de NetApp (requiere inicio de sesión).

- **Software antivirus**

Este es un software proporcionado por los socios que analiza los archivos en busca de virus u otro código malicioso. Al configurar el software, se especifican las acciones correctivas que se van a realizar en los archivos infectados.

Configuración del software VSCAN

Debe configurar estos ajustes de software en el servidor Vscan.

- **Piscina del escáner**

Esta configuración define los servidores Vscan y los usuarios con privilegios que se pueden conectar a SVM. También define un período de tiempo de espera de solicitud de exploración, tras el cual la solicitud de exploración se envía a un servidor Vscan alternativo si hay uno disponible.



Debe establecer el período de tiempo de espera en el software antivirus del servidor Vscan en cinco segundos menos que el período de tiempo de espera de solicitud de exploración del grupo de análisis. Esto evitará situaciones en las que el acceso al archivo se retrase o rechace por completo porque el período de tiempo de espera del software es mayor que el período de tiempo de espera de la solicitud de exploración.

- **Usuario privilegiado**

Este ajuste es una cuenta de usuario de dominio que un servidor Vscan utiliza para conectarse a la SVM. La cuenta debe existir en la lista de usuarios con privilegios del grupo de escáneres.

- **Directiva del escáner**

Esta configuración determina si un conjunto de escáneres está activo. Las políticas de escáner están definidas por el sistema, por lo que no puede crear políticas de escáner personalizadas. Solo estas tres políticas están disponibles:

- `Primary` especifica que el grupo de escáneres está activo.
- `Secondary` Especifica que el grupo de escáneres está activo, sólo cuando no hay ningún servidor Vscan conectado en el grupo de escáneres principal.
- `Idle` especifica que el grupo de escáneres está inactivo.

- **Política de acceso**

Esta configuración define el ámbito de una exploración en acceso. Puede especificar el tamaño máximo de archivo que se va a escanear, las extensiones de archivo y las rutas que se van a incluir en el escaneo, y las extensiones de archivo y las rutas de acceso que se van a excluir del escaneo.

De forma predeterminada, solo se analizan los volúmenes de lectura/escritura. Puede especificar filtros que permitan el análisis de volúmenes de sólo lectura o que restrinjan el análisis de archivos abiertos con el acceso de ejecución:

- `scan-ro-volume` permite analizar volúmenes de solo lectura.
- `scan-execute-access` restringe el escaneo a archivos abiertos con acceso de ejecución.



“Ejecutar acceso” es diferente de “ejecutar permiso”. Un cliente dado tendrá “acceso de ejecución” en un archivo ejecutable solo si el archivo fue abierto con “intención de ejecución”.

Puede ajustar la `scan-mandatory` Opción de desactivar para especificar que se permite el acceso al archivo cuando no hay servidores Vscan disponibles para el análisis de virus. En el modo de acceso puede elegir entre estas dos opciones mutuamente excluyentes:

- **Obligatorio:** Con esta opción, Vscan intenta entregar la solicitud de escaneo al servidor hasta que caduque el período de tiempo de espera. Si el servidor no acepta la solicitud de escaneo, se rechaza la solicitud de acceso del cliente.
- **No Obligatorio:** Con esta opción, Vscan siempre permite el acceso del cliente, independientemente de que haya o no un servidor Vscan disponible para la detección de virus.

• Tarea a petición

Esta configuración define el ámbito de una exploración bajo demanda. Puede especificar el tamaño máximo de archivo que se va a escanear, las extensiones de archivo y las rutas que se van a incluir en el escaneo, y las extensiones de archivo y las rutas de acceso que se van a excluir del escaneo. Los archivos de los subdirectorios se analizan de forma predeterminada.

Utilice una programación cron para especificar cuándo se ejecuta la tarea. Puede utilizar el `vserver vscan on-demand-task run` comando para ejecutar la tarea de inmediato.

• Perfil de operaciones de archivos Vscan (sólo escaneado en tiempo real)

La `vscan-fileop-profile` parámetro para `vserver cifs share create` El comando define qué operaciones de archivos SMB desencadenan el análisis de virus. De manera predeterminada, el parámetro se establece en `standard`, Que es la mejor práctica de NetApp. Puede ajustar este parámetro como sea necesario al crear o modificar un recurso compartido de SMB:

- `no-scan` especifica que las exploraciones de virus nunca se activan para el recurso compartido.
- `standard` especifica que las operaciones de apertura, cierre y cambio de nombre activan los análisis de virus.
- `strict` especifica que las exploraciones de virus se activan mediante operaciones de apertura, lectura, cierre y cambio de nombre.

La `strict` profile proporciona una seguridad mejorada para situaciones en las que varios clientes acceden a un archivo simultáneamente. Si un cliente cierra un archivo después de escribir un virus y el mismo archivo permanece abierto en un segundo cliente, `strict` garantiza que una operación de lectura del segundo cliente active un análisis antes de cerrar el archivo.

Debe tener cuidado de restringir el `strict`` se accederá simultáneamente a los recursos compartidos que contengan archivos que prevé. Dado que este perfil genera más solicitudes de análisis, puede afectar al rendimiento.

- `writes-only` especifica que las exploraciones de virus se activan sólo cuando se cierran los archivos modificados.

Desde `writes-only` genera menos solicitudes de escaneo, normalmente mejora el rendimiento.

Si utiliza este perfil, el escáner debe estar configurado para eliminar o poner en cuarentena los archivos infectados que no se pueden reparar, por lo que no se puede acceder a ellos. Si, por ejemplo, un cliente cierra un archivo tras escribir un virus y el archivo no se repara, elimina ni pone en cuarentena, ningún cliente que acceda al archivo `without` escribir a él será infectado.



Si una aplicación cliente realiza una operación de cambio de nombre, el archivo se cierra con el nuevo nombre y no se analiza. Si tales operaciones plantean un problema de seguridad en su entorno, debe utilizar el `standard` o `strict` perfil.

Soluciones de partners de VSCAN

NetApp colabora con Trellix, Symantec, Trend Micro y Sentinel One para ofrecer soluciones antivirus y antimalware líderes del sector que se basan en la tecnología Vscan de ONTAP. Estas soluciones le ayudan a analizar los archivos en busca de malware y corregir cualquier archivo afectado.

Tal y como se muestra en la siguiente tabla, los detalles de interoperabilidad de Trellix, Symantec y Trend Micro se conservan en la matriz de interoperabilidad de NetApp. También puede encontrar información sobre la interoperabilidad de Trellix y Symantec en los sitios web asociados. Los detalles de interoperabilidad de Sentinel One y otros nuevos socios serán mantenidos por el socio en sus sitios web.

| Como partner | Documentación de la solución | Detalles de interoperabilidad |
|--------------------------------|---|--|
| Trellix (anteriormente McAfee) | "Documentación del producto Trellix" | <ul style="list-style-type: none">• "Herramienta de matriz de interoperabilidad de NetApp"• "Plataformas compatibles con Endpoint Security Storage Protection (trellix.com)" |
| Symantec | "Symantec Protection Engine 9.0.0" | <ul style="list-style-type: none">• "Herramienta de matriz de interoperabilidad de NetApp"• "Matriz de compatibilidad para dispositivos asociados certificados con Symantec Protection Engine (SPE) para almacenamiento conectado a la red (NAS) 9.x.x."• "Matriz de compatibilidad para dispositivos de partners certificados con Symantec Protection Engine (SPE) para almacenamiento conectado a la red (NAS) 8.x (broadcom.com)" |
| Trend Micro | "Guía de inicio de Trend Micro ServerProtect for Storage 6,0" | "Herramienta de matriz de interoperabilidad de NetApp" |

| Como partner | Documentación de la solución | Detalles de interoperabilidad |
|--------------|---|-------------------------------|
| Sentinel One | <ul style="list-style-type: none"> • "SentinelOne Singularity Cloud Data Security" • "Compatibilidad con SentinelOne" <p>Este enlace requiere una conexión de usuario. Puede solicitar acceso desde Sentinel One.</p> | Instinto profundo |

Instalación y configuración del servidor VSCAN

Instalación y configuración del servidor VSCAN

Configure uno o más servidores Vscan para asegurarse de que los archivos de su sistema se analicen en busca de virus. Siga las instrucciones proporcionadas por su proveedor para instalar y configurar el software antivirus en el servidor.

Siga las instrucciones del archivo README proporcionado por NetApp para instalar y configurar el conector antivirus de ONTAP. También puede seguir las instrucciones de la ["Instale la página Conector antivirus de ONTAP"](#).



Para la recuperación ante desastres y las configuraciones de MetroCluster, debe configurar servidores Vscan independientes para los clústeres de ONTAP principal/local y secundario/asociado.

Requisitos del software antivirus

- Para obtener información acerca de los requisitos de software antivirus, consulte la documentación del proveedor.
- Para obtener información acerca de los proveedores, software y versiones compatibles con Vscan, consulte ["Soluciones de partners de VSCAN"](#) página.

Requisitos del conector antivirus de ONTAP

- Puede descargar el conector antivirus de ONTAP desde la página **Descarga de software** del sitio de soporte de NetApp. ["Descargas de NetApp: Software"](#)
- Para obtener información sobre las versiones de Windows compatibles con el conector antivirus de ONTAP y los requisitos de interoperabilidad, consulte ["Soluciones de partners de VSCAN"](#).



Puede instalar diferentes versiones de servidores Windows para diferentes servidores Vscan en un clúster.

- .NET 3.0 o posterior debe estar instalado en el servidor Windows.
- Debe estar habilitado SMB 2.0 en el servidor de Windows.

Instale el conector antivirus de ONTAP

Instale el conector antivirus ONTAP en el servidor Vscan para permitir la comunicación entre el sistema que ejecuta ONTAP y el servidor Vscan. Cuando el conector antivirus ONTAP está instalado, el software antivirus puede comunicarse con una o más máquinas virtuales de almacenamiento (SVM).

Acerca de esta tarea

- Consulte "[Soluciones de partners de VSCAN](#)" Para obtener información sobre los protocolos compatibles, las versiones del software del proveedor de antivirus, las versiones de ONTAP, los requisitos de interoperabilidad y los servidores Windows.
- Se debe instalar .NET 4.5.1 o posterior.
- El conector antivirus ONTAP puede ejecutarse en una máquina virtual. Sin embargo, para obtener el mejor rendimiento, NetApp recomienda utilizar una máquina virtual dedicada para el análisis antivirus.
- SMB 2,0 debe estar habilitado en el servidor Windows en el que está instalando y ejecutando el conector antivirus de ONTAP.

Antes de empezar

- Descargue el archivo de instalación del conector antivirus de ONTAP desde el sitio de soporte y guárdelo en un directorio del disco duro.
- Compruebe que cumple los requisitos para instalar el conector antivirus de ONTAP.
- Compruebe que dispone de privilegios de administrador para instalar Antivirus Connector.

Pasos

1. Inicie el asistente de instalación de Antivirus Connector ejecutando el archivo de configuración adecuado.
2. Seleccione *Siguiente*. Se abre el cuadro de diálogo Carpeta de destino.
3. Seleccione *Next* para instalar el conector antivirus en la carpeta que aparece en la lista o seleccione *Change* para instalarlo en una carpeta diferente.
4. Se abre el cuadro de diálogo Credenciales de servicio de Windows del conector AV de ONTAP.
5. Ingrese sus credenciales de servicio de Windows o seleccione **Agregar** para seleccionar un usuario. Para un sistema ONTAP, este usuario debe ser un usuario de dominio válido y debe existir en la configuración del pool de análisis de la SVM.
6. Seleccione **Siguiente**. Se abre el cuadro de diálogo Preparado para instalar el programa.
7. Seleccione **Instalar** para comenzar la instalación o seleccione **Atrás** si desea realizar cambios en la configuración.
Se abre un cuadro de estado y traza el progreso de la instalación, seguido del cuadro de diálogo InstallShield Wizard Completed.
8. Active la casilla de comprobación Configure ONTAP LIF si desea continuar con la configuración de la gestión de ONTAP o de las LIF de datos.
Debe configurar al menos una LIF de datos o de gestión de ONTAP para poder utilizar este servidor Vscan.
9. Seleccione la casilla de verificación Mostrar el **registro de Windows Installer** si desea ver los registros de instalación.
10. Seleccione **Finish** para finalizar la instalación y cerrar el asistente InstallShield.
El icono de configuración de LIF de ONTAP* se guarda en el escritorio para configurar las LIF de ONTAP.
11. Agregue una SVM al conector antivirus.

Puede añadir un SVM al conector antivirus añadiendo una LIF de gestión ONTAP, pollada para recuperar la lista de LIF de datos, o bien configurando directamente el LIF o LIF con datos. También debe proporcionar la información de sondeo y las credenciales de la cuenta de administrador de ONTAP si se configuró la LIF de gestión de ONTAP.

- Compruebe que la LIF de gestión o la dirección IP de la SVM estén habilitadas para management-https. Esto no es necesario cuando solo está configurando LIF de datos.
- Compruebe que ha creado una cuenta de usuario para la aplicación HTTP y que ha asignado un rol que tiene (al menos de sólo lectura) acceso al /api/network/ip/interfaces API DE REST. Para obtener más información sobre la creación de un usuario, consulte "[seguridad rol de inicio de sesión crear](#)" y.. "[seguridad de inicio de sesión creado](#)" Páginas manuales de ONTAP.



También puede usar el usuario de dominio como cuenta añadiendo una SVM de túnel de autenticación para una SVM administrativa. Para obtener más información, consulte "[creación de dominio de conexión de seguridad-túnel](#)" El comando man de ONTAP o utilice el /api/security/acccounts y.. /api/security/roles API REST para configurar la cuenta y el rol de administrador.

Pasos

1. Haga clic con el botón derecho del ratón en el icono de configuración de LIF de ONTAP*, que se guardó en su escritorio cuando completó la instalación del conector antivirus y, a continuación, seleccione * Ejecutar como administrador *.
2. En el cuadro de diálogo Configure ONTAP LIF, seleccione el tipo de configuración preferido y, a continuación, realice las siguientes acciones:

| Para crear este tipo de LIF... | Realice estos pasos... |
|--------------------------------|--|
| LIF de datos | <div>a. Establezca la función en los datos.</div> <div>b. Establezca el protocolo de datos en «cifs».</div> <div>c. Establezca la «política de cortafuegos» en «datos».</div> <div>d. Establezca la «política de servicio» en «archivos de datos predeterminados».</div> |
| LIF de gestión | <div>a. Establecer “Rol* en “Datos”</div> <div>b. Establezca el protocolo de datos en ninguno.</div> <div>c. Establezca la política de firewall en «gestión»</div> <div>d. Establezca la política de servicio en la gestión predeterminada.</div> |

Más información acerca de "[Crear una LIF](#)".

Después de crear una LIF, introduzca la dirección IP o la LIF de gestión o la dirección IP de la SVM que desea añadir. También puede introducir la LIF de gestión del clúster. Si especifica la LIF de gestión de clúster, todas las SVM dentro de ese clúster que sirven SMB pueden utilizar el servidor Vscan.



Cuando se requiere autenticación Kerberos para los servidores Vscan, cada LIF de datos de SVM debe tener un nombre DNS único, y debe registrarlo como nombre principal de servidor (SPN) con Windows Active Directory. Cuando no hay un nombre DNS único disponible para cada LIF de datos o registrado como SPN, el servidor Vscan utiliza el mecanismo NT LAN Manager para la autenticación. Si agrega o modifica los nombres DNS y los SPN después de conectar el servidor Vscan, debe reiniciar el servicio Antivirus Connector en el servidor Vscan para aplicar los cambios.

3. Para configurar una LIF de gestión, introduzca la duración del sondeo en segundos. La duración del sondeo es la frecuencia con la que el Antivirus Connector comprueba si hay cambios en las SVM o en la configuración LIF del clúster. El intervalo de sondeo predeterminado es de 60 segundos.
4. Introduzca el nombre de cuenta de administrador de ONTAP y la contraseña para configurar una LIF de gestión.
5. Haga clic en **Test** para comprobar la conectividad y verificar la autenticación. La autenticación solo se verifica para una configuración de LIF de gestión.
6. Haga clic en **Update** para agregar la LIF a la lista de LIF a la que sondear o para conectarse.
7. Haga clic en **Guardar** para guardar la conexión al registro.
8. Haga clic en **Exportar** si desea exportar la lista de conexiones a un archivo de importación o exportación de registro. Esto resulta útil si varios servidores Vscan utilizan el mismo conjunto de LIF de datos o gestión.

Consulte "[Configure la página Conector de antivirus de ONTAP](#)" para opciones de configuración.

Configure el conector antivirus de ONTAP

Configure el conector antivirus de ONTAP para especificar una o varias máquinas virtuales de almacenamiento (SVM) a las que desee conectarse. Para ello, introduzca la LIF de gestión de ONTAP, la información de encuestas y las credenciales de la cuenta de administrador de ONTAP, o solo la LIF de datos. También es posible modificar los detalles de una conexión de SVM o quitarla. De forma predeterminada, el conector antivirus de ONTAP utiliza las API DE REST para recuperar la lista de LIF de datos si está configurada la LIF de gestión de ONTAP.

Modifique los detalles de una conexión de SVM

Para actualizar los detalles de una conexión de máquina virtual de almacenamiento (SVM), que se añadió al conector antivirus, modifique el LIF de gestión de ONTAP y la información de sondeo. No se pueden actualizar los LIF de datos después de que se hayan añadido. Para actualizar las LIF de datos, primero debe eliminarlas y volver a añadirlas con la nueva dirección IP o LIF.

Antes de empezar

Compruebe que ha creado una cuenta de usuario para la aplicación HTTP y que ha asignado un rol que tiene (al menos de sólo lectura) acceso al `/api/network/ip/interfaces` API DE REST.

Para obtener más información sobre la creación de un usuario, consulte "[seguridad rol de inicio de sesión crear](#)" y la "[seguridad de inicio de sesión creado](#)" comandos.

También puede usar el usuario de dominio como cuenta añadiendo una SVM de túnel de autenticación para una SVM administrativa.

Para obtener más información, consulte "[creación de dominio de conexión de seguridad-túnel](#)" Página del comando `man` de ONTAP.

Pasos

1. Haga clic con el botón derecho en el icono de configuración de LIF de ONTAP*, que se guardó en su escritorio cuando completó la instalación del conector antivirus y, a continuación, seleccione * Ejecutar como administrador *. Se abre el cuadro de diálogo Configurar LIF de ONTAP.
2. Seleccione la dirección IP de SVM y, a continuación, haga clic en **Actualizar**.
3. Actualice la información, según sea necesario.
4. Haga clic en **Guardar** para actualizar los detalles de conexión en el registro.
5. Haga clic en **Exportar** si desea exportar la lista de conexiones a una importación de registro o a un archivo de exportación de registro.
Esto resulta útil si varios servidores Vscan utilizan el mismo conjunto de LIF de datos o gestión.

Elimine una conexión SVM del conector antivirus

Si ya no requiere una conexión de SVM, puede quitarla.

Pasos

1. Haga clic con el botón derecho en el icono de configuración de LIF de ONTAP*, que se guardó en su escritorio cuando completó la instalación del conector antivirus y, a continuación, seleccione * Ejecutar como administrador *. Se abre el cuadro de diálogo Configurar LIF de ONTAP.
2. Seleccione una o más direcciones IP de SVM y, a continuación, haga clic en **Eliminar**.
3. Haga clic en **Guardar** para actualizar los detalles de conexión en el registro.
4. Haga clic en **Exportar** si desea exportar la lista de conexiones a un archivo de importación o exportación de registro.
Esto resulta útil si varios servidores Vscan utilizan el mismo conjunto de LIF de datos o gestión.

Solucionar problemas

Antes de empezar

Al crear valores de registro en este procedimiento, utilice el panel lateral derecho.

Puede activar o desactivar los registros de Antivirus Connector con fines de diagnóstico. Por defecto, estos logs están desactivados. Para mejorar el rendimiento, debe mantener los registros del conector antivirus desactivados y solo habilitarlos para eventos críticos.

Pasos

1. Seleccione **Inicio**, escriba "regedit" en el cuadro de búsqueda y, a continuación, seleccione `regedit.exe` En la lista Programas.
2. En **Editor del Registro**, busque la siguiente subclave para el Conector de Antivirus de ONTAP:
`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. Cree valores de registro proporcionando el tipo, el nombre y los valores mostrados en la siguiente tabla:

| Tipo | Nombre | Valores |
|--------|-----------|---------------|
| Cadena | Tracepath | c:\avshim.log |

Este valor de registro puede ser cualquier otra ruta válida.

4. Cree otro valor de registro proporcionando el tipo, el nombre, los valores y la información de registro que se muestra en la siguiente tabla:

| Tipo | Nombre | Registro crítico | Registro intermedio | Registro detallado |
|-------|-------------------|------------------|---------------------|--------------------|
| DWORD | Nivel de tracción | 1 | 2 o 3 | 4 |

Esto activa los registros de Antivirus Connector que se guardan en el valor de ruta proporcionado en TracePath en el paso 3.

5. Desactive los registros de Antivirus Connector eliminando los valores de registro que creó en los pasos 3 y 4.
6. Crear otro valor de registro de tipo "MULTI_SZ" con el nombre "LogRotation" (sin comillas). En LogRotation, Proporcione "LogFileSize:1" como una entrada para el tamaño de rotación (donde 1 representa 1MB) y en la siguiente línea, proporcione "logFileCount:5" como un entrada para el límite de rotación (5 es el límite).



Estos valores son opcionales. Si no se proporcionan, los valores predeterminados de los archivos 20MB y 10 se utilizan para el tamaño de rotación y el límite de rotación respectivamente. Los valores enteros proporcionados no proporcionan valores decimales ni de fracción. Si proporciona valores superiores a los predeterminados, se utilizan los valores predeterminados en su lugar.

7. Para desactivar la rotación de log configurada por el usuario, elimine los valores de registro que creó en el Paso 6.

Banner personalizable

Un banner personalizado le permite colocar una declaración legalmente vinculante y una exención de responsabilidad de acceso al sistema en la ventana *Configurar ONTAP LIF API*.

Paso

1. Modifique el banner predeterminado actualizando el contenido del `banner.txt` en el directorio de instalación y, a continuación, guarde los cambios.
Debe volver a abrir la ventana *Configure ONTAP LIF API* para ver los cambios que se reflejan en el banner.

Active el modo Ordenanza ampliada (EO)

Puede activar y desactivar el modo de ordenanza extendida (EO) para un funcionamiento seguro.

Pasos

1. Seleccione **Inicio**, escriba "regedit" en el cuadro de búsqueda y, a continuación, seleccione `regedit.exe` En la lista Programas.
2. En el **Editor del Registro**, busque la siguiente subclave para el conector antivirus de ONTAP:
`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. En el panel de la derecha, cree un nuevo valor de registro del tipo "DWORD" con el nombre "EO_Mode" (sin comillas) y el valor "1" (sin comillas) para habilitar el modo EO o el valor "0" (sin comillas) para desactivar el modo EO.



De forma predeterminada, si el `EO_Mode` La entrada del registro está ausente, el modo EO está desactivado. Cuando habilita el modo EO, debe configurar tanto el servidor de syslog externo como la autenticación de certificados mutuos.

Configure el servidor de syslog externo

Antes de empezar

Tenga en cuenta que cuando cree valores de registro en este procedimiento, utilice el panel lateral derecho.

Pasos

1. Seleccione **Inicio**, escriba “regedit” en el cuadro de búsqueda y, a continuación, seleccione `regedit.exe` En la lista Programas.
2. En **Editor del Registro**, cree la siguiente subclave para el conector antivirus de ONTAP para la configuración syslog:
`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0\syslog`
3. Cree un valor de registro proporcionando el tipo, el nombre y el valor como se muestra en la siguiente tabla:

| Tipo | Nombre | Valor |
|-------|----------------|-------|
| DWORD | syslog_enabled | 1 o 0 |

Tenga en cuenta que un valor «1» activa el syslog y un valor «0» lo desactiva.

4. Cree otro valor de registro proporcionando la información que se muestra en la siguiente tabla:

| Tipo | Nombre |
|--------|-------------|
| REG_SZ | Host_syslog |

Proporcione la dirección IP o el nombre de dominio del host de syslog para el campo Value.

5. Cree otro valor de registro proporcionando la información que se muestra en la siguiente tabla:

| Tipo | Nombre |
|--------|---------------|
| REG_SZ | Puerto_syslog |

Proporcione el número de puerto en el que se ejecuta el servidor de syslog en el campo Value.

6. Cree otro valor de registro proporcionando la información que se muestra en la siguiente tabla:

| Tipo | Nombre |
|--------|------------------|
| REG_SZ | Protocolo_syslog |

Introduzca el protocolo que se está utilizando en el servidor de syslog, «tcp» o «udp», en el campo Valor.

7. Cree otro valor de registro proporcionando la información que se muestra en la siguiente tabla:

| Tipo | Nombre | CRIT_LOG | AVISO_LOG | INFORMACIÓN_LOG | LOG_DEBUG |
|-------|--------------|----------|-----------|-----------------|-----------|
| DWORD | Nivel_syslog | 2 | 5 | 6 | 7 |

8. Cree otro valor de registro proporcionando la información que se muestra en la siguiente tabla:

| Tipo | Nombre | Valor |
|-------|------------|-------|
| DWORD | syslog_tls | 1 o 0 |

Tenga en cuenta que un valor «1» habilita syslog con Transport Layer Security (TLS) y un valor «0» deshabilita syslog con TLS.

Asegúrese de que un servidor syslog externo configurado se ejecute sin problemas

- Si la clave está ausente o tiene un valor nulo:
 - El protocolo por defecto es «tcp».
 - El puerto de forma predeterminada es «514» para «tcp/udp» normal y, de forma predeterminada, «6514» para TLS.
 - El nivel syslog se establece de forma predeterminada en 5 (LOG_NOTE).
- Para confirmar que syslog está habilitado, se debe verificar que el `syslog_enabled` el valor es «1». Cuando la `syslog_enabled` El valor es 1. Debe poder iniciar sesión en el servidor remoto configurado tanto si el modo EO está activado como si no.
- Si el modo EO está establecido en «1» y cambia el `syslog_enabled` valor de «1» a «0», se aplica lo siguiente:
 - No es posible iniciar el servicio si syslog no está habilitado en modo EO.
 - Si el sistema se está ejecutando en un estado estable, aparece una advertencia que indica que syslog no se puede desactivar en el modo EO y syslog se establece forzosamente en «1», que puede ver en el registro. Si esto ocurre, primero debe deshabilitar el modo EO y, a continuación, desactivar syslog.
- Si el servidor syslog no puede ejecutarse correctamente cuando el modo EO y syslog están habilitados, el servicio se detiene. Esto puede ocurrir por uno de los siguientes motivos:
 - Se configuró un `syslog_host` no válido o no.
 - Se ha configurado un protocolo no válido aparte de UDP o TCP.
 - Un número de puerto no es válido.
- Para una configuración TCP o TLS sobre TCP, si el servidor no está escuchando en el puerto IP, la conexión falla y el servicio se cierra.

Configure la autenticación de certificado mutuo X.509

La autenticación mutua basada en certificado X.509 es posible para la comunicación de capa de sockets seguros (SSL) entre el conector antivirus y ONTAP en la ruta de administración. Si el modo EO está activado y no se encuentra el certificado, el conector AV finaliza. Realice el siguiente procedimiento en el conector antivirus:

Pasos

1. El conector antivirus busca el certificado de cliente del conector antivirus y el certificado de la entidad de certificación (CA) para el servidor NetApp en la ruta del directorio desde donde el conector antivirus ejecuta el directorio de instalación. Copie los certificados en esta ruta de acceso de directorio fija.
2. Incruste el certificado de cliente y su clave privada en el formato PKCS12 y asígnele el nombre "AV_CLIENT.P12".
3. Asegúrese de que el certificado de CA (junto con cualquier autoridad de firma intermedia hasta la CA raíz) utilizado para firmar el certificado para el servidor NetApp tenga el formato de correo mejorado de privacidad (PEM) y el nombre «ontap_ca.pem». Colóquelo en el directorio de instalación de Antivirus Connector. En el sistema NetApp ONTAP, instale el certificado de CA (junto con cualquier autoridad de firma intermedia hasta la CA raíz) que se utiliza para firmar el certificado de cliente para el conector antivirus en ONTAP como certificado de tipo client-ca.

Configurar grupos de escáneres

Descripción general de la configuración de los pools de escáner

Un grupo de escáneres define los servidores Vscan y los usuarios con privilegios que pueden conectarse a las SVM. Una directiva de escáner determina si un grupo de escáneres está activo.



Si utiliza una política de exportación en un servidor SMB, debe agregar cada servidor Vscan a la política de exportación.

Cree un pool de escáneres en un único clúster

Un grupo de escáneres define los servidores Vscan y los usuarios con privilegios que pueden conectarse a las SVM. Puede crear un pool de escáner para una SVM individual o para todas las SVM de un clúster.

Lo que necesitará

- Los SVM y los servidores Vscan deben estar en el mismo dominio o en dominios de confianza.
- Para los pools de análisis definidos para una SVM individual, debe haber configurado el conector antivirus de ONTAP con la LIF de gestión de SVM o la LIF de datos de SVM.
- Para los pools de análisis definidos para todas las SVM de un clúster, debe haber configurado el conector antivirus de ONTAP con la LIF de gestión de clúster.
- La lista de usuarios con privilegios debe incluir la cuenta de usuario de dominio que el servidor Vscan utiliza para conectarse a la SVM.
- Una vez configurado el grupo de escáneres, compruebe el estado de conexión a los servidores.

Pasos

1. Crear un grupo de escáneres:

```
vserver vscan scanner-pool create -vserver data_SVM|cluster_admin_SVM -scanner
-pool scanner_pool -hostnames Vscan_server_hostnames -privileged-users
privileged_users
```

- Especifique una SVM de datos para un pool definido para una SVM individual y especifique una SVM de administrador de clúster para un pool definido para todas las SVM de un clúster.

- Especifique una dirección IP o FQDN para cada nombre de host del servidor Vscan.
- Especifique el dominio y el nombre de usuario de cada usuario con privilegios.
Para obtener una lista completa de las opciones, consulte la página de manual del comando.

El siguiente comando crea un grupo de escáneres denominado SP en la vs1 SVM:

```
cluster1::> vserver vscan scanner-pool create -vserver vs1 -scanner-pool
SP -hostnames 1.1.1.1,vmwin204-27.fsct.nb -privileged-users
cifs\u1,cifs\u2
```

2. Compruebe que se ha creado el grupo de escáneres:

```
vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner
-pool scanner_pool
```

Para obtener una lista completa de las opciones, consulte la página de manual del comando.

El siguiente comando muestra los detalles de SP grupo de escáneres:

```
cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool
SP

Vserver: vs1
Scanner Pool: SP
Applied Policy: idle
Current Status: off
Cluster on Which Policy Is Applied: -
Scanner Pool Config Owner: vserver
List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
27.fsct.nb
List of Privileged Users: cifs\u1, cifs\u2
```

También puede utilizar el `vserver vscan scanner-pool show` Comando para ver todos los pools de análisis de una SVM. Para obtener una sintaxis de comando completa, consulte la página de manual del comando.

Crear grupos de escáneres en configuraciones de MetroCluster

Debe crear pools de análisis primarios y secundarios en cada clúster en una configuración de MetroCluster que corresponda a las SVM primarias y secundarias en el clúster.

Lo que necesitará

- Los SVM y los servidores Vscan deben estar en el mismo dominio o en dominios de confianza.

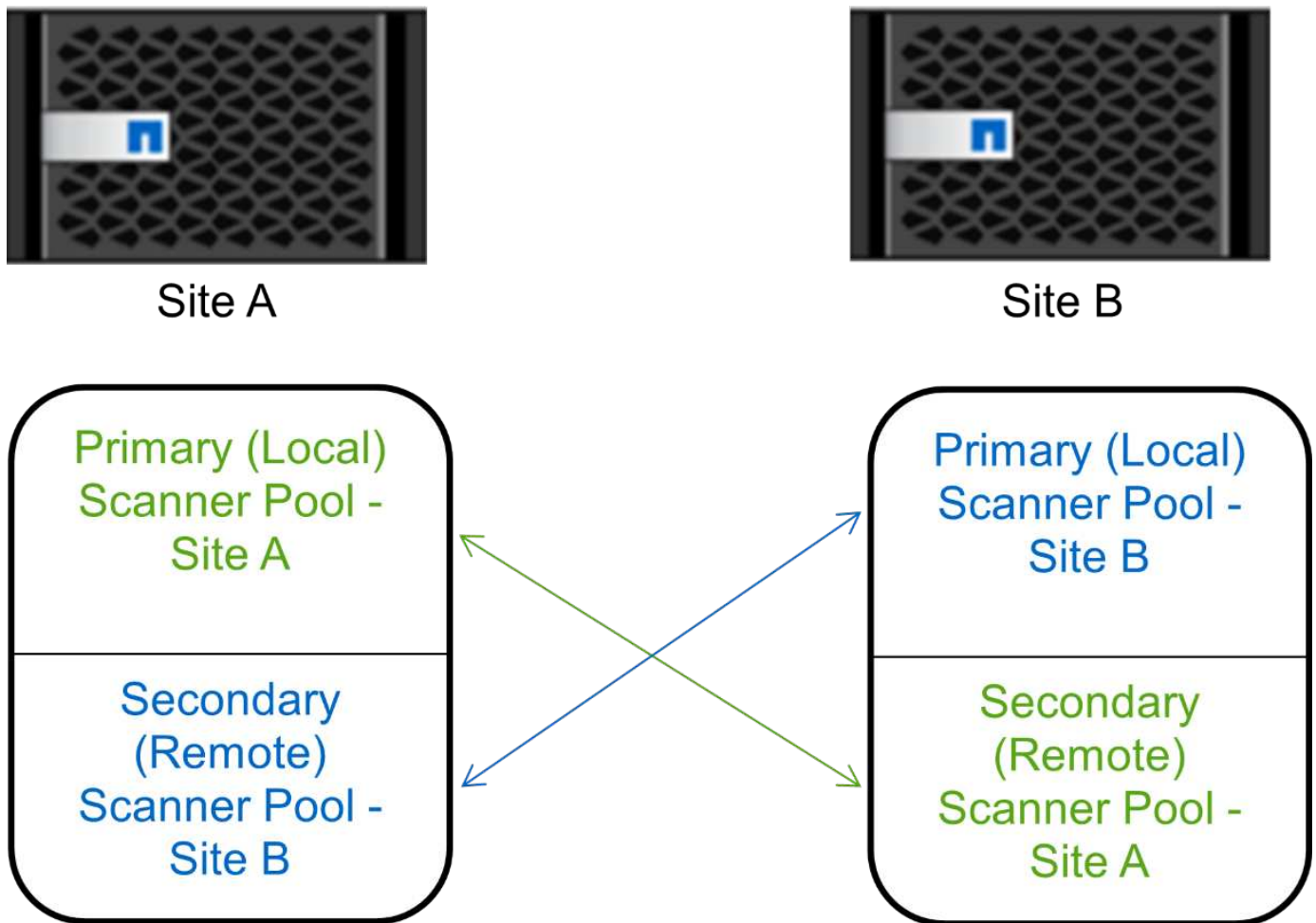
- Para los pools de análisis definidos para una SVM individual, debe haber configurado el conector antivirus de ONTAP con la LIF de gestión de SVM o la LIF de datos de SVM.
- Para los pools de análisis definidos para todas las SVM de un clúster, debe haber configurado el conector antivirus de ONTAP con la LIF de gestión de clúster.
- La lista de usuarios con privilegios debe incluir la cuenta de usuario de dominio que el servidor Vscan utiliza para conectarse a la SVM.
- Una vez configurado el grupo de escáneres, compruebe el estado de conexión a los servidores.

Acerca de esta tarea

Las configuraciones de MetroCluster protegen los datos mediante la implementación de dos clústeres reflejados físicamente independientes. Cada clúster replica de forma síncrona los datos y la configuración de SVM del otro. Una SVM primaria en el clúster local proporciona datos cuando el clúster está en línea. Una SVM secundaria en el clúster local proporciona datos cuando el clúster remoto está sin conexión.

Esto significa que debe crear pools de análisis primarios y secundarios en cada clúster en una configuración de MetroCluster; el pool secundario se activa cuando el clúster comienza a suministrar datos a partir de la SVM secundaria. Para la recuperación ante desastres, la configuración es similar a MetroCluster.

En esta figura se muestra una configuración MetroCluster/DR típica.



Pasos

1. Crear un grupo de escáneres:

```
vserver vscan scanner-pool create -vserver data_SVM|cluster_admin_SVM -scanner
```

```
-pool scanner_pool -hostnames Vscan_server_hostnames -privileged-users  
privileged_users
```

- Especifique una SVM de datos para un pool definido para una SVM individual y especifique una SVM de administrador de clúster para un pool definido para todas las SVM de un clúster.
- Especifique una dirección IP o FQDN para cada nombre de host del servidor Vscan.
- Especifique el dominio y el nombre de usuario de cada usuario con privilegios.



Debe crear todos los pools de escáner desde el clúster que contiene la SVM principal.

Para obtener una lista completa de las opciones, consulte la página de manual del comando.

Los siguientes comandos crean pools de análisis principales y secundarios en cada clúster en una configuración de MetroCluster:

```
cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -  
scanner-pool pool1_for_site1 -hostnames scan1 -privileged-users cifs  
\u1,cifs\u2
```

```
cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -  
scanner-pool pool1_for_site2 -hostnames scan1 -privileged-users cifs  
\u1,cifs\u2
```

```
cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -  
scanner-pool pool2_for_site1 -hostnames scan2 -privileged-users cifs  
\u1,cifs\u2
```

```
cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -  
scanner-pool pool2_for_site2 -hostnames scan2 -privileged-users cifs  
\u1,cifs\u2
```

2. Compruebe que se han creado los grupos de escáneres:

```
vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner  
-pool scanner_pool
```

Para obtener una lista completa de las opciones, consulte la página de manual del comando.

El siguiente comando muestra los detalles del grupo de escáneres pool1:

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1
```

```

Vserver: cifssvm1
Scanner Pool: pool1_for_site1
Applied Policy: idle
Current Status: off
Cluster on Which Policy Is Applied: -
Scanner Pool Config Owner: vserver
List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
List of Privileged Users: cifs\u1,cifs\u2
```

También puede utilizar el `vserver vscan scanner-pool show` Comando para ver todos los pools de análisis de una SVM. Para obtener una sintaxis de comando completa, consulte la página de manual del comando.

Aplicar una política de escáner en un único clúster

Una directiva de escáner determina si un grupo de escáneres está activo. Debe activar un grupo de escáneres para que los servidores Vscan que define puedan conectarse a una SVM.

Acerca de esta tarea

- Sólo puede aplicar una directiva de escáner a un grupo de escáneres.
- Si ha creado un pool de escáner para todas las SVM de un clúster, debe aplicar una política de escáner en cada SVM de forma individual.

Pasos

1. Aplicar una política de escáner:

```
vserver vscan scanner-pool apply-policy -vserver data_SVM -scanner-pool
scanner_pool -scanner-policy primary|secondary|idle -cluster
cluster_to_apply_policy_on
```

Una directiva de escáner puede tener uno de los siguientes valores:

- `Primary` especifica que el grupo de escáneres está activo.
- `Secondary` Especifica que el grupo de escáneres está activo sólo si no hay ninguno de los servidores Vscan del grupo de escáneres primario conectado.
- `Idle` especifica que el grupo de escáneres está inactivo.

En el siguiente ejemplo se muestra el nombre del grupo de escáneres SP en la vs1 SVM está activa:

```
cluster1::> vserver vscan scanner-pool apply-policy -vserver vs1
-scanner-pool SP -scanner-policy primary
```

2. Compruebe que el grupo de escáneres está activo:

```
vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner
-pool scanner_pool
```

Para obtener una lista completa de las opciones, consulte la página de manual del comando.

El siguiente comando muestra los detalles de SP grupo de escáneres:

```
cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool
SP

Vserver: vs1
Scanner Pool: SP
Applied Policy: primary
Current Status: on
Cluster on Which Policy Is Applied: cluster1
Scanner Pool Config Owner: vserver
List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
27.fsct.nb
List of Privileged Users: cifs\u1, cifs\u2
```

Puede utilizar el `vserver vscan scanner-pool show-active` Comando para ver los pools de análisis activos en una SVM. Para obtener la sintaxis completa del comando, consulte la página de manual del comando.

Aplicar directivas de escáner en las configuraciones de MetroCluster

Una directiva de escáner determina si un grupo de escáneres está activo. Debe aplicar una política de escáner a los pools de análisis principal y secundario de cada clúster de una configuración de MetroCluster.

Acerca de esta tarea

- Sólo puede aplicar una directiva de escáner a un grupo de escáneres.
- Si ha creado un pool de escáner para todas las SVM de un clúster, debe aplicar una política de escáner en cada SVM de forma individual.
- Para la recuperación ante desastres y las configuraciones de MetroCluster, debe aplicar una directiva de escáner a cada grupo de escáneres del clúster local y del clúster remoto.
- En la política que cree para el clúster local, debe especificar el clúster local en el `cluster` parámetro. En la política que crea para el clúster remoto, debe especificar el clúster remoto en la `cluster` parámetro. A continuación, el clúster remoto puede hacerse cargo de las operaciones de detección de virus en caso de

desastre.

Pasos

1. Aplicar una política de escáner:

```
vserver vscan scanner-pool apply-policy -vserver data_SVM -scanner-pool  
scanner_pool -scanner-policy primary|secondary|idle -cluster  
cluster_to_apply_policy_on
```

Una directiva de escáner puede tener uno de los siguientes valores:

- ° Primary especifica que el grupo de escáneres está activo.
- ° Secondary Especifica que el grupo de escáneres está activo sólo si no hay ninguno de los servidores Vscan del grupo de escáneres primario conectado.
- ° Idle especifica que el grupo de escáneres está inactivo.



Debe aplicar todas las políticas de análisis del clúster que contiene la SVM principal.

Los siguientes comandos aplican políticas de análisis a los pools de análisis principal y secundario de cada clúster en una configuración de MetroCluster:

```
cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1  
-scanner-pool pool1_for_site1 -scanner-policy primary -cluster cluster1  
  
cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1  
-scanner-pool pool2_for_site1 -scanner-policy secondary -cluster  
cluster1  
  
cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1  
-scanner-pool pool1_for_site2 -scanner-policy primary -cluster cluster2  
  
cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1  
-scanner-pool pool2_for_site2 -scanner-policy secondary -cluster  
cluster2
```

2. Compruebe que el grupo de escáneres está activo:

```
vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner  
-pool scanner_pool
```

Para obtener una lista completa de las opciones, consulte la página de manual del comando.

El siguiente comando muestra los detalles del grupo de escáneres pool1:

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1
```

```

Vserver: cifssvm1
Scanner Pool: pool1_for_site1
Applied Policy: primary
Current Status: on
Cluster on Which Policy Is Applied: cluster1
Scanner Pool Config Owner: vserver
List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
List of Privileged Users: cifs\u1,cifs\u2
```

Puede utilizar el `vserver vscan scanner-pool show-active` Comando para ver los pools de análisis activos en una SVM. Para obtener una sintaxis de comando completa, consulte la página de manual del comando.

Comandos para administrar grupos de escáneres

Puede modificar y eliminar grupos de escáneres y administrar usuarios con privilegios y servidores Vscan para un grupo de escáneres. También puede ver información resumida sobre el conjunto de escáneres.

| Si desea... | Introduzca el siguiente comando... |
|--|---|
| Modificar un grupo de escáneres | <code>vserver vscan scanner-pool modify</code> |
| Eliminar un grupo de escáneres | <code>vserver vscan scanner-pool delete</code> |
| Agregar usuarios con privilegios a un grupo de escáneres | <code>vserver vscan scanner-pool privileged-users add</code> |
| Eliminar usuarios con privilegios de un grupo de escáneres | <code>vserver vscan scanner-pool privileged-users remove</code> |
| Agregue servidores Vscan a un grupo de escáneres | <code>vserver vscan scanner-pool servers add</code> |
| Eliminar servidores Vscan de un grupo de escáneres | <code>vserver vscan scanner-pool servers remove</code> |
| Ver resumen y detalles de un grupo de escáneres | <code>vserver vscan scanner-pool show</code> |
| Ver usuarios con privilegios para un grupo de escáneres | <code>vserver vscan scanner-pool privileged-users show</code> |

| | |
|---|--|
| Vea los servidores Vscan de todos los grupos de escáneres | <code>vserver vscan scanner-pool servers show</code> |
|---|--|

Para obtener más información sobre estos comandos, consulte las páginas man.

Configurar el análisis en tiempo real

Crear una política de acceso

Una directiva en tiempo real define el ámbito de un análisis en tiempo real. Puede crear una política de acceso para una SVM individual o para todas las SVM de un clúster. Si creó una política de acceso para todas las SVM de un clúster, debe habilitar la política en cada SVM de forma individual.

Acerca de esta tarea

- Puede especificar el tamaño máximo de archivo que se va a escanear, las extensiones de archivo y las rutas que se van a incluir en el escaneo, y las extensiones de archivo y las rutas de acceso que se van a excluir del escaneo.
- Puede ajustar la `scan-mandatory` Opción de desactivar para especificar que se permite el acceso al archivo cuando no hay servidores Vscan disponibles para el análisis de virus.
- De forma predeterminada, ONTAP crea una política de acceso llamada «default_cifs» y la habilita para todas las SVM de un clúster.
- Cualquier archivo que califique para la exclusión de exploración basada en `paths-to-exclude`, `file-ext-to-exclude`, o `max-file-size` los parámetros no se consideran para la adquisición, incluso si el `scan-mandatory` la opción está activada. (Compruebe esto "resolución de problemas" sección para los problemas de conectividad relacionados con el `scan-mandatory` opcional.)
- De forma predeterminada, solo se analizan los volúmenes de lectura/escritura. Puede especificar filtros que permitan el análisis de volúmenes de sólo lectura o que restrinjan el análisis de archivos abiertos con acceso de ejecución.
- La detección de virus no se realiza en un recurso compartido de SMB para el cual el parámetro continuamente disponible se establece en Yes.
- Consulte "Arquitectura de antivirus" Sección para obtener detalles sobre *Vscan file-operations profile*.
- Puede crear un máximo de diez (10) políticas de acceso por SVM. Sin embargo, solo puede habilitar una política de acceso a la vez.
 - Puede excluir un máximo de cien (100) rutas y extensiones de archivos del análisis de virus en una política de acceso.
- Algunas recomendaciones de exclusión de archivos:
 - Considere la posibilidad de excluir archivos grandes (se puede especificar el tamaño de archivo) del análisis de virus porque pueden provocar una respuesta lenta o tiempos de espera de solicitudes de análisis para los usuarios de CIFS. El tamaño de archivo predeterminado para la exclusión es 2GB.
 - Considere la posibilidad de excluir extensiones de archivo como `.vhd` y `.tmp` debido a que los archivos con estas extensiones pueden no ser adecuados para escanear.
 - Considere la posibilidad de excluir las rutas de archivos, como el directorio en cuarentena o las rutas en las que sólo se almacenan los discos duros virtuales o las bases de datos.
 - Verifique que todas las exclusiones están especificadas en la misma política, porque sólo se puede

activar una política a la vez. NetApp recomienda tener el mismo conjunto de exclusiones especificado en el motor antivirus.

- Se necesita una política de acceso para un [análisis bajo demanda](#). Para evitar la búsqueda en acceso, debe establecer `-scan-files-with-no-ext` hasta `false` y. `-file-ext-to-exclude` a `*` para excluir todas las extensiones.

Pasos

1. Cree una política de acceso:

```
vserver vscan on-access-policy create -vserver data_SVM|cluster_admin_SVM
-policy-name policy_name -protocol CIFS -max-file-size
max_size_of_files_to_scan -filters [scan-ro-volume,][scan-execute-access]
-file-ext-to-include extensions_of_files_to_include -file-ext-to-exclude
extensions_of_files_to_exclude -scan-files-with-no-ext true|false -paths-to
-exclude paths_of_files_to_exclude -scan-mandatory on|off
```

- Especifique una SVM de datos para una política definida para una SVM individual, una SVM de administrador de clúster para una política definida para todas las SVM de un clúster.
- La `-file-ext-to-exclude` el ajuste anula la `-file-ext-to-include` ajuste.
- Configurado `-scan-files-with-no-ext true` para analizar archivos sin extensiones.
El siguiente comando crea una política de acceso llamada `Policy1` en la `vs1` SVM:

```
cluster1::> vserver vscan on-access-policy create -vserver vs1 -policy
-name Policy1 -protocol CIFS -filters scan-ro-volume -max-file-size 3GB
-file-ext-to-include "mp*", "tx*" -file-ext-to-exclude "mp3", "txt" -scan
-files-with-no-ext false -paths-to-exclude "\vol\ a b\"," \vol\ a, b\"
```

2. Compruebe que se ha creado la política de acceso: `vserver vscan on-access-policy show -instance data_SVM|cluster_admin_SVM -policy-name name`

Para obtener una lista completa de las opciones, consulte la página de manual del comando.

El siguiente comando muestra los detalles de `Policy1` política:


```
cluster1::> vserver vscan on-access-policy show -instance vs1 -policy
-name Policy1
```

```
                Vserver: vs1
                Policy: Policy1
                Policy Status: off
                Policy Config Owner: vserver
                File-Access Protocol: CIFS
                Filters: scan-ro-volume
                Mandatory Scan: on
Max File Size Allowed for Scanning: 3GB
                File Paths Not to Scan: \vol\ a b\, \vol\ a,b\
                File Extensions Not to Scan: mp3, txt
                File Extensions to Scan: mp*, tx*
                Scan Files with No Extension: false
```

Activar una política de acceso

Una directiva en tiempo real define el ámbito de un análisis en tiempo real. Debe habilitar una política de acceso en una SVM antes de que se puedan analizar los archivos.

Si creó una política de acceso para todas las SVM de un clúster, debe habilitar la política en cada SVM de forma individual. Solo puede habilitar una política de acceso en una SVM a la vez.

Pasos

1. Activar una política de acceso:

```
vserver vscan on-access-policy enable -vserver data_SVM -policy-name
policy_name
```

El siguiente comando habilita una política de acceso llamada `Policy1` en la `vs1` SVM:

```
cluster1::> vserver vscan on-access-policy enable -vserver vs1 -policy
-name Policy1
```

2. Compruebe que la política de acceso está activada:

```
vserver vscan on-access-policy show -instance data_SVM -policy-name
policy_name
```

Para obtener una lista completa de las opciones, consulte la página de manual del comando.

El siguiente comando muestra los detalles de `Policy1` política de acceso:

```
cluster1::> vserver vscan on-access-policy show -instance vs1 -policy
-name Policy1
```

```
                Vserver: vs1
                Policy: Policy1
                Policy Status: on
                Policy Config Owner: vserver
                File-Access Protocol: CIFS
                Filters: scan-ro-volume
                Mandatory Scan: on
Max File Size Allowed for Scanning: 3GB
                File Paths Not to Scan: \vol\ a b\, \vol\ a,b\
                File Extensions Not to Scan: mp3, txt
                File Extensions to Scan: mp*, tx*
                Scan Files with No Extension: false
```

Modifique el perfil de operaciones de archivos Vscan para un recurso compartido de SMB

El perfil *Vscan file-operations* para un recurso compartido SMB define las operaciones en el recurso compartido que pueden activar el análisis. De manera predeterminada, el parámetro se establece en `standard`. Es posible ajustar el parámetro según sea necesario al crear o modificar un recurso compartido de SMB.

Consulte ["Arquitectura de antivirus"](#) Sección para obtener detalles sobre *Vscan file-operations profile*.



La detección de virus no se realiza en un recurso compartido de SMB que tenga el `continuously-available` parámetro establecido en `Yes`.

Paso

1. Modifique el valor del perfil de operaciones de archivo Vscan para un recurso compartido de SMB:

```
vserver cifs share modify -vserver data_SVM -share-name share -path share_path
-vscan-fileop-profile no-scan|standard|strict|writes-only
```

Para obtener una lista completa de las opciones, consulte la página de manual del comando.

El siguiente comando cambia el perfil de operaciones del archivo Vscan para un recurso compartido de SMB a `strict`:

```
cluster1::> vserver cifs share modify -vserver vs1 -share-name
SALES_SHARE -path /sales -vscan-fileop-profile strict
```

Comandos para gestionar políticas en acceso

Puede modificar, deshabilitar o eliminar una política de acceso. Puede ver un resumen y

detalles de la política.

| Si desea... | Introduzca el siguiente comando... |
|---|--|
| Crear una política de acceso | <code>vserver vscan on-access-policy create</code> |
| Modifique una política de acceso | <code>vserver vscan on-access-policy modify</code> |
| Activar una política de acceso | <code>vserver vscan on-access-policy enable</code> |
| Deshabilitar una política de acceso | <code>vserver vscan on-access-policy disable</code> |
| Eliminar una política de acceso | <code>vserver vscan on-access-policy delete</code> |
| Consulte el resumen y los detalles de una política de acceso | <code>vserver vscan on-access-policy show</code> |
| Agregar a la lista de rutas de acceso que se van a excluir | <code>vserver vscan on-access-policy paths-to-exclude add</code> |
| Eliminar de la lista de rutas de acceso que se van a excluir | <code>vserver vscan on-access-policy paths-to-exclude remove</code> |
| Consulte la lista de rutas de acceso que desea excluir | <code>vserver vscan on-access-policy paths-to-exclude show</code> |
| Agregar a la lista de extensiones de archivo que se van a excluir | <code>vserver vscan on-access-policy file-ext-to-exclude add</code> |
| Eliminar de la lista de extensiones de archivo que se van a excluir | <code>vserver vscan on-access-policy file-ext-to-exclude remove</code> |
| Consulte la lista de extensiones de archivo que se van a excluir | <code>vserver vscan on-access-policy file-ext-to-exclude show</code> |
| Agregar a la lista de extensiones de archivo que se incluirán | <code>vserver vscan on-access-policy file-ext-to-include add</code> |
| Eliminar de la lista de extensiones de archivo que se van a incluir | <code>vserver vscan on-access-policy file-ext-to-include remove</code> |
| Consulte la lista de extensiones de archivo que se incluirán | <code>vserver vscan on-access-policy file-ext-to-include show</code> |

Para obtener más información sobre estos comandos, consulte las páginas man.

Configurar el análisis bajo demanda

Configurar la descripción general del análisis bajo demanda

Puede utilizar el análisis bajo demanda para comprobar los archivos en busca de virus de forma inmediata o programada.

Puede que desee ejecutar análisis sólo en horas de menor actividad, por ejemplo, o puede que desee analizar archivos muy grandes que se excluyeron de un análisis en tiempo real. Puede utilizar una programación cron para especificar cuándo se ejecuta la tarea.

Acerca de este tema

- Puede asignar una programación al crear una tarea.
- Solo se puede programar una tarea a la vez en un SVM.
- El análisis bajo demanda no admite el análisis de enlaces simbólicos o archivos de flujo.



El análisis bajo demanda no admite el análisis de enlaces simbólicos o archivos de flujo.



Para crear una tarea bajo demanda, debe haber al menos una política de acceso en curso activada. Puede ser la política predeterminada o un usuario creado en la política de acceso.

Crear una tarea bajo demanda

Una tarea a petición define el alcance de la exploración de virus a petición. Puede especificar el tamaño máximo de los archivos que se van a analizar, las extensiones y rutas de acceso de los archivos que se van a incluir en el análisis, así como las extensiones y rutas de acceso de los archivos que se van a excluir del análisis. Los archivos de los subdirectorios se analizan de forma predeterminada.

Acerca de esta tarea

- Puede haber un máximo de diez (10) tareas bajo demanda para cada SVM, pero solo una puede estar activa.
- Una tarea a petición crea un informe, que contiene información sobre las estadísticas relacionadas con las exploraciones. Se puede acceder a este informe con un comando o descargando el archivo de informe creado por la tarea en la ubicación definida.

Antes de empezar

- Debe tener [se ha creado una política de acceso](#). La política puede ser una predeterminada o creada por el usuario. Sin la política de acceso, no puede activar el análisis.

Pasos

1. Crear una tarea bajo demanda:

```
vserver vscan on-demand-task create -vserver data_SVM -task-name task_name
-scan-paths paths_of_files_to_scan -report-directory report_directory_path
-report-expiry-time expiration_time_for_report -schedule cron_schedule -max
-file-size max_size_of_files_to_scan -paths-to-exclude paths -file-ext-to
-exclude file_extensions -file-ext-to-include file_extensions -scan-files-with
-no-ext true|false -directory-recursion true|false
```

- La `-file-ext-to-exclude` el ajuste anula la `-file-ext-to-include` ajuste.
- Configurado `-scan-files-with-no-ext true` para analizar archivos sin extensiones.

Para obtener una lista completa de opciones, consulte ["referencia de comandos"](#).

El siguiente comando crea una tarea bajo demanda denominada `Task1` En el `'VS1'SVM`:

```
cluster1::> vserver vscan on-demand-task create -vserver vs1 -task-name
Task1 -scan-paths "/vol1/", "/vol2/cifs/" -report-directory "/report"
-schedule daily -max-file-size 5GB -paths-to-exclude "/vol1/cold-files/"
-file-ext-to-include "vmdk?", "mp*" -file-ext-to-exclude "mp3", "mp4"
-scan-files-with-no-ext false
[Job 126]: Vscan On-Demand job is queued. Use the "job show -id 126"
command to view the status.
```

+



Puede utilizar el `job show` comando para ver el estado del trabajo. Puede utilizar el `job pause` y.. `job resume` comandos para pausar y reiniciar el trabajo o el `job stop` comando para finalizar el trabajo.

2. Compruebe que la tarea bajo demanda se ha creado:

```
vserver vscan on-demand-task show -instance data_SVM -task-name task_name
```

Para obtener una lista completa de las opciones, consulte la página de manual del comando.

El siguiente comando muestra los detalles de `Task1` tarea:

```
cluster1::> vserver vscan on-demand-task show -instance vs1 -task-name Task1
```

```
                Vserver: vs1
                Task Name: Task1
                List of Scan Paths: /vol1/, /vol2/cifs/
                Report Directory Path: /report
                Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
                File Paths Not to Scan: /vol1/cold-files/
                File Extensions Not to Scan: mp3, mp4
                File Extensions to Scan: vmdk?, mp*
Scan Files with No Extension: false
                Request Service Timeout: 5m
                Cross Junction: true
                Directory Recursion: true
                Scan Priority: low
                Report Log Level: info
                Expiration Time for Report: -
```

Después de terminar

Debe habilitar el análisis en la SVM antes de que se ejecute la tarea programada.

Programar una tarea bajo demanda

Puede crear una tarea sin asignar una programación y utilizar el `vserver vscan on-demand-task schedule` comando para asignar una programación o agregar una programación al crear la tarea.

Acerca de esta tarea

La programación asignada con `vserver vscan on-demand-task schedule` el comando anula una programación que ya se ha asignado con el `vserver vscan on-demand-task create` comando.

Pasos

1. Programar una tarea bajo demanda:

```
vserver vscan on-demand-task schedule -vserver data_SVM -task-name task_name
-schedule cron_schedule
```

El siguiente comando programa una tarea en tiempo de acceso denominada Task2 en la vs2 SVM:

```
cluster1::> vserver vscan on-demand-task schedule -vserver vs2 -task
-name Task2 -schedule daily
[Job 142]: Vscan On-Demand job is queued. Use the "job show -id 142"
command to view the status.
```

Para ver el estado del trabajo, utilice `job show` comando. La `job pause` y `job resume` comandos, pausar y reiniciar respectivamente el trabajo; el `job stop` el comando finaliza el trabajo.

2. Compruebe que la tarea bajo demanda se ha programado:

```
vserver vscan on-demand-task show -instance data_SVM -task-name task_name
```

Para obtener una lista completa de las opciones, consulte la página de manual del comando.

El siguiente comando muestra los detalles de Task 2 tarea:

```
cluster1::> vserver vscan on-demand-task show -instance vs2 -task-name Task2

Vserver: vs2
Task Name: Task2
List of Scan Paths: /vol1/, /vol2/cifs/
Report Directory Path: /report
Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
File Paths Not to Scan: /vol1/cold-files/
File Extensions Not to Scan: mp3, mp4
File Extensions to Scan: vmdk, mp*
Scan Files with No Extension: false
Request Service Timeout: 5m
Cross Junction: true
Directory Recursion: true
Scan Priority: low
Report Log Level: info
```

Después de terminar

Debe habilitar el análisis en la SVM antes de que se ejecute la tarea programada.

Ejecute una tarea bajo demanda de inmediato

Puede ejecutar una tarea bajo demanda inmediatamente, independientemente de que haya asignado una programación.

Antes de empezar

Debe haber habilitado el análisis en la SVM.

Paso

1. Ejecute una tarea bajo demanda de inmediato:

```
vserver vscan on-demand-task run -vserver data_SVM -task-name task_name
```

El siguiente comando ejecuta una tarea en tiempo de acceso llamada Task1 en la vs1 SVM:

```
cluster1::> vserver vscan on-demand-task run -vserver vs1 -task-name Task1
[Job 161]: Vscan On-Demand job is queued. Use the "job show -id 161" command to view the status.
```



Puede utilizar el `job show` comando para ver el estado del trabajo. Puede utilizar el `job pause` y.. `job resume` comandos para pausar y reiniciar el trabajo o el `job stop` comando para finalizar el trabajo.

Comandos para gestionar tareas bajo demanda

Puede modificar, eliminar o desprogramar una tarea bajo demanda. Puede ver un resumen y detalles de la tarea, así como administrar informes para la tarea.

| Si desea... | Introduzca el siguiente comando... |
|---|---|
| Crear una tarea bajo demanda | <code>vserver vscan on-demand-task create</code> |
| Modifique una tarea bajo demanda | <code>vserver vscan on-demand-task modify</code> |
| Eliminar una tarea bajo demanda | <code>vserver vscan on-demand-task delete</code> |
| Ejecute una tarea bajo demanda | <code>vserver vscan on-demand-task run</code> |
| Programar una tarea bajo demanda | <code>vserver vscan on-demand-task schedule</code> |
| Desprogramar una tarea bajo demanda | <code>vserver vscan on-demand-task unschedule</code> |
| Vea el resumen y los detalles de una tarea bajo demanda | <code>vserver vscan on-demand-task show</code> |
| Ver informes bajo demanda | <code>vserver vscan on-demand-task report show</code> |
| Eliminar informes bajo demanda | <code>vserver vscan on-demand-task report delete</code> |

Para obtener más información sobre estos comandos, consulte las páginas man.

Prácticas recomendadas para configurar la funcionalidad antivirus externa en ONTAP

Tenga en cuenta las siguientes recomendaciones para configurar la funcionalidad de configuración en ONTAP.

- Restringir a los usuarios con privilegios a las operaciones de exploración de virus. Los usuarios normales no deben utilizar credenciales de usuario con privilegios. Esta restricción se puede lograr desactivando los derechos de inicio de sesión para los usuarios con privilegios en Active Directory.
- No es necesario que los usuarios con privilegios formen parte de ningún grupo de usuarios que tenga un gran número de derechos en el dominio, como el grupo de administradores o el grupo de operadores de copia de seguridad. Sólo el sistema de almacenamiento debe validar los usuarios con privilegios para que puedan crear conexiones de servidor Vscan y acceder a archivos para análisis de virus.
- Utilice los equipos que ejecutan servidores Vscan solo para fines de detección de virus. Para desalentar el uso general, desactive los servicios de terminal de Windows y otras disposiciones de acceso remoto en estas máquinas, y otorgue el derecho de instalar nuevo software en estas máquinas solo a los administradores.
- Dedicar los servidores Vscan a la detección de virus y no los utilice para otras operaciones, como las copias de seguridad. Puede decidir ejecutar el servidor Vscan como una máquina virtual (VM). Si ejecuta el servidor Vscan como equipo virtual, asegúrese de que los recursos asignados a la máquina virtual no se comparten y son suficientes para realizar análisis de virus.
- Proporcione una capacidad adecuada de CPU, memoria y disco al servidor Vscan para evitar la asignación excesiva de recursos. La mayoría de los servidores Vscan están diseñados para usar varios servidores principales de CPU y para distribuir la carga entre las CPU.
- NetApp recomienda utilizar una red dedicada con una VLAN privada para la conexión desde la SVM al servidor Vscan para que el tráfico de análisis no se vea afectado por otro tráfico de red del cliente. Cree una tarjeta de interfaz de red (NIC) separada dedicada a la VLAN antivirus en el servidor Vscan y a las LIF de datos del SVM. Este paso simplifica la administración y la solución de problemas en caso de que surjan problemas de red. El tráfico antivirus debe segregarse mediante una red privada. El servidor antivirus debe configurarse para comunicarse con el controlador de dominio (DC) y ONTAP de una de las siguientes maneras:
 - El DC debe comunicarse con los servidores antivirus a través de la red privada que se utiliza para segregar el tráfico.
 - El servidor antivirus y DC deben comunicarse a través de una red diferente (no la red privada mencionada anteriormente), que no es la misma que la red de cliente CIFS.
 - Para habilitar la autenticación de Kerberos para la comunicación antivirus, cree una entrada DNS para las LIF privadas y un nombre principal de servicio en el DC correspondiente a la entrada de DNS creada para la LIF privada. Utilice este nombre cuando agregue una LIF al conector antivirus. El DNS debe ser capaz de devolver un nombre único para cada LIF privado conectado al conector antivirus.



Si la LIF para el tráfico de Vscan está configurada en un puerto distinto al de la LIF para el tráfico de cliente, la LIF Vscan puede conmutar por error a otro nodo si se produce un fallo de puerto. El cambio hace que el servidor Vscan no sea accesible desde el nuevo nodo y las notificaciones de escaneo para las operaciones de archivo en el nodo fallan. Compruebe que se puede acceder al servidor Vscan a través de al menos una LIF en un nodo para que pueda procesar solicitudes de análisis de operaciones de archivo realizadas en ese nodo.

- Conecte el sistema de almacenamiento de NetApp y el servidor Vscan utilizando al menos una red 1GbE.
- Para un entorno con varios servidores Vscan, conecte todos los servidores que tengan conexiones de red similares de alto rendimiento. La conexión de los servidores Vscan mejora el rendimiento al permitir el uso compartido de la carga.
- Para sitios remotos y sucursales, NetApp recomienda usar un servidor Vscan local en lugar de un servidor Vscan remoto porque el primero es un candidato perfecto para alta latencia. Si el costo es un factor, use un ordenador portátil o PC para una protección antivirus moderada. Puede programar análisis periódicos completos del sistema de archivos compartiendo los volúmenes o qtrees y analizándolos desde cualquier

sistema del sitio remoto.

- Utilice varios servidores Vscan para analizar los datos de la SVM con fines de equilibrio de carga y redundancia. La cantidad de carga de trabajo CIFS y el tráfico antivirus resultante varían según la máquina virtual de almacenamiento. Supervisar la latencia de detección de virus y CIFS en la controladora de almacenamiento. Supervise la tendencia de los resultados a lo largo del tiempo. Si la latencia de CIFS y la latencia de análisis de virus aumentan debido a la CPU o las colas de aplicaciones en los servidores Vscan más allá de los umbrales de tendencias, es posible que los clientes CIFS experimenten largos tiempos de espera. Agregar servidores Vscan adicionales para distribuir la carga.
- Instale la última versión del conector antivirus de ONTAP.
- Mantenga actualizados los motores y definiciones antivirus. Consulte a los socios para obtener recomendaciones sobre la frecuencia con la que debe actualizar.
- En un entorno multi-tenancy, un pool de escáner (pool de servidores Vscan) se puede compartir con varias SVM siempre que los servidores Vscan y las SVM formen parte del mismo dominio o dominio de confianza.
- La política de software antivirus para los archivos infectados debe establecerse en “eliminar” o “cuarentena”, que es el valor predeterminado establecido por la mayoría de los proveedores de antivirus. Si vscan-fileop-profile se establece en “WRITE_ONLY”, y si se encuentra un archivo infectado, el archivo permanece en el recurso compartido y se puede abrir porque abrir un archivo no desencadena una exploración. El análisis antivirus solo se activa después de cerrar el archivo.
- La scan-engine timeout el valor debe ser menor que el scanner-pool request-timeout valor. Si se establece con un valor mayor, el acceso a los archivos podría retrasarse y podría agotarse el tiempo de espera en algún momento.
Para evitarlo, configure la scan-engine timeout a 5 segundos menos que el scanner-pool request-timeout valor. Consulte la documentación del proveedor del motor de escaneo para obtener instrucciones sobre cómo cambiar el scan-engine timeout configuración. La scanner-pool timeout se puede cambiar utilizando el siguiente comando en modo avanzado y proporcionando el valor adecuado para el request-timeout parámetro:
`vserver vscan scanner-pool modify.`
- En un entorno con un tamaño adecuado para cargas de trabajo de análisis de acceso y que requiera el uso de análisis bajo demanda, NetApp recomienda programar el trabajo de análisis bajo demanda en horas de menor actividad para evitar cargas adicionales en la infraestructura antivirus existente.

Obtenga más información sobre las prácticas recomendadas específicas para los partners en ["Soluciones de partners de VSCAN"](#).

Habilite la detección de virus en un SVM

Es necesario habilitar el análisis de virus en una SVM para que se pueda ejecutar un análisis bajo demanda o en tiempo real.

Pasos

1. Habilitar la detección de virus en una SVM:

```
vserver vscan enable -vserver data_SVM
```



Puede utilizar el `vserver vscan disable` comando para desactivar la detección de virus, si es necesario.

El siguiente comando habilita el análisis de virus en vs1 SVM:

```
cluster1::> vserver vscan enable -vserver vs1
```

2. Compruebe que la detección de virus está habilitada en la SVM:

```
vserver vscan show -vserver data_SVM
```

Para obtener una lista completa de las opciones, consulte la página de manual del comando.

El siguiente comando muestra el estado de Vscan del vs1 SVM:

```
cluster1::> vserver vscan show -vserver vs1

Vserver: vs1
Vscan Status: on
```

Restablece el estado de los archivos capturados

En ocasiones, es posible que desee restablecer el estado de análisis de los archivos analizados correctamente en una SVM mediante el `vserver vscan reset` comando para descartar la información almacenada en caché para los archivos. Es posible que desee utilizar este comando para reiniciar el procesamiento de análisis de virus en caso de un análisis mal configurado, por ejemplo.

Acerca de esta tarea

Después de ejecutar el `vserver vscan reset` comando, todos los archivos elegibles se analizarán la próxima vez que se acceda a ellos.



Este comando puede afectar negativamente al rendimiento, dependiendo del número y el tamaño de los archivos que se van a volver a analizar.

Lo que necesitará

Se requieren privilegios avanzados para esta tarea.

Pasos

1. Cambie al nivel de privilegio avanzado:

```
set -privilege advanced
```

2. Restablecer el estado de los archivos capturados:

```
vserver vscan reset -vserver data_SVM
```

El siguiente comando restablece el estado de los archivos capturados en vs1 SVM:

```
cluster1::> vserver vscan reset -vserver vs1
```

Ver la información del registro de eventos de Vscan

Puede utilizar el `vserver vscan show-events` Comando para ver información de registro de eventos sobre archivos infectados, actualizaciones en servidores Vscan y similares. Puede ver información sobre eventos del clúster o de los nodos, SVM o servidores Vscan.

Antes de empezar

Se necesitan privilegios avanzados para ver el registro de eventos Vscan.

Pasos

1. Cambie al nivel de privilegio avanzado:

```
set -privilege advanced
```

2. Ver información del registro de eventos de Vscan:

```
vserver vscan show-events
```

Para obtener una lista completa de las opciones, consulte la página de manual del comando.

El siguiente comando muestra información del registro de eventos para el clúster `cluster1`:

```
cluster1::*> vserver vscan show-events
```

| Vserver | Node | Server | Event Type | Event Time |
|---------------------------|------------|-------------|-------------------|------------|
| ----- | ----- | ----- | ----- | |
| vs1 | Cluster-01 | 192.168.1.1 | file-infected | 9/5/2014 |
| 11:37:38 | | | | |
| vs1 | Cluster-01 | 192.168.1.1 | scanner-updated | 9/5/2014 |
| 11:37:08 | | | | |
| vs1 | Cluster-01 | 192.168.1.1 | scanner-connected | 9/5/2014 |
| 11:34:55 | | | | |
| 3 entries were displayed. | | | | |

Supervise y solucione problemas de conectividad

Posibles problemas de conectividad relacionados con la opción de adquisición obligatoria

Puede utilizar el `vserver vscan connection-status show` Comandos para ver información acerca de las conexiones del servidor Vscan que puede resultar útil para solucionar problemas de conectividad.

De forma predeterminada, la `scan-mandatory` La opción para el análisis en tiempo real deniega el acceso a archivos cuando no hay disponible una conexión de servidor Vscan para el análisis. Aunque esta opción ofrece importantes funciones de seguridad, puede dar lugar a problemas en algunas situaciones.

- Antes de habilitar el acceso de cliente, debe asegurarse de que al menos un servidor Vscan esté conectado a una SVM en cada nodo que tenga una LIF. Si necesita conectar servidores a las SVM después de habilitar el acceso de cliente, debe desactivar el `scan-mandatory` Opción en la SVM para asegurarse de que no se deniega el acceso al archivo porque no hay una conexión de servidor Vscan disponible. Puede volver a activar la opción después de haber conectado el servidor.
- Si un LIF de destino aloja todas las conexiones del servidor Vscan para una SVM, la conexión entre el servidor y la SVM se perderá si se migra el LIF. Para asegurarse de que no se deniega el acceso a los archivos porque no hay una conexión de servidor Vscan disponible, debe desactivar el `scan-mandatory` Opción antes de migrar la LIF. Puede volver a activar la opción después de migrar el LIF.

Cada SVM debe tener al menos dos servidores Vscan asignados. Se recomienda conectar los servidores Vscan al sistema de almacenamiento a través de una red diferente a la utilizada para el acceso de los clientes.

Comandos para ver el estado de conexión del servidor Vscan

Puede utilizar el `vserver vscan connection-status show` Comandos para ver información resumida y detallada acerca del estado de conexión del servidor Vscan.

| Si desea... | Introduzca el siguiente comando... |
|--|---|
| Ver un resumen de las conexiones del servidor Vscan | <code>vserver vscan connection-status show</code> |
| Ver detalles de las conexiones del servidor Vscan | <code>vserver vscan connection-status show-all</code> |
| Ver detalles de los servidores Vscan conectados | <code>vserver vscan connection-status show-connected</code> |
| Ver detalles de los servidores Vscan disponibles que no están conectados | <code>vserver vscan connection-status show-not-connected</code> |

Para obtener más información sobre estos comandos, consulte ["Páginas manuales de ONTAP"](#).

Solucionar problemas de detección de virus

Para los problemas comunes de detección de virus, existen posibles causas y formas de resolverlos. La detección de virus también se conoce como Vscan.

| Problema | Cómo resolverlo |
|----------|-----------------|
|----------|-----------------|

| | |
|---|---|
| Los servidores Vscan no se pueden conectar El sistema de almacenamiento Clustered ONTAP de NetApp. | Compruebe si la configuración del grupo de escáner especifica la dirección IP del servidor Vscan. Compruebe también si los usuarios con privilegios permitidos en la lista de grupos de escáneres están activos. Para comprobar el conjunto de escáneres, ejecute el <code>vserver vscan scanner-pool show</code> comando en el símbolo del sistema de almacenamiento. Si los servidores Vscan siguen sin poder conectarse, es posible que haya un problema con la red. |
| Los clientes observan una alta latencia. | Probablemente sea el momento de agregar más servidores Vscan al grupo de escáneres. |
| Se activan demasiadas adquisiciones. | Modifique el valor de <code>vscan-fileop-profile</code> parámetro que permite restringir el número de operaciones de archivos supervisadas para el análisis de virus. |
| Algunos archivos no se están escaneando. | Compruebe la política de acceso. Es posible que la ruta de acceso de estos archivos se haya agregado a la lista de exclusión de ruta de acceso o que su tamaño supere el valor configurado para las exclusiones. Para comprobar la política de acceso, ejecute <code>vserver vscan on-access-policy show</code> comando en el símbolo del sistema de almacenamiento. |
| Se ha denegado el acceso al archivo. | Compruebe si el valor <code>scan-mandatory</code> está especificado en la configuración de la política. Esta opción deniega el acceso a los datos si no hay servidores Vscan conectados. Modifique la configuración según sea necesario. |

Supervise el estado y las actividades de rendimiento

Puede supervisar los aspectos críticos del módulo Vscan, como el estado de conexión del servidor Vscan,

El estado de los servidores Vscan y el número de archivos que se han analizado. Esta información ayuda

Diagnosticar problemas relacionados con el servidor Vscan.

Ver información de conexión del servidor Vscan

Puede ver el estado de conexión de los servidores Vscan para gestionar las conexiones que ya están en uso y las conexiones disponibles para su uso. Varios comandos muestran información Acerca del estado de conexión de los servidores Vscan.

| | |
|------------|-------------------------|
| Comando... | Información mostrada... |
|------------|-------------------------|

| | |
|---|---|
| <code>vserver vscan connection-status show</code> | Resumen del estado de conexión |
| <code>vserver vscan connection-status show-all</code> | Información detallada sobre el estado de la conexión |
| <code>vserver vscan connection-status show-not-connected</code> | Estado de las conexiones disponibles pero no conectadas |
| <code>vserver vscan connection-status show-connected</code> | Información sobre el servidor Vscan conectado |

Para obtener más información sobre estos comandos, consulte ["páginas de manual"](#).

Ver estadísticas del servidor Vscan

Puede ver estadísticas específicas del servidor Vscan para supervisar el rendimiento y diagnosticar problemas relacionados con

detección de virus. Debe recopilar una muestra de datos para poder utilizar el `statistics show` comando a.

Mostrar las estadísticas del servidor Vscan.

Para completar una muestra de datos, realice el siguiente paso:

Paso

1. Ejecute el `statistics start` y la optional `statistics` comando stop.

Ver estadísticas de las solicitudes y latencias del servidor Vscan

Puede usar ONTAP `offbox_vscan` Contadores por SVM para supervisar la tasa de Vscan

Las solicitudes de servidor que se envían y reciben por segundo y las latencias de los servidores en todas las secuencias virtuales

servidores. Para ver estas estadísticas, realice el siguiente paso:

Paso

1. Ejecute el resultado de estadísticas `object offbox_vscan -instance SVM` con el siguientes contadores:

| Contador... | Información mostrada... |
|---|---|
| <code>scan_request_dispatched_rate</code> | Número de solicitudes de detección de virus enviadas desde ONTAP a los servidores Vscan por segundo |
| <code>scan_noti_received_rate</code> | Número de solicitudes de detección de virus recibidas por ONTAP desde los servidores Vscan por segundo |
| <code>dispatch_latency</code> | Latencia dentro de ONTAP para identificar un servidor Vscan disponible y enviar la solicitud a ese servidor Vscan |

| | |
|--------------|--|
| scan_latency | Latencia de ida y vuelta desde ONTAP al servidor Vscan, incluido el tiempo para que se ejecute el análisis |
|--------------|--|

Ejemplo de estadísticas generadas a partir de un contador de vscan del buzón de ONTAP

```
Object: offbox_vscan
Instance: SVM
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 2 (complete_aggregation)
Counter Value
-----
scan_request_dispatched_rate 291
scan_noti_received_rate 292
dispatch_latency 43986us
scan_latency 3433501us
-----
```

Vea estadísticas de solicitudes y latencias de servidores Vscan individuales

Puede usar ONTAP `offbox_vscan_server` Contadores en un servidor Vscan por SVM, por cada servidor Vscan externo,

Y por nodo para supervisar la tasa de solicitudes de servidor Vscan enviadas y la latencia del servidor activada

Cada servidor Vscan individualmente. Para recopilar esta información, realice el siguiente paso:

Paso

1. Ejecute el `statistics show -object offbox_vscan -instance SVM:servername:nodename` comando con los siguientes contadores:

| Contador... | Información mostrada... |
|------------------------------|--|
| scan_request_dispatched_rate | Número de solicitudes de detección de virus enviadas desde ONTAP |
| scan_latency | Latencia de ida y vuelta desde ONTAP al servidor Vscan, incluido el tiempo para que se ejecute el análisis A los servidores Vscan por segundo |

Ejemplo de estadísticas generadas a partir de un contador ONTAP `offbox_vscan_server`


```
Object: offbox_vscan_server
Instance: SVM:vscan_server:node
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 1 (complete_aggregation)
Counter Value
```

```
-----
scan_request_dispatched_rate 291
scan_latency 3433830us
-----
```

Ver estadísticas para el uso del servidor Vscan

También puede utilizar ONTAP `offbox_vscan_server` Contadores para recopilar la utilización del servidor Vscan

estadísticas. Estas estadísticas se realizan para cada SVM, cada servidor Vscan externo, y por nodo. Ellos Incluya el uso de CPU en el servidor Vscan, la profundidad de cola para las operaciones de escaneo en el servidor Vscan

(actual y máximo), memoria usada y red usada.

Estas estadísticas son reenviadas por el conector antivirus a los contadores de estadísticas dentro de ONTAP. Ellos

se basan en datos sondeados cada 20 segundos y deben recopilarse varias veces para obtener precisión; de lo contrario, los valores que se muestran en las estadísticas solo reflejan el último sondeo. La utilización de CPU y las colas son particularmente importante para monitorear y analizar. Un valor alto para una cola promedio puede indicar que el

El servidor VSCAN tiene un cuello de botella.

Para recopilar estadísticas de uso para el servidor Vscan en un servidor Vscan por SVM, por servidor Vscan externo y por nodo

base, complete el siguiente paso:

Paso

1. Recopilar estadísticas de utilización del servidor Vscan

Ejecute el `statistics show -object offbox_vscan_server -instance SVM:servername:nodename` comando con lo siguiente `offbox_vscan_server` contadores:

| Contador... | Información mostrada... |
|--|---|
| <code>scanner_stats_pct_cpu_used</code> | Uso de CPU en el servidor Vscan |
| <code>scanner_stats_pct_input_queue_avg</code> | Cola media de solicitudes de exploración en el servidor Vscan |
| <code>scanner_stats_pct_input_queue_hiwatermark</code> | Cola pico de solicitudes de exploración en el servidor Vscan |

| | |
|--------------------------------|--|
| scanner_stats_pct_mem_used | Memoria utilizada en el servidor Vscan |
| scanner_stats_pct_network_used | Red utilizada en el servidor Vscan |

Ejemplo de estadísticas de utilización para el servidor Vscan

```
Object: offbox_vscan_server
Instance: SVM:vscan_server:node
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 1 (complete_aggregation)
Counter Value
-----
scanner_stats_pct_cpu_used 51
scanner_stats_pct_dropped_requests 0
scanner_stats_pct_input_queue_avg 91
scanner_stats_pct_input_queue_hiwatermark 100
scanner_stats_pct_mem_used 95
scanner_stats_pct_network_used 4
-----
```

Auditar eventos NAS en SVM

Seguimiento de seguridad y auditoría de SMB y NFS

Puede utilizar las funciones de auditoría de acceso a archivos disponibles para los protocolos SMB y NFS con ONTAP, como la auditoría nativa y la gestión de políticas de archivos mediante FPolicy.

Debe diseñar e implementar la auditoría de eventos de acceso a archivos SMB y NFS bajo las siguientes circunstancias:

- Se ha configurado el acceso básico a archivos del protocolo SMB y NFS.
- Desea crear y mantener una configuración de auditoría mediante uno de los siguientes métodos:
 - Funcionalidad nativa de ONTAP
 - Servidores FPolicy externos

Auditar eventos NAS en SVM

La auditoría de eventos de NAS es una medida de seguridad que le permite realizar un seguimiento y registrar determinados eventos de SMB y NFS en máquinas virtuales de almacenamiento (SVM). Esto le ayuda a realizar un seguimiento de los posibles problemas de seguridad y proporciona pruebas de cualquier violación de la seguridad. También puede configurar y auditar las directivas de acceso central de Active Directory para ver cuál sería el resultado de implementarlas.

Eventos de SMB

Puede auditar los siguientes eventos:

- Eventos de acceso a archivos y carpetas SMB

Es posible auditar los eventos de acceso a archivos SMB y carpetas que se producen en los objetos almacenados en volúmenes FlexVol que pertenecen a las SVM habilitadas para auditoría.

- Eventos de inicio y cierre de sesión en SMB

Puede auditar eventos de inicio y cierre de sesión SMB para servidores SMB en SVM.

- Eventos de configuración de directivas de acceso central

Puede auditar el acceso efectivo de objetos en servidores SMB usando permisos aplicados a través de políticas de acceso central propuestas. La auditoría a través de la configuración de las políticas de acceso central permite ver cuáles son los efectos de las políticas de acceso central antes de implementarlas.

La auditoría de la configuración de la directiva de acceso central se configura mediante GPO de Active Directory; sin embargo, la configuración de auditoría de SVM debe configurarse para auditar eventos de configuración de directivas de acceso central.

Aunque puede habilitar la configuración de directivas de acceso central en la configuración de auditoría sin habilitar Dynamic Access Control en el servidor SMB, los eventos de configuración de directivas de acceso central sólo se generan si el control de acceso dinámico está habilitado. El control de acceso dinámico se activa mediante una opción de servidor SMB. No está habilitado de forma predeterminada.

Eventos de NFS

Puede auditar los eventos de archivo y directorio usando las ACL de NFSv4 en objetos almacenados en SVM.

Cómo funciona la auditoría

Conceptos básicos de auditoría

Para comprender la auditoría en ONTAP, debe conocer algunos conceptos básicos de auditoría.

- **Archivos de ensayo**

Los archivos binarios intermedios en nodos individuales en los que se almacenan los registros de auditoría antes de la consolidación y la conversión. Los archivos de almacenamiento provisional se encuentran en volúmenes de almacenamiento provisional.

- **Volumen de estadificación**

Un volumen dedicado creado por ONTAP para almacenar archivos provisional. Hay un volumen de almacenamiento provisional por agregado. Todas las máquinas virtuales de almacenamiento (SVM) habilitadas para auditoría comparten los volúmenes de almacenamiento para almacenar registros de auditoría de acceso a los datos de los volúmenes de datos de ese agregado en particular. Los registros de auditoría de cada SVM se almacenan en un directorio independiente dentro del volumen provisional.

Los administradores de clúster pueden ver información sobre la configuración provisional de los volúmenes, pero no se permite la mayoría de las demás operaciones de volumen. Solo ONTAP puede

crear volúmenes de almacenamiento provisional. ONTAP asigna automáticamente un nombre a la configuración provisional de los volúmenes. Todos los nombres de volúmenes de almacenamiento provisional comienzan por MDV_aud_ Seguido del UUID del agregado que contiene ese volumen de almacenamiento provisional (por ejemplo: MDV_aud_1d0131843d4811e296fc123478563412.)

- **Volúmenes del sistema**

Un volumen FlexVol que contiene metadatos especiales, como metadatos para registros de auditoría de servicios de archivos. La SVM de administrador es propietaria de los volúmenes de sistemas, que son visibles en el clúster. El almacenamiento provisional de volúmenes es un tipo de volumen del sistema.

- **Tarea de consolidación**

Tarea que se crea al activar la auditoría. Esta tarea de larga ejecución en cada SVM toma los registros de auditoría de archivos staging en los nodos miembros de la SVM. Esta tarea fusiona los registros de auditoría en orden cronológico ordenado y los convierte a continuación en un formato de registro de eventos legible para el usuario especificado en la configuración de auditoría, ya sea en el formato de archivo EVTX o XML. Los registros de eventos convertidos se almacenan en el directorio del registro de eventos de auditoría especificado en la configuración de auditoría de SVM.

Cómo funciona el proceso de auditoría de ONTAP

El proceso de auditoría de ONTAP es diferente del proceso de auditoría de Microsoft. Antes de configurar la auditoría, debe comprender cómo funciona el proceso de auditoría de ONTAP.

Los registros de auditoría se almacenan inicialmente en archivos de configuración binaria en nodos individuales. Si la auditoría está habilitada en una SVM, cada nodo miembro mantiene archivos provisional para esa SVM. Periódicamente, se consolidan y convierten en registros de eventos legibles por el usuario, que se almacenan en el directorio del registro de eventos de auditoría de la SVM.

Proceso cuando la auditoría está habilitada en una SVM

La auditoría solo se puede habilitar en las SVM. Cuando el administrador de almacenamiento permite auditar la SVM, el subsistema de auditoría comprueba si hay volúmenes de almacenamiento provisional presentes. Debe existir un volumen de almacenamiento provisional para cada agregado que contenga los volúmenes de datos que pertenece a la SVM. El subsistema de auditoría crea los volúmenes de almacenamiento provisional necesarios si no existen.

El subsistema de auditoría también completa otras tareas de requisitos previos antes de activar la auditoría:

- El subsistema de auditoría verifica que la ruta de acceso del directorio de registro esté disponible y no contenga enlaces simbólicos.

El directorio de registro debe existir como ruta dentro del espacio de nombres de la SVM. Se recomienda crear un nuevo volumen o un qtree para almacenar los archivos de registro de auditoría. El subsistema de auditoría no asigna una ubicación de archivo de registro predeterminada. Si la ruta de acceso del directorio de registro especificada en la configuración de auditoría no es una ruta válida, la auditoría de la creación de la configuración falla con el `The specified path "/path" does not exist in the namespace belonging to Vserver "Vserver_name" error.`

Se produce un error en la creación de la configuración si el directorio existe pero contiene enlaces simbólicos.

- La auditoría programa la tarea de consolidación.

Una vez programada esta tarea, se habilita la auditoría. La configuración de auditoría de SVM y los archivos de registro persisten durante un reinicio o si los servidores NFS o SMB se detienen o se reinician.

Consolidación de registros de eventos

La consolidación de registros es una tarea programada que se ejecuta de forma rutinaria hasta que se deshabilita la auditoría. Cuando la auditoría está deshabilitada, la tarea de consolidación verifica que todos los registros restantes se consolidan.

Auditoría garantizada

De forma predeterminada, la auditoría está garantizada. ONTAP garantiza que se registran todos los eventos de acceso a archivos auditables (según lo especificado por las ACL de política de auditoría configuradas), incluso si un nodo no está disponible. No se puede completar una operación de archivo solicitada hasta que el registro de auditoría de esa operación se guarde en el volumen provisional en un almacenamiento persistente. Si los registros de auditoría no se pueden guardar en el disco de los archivos de almacenamiento provisional, ya sea por falta de espacio o por otros problemas, se deniegan las operaciones de cliente.



Un administrador, o usuario de cuenta con acceso de nivel de privilegio, puede omitir la operación de registro de auditoría de archivos mediante las API DE REST o el SDK para de gestión de NetApp. Puede determinar si se han realizado acciones de archivo con las API DE REST o SDK para facilitar la gestión de NetApp. Para ello, revise los registros del historial de comandos almacenados en la `audit.log` archivo.

Para obtener más información acerca de los registros de auditoría del historial de comandos, consulte la sección "Gestión del registro de auditoría para actividades de administración" en ["Administración del sistema"](#).

Proceso de consolidación cuando un nodo no está disponible

Si no está disponible un nodo que contiene volúmenes que pertenecen a una SVM con auditoría habilitada, el comportamiento de la tarea de consolidación de auditoría depende de si está disponible el partner de conmutación por error (SFO) del almacenamiento del nodo (o el partner de alta disponibilidad en el caso de un clúster de dos nodos):

- Si el volumen de almacenamiento provisional está disponible a través del partner SFO, se analizan los volúmenes de almacenamiento provisional notificados por última vez desde el nodo y la consolidación continúa con normalidad.
- Si el partner SFO no está disponible, la tarea crea un archivo de registro parcial.

Cuando no se puede acceder a un nodo, la tarea de consolidación consolida los registros de auditoría de los demás nodos disponibles de esa SVM. Para identificar que no se ha completado, la tarea agrega el sufijo `.partial` al nombre de archivo consolidado.

- Una vez que el nodo no disponible está disponible, los registros de auditoría de ese nodo se consolidan con los registros de auditoría de los otros nodos en ese momento.
- Se conservan todos los registros de auditoría.

Rotación del registro de eventos

Los archivos de registro de eventos de auditoría se rotan cuando alcanzan un tamaño de registro de umbral

configurado o en un programa configurado. Cuando se gira un archivo de registro de eventos, la tarea de consolidación programada cambia primero el nombre del archivo convertido activo a un archivo de archivo con fecha temporal y, a continuación, crea un nuevo archivo de registro de eventos convertido activo.

Proceso cuando la auditoría está deshabilitada en la SVM

Cuando la auditoría está deshabilitada en la SVM, la tarea de consolidación se activa una vez final. Todos los registros de auditoría pendientes y registrados se registran en un formato legible por el usuario. Los registros de eventos existentes almacenados en el directorio de registro de eventos no se eliminan cuando la auditoría está deshabilitada en la SVM y están disponibles para su visualización.

Después de consolidar todos los archivos staging existentes de esa SVM, la tarea de consolidación se elimina de la programación. Al deshabilitar la configuración de auditoría de la SVM, no se quita la configuración de auditoría. Un administrador de almacenamiento puede volver a habilitar la auditoría en cualquier momento.

El trabajo de consolidación de auditoría, que se crea al habilitar la auditoría, supervisa la tarea de consolidación y vuelve a crearla si la tarea de consolidación se cierra debido a un error. Los usuarios no pueden suprimir el trabajo de consolidación de auditoría.

Requisitos y consideraciones de auditoría

Antes de configurar y habilitar la auditoría en una máquina virtual de almacenamiento (SVM), debe tener en cuenta ciertos requisitos y consideraciones.

- El número máximo de SVM admitidas para la auditoría depende de la versión de ONTAP:

| Versión de ONTAP | Máximo |
|-------------------|--------|
| 9,8 y anteriores | 50 |
| 9.9.1 y posterior | 400 |

- La auditoría no está vinculada a las licencias de SMB o NFS.

Puede configurar y habilitar la auditoría aunque las licencias de SMB y NFS no estén instaladas en el clúster.

- La auditoría de NFS admite ACE de seguridad (tipo U).
- Para la auditoría de NFS no hay ninguna asignación entre los bits de modo y los ACE de auditoría.

Al convertir ACL a bits de modo, se omiten los ACE de auditoría. Al convertir bits de modo a ACL, no se generan ACE de auditoría.

- El directorio especificado en la configuración de auditoría debe existir.

Si no existe, el comando para crear la configuración de auditoría falla.

- El directorio especificado en la configuración de auditoría debe cumplir los siguientes requisitos:

- El directorio no debe contener enlaces simbólicos.

Si el directorio especificado en la configuración de auditoría contiene enlaces simbólicos, el comando para crear la configuración de auditoría falla.

- Debe especificar el directorio mediante una ruta absoluta.

No debe especificar una ruta de acceso relativa, por ejemplo, `/vs1/./.`.

- La auditoría depende de que haya espacio disponible en los volúmenes de almacenamiento provisional.

Debe conocer y disponer de un plan para garantizar que haya espacio suficiente para la configuración de volúmenes en agregados que contengan volúmenes auditados.

- La auditoría depende de que haya espacio disponible en el volumen que contiene el directorio donde se almacenan los registros de eventos convertidos.

Debe conocer y tener un plan para garantizar que haya espacio suficiente en los volúmenes utilizados para almacenar registros de eventos. Puede especificar el número de registros de eventos que se conservarán en el directorio de auditoría mediante el `-rotate-limit` al crear una configuración de auditoría, que puede ayudar a garantizar que haya suficiente espacio disponible para los registros de eventos en el volumen.

- Aunque puede habilitar la configuración de directivas de acceso central en la configuración de auditoría sin habilitar el control de acceso dinámico en el servidor SMB, debe habilitarse el control de acceso dinámico para generar eventos de configuración de directivas de acceso central.

El control de acceso dinámico no está activado de forma predeterminada.

Agregar consideraciones de espacio al habilitar la auditoría

Cuando se crea una configuración de auditoría y se habilita la auditoría en al menos una máquina virtual de almacenamiento (SVM) del clúster, el subsistema de auditoría crea volúmenes de almacenamiento provisional en todos los agregados existentes y en todos los nuevos agregados creados. Debe tener en cuenta ciertas consideraciones de espacio de los agregados al habilitar la auditoría en el clúster.

La creación provisional de volúmenes puede fallar debido a la falta de espacio en un agregado. Esto puede suceder si crea una configuración de auditoría y los agregados existentes no tienen suficiente espacio para contener el volumen de almacenamiento provisional.

Debe asegurarse de que haya espacio suficiente en los agregados existentes para los volúmenes de almacenamiento provisional antes de habilitar la auditoría en una SVM.

Limitaciones del tamaño de los registros de auditoría en los archivos de almacenamiento provisional

El tamaño de un registro de auditoría en un archivo provisional no puede ser superior a 32 KB.

Cuando se pueden producir registros de auditoría grandes

Los registros de auditoría de gran tamaño pueden producirse durante la auditoría de gestión en uno de los siguientes casos:

- Agregar o eliminar usuarios a o de grupos con un gran número de usuarios.
- Adición o eliminación de una lista de control de acceso (ACL) de recurso compartido de archivos en un recurso compartido de archivos con un gran número de usuarios de recursos compartidos de archivos.
- Otros escenarios.

Deshabilite la auditoría de gestión para evitar este problema. Para ello, modifique la configuración de auditoría

y elimine lo siguiente de la lista de tipos de eventos de auditoría:

- recurso compartido de archivos
- cuenta de usuario
- grupo de seguridad
- autorización-cambio de política

Tras la eliminación, el subsistema de auditoría de servicios de archivos no los auditará.

Los efectos de los registros de auditoría que son demasiado grandes

- Si el tamaño de un registro de auditoría es demasiado grande (más de 32 KB), no se crea el registro de auditoría y el subsistema de auditoría genera un mensaje de sistema de gestión de eventos (EMS) similar al siguiente:

```
File Services Auditing subsystem failed the operation or truncated an audit
record because it was greater than max_audit_record_size value. Vserver
UUID=%s, event_id=%u, size=%u
```

Si la auditoría está garantizada, la operación de archivo falla porque no se puede crear su registro de auditoría.

- Si el tamaño del registro de auditoría es superior a 9,999 bytes, se muestra el mismo mensaje EMS que se ha mencionado anteriormente. Se crea un registro de auditoría parcial y falta el valor de clave mayor.
- Si el registro de auditoría supera los 2,000 caracteres, aparece el siguiente mensaje de error en lugar del valor real:

```
The value of this field was too long to display.
```

Qué son los formatos de registro de eventos de auditoría admitidos

Los formatos de archivo admitidos para los registros de eventos de auditoría convertidos son EVTX y.. XML formatos de archivo.

Puede especificar el tipo de formato de archivo al crear la configuración de auditoría. De forma predeterminada, ONTAP convierte los registros binarios en EVTX formato de archivo.

Ver los registros de eventos de auditoría

Puede usar los registros de eventos de auditoría para determinar si tiene una seguridad de archivos adecuada y si se han intentado acceder a archivos y carpetas de forma incorrecta. Puede ver y procesar los registros de eventos de auditoría guardados en el EVTX o. XML formatos de archivo.

- EVTX formato de archivo

Puede abrir el convertido EVTX Registros de eventos de auditoría como archivos guardados mediante el Visor de sucesos de Microsoft.

Hay dos opciones que puede utilizar al ver registros de eventos mediante el Visor de eventos:

- Vista general

La información que es común a todos los eventos se muestra para el registro de eventos. En esta versión de ONTAP, no se muestran los datos específicos del evento para el registro de eventos. Puede utilizar la vista detallada para mostrar datos específicos de un evento.

- Vista detallada

Ofrece una vista sencilla y una vista XML. La vista descriptivo y la vista XML muestran tanto la información que es común a todos los eventos como los datos específicos del evento para el registro de eventos.

- XML formato de archivo

Puede ver y procesar XML registros de eventos de auditoría en aplicaciones de terceros compatibles con XML formato de archivo. Las herramientas de visualización XML se pueden utilizar para ver los registros de auditoría siempre que tenga el esquema XML y la información sobre las definiciones de los campos XML. Para obtener más información sobre el esquema y las definiciones XML, consulte "[Referencia del esquema de auditoría de ONTAP](#)".

Cómo se visualizan los registros de auditoría activos mediante el Visor de sucesos

Si se ejecuta el proceso de consolidación de auditoría en el clúster, el proceso de consolidación añade nuevos registros al archivo de registro de auditoría activo para máquinas virtuales de almacenamiento (SVM) habilitadas para auditoría. Se puede acceder a este registro de auditoría activo y abrirlo a través de un recurso compartido SMB en el Visor de eventos de Microsoft.

Además de ver los registros de auditoría existentes, el Visor de sucesos dispone de una opción de actualización que permite actualizar el contenido de la ventana de la consola. Si los registros recién anexados se pueden ver en el Visor de eventos depende de si los bloqueos oportunistas están habilitados en el recurso compartido utilizado para acceder al registro de auditoría activo.

| Bloqueos oportunistas en el recurso compartido | Comportamiento |
|--|--|
| Activado | El Visor de sucesos abre el registro que contiene eventos escritos hasta ese momento. La operación de actualización no actualiza el registro con nuevos eventos incorporados en el proceso de consolidación. |
| Deshabilitado | El Visor de sucesos abre el registro que contiene eventos escritos hasta ese momento. La operación de actualización actualiza el registro con nuevos eventos anexados por el proceso de consolidación. |



Esta información sólo se aplica para EVTX registros de eventos. XML Los registros de eventos se pueden ver a través de SMB en un explorador o mediante NFS mediante cualquier editor o visor XML.

Eventos SMB que se pueden auditar

Eventos SMB que se pueden auditar con información general

ONTAP puede auditar determinados eventos SMB, incluidos determinados eventos de acceso a archivos y carpetas, determinados eventos de inicio y cierre de sesión y eventos de configuración de directivas de acceso central. Saber qué eventos de acceso se pueden auditar es útil cuando se interpretan los resultados de los registros de eventos.

Los siguientes eventos SMB adicionales se pueden auditar en ONTAP 9.2 y versiones posteriores:

| ID DE EVENTO (EVT/EVTX) | Evento | Descripción | Categoría |
|-------------------------|---|---|-------------------|
| 4670 | Se han cambiado los permisos de objeto | ACCESO A OBJETOS: Se han cambiado los permisos. | Acceso a archivos |
| 4907 | Se ha cambiado la configuración de auditoría de objetos | ACCESO A OBJETOS: Se ha cambiado la configuración de auditoría. | Acceso a archivos |
| 4913 | Se ha cambiado la política de acceso central de objetos | ACCESO A OBJETOS: SE HA CAMBIADO LA TAPA. | Acceso a archivos |

Los siguientes eventos del bloque de mensajes del servidor pueden auditarse en ONTAP 9.0 y versiones posteriores:

| ID DE EVENTO (EVT/EVTX) | Evento | Descripción | Categoría |
|-------------------------|--|---|----------------------------------|
| 540/4624 | Una cuenta se ha conectado correctamente | INICIO de SESIÓN/CIERRE DE SESIÓN: Inicio de sesión en la red (SMB). | Inicio de sesión y cierre sesión |
| 529/4625 | No se pudo iniciar sesión en una cuenta | INICIO de SESIÓN/CIERRE DE SESIÓN: Nombre de usuario desconocido o contraseña incorrecta. | Inicio de sesión y cierre sesión |
| 530/4625 | No se pudo iniciar sesión en una cuenta | INICIO de SESIÓN/CIERRE DE SESIÓN: Restricción del tiempo de inicio de sesión de la cuenta. | Inicio de sesión y cierre sesión |
| 531/4625 | No se pudo iniciar sesión en una cuenta | INICIO de SESIÓN/CIERRE DE SESIÓN: Cuenta desactivada actualmente. | Inicio de sesión y cierre sesión |

| | | | |
|----------|---|--|----------------------------------|
| 532/4625 | No se pudo iniciar sesión en una cuenta | INICIO de SESIÓN/CIERRE DE SESIÓN: La cuenta de usuario ha caducado. | Inicio de sesión y cierre sesión |
| 533/4625 | No se pudo iniciar sesión en una cuenta | INICIO de SESIÓN/CIERRE DE SESIÓN: El usuario no puede iniciar sesión en este equipo. | Inicio de sesión y cierre sesión |
| 534/4625 | No se pudo iniciar sesión en una cuenta | INICIO de SESIÓN/CIERRE DE SESIÓN: El usuario no ha concedido el tipo de inicio de sesión aquí. | Inicio de sesión y cierre sesión |
| 535/4625 | No se pudo iniciar sesión en una cuenta | INICIO de SESIÓN/CIERRE DE SESIÓN: La contraseña del usuario ha caducado. | Inicio de sesión y cierre sesión |
| 537/4625 | No se pudo iniciar sesión en una cuenta | INICIO de SESIÓN/CIERRE DE SESIÓN: Error de inicio de sesión por motivos distintos a los anteriores. | Inicio de sesión y cierre sesión |
| 539/4625 | No se pudo iniciar sesión en una cuenta | INICIO de SESIÓN/CIERRE DE SESIÓN: Cuenta bloqueada. | Inicio de sesión y cierre sesión |
| 538/4634 | Se ha cerrado una cuenta | INICIO de SESIÓN/CIERRE DE SESIÓN: Cierre de sesión del usuario local o de la red. | Inicio de sesión y cierre sesión |
| 560/4656 | Abra objeto/Crear objeto | ACCESO A OBJETOS: Objeto (archivo o directorio) abierto. | Acceso a archivos |
| 563/4659 | Abrir objeto con la intención de eliminar | ACCESO A OBJETOS: Se ha solicitado un controlador a un objeto (archivo o directorio) con el propósito de eliminar. | Acceso a archivos |
| 564/4660 | Eliminar objeto | ACCESO A OBJETOS: Eliminar objeto (archivo o directorio). ONTAP genera este evento cuando un cliente de Windows intenta eliminar el objeto (archivo o directorio). | Acceso a archivos |

| | | | |
|---------------------------------------|---|---|-------------------|
| 567/4663 | Leer objeto/escribir objeto/obtener atributos de objeto/establecer atributos de objeto | ACCESO A OBJETOS: Intento de acceso al objeto (lectura, escritura, Get Attribute, set attribute). Nota: para este evento, ONTAP sólo audita la primera operación de lectura y escritura de SMB (éxito o fallo) en un objeto. Esto impide que ONTAP cree demasiadas entradas de registro cuando un único cliente abre un objeto y realiza muchas operaciones de lectura o escritura sucesivas al mismo objeto. | Acceso a archivos |
| NA/4664 | Vínculo rígido | ACCESO A OBJETOS: Se ha intentado crear un vínculo rígido. | Acceso a archivos |
| NA/4818 PULG | La directiva de acceso central propuesta no concede los mismos permisos de acceso que la directiva de acceso central actual | ACCESO A OBJETOS: Configuración de la directiva de acceso central. | Acceso a archivos |
| ID de evento DE Data ONTAP NA/NA 9999 | Cambiar nombre de objeto | ACCESO A OBJETOS: Objeto cambiado de nombre. Este es un evento de ONTAP. Actualmente no es compatible con Windows como un único evento. | Acceso a archivos |
| ID Evento Data ONTAP NA/NA 9998 | Desvincular objeto | ACCESO A OBJETOS: Objeto no vinculado. Este es un evento de ONTAP. Actualmente no es compatible con Windows como un único evento. | Acceso a archivos |

Información adicional sobre el evento 4656

La `HandleID` etiqueta la auditoría XML el evento contiene el controlador del objeto (archivo o directorio) al que se tiene acceso. La `HandleID` La etiqueta para el evento EVTX 4656 contiene información diferente dependiendo de si el evento abierto es para crear un nuevo objeto o para abrir un objeto existente:

- Si el evento abierto es una solicitud abierta para crear un nuevo objeto (archivo o directorio), el `HandleID` La etiqueta del evento XML de auditoría muestra un campo vacío `HandleID` (por ejemplo: `<Data Name="HandleID">0000000000000000;00;00000000;00000000</Data>`).

La `HandleID` Está vacío porque la solicitud ABIERTA (para crear un nuevo objeto) se audita antes de que se produzca la creación real del objeto y antes de que exista un controlador. Los eventos auditados posteriores del mismo objeto tienen el control de objeto correcto en `HandleID` etiquetar.

- Si el evento abierto es una solicitud abierta para abrir un objeto existente, el evento de auditoría tendrá el

controlador asignado de ese objeto en el `HandleID` tag (por ejemplo: `<Data Name="HandleID">00000000000401;00;000000ea;00123ed4</Data>`).

Determine cuál es la ruta completa al objeto auditado

Ruta del objeto impresa en `<ObjectName>` la etiqueta de un registro de auditoría contiene el nombre del volumen (entre paréntesis) y la ruta relativa desde la raíz del volumen que contiene. Si desea determinar la ruta completa del objeto auditado, incluida la ruta de unión, hay algunos pasos que debe seguir.

Pasos

- 1. Para determinar el nombre del volumen y la ruta relativa al objeto auditado, consulte la `<ObjectName>` etiqueta el evento de auditoría.

En este ejemplo, el nombre del volumen es "data1" y la ruta relativa al archivo es `/dir1/file.txt`:

```
<Data Name="ObjectName"> (data1);/dir1/file.txt </Data>
```

- 2. Con el nombre del volumen determinado en el paso anterior, determine cuál es la ruta de unión para el volumen que contiene el objeto auditado:

En este ejemplo, el nombre del volumen es "data1" y la ruta de unión del volumen que contiene el objeto auditado es `/data/data1`:

```
volume show -junction -volume data1
```

| | | Junction | | Junction | |
|---------|--------|-------------|--------|---------------|-------------|
| Vserver | Volume | Language | Active | Junction Path | Path Source |
| vs1 | data1 | en_US.UTF-8 | true | /data/data1 | RW_volume |

- 3. Determine la ruta completa al objeto auditado anexando la ruta relativa que se encuentra en `<ObjectName>` etiqueta la ruta de unión para el volumen.

En este ejemplo, la ruta de unión para el volumen:

```
/data/data1/dir1/file.text
```

Consideraciones al auditar enlaces simbólicos y enlaces duros

Hay ciertas consideraciones que usted debe tener en cuenta al auditar enlaces simbólicos y vínculos duros.

Un registro de auditoría contiene información sobre el objeto que se está auditando, incluida la ruta al objeto auditado, que se identifica en la `ObjectName` etiquetar. Usted debe ser consciente de cómo los caminos para enlaces simbólicos y enlaces duros se graban en el `ObjectName` etiquetar.

Enlaces simbólicos

Un symlink es un archivo con un inodo independiente que contiene un puntero a la ubicación de un objeto de destino, conocido como el destino. Al acceder a un objeto mediante un enlace simbólico, ONTAP interpreta automáticamente el enlace simbólico y sigue la ruta real independiente del protocolo canónico al objeto de destino del volumen.

En el siguiente ejemplo de salida, hay dos enlaces simbólicos, ambos apuntando a un archivo llamado `target.txt`. Uno de los enlaces simbólicos es un enlace simbólico relativo y uno es un enlace absoluto. Si cualquiera de los enlaces simbólicos se auditan, el `ObjectName` etiqueta en el evento de auditoría contiene la ruta al archivo `target.txt`:

```
[root@host1 audit]# ls -l
total 0
lrwxrwxrwx 1 user1 group1 37 Apr  2 10:09 softlink_fullpath.txt ->
/data/audit/target.txt
lrwxrwxrwx 1 user1 group1 10 Apr  2 09:54 softlink.txt -> target.txt
-rwxrwxrwx 1 user1 group1 16 Apr  2 10:05 target.txt
```

Vínculos duros

Un vínculo rígido es una entrada de directorio que asocia un nombre a un archivo existente en un sistema de archivos. El enlace rígido apunta a la ubicación del inodo del archivo original. De forma similar a cómo ONTAP interpreta los enlaces simbólicos, ONTAP interpreta el vínculo duro y sigue la ruta canónica real al objeto de destino del volumen. Cuando se audita el acceso a un objeto de vínculo duro, el evento de auditoría registra esta ruta canónica absoluta en el `ObjectName` etiquetar en lugar de la ruta de enlace rígida.

Consideraciones al auditar flujos de datos NTFS alternativos

Hay ciertas consideraciones que debe tener en cuenta al auditar archivos con flujos de datos alternativos NTFS.

La ubicación de un objeto que se va a auditar se registra en un registro de eventos mediante dos etiquetas, la `ObjectName` etiqueta (la ruta) y el `HandleID` etiqueta (el asa). Para identificar correctamente qué solicitudes de flujo se están registrando, debe tener en cuenta qué registros de ONTAP hay en estos campos para flujos de datos alternativos NTFS:

- ID DE EVT: 4656 eventos (abrir y crear eventos de auditoría)
 - La ruta de la secuencia de datos alternativa se registra en la `ObjectName` etiquetar.
 - El controlador de la secuencia de datos alternativa se registra en la `HandleID` etiquetar.
- ID DE EVT: 4663 eventos (el resto de eventos de auditoría, como leído, Write, getattr, etc.)
 - La ruta del archivo base, no la secuencia de datos alternativa, se registra en la `ObjectName` etiquetar.
 - El controlador de la secuencia de datos alternativa se registra en la `HandleID` etiquetar.

Ejemplo

El ejemplo siguiente ilustra cómo identificar EVT ID: Eventos 4663 para flujos de datos alternativos mediante el `HandleID` etiquetar. Aunque la `ObjectName` etiqueta (ruta) registrada en el evento de auditoría de lectura es en la ruta de acceso del archivo base, la `HandleID` la etiqueta se puede utilizar para identificar el evento

como un registro de auditoría para la corriente de datos alternativa.

Los nombres de los archivos de flujo toman el formulario `base_file_name:stream_name`. En este ejemplo, la `dir1` el directorio contiene un archivo base con una secuencia de datos alternativa que tiene las siguientes rutas:

```
/dir1/file1.txt  
/dir1/file1.txt:stream1
```



El resultado del ejemplo de evento siguiente se truncará como se indica; la salida no muestra todas las etiquetas de salida disponibles para los eventos.

Para un ID de EVTX 4656 (evento de auditoría abierto), la salida de registro de auditoría para la corriente de datos alternativa registra el nombre de la corriente de datos alternativa en `ObjectName` etiqueta:

```
- <Event>  
- <System>  
  <Provider Name="Netapp-Security-Auditing" />  
  <EventID>4656</EventID>  
  <EventName>Open Object</EventName>  
  [...]  
</System>  
- <EventData>  
  [...]  
  **<Data Name="ObjectType">Stream</Data>  
  <Data Name="HandleID">000000000000401;00;000001e4;00176767</Data>  
  <Data Name="ObjectName">\(data1\);/dir1/file1.txt:stream1</Data>  
  **  
  [...]  
</EventData>  
</Event>  
- <Event>
```

Para un ID de EVTX 4663 (evento de auditoría de lectura), la salida de registro de auditoría de la misma corriente de datos alternativa registra el nombre del archivo base en `ObjectName` sin embargo, el `HandleID` tag es el identificador de la secuencia de datos alternativa y se puede utilizar para correlacionar este evento con la secuencia de datos alternativa:

```

- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4663</EventID>
  <EventName>Read Object</EventName>
  [...]
</System>
- <EventData>
  [...]
  **<Data Name="ObjectType">Stream</Data>
  <Data Name="HandleID">000000000000401;00;000001e4;00176767</Data>
  <Data Name="ObjectName">\\(data1\\);/dir1/file1.txt</Data> **
  [...]
</EventData>
</Event>
- <Event>

```

Eventos de acceso a archivos y directorios NFS que se pueden auditar

ONTAP puede auditar determinados eventos de acceso a archivos y directorios NFS. Saber qué eventos de acceso se pueden auditar es útil cuando se interpretan los resultados de los registros de eventos de auditoría convertidos.

Puede auditar los siguientes eventos de acceso a archivos NFS y directorio:

- LEA
- ABIERTO
- CIERRE
- ESCALERA DE MANO
- ESCRITURA
- SETATTR
- CREE
- ENLACE
- OPENATTR
- QUITAR
- GETATTR
- VERIFICACIÓN
- NVERIFICAR
- CAMBIAR EL NOMBRE

Para auditar de forma fiable los eventos de CAMBIO de NOMBRE de NFS, debe configurar los ACE de auditoría en los directorios en lugar de en los archivos porque no se comprueba si hay una operación DE CAMBIO de NOMBRE si los permisos de directorio son suficientes.

Planifique la configuración de auditoría

Antes de configurar la auditoría de máquinas virtuales de almacenamiento (SVM), debe comprender qué opciones de configuración están disponibles y planificar los valores que desea establecer para cada opción. Esta información puede ayudarle a configurar la configuración de auditoría que se ajuste a sus necesidades empresariales.

Hay ciertos parámetros de configuración que son comunes a todas las configuraciones de auditoría.

Además, existen ciertos parámetros que se pueden utilizar para especificar qué métodos se utilizan al girar los registros de auditoría consolidados y convertidos. Puede especificar uno de los tres métodos siguientes al configurar la auditoría:

- Rotar registros según el tamaño del registro
 - Rotar registros según un programa
 - Rotar registros según el tamaño del registro y la programación (el evento que ocurra primero)
- F

Siempre debe establecerse al menos uno de los métodos de rotación de log.

Parámetros comunes a todas las configuraciones de auditoría

Hay dos parámetros necesarios que debe especificar al crear la configuración de auditoría. También puede especificar tres parámetros opcionales:

| Tipo de información | Opción | Obligatorio | Incluya | Sus valores |
|--|------------------------------------|-------------|---------|-------------|
| <i>SVM name</i> Nombre de la SVM en la que se creará la configuración de auditoría. La SVM ya debe existir. | <code>-vserver vserver_name</code> | Sí | Sí | |

| | | | | |
|---|-------------------|----|----|--|
| <p><i>Ruta de destino del registro</i></p> <p>Especifica el directorio en el que se almacenan los registros de auditoría convertidos, normalmente un volumen o qtree dedicados. La ruta ya debe existir en el espacio de nombres de la SVM.</p> <p>La ruta puede tener hasta 864 caracteres y debe tener permisos de lectura y escritura.</p> <p>Si la ruta no es válida, el comando de configuración de auditoría falla.</p> <p>Si la SVM es un origen de recuperación ante desastres de SVM, la ruta de destino de registros no puede estar en el volumen raíz. Esto se debe a que el contenido del volumen raíz no se replica en el destino de recuperación ante desastres.</p> <p>No se puede utilizar un volumen de FlexCache como destino del registro (ONTAP 9.7 y versiones posteriores).</p> | -destination text | Sí | Sí | |
|---|-------------------|----|----|--|

| | | | | |
|---|---------------------------------------|---------------------------------------|---------------------------------|--------------------------------|
| <p><i>Categorías de eventos para auditar</i></p> <p>Especifica las categorías de eventos que se van a auditar. Se pueden auditar las siguientes categorías de eventos:</p> <ul style="list-style-type: none"> • Eventos de acceso a los archivos (SMB y NFSv4) • Eventos de inicio y cierre de sesión en SMB • Eventos de configuración de directivas de acceso central <p>Los eventos de almacenamiento provisional de políticas de acceso central están disponibles a partir de los dominios de Active Directory de Windows 2012.</p> <ul style="list-style-type: none"> • Eventos de categoría de recursos compartidos de archivos • Auditar eventos de cambio de directivas • Eventos de gestión de cuentas de usuario local • Eventos de gestión del grupo de seguridad • Eventos de cambio de directiva de autorización <p>El valor predeterminado es auditar el acceso a archivos y los eventos de inicio y cierre de sesión de SMB.</p> <p>Nota: antes de poder especificar <code>cap-staging</code> Como categoría de evento, debe existir un servidor SMB en la SVM. Aunque puede habilitar la configuración de directivas de acceso central en la configuración de auditoría sin habilitar Dynamic Access Control en el servidor SMB, los eventos de configuración de directivas de acceso central sólo se generan si el control de acceso dinámico está habilitado. El control de acceso dinámico se activa mediante una opción de servidor SMB. No está habilitado de forma predeterminada.</p> | <p><code>-events {file-ops</code></p> | <p><code>cifs-logon-logoff</code></p> | <p><code>cap-staging</code></p> | <p><code>file-share</code></p> |
|---|---------------------------------------|---------------------------------------|---------------------------------|--------------------------------|

| | | | | |
|---------------------|--------------|--|------------------------------|-------|
| audit-policy-change | user-account | security-group | authorization-policy-change} | No |
| | | <p><i>Formato de salida del archivo de registro</i></p> <p>Determina el formato de salida de los registros de auditoría. El formato de salida puede ser específico de ONTAP XML O Microsoft Windows EVTX formato de registro. De forma predeterminada, el formato de salida es EVTX.</p> | -format {xml | evtx} |

| | | | |
|----|--|---|---------------------------------------|
| No | | <p><i>Límite de rotación de los archivos de registro</i></p> <p>Determina cuántos archivos de registro de auditoría se retendrán antes de rotar el archivo de registro más antiguo. Por ejemplo, si introduce un valor de 5, se conservan los cinco últimos archivos de registro.</p> <p>Valor de 0 indica que se conservan todos los archivos de registro. El valor predeterminado es 0.</p> | <p>-rotate -limit integer</p> |
|----|--|---|---------------------------------------|

Parámetros que se utilizan para determinar cuándo rotar registros de eventos de auditoría

Rotar registros según el tamaño del registro

El valor predeterminado es girar los registros de auditoría en función del tamaño.

- El tamaño predeterminado del registro es 100 MB
- Si desea utilizar el método de rotación de registro predeterminado y el tamaño de registro predeterminado, no necesita configurar ningún parámetro específico para la rotación de registros.
- Si desea rotar los registros de auditoría según un tamaño de registro solo, utilice el siguiente comando para anular la definición del `-rotate-schedule-minute` parámetro: `vserver audit modify -vserver vs0 -destination / -rotate-schedule-minute -`

Si no desea utilizar el tamaño predeterminado del registro, puede configurar el `-rotate-size` parámetro para especificar un tamaño de registro personalizado:

| Tipo de información | Opción | Obligatorio | Incluya | Sus valores |
|--|--|-------------|---------|-------------|
| <i>Límite de tamaño de archivo de registro</i> Determina el límite de tamaño del archivo del registro de auditoría. | <code>-rotate-size {integer}[KB</code> | MB | GB | TB |

Rotar registros en función de un horario

Si opta por rotar los registros de auditoría según una programación, puede programar la rotación del registro utilizando los parámetros de rotación basados en tiempo en cualquier combinación.

- Si utiliza rotación basada en tiempo, el `-rotate-schedule-minute` el parámetro es obligatorio.
- Todos los demás parámetros de rotación basados en el tiempo son opcionales.
- El programa de rotación se calcula utilizando todos los valores relacionados con el tiempo.

Por ejemplo, si especifica solo el `-rotate-schedule-minute` parámetro, los archivos de registro de auditoría se rotan en función de los minutos especificados en todos los días de la semana, durante todas las horas en todos los meses del año.

- Si especifica solo uno o dos parámetros de rotación basados en la hora (por ejemplo, `-rotate-schedule-month` y.. `-rotate-schedule-minutes`), los archivos de registro se rotan en función de los valores de minutos que haya especificado en todos los días de la semana, durante todas las horas, pero sólo durante los meses especificados.

Por ejemplo, puede especificar que el registro de auditoría se va a rotar durante los meses de enero, marzo y agosto todos los lunes, miércoles y sábados a las 10:30 a.m.

- Si especifica valores para ambos `-rotate-schedule-dayofweek` y.. `-rotate-schedule-day`, se consideran independientes.

Por ejemplo, si especifica `-rotate-schedule-dayofweek` Como viernes y. `-rotate-schedule-day` Como 13, los registros de auditoría se girarían cada viernes y el día 13 del mes especificado, no sólo cada viernes 13.

- Si desea rotar los registros de auditoría según una programación solo, se debe utilizar el siguiente comando para anular la definición del `-rotate-size` parámetro: `vserver audit modify -vserver vs0 -destination / -rotate-size -`

Puede utilizar la siguiente lista de parámetros de auditoría disponibles para determinar qué valores utilizar para configurar una programación para las rotaciones del registro de eventos de auditoría:

| Tipo de información | Opción | Obligatorio | Incluya | Sus valores |
|---|---|-------------|---------|-------------|
| <p><i>Registro del programa de rotación: Mes</i></p> <p>Determina la programación mensual para registros de auditoría giratorios.</p> <p>Los valores válidos son <code>January</code> por <code>December</code>, y <code>all</code>. Por ejemplo, puede especificar que el registro de auditoría se va a rotar durante los meses enero, marzo y agosto.</p> | <p><code>-rotate-schedule-month</code> <code>chron_month</code></p> | No | | |
| <p><i>Registro del programa de rotación: Día de la semana</i></p> <p>Determina la programación diaria (día de la semana) para los registros de auditoría giratorios.</p> <p>Los valores válidos son <code>Sunday</code> por <code>Saturday</code>, y <code>all</code>. Por ejemplo, puede especificar que el registro de auditoría se gire los martes y viernes o durante todos los días de una semana.</p> | <p><code>-rotate-schedule-dayofweek</code> <code>chron_dayofweek</code></p> | No | | |
| <p><i>Registro del programa de rotación: Día</i></p> <p>Determina el día del programa del mes para rotar el registro de auditoría.</p> <p>Los valores válidos van desde 1 por 31. Por ejemplo, puede especificar que el registro de auditoría se va a rotar los días 10 y 20 del mes, o todos los días del mes.</p> | <p><code>-rotate-schedule-day</code> <code>chron_dayofmonth</code></p> | No | | |

| | | | | |
|---|---|---|--|--|
| <p>Registro de la rotación del programa: Hora</p> <p>Determina la programación horaria para rotar el registro de auditoría.</p> <p>Los valores válidos van desde 0 (medianoche) a. 23 (a las 11:00). Especificando <code>all</code> gira los registros de auditoría cada hora. Por ejemplo, puede especificar que el registro de auditoría se gire a las 6 (6 a.m.) y 18 (6 p.m.).</p> | <p><code>-rotate-schedule-hour</code> <code>chron_hour</code></p> | No | | |
| <p>Registro del programa de rotación: Minuto</p> <p>Determina la programación de minutos para rotar el registro de auditoría.</p> <p>Los valores válidos van desde 0 para 59. Por ejemplo, puede especificar que el registro de auditoría se va a rotar a 30 minutos.</p> | <p><code>-rotate-schedule-minute</code> <code>chron_minute</code></p> | Sí, si se configura la rotación del registro basada en horario; de lo contrario, no | | |

Rotar registros según el tamaño del registro y el horario

Puede elegir girar los archivos de registro según el tamaño del registro y una programación configurando ambos `-rotate-size` parámetros y parámetros de rotación basados en tiempo en cualquier combinación. Por ejemplo: Si `-rotate-size` Se establece en 10 MB y. `-rotate-schedule-minute` Se establece en 15, los archivos de registro giran cuando el tamaño del archivo de registro alcanza 10 MB o en el 15 minuto de cada hora (el evento que ocurra primero).

Cree una configuración de auditoría de archivos y directorios en las SVM

Cree la configuración de auditoría

La creación de una configuración de auditoría de archivos y directorios en la máquina virtual de almacenamiento (SVM) incluye comprender las opciones de configuración disponibles, planificar la configuración y, a continuación, configurar y habilitar la configuración. A continuación, puede mostrar información sobre la configuración de auditoría para confirmar que la configuración resultante es la configuración deseada.

Antes de comenzar a auditar los eventos del archivo y el directorio, debe crear una configuración de auditoría en la máquina virtual de almacenamiento (SVM).

Antes de empezar

Si piensa en crear una configuración de auditoría para la configuración de la política de acceso central, debe haber un servidor SMB en la SVM.



- Aunque puede habilitar la configuración de directivas de acceso central en la configuración de auditoría sin habilitar Dynamic Access Control en el servidor SMB, los eventos de configuración de directivas de acceso central sólo se generan si el control de acceso dinámico está habilitado.

El control de acceso dinámico se activa mediante una opción de servidor SMB. No está habilitado de forma predeterminada.

- Si los argumentos de un campo en un comando no son válidos, por ejemplo, entradas no válidas para campos, entradas duplicadas y entradas no existentes, el comando falla antes de la fase de auditoría.

Estos errores no generan un registro de auditoría.

Acerca de esta tarea

Si la SVM es un origen de recuperación ante desastres de SVM, la ruta de destino no puede estar en el volumen raíz.

Paso

1. Con la información de la hoja de trabajo de planificación, cree la configuración de auditoría para rotar los registros de auditoría según el tamaño del registro o una programación:

| | |
|---|--|
| Si desea rotar registros de auditoría en... | Introduzca... |
| Tamaño del registro | `vserver audit create -vserver vserver_name -destination path -events [{file-ops |
| cifs-logon-logoff | cap-staging |
| file-share | authorization-policy-change |
| user-account | security-group |
| authorization-policy-change}] [-format {xml | evtx}] [-rotate-limit integer] [-rotate-size {integer[KB |
| MB | GB |
| TB | PB]}` |
| Un programa | `vserver audit create -vserver vserver_name -destination path -events [{file-ops |
| cifs-logon-logoff | cap-staging}] [-format {xml |

Ejemplos

En el ejemplo siguiente se crea una configuración de auditoría que audita las operaciones de archivos y los eventos de inicio y cierre de sesión de SMB (el valor predeterminado) mediante la rotación basada en tamaño. El formato de registro es `EVTX` (el valor predeterminado). Los registros se almacenan en la `/audit_log` directorio. El límite de tamaño del archivo de registro es 200 MB. Los registros se giran cuando alcanzan los 200 MB de tamaño:

```
cluster1::> vservers audit create -vservers vs1 -destination /audit_log
-rotate-size 200MB
```

En el ejemplo siguiente se crea una configuración de auditoría que audita las operaciones de archivos y los eventos de inicio y cierre de sesión de SMB (el valor predeterminado) mediante la rotación basada en tamaño. El formato de registro es `EVTX` (el valor predeterminado). Los registros se almacenan en la `/cifs_event_logs` directorio. El límite de tamaño del archivo de registro es 100 MB (el valor predeterminado), y el límite de rotación del registro es 5:

```
cluster1::> vservers audit create -vservers vs1 -destination
/cifs_event_logs -rotate-limit 5
```

En el ejemplo siguiente se crea una configuración de auditoría que audita las operaciones de archivos, los eventos de inicio y cierre de sesión de CIFS y los eventos de almacenamiento provisional de directivas de acceso central mediante rotación basada en tiempo. El formato de registro es `EVTX` (el valor predeterminado). Los registros de auditoría se rotan mensualmente, a las 12:30 p.m. en todos los días de la semana. El límite de rotación del registro es 5:

```
cluster1::> vservers audit create -vservers vs1 -destination /audit_log
-events file-ops,cifs-logon-logoff,file-share,audit-policy-change,user-
account,security-group,authorization-policy-change,cap-staging -rotate
-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule-hour
12 -rotate-schedule-minute 30 -rotate-limit 5
```

Habilite la auditoría en la SVM

Después de terminar de configurar la auditoría, debe habilitar la auditoría en la máquina virtual de almacenamiento (SVM).

Lo que necesitará

La configuración de auditoría de SVM ya debe existir.

Acerca de esta tarea

Cuando se inicia por primera vez una configuración de descarte de ID de recuperación de desastres de SVM (una vez finalizada la inicialización de SnapMirror) y la SVM tiene una configuración de auditoría, ONTAP deshabilita automáticamente la configuración de auditoría. La auditoría se deshabilita en la SVM de solo lectura para evitar que los volúmenes provisionales se llenen. Solo puede habilitar la auditoría después de que se rompa la relación de SnapMirror y de que la SVM sea de lectura y escritura.

Paso

1. Habilitar la auditoría en la SVM:

```
vservers audit enable -vservers vservers_name

vservers audit enable -vservers vs1
```

Compruebe la configuración de auditoría

Después de completar la configuración de auditoría, debe comprobar que la auditoría está configurada correctamente y que está activada.

Pasos

1. Compruebe la configuración de auditoría:

```
vserver audit show -instance -vserver vserver_name
```

El siguiente comando aparece de una lista de todas las auditorías de la información de configuración de la máquina virtual de almacenamiento (SVM) vs1:

```
vserver audit show -instance -vserver vs1
```

```
Vserver: vs1
Auditing state: true
Log Destination Path: /audit_log
Categories of Events to Audit: file-ops
Log Format: evt
Log File Size Limit: 200MB
Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
Log Rotation Schedule: Day: -
Log Rotation Schedule: Hour: -
Log Rotation Schedule: Minute: -
Rotation Schedules: -
Log Files Rotation Limit: 0
```

Configurar directivas de auditoría de archivos y carpetas

Configurar directivas de auditoría de archivos y carpetas

Implementar la auditoría en eventos de acceso a archivos y carpetas es un proceso de dos pasos. En primer lugar, debe crear y habilitar una configuración de auditoría en las máquinas virtuales de almacenamiento (SVM). En segundo lugar, debe configurar políticas de auditoría en los archivos y carpetas que desea supervisar. Es posible configurar políticas de auditoría para supervisar los intentos de acceso correctos y los fallidos.

Puede configurar directivas de auditoría de SMB y NFS. Las políticas de auditoría de SMB y NFS tienen distintos requisitos de configuración y funcionalidades de auditoría.

Si se configuran las políticas de auditoría adecuadas, ONTAP supervisa los eventos de acceso SMB y NFS tal como se especifica en las políticas de auditoría solo si se ejecutan los servidores SMB o NFS.

Configurar directivas de auditoría en directorios y archivos de seguridad NTFS

Para poder auditar operaciones de archivo y directorio, debe configurar políticas de auditoría en los archivos y directorios para los que desea recopilar información de auditoría. Esto se suma a la configuración y habilitación de la auditoría. Puede configurar políticas de auditoría de NTFS mediante la ficha Seguridad de Windows o mediante la interfaz de línea de comandos de ONTAP.

Configuración de directivas de auditoría NTFS mediante la ficha Seguridad de Windows

Puede configurar directivas de auditoría NTFS en archivos y directorios mediante la ficha **Seguridad de Windows** de la ventana Propiedades de Windows. Este es el mismo método que se utiliza al configurar directivas de auditoría en datos que residen en un cliente de Windows, lo que permite utilizar la misma interfaz gráfica de usuario que está acostumbrado a utilizar.

Lo que necesitará

La auditoría debe configurarse en la máquina virtual de almacenamiento (SVM) que contenga los datos a los que se aplican las listas de control de acceso del sistema (SACL).

Acerca de esta tarea

La configuración de directivas de auditoría NTFS se realiza agregando entradas a SACL NTFS que están asociadas con un descriptor de seguridad NTFS. El descriptor de seguridad se aplica entonces a los archivos y directorios NTFS. La interfaz gráfica de usuario de Windows se encarga automáticamente de estas tareas. El descriptor de seguridad puede contener listas de control de acceso discrecional (DACL) para aplicar permisos de acceso a archivos y carpetas, SACL para auditoría de archivos y carpetas o SACL y DACL.

Para establecer directivas de auditoría NTFS mediante la ficha Seguridad de Windows, siga los pasos que se indican a continuación en un host de Windows:

Pasos

1. En el menú **Herramientas** del Explorador de Windows, seleccione **asignar unidad de red**.
2. Complete el cuadro **Unidad de red de mapas**:

a. Seleccione una letra **Unidad**.

b. En el cuadro **carpeta**, escriba el nombre del servidor SMB que contiene el recurso compartido, manteniendo los datos que desea auditar y el nombre del recurso compartido.

Puede especificar la dirección IP de la interfaz de datos para el servidor SMB en lugar del nombre del servidor SMB.

Si el nombre de su servidor SMB es «MMB_SERVER» y su cuota se denomina «shara1», debe introducir \\SMB_SERVER\share1.

c. Haga clic en **Finalizar**.

La unidad seleccionada está montada y lista con la ventana del Explorador de Windows que muestra archivos y carpetas contenidos en el recurso compartido.

3. Seleccione el archivo o directorio para el que desea habilitar el acceso de auditoría.
4. Haga clic con el botón secundario del ratón en el archivo o directorio y seleccione **Propiedades**.
5. Seleccione la ficha **Seguridad**.

6. Haga clic en **Avanzado**.
7. Seleccione la ficha **Auditoría**.
8. Realice las acciones deseadas:

| Si quieres | Haga lo siguiente |
|---|---|
| Configurar la auditoría para un nuevo usuario o grupo | <ol style="list-style-type: none"> a. Haga clic en Agregar. b. En el cuadro Escriba el nombre del objeto que desea seleccionar , escriba el nombre del usuario o grupo que desea agregar. c. Haga clic en Aceptar. |
| Quitar la auditoría de un usuario o grupo | <ol style="list-style-type: none"> a. En el cuadro Escriba el nombre del objeto que desea seleccionar , seleccione el usuario o el grupo que desea eliminar. b. Haga clic en Quitar. c. Haga clic en Aceptar. d. Omitir el resto de este procedimiento. |
| Auditoría de cambios para un usuario o grupo | <ol style="list-style-type: none"> a. En el cuadro Escriba el nombre del objeto que desea seleccionar , seleccione el usuario o el grupo que desea cambiar. b. Haga clic en Editar. c. Haga clic en Aceptar. |

Si va a configurar la auditoría de un usuario o grupo o si va a cambiar la auditoría de un usuario o grupo existente, se abre el cuadro Entrada de auditoría de <objeto>.

9. En el cuadro **aplicar a**, seleccione cómo desea aplicar esta entrada de auditoría.

Puede seleccionar una de las siguientes opciones:

- **Esta carpeta, subcarpetas y archivos**
- **Esta carpeta y subcarpetas**
- **Sólo esta carpeta**
- **Esta carpeta y archivos**
- **Sólo subcarpetas y archivos**
- **Sólo subcarpetas**
- **Solo archivos**

Si está configurando la auditoría en un solo archivo, la casilla **Aplicar a** no está activa. El valor del cuadro **aplicar a** se establece de forma predeterminada en **este objeto sólo**.



Dado que la auditoría requiere recursos de SVM, seleccione solo el nivel mínimo que proporciona los eventos de auditoría que cumplen sus requisitos de seguridad.

10. En el cuadro **Access**, seleccione lo que desea auditar y si desea auditar eventos, eventos de error o

ambos correctos.

- Para auditar eventos correctos, seleccione el cuadro éxito.
- Para auditar eventos de error, seleccione el cuadro error.

Seleccione sólo las acciones que necesite supervisar para cumplir sus requisitos de seguridad. Para obtener más información acerca de estos eventos auditables, consulte la documentación de Windows. Puede auditar los siguientes eventos:

- **Control total**
- **Carpeta Traverse / archivo de ejecución**
- **Lista de carpetas / lectura de datos**
- **Leer atributos**
- **Leer atributos extendidos**
- **Crear archivos / escribir datos**
- **Crear carpetas / anexar datos**
- **Escribir atributos**
- **Escriba atributos extendidos**
- **Eliminar subcarpetas y archivos**
- **Eliminar**
- **Leer permisos**
- **Cambiar permisos**
- **Tome la propiedad**

11. Si no desea que la configuración de auditoría se propague a los archivos y carpetas posteriores del contenedor original, seleccione la casilla **aplicar estas entradas de auditoría a objetos y/o contenedores dentro de este contenedor únicamente** .

12. Haga clic en **aplicar**.

13. Cuando termine de agregar, eliminar o editar entradas de auditoría, haga clic en **Aceptar**.

Se cierra el cuadro Entrada de auditoría para <object>.

14. En el cuadro **Auditoría**, seleccione la configuración de herencia de esta carpeta.

Seleccione sólo el nivel mínimo que proporciona los eventos de auditoría que cumplen sus requisitos de seguridad. Puede elegir una de las siguientes opciones:

- Seleccione incluir entradas de auditoría heredables en el cuadro primario de este objeto.
- Seleccione el cuadro Reemplazar todas las entradas de auditoría heredables existentes en todos los descendientes con entradas de auditoría heredables de este objeto.
- Seleccione ambas casillas.
- Seleccione ninguna casilla.

Si está configurando SACL en un único archivo, el cuadro Reemplazar todas las entradas de auditoría heredables existentes en todos los descendientes con entradas de auditoría heredables de este objeto no está presente en el cuadro Auditoría .

15. Haga clic en **Aceptar**.

Se cierra el cuadro Auditoría.

Configurar políticas de auditoría de NTFS mediante la interfaz de línea de comandos de ONTAP

Puede configurar políticas de auditoría en archivos y carpetas mediante la interfaz de línea de comandos de ONTAP. Esto le permite configurar políticas de auditoría NTFS sin necesidad de conectarse a los datos mediante un recurso compartido SMB en un cliente Windows.

Puede configurar directivas de auditoría NTFS mediante el `vserver security file-directory` familia de comandos.

Sólo puede configurar SACL NTFS mediante la CLI. La configuración de SACL de NFSv4 no es compatible con esta familia de comandos de ONTAP. Consulte las páginas del manual para obtener más información acerca del uso de estos comandos para configurar y agregar SACL NTFS a archivos y carpetas.

Configurar la auditoría para directorios y archivos de estilo de seguridad UNIX

Para configurar la auditoría de directorios y archivos de estilo de seguridad de UNIX, debe añadir ACE de auditoría a NFSv4.x ACL. Esto le permite supervisar determinados eventos de acceso a archivos y directorios de NFS con fines de seguridad.

Acerca de esta tarea

Para NFSv4.x, tanto los valores ACs discrecionales como los del sistema se almacenan en la misma ACL. No se almacenan en DACL y SACL independientes. Por lo tanto, debe tener cuidado al agregar ACE de auditoría a una ACL existente para evitar sobrescribir y perder una ACL existente. El orden en el que se agregan los ACE de auditoría a una ACL existente no importa.

Pasos

1. Recupere la ACL existente para el archivo o directorio mediante el `nfs4_getfacl` o comando equivalente.

Para obtener más información sobre la manipulación de ACL, consulte las páginas de manual del cliente NFS.

2. Añada las ACE de auditoría deseadas.
3. Aplique la ACL actualizada al archivo o directorio mediante `nfs4_setfacl` o comando equivalente.

Muestra información sobre las directivas de auditoría aplicadas a los archivos y directorios

Muestra información sobre las directivas de auditoría mediante la ficha Seguridad de Windows

Puede mostrar información acerca de las directivas de auditoría que se han aplicado a archivos y directorios mediante la ficha Seguridad de la ventana Propiedades de Windows. Este es el mismo método utilizado para los datos que se encuentran en un servidor de Windows, con el que los clientes pueden utilizar la misma interfaz gráfica de usuario que están acostumbrados a utilizar.

Acerca de esta tarea

La visualización de información acerca de las directivas de auditoría aplicadas a archivos y directorios permite verificar que se han establecido las listas de control de acceso del sistema (SACL) adecuadas en archivos y

carpetas especificados.

Para mostrar información acerca de SACL que se han aplicado a archivos y carpetas NTFS, lleve a cabo los siguientes pasos en un host de Windows.

Pasos

1. En el menú **Herramientas** del Explorador de Windows, seleccione **asignar unidad de red**.
2. Complete el cuadro de diálogo **asignar unidad de red**:
 - a. Seleccione una letra **Unidad**.
 - b. En el cuadro **carpeta**, escriba la dirección IP o el nombre del servidor SMB de la máquina virtual de almacenamiento (SVM) que contiene el recurso compartido que contiene tanto los datos que desea auditar como el nombre del recurso compartido.

Si el nombre de su servidor SMB es «MMB_SERVER» y su cuota se denomina «shara1», debe introducir \\SMB_SERVER\share1.



Puede especificar la dirección IP de la interfaz de datos para el servidor SMB en lugar del nombre del servidor SMB.

- c. Haga clic en **Finalizar**.

La unidad seleccionada está montada y lista con la ventana del Explorador de Windows que muestra archivos y carpetas contenidos en el recurso compartido.

3. Seleccione el archivo o directorio para el que se muestra información de auditoría.
4. Haga clic con el botón derecho del ratón en el archivo o directorio y seleccione **Propiedades**.
5. Seleccione la ficha **Seguridad**.
6. Haga clic en **Avanzado**.
7. Seleccione la ficha **Auditoría**.
8. Haga clic en **continuar**.

Se abre el cuadro Auditoría. El cuadro **Entradas de auditoría** muestra un resumen de los usuarios y grupos que tienen SACL aplicados a ellos.

9. En el cuadro **Entradas de auditoría**, seleccione el usuario o grupo cuyas entradas de SACL desee mostrar.
10. Haga clic en **Editar**.

Se abre el cuadro Entrada de auditoría para <object>.

11. En el cuadro **Access**, vea las SACL actuales que se aplican al objeto seleccionado.
12. Haga clic en **Cancelar** para cerrar el cuadro **Entrada de auditoría para <object>**.
13. Haga clic en **Cancelar** para cerrar el cuadro **Auditoría**.

Muestra información sobre las políticas de auditoría de NTFS en los volúmenes de FlexVol usando la interfaz de línea de comandos

Puede mostrar información acerca de las directivas de auditoría NTFS en los volúmenes FlexVol, incluidos los estilos de seguridad y los estilos de seguridad efectivos, los

permisos que se aplican e información acerca de las listas de control de acceso al sistema. Puede utilizar la información para validar la configuración de seguridad o para solucionar problemas de auditoría.

Acerca de esta tarea

La visualización de información acerca de las directivas de auditoría aplicadas a archivos y directorios permite verificar que se han establecido las listas de control de acceso del sistema (SACL) adecuadas en archivos y carpetas especificados.

Debe proporcionar el nombre de la máquina virtual de almacenamiento (SVM) y la ruta a los archivos o carpetas cuya información de auditoría desee mostrar. Puede mostrar el resultado en forma de resumen o como una lista detallada.

- Los volúmenes y qtrees de estilo de seguridad NTFS sólo utilizan listas de control de acceso al sistema (SACL) NTFS para las directivas de auditoría.
- Los archivos y carpetas de un volumen mixto de estilo de seguridad con seguridad efectiva NTFS pueden tener directivas de auditoría NTFS aplicadas.

Los volúmenes y qtrees de estilo de seguridad mixtos pueden contener archivos y directorios que utilizan permisos de archivo de UNIX, bits de modo o ACL de NFSv4 y algunos archivos y directorios que utilizan permisos de archivo NTFS.

- El nivel superior de un volumen de estilo de seguridad mixto puede tener seguridad efectiva de UNIX o NTFS y puede que no contenga SACL NTFS.
- Debido a que la seguridad de Access Guard a nivel de almacenamiento se puede configurar en un volumen o qtree de estilo de seguridad mixto incluso si el estilo de seguridad efectivo del volumen raíz o qtree es UNIX, El resultado de una ruta de volumen o qtree en la que se configuró Storage-Level Access Guard puede mostrar tanto el archivo normal como la carpeta NFSv4 SACL y Storage-Level Access Guard NTFS SACL.
- Si la ruta de acceso que se introduce en el comando es para los datos con seguridad efectiva NTFS, la salida también muestra información sobre los ACE de control dinámico de acceso si el Control dinámico de acceso está configurado para la ruta de acceso del archivo o directorio dada.
- Cuando se muestra información de seguridad sobre archivos y carpetas con seguridad efectiva NTFS, los campos de salida relacionados con UNIX contienen información de permisos de archivo UNIX de sólo visualización.

Los archivos y carpetas de estilo de seguridad NTFS utilizan sólo permisos de archivo NTFS y usuarios y grupos de Windows al determinar los derechos de acceso a archivos.

- El resultado de ACL se muestra solo para los archivos y las carpetas con seguridad NTFS o NFSv4.

Este campo está vacío para archivos y carpetas que utilizan la seguridad de UNIX que solo tienen aplicados permisos de bit de modo (sin ACL de NFSv4).

- Los campos de salida de propietario y grupo de la salida ACL se aplican sólo en el caso de los descriptores de seguridad NTFS.

Paso

1. Mostrar la configuración de la directiva de auditoría de archivos y directorios con el nivel de detalle deseado:

| | |
|--|---|
| <input type="text" value="Si desea mostrar información..."/> | <input type="text" value="Introduzca el siguiente comando..."/> |
|--|---|

| | |
|--------------------------|--|
| En forma de resumen | <code>vserver security file-directory show -vserver vserver_name -path path</code> |
| Como una lista detallada | <code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code> |

Ejemplos

En el ejemplo siguiente se muestra la información de la directiva de auditoría de la ruta de acceso `/corp` En SVM `vs1`. La ruta de acceso tiene seguridad efectiva NTFS. El descriptor de seguridad NTFS contiene UNA entrada SACL CORRECTA y UNA entrada SACL SUCCESS/FAIL.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
      Vserver: vs1
      File Path: /corp
      File Inode Number: 357
      Security Style: ntfs
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0x8014
            Owner:DOMAIN\Administrator
            Group:BUILTIN\Administrators
            SACL - ACEs
                  ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                  SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
            DACL - ACEs
                  ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                  ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                  ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                  ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

En el ejemplo siguiente se muestra la información de la directiva de auditoría de la ruta de acceso `/datavol1` En SVM `vs1`. La ruta de acceso contiene tanto SACL de archivo normal como de carpeta y SACL de Storage-Level Access Guard.

```

cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

      Vserver: vs1
      File Path: /datavol1
      File Inode Number: 77
      Security Style: ntfs
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0xaa14
            Owner: BUILTIN\Administrators
            Group: BUILTIN\Administrators
            SACL - ACEs
              AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
            DACL - ACEs
              ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
              ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

      Storage-Level Access Guard security
      SACL (Applies to Directories):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
      DACL (Applies to Directories):
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
      SACL (Applies to Files):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
      DACL (Applies to Files):
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

Formas de mostrar información acerca de las políticas de auditoría y seguridad de archivos

Puede utilizar el carácter comodín (*) para mostrar información acerca de las directivas de auditoría y seguridad de archivos de todos los archivos y directorios de una ruta de

acceso determinada o de un volumen raíz.

El carácter comodín (*) se puede utilizar como último subcomponente de una ruta de directorio dada debajo de la cual se desea mostrar información de todos los archivos y directorios.

Si desea mostrar información de un archivo o directorio en particular denominado "**", entonces debe proporcionar la ruta completa dentro de comillas dobles (" ").

Ejemplo

El siguiente comando con el carácter comodín muestra la información sobre todos los archivos y directorios debajo de la ruta de acceso /1/ De SVM vs1:

```

cluster::> vserver security file-directory show -vserver vs1 -path /1/*

      Vserver: vs1
      File Path: /1/1
      Security Style: mixed
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0x8514
            Owner:BUILTIN\Administrators
            Group:BUILTIN\Administrators
            DACL - ACEs
            ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)

      Vserver: vs1
      File Path: /1/1/abc
      Security Style: mixed
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0x8404
            Owner:BUILTIN\Administrators
            Group:BUILTIN\Administrators
            DACL - ACEs
            ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)

```

El siguiente comando muestra la información de un archivo denominado "" en la ruta de acceso /vol1/a De SVM vs1. La ruta está entre comillas dobles (" ").

```
cluster::> vserver security file-directory show -vserver vs1 -path  
"/vol1/a/*"
```

```
        Vserver: vs1  
        File Path: "/vol1/a/*"  
        Security Style: mixed  
        Effective Style: unix  
        DOS Attributes: 10  
        DOS Attributes in Text: ----D---  
        Expanded Dos Attributes: -  
            Unix User Id: 1002  
            Unix Group Id: 65533  
            Unix Mode Bits: 755  
        Unix Mode Bits in Text: rwxr-xr-x  
        ACLs: NFSV4 Security Descriptor  
            Control:0x8014  
            SACL - ACEs  
                AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA  
            DACL - ACEs  
                ALLOW-EVERYONE@-0x1f00a9-FI|DI  
                ALLOW-OWNER@-0x1f01ff-FI|DI  
                ALLOW-GROUP@-0x1200a9-IG
```

Eventos de cambio de la interfaz de línea de comandos que se pueden auditar

Eventos de cambio de la CLI que se pueden auditar de información general

ONTAP puede auditar determinados eventos de cambio de CLI, como determinados eventos de uso compartido de SMB, determinados eventos de política de auditoría, determinados eventos de grupo de seguridad local, eventos de grupo de usuarios local y eventos de política de autorización. Comprender qué eventos de cambio se pueden auditar resulta útil al interpretar los resultados de los registros de eventos.

Puede gestionar los eventos de cambio de la CLI de la máquina virtual de almacenamiento (SVM) mediante la rotación manual de los registros de auditoría, la habilitación o la deshabilitación de la auditoría, la visualización de información sobre los eventos de cambio de auditoría, la modificación de los eventos de cambio de auditoría y la eliminación de eventos de cambio de auditoría.

Como administrador, si ejecuta cualquier comando para cambiar la configuración relacionada con los eventos de recurso compartido de SMB, grupo de usuarios local, grupo de seguridad local, política de autorización y política de auditoría, se genera un registro y se auditan el evento correspondiente:

| Categoría de auditoría | Eventos | ID de evento | Ejecute este comando... |
|------------------------|---------------------|--|-------------------------|
| Auditoría de Mhost | cambio de políticas | [4719] Configuración de auditoría modificada | `vserver audit disable |

| | | | |
|--|--|--|--|
| enable | modify` | recurso compartido de archivos | [5142] se ha añadido un recurso compartido de red |
| vserver cifs share create | [5143] se ha modificado el recurso compartido de red | vserver cifs share modify `vserver cifs share create | modify |
| delete` `vserver cifs share add | remove` | [5144] recurso compartido de red eliminado | vserver cifs share delete |
| Auditoría | cuenta de usuario | [4720] Usuario local creado | vserver cifs users-and-groups local-user create vserver services name-service unix-user create |
| [4722] Usuario local activado | `vserver cifs users-and-groups local-user create | modify` | [4724] restablecimiento de contraseña de usuario local |
| vserver cifs users-and-groups local-user set-password | [4725] Usuario local desactivado | `vserver cifs users-and-groups local-user create | modify` |
| [4726] Usuario local eliminado | vserver cifs users-and-groups local-user delete vserver services name-service unix-user delete | [4738] Cambio de usuario local | vserver cifs users-and-groups local-user modify vserver services name-service unix-user modify |
| [4781] Cambiar nombre de usuario local | vserver cifs users-and-groups local-user rename | grupo de seguridad | [4731] Grupo de seguridad local creado |
| vserver cifs users-and-groups local-group create vserver services name-service unix-group create | [4734] Grupo de seguridad local eliminado | vserver cifs users-and-groups local-group delete vserver services name-service unix-group delete | [4735] Grupo de seguridad local modificado |

| | | | |
|--|--|--|---|
| <code>`vserver cifs users-and-groups local-group rename</code> | <code>modify` vserver services name-service unix-group modify</code> | [4732] Usuario agregado al grupo local | <code>vserver cifs users-and-groups local-group add-members vserver services name-service unix-group adduser</code> |
| [4733] el usuario ha eliminado del grupo local | <code>vserver cifs users-and-groups local-group remove-members vserver services name-service unix-group deluser</code> | autorización-cambio de política | [4704] Derechos de usuario asignados |
| <code>vserver cifs users-and-groups privilege add-privilege</code> | [4705] Derechos de usuario eliminados | <code>`vserver cifs users-and-groups privilege remove-privilege</code> | <code>reset-privilege`</code> |

Gestione el evento de archivos compartidos

Cuando se configura un evento de recurso compartido de archivos para una máquina virtual de almacenamiento (SVM) y se habilita una auditoría, se generan eventos de auditoría. Los eventos de uso compartido de archivos se generan cuando se modifica el recurso compartido de red de SMB mediante `vserver cifs share` comandos relacionados.

Los eventos de uso compartido de archivos con los id de evento 5142, 5143 y 5144 se generan cuando se añade, se modifica o se elimina un recurso compartido de red de SMB para la SVM. La configuración de recursos compartidos de red de SMB se modifica con el `cifs share access control create|modify|delete` comandos.

En el siguiente ejemplo, se muestra un evento de recurso compartido de archivos con el ID 5143 que se genera cuando se crea un objeto compartido denominado 'audit_dest':


```

netapp-clus1::*> cifs share create -share-name audit_dest -path
/audit_dest
- System
  - Provider
    [ Name]   NetApp-Security-Auditing
    [ Guid]   {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
    EventID  5142
    EventName Share Object Added
    ...
    ...
    ShareName audit_dest
    SharePath /audit_dest
    ShareProperties oplocks;browsable;changenotify;show-previous-versions;
    SD O:BAG:S-1-5-21-2447422786-1297661003-4197201688-513D:(A;;;FA;;;WD)

```

Gestionar evento de cambio de política de auditoría

Cuando se configura un evento de cambio de política de auditoría para una máquina virtual de almacenamiento (SVM) y se habilita una auditoría, se generan eventos de auditoría. Los eventos de cambio de directiva de auditoría se generan cuando se modifica una directiva de auditoría mediante `vserver audit` comandos relacionados.

El evento `audit-policy-change` con el event-id 4719 se genera siempre que se deshabilita, habilita o modifica una directiva de auditoría y ayuda a identificar cuándo un usuario intenta deshabilitar la auditoría para cubrir las pistas. Se configura de forma predeterminada y requiere que se deshabilite los privilegios de diagnóstico.

En el siguiente ejemplo, se muestra un evento de cambio de política de auditoría con el ID 4719 generado cuando se deshabilita una auditoría:

```

netapp-clus1::*> vserver audit disable -vserver vserver_1
- System
  - Provider
    [ Name]   NetApp-Security-Auditing
    [ Guid]   {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
    EventID  4719
    EventName Audit Disabled
    ...
    ...
    SubjectUserName admin
    SubjectUserSid 65533-1001
    SubjectDomainName ~
    SubjectIP console
    SubjectPort

```

Gestionar evento de cuenta de usuario

Cuando se configura un evento de cuenta de usuario para una máquina virtual de almacenamiento (SVM) y se habilita una auditoría, se generan eventos de auditoría.

Los eventos de cuenta de usuario con los id de evento 4720, 4722, 4724, 4725, 4726, 4738, y 4781 se generan cuando se crea o se elimina un usuario local de SMB o NFS del sistema, se habilita la cuenta de usuario local, se deshabilita o se modifica, y se restablece o se cambia la contraseña de usuario local de SMB. Los eventos de la cuenta de usuario se generan cuando se modifica una cuenta de usuario mediante `vserver cifs users-and-groups <local user>y..vserver services name-service <unix user>` comandos.

En el siguiente ejemplo, se muestra un evento de cuenta de usuario con el ID 4720 generado cuando se crea un usuario de SMB local:

```
netapp-clus1::~*> vserver cifs users-and-groups local-user create -user
-name testuser -is-account-disabled false -vserver vserver_1
Enter the password:
Confirm the password:

- System
- Provider
  [ Name]   NetApp-Security-Auditing
  [ Guid]   {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
EventID 4720
EventName Local Cifs User Created
...
...
TargetUserName testuser
TargetDomainName NETAPP-CLUS1
TargetSid S-1-5-21-2447422786-1297661003-4197201688-1003
TargetType CIFS
DisplayName testuser
PasswordLastSet 1472662216
AccountExpires NO
PrimaryGroupId 513
UserAccountControl %%0200
SidHistory ~
PrivilegeList ~
```

En el siguiente ejemplo se muestra un evento de cuenta de usuario con el ID 4781 generado, cuando se cambia el nombre de usuario de SMB local creado en el ejemplo anterior:

```

netapp-clus1::~*> vserver cifs users-and-groups local-user rename -user
-name testuser -new-user-name testuser1
- System
- Provider
  [ Name]   NetApp-Security-Auditing
  [ Guid]   {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
  EventID  4781
  EventName Local Cifs User Renamed
  ...
  ...
  OldTargetUserName testuser
  NewTargetUserName testuser1
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1000
  TargetType CIFS
  SidHistory ~
  PrivilegeList ~

```

Gestionar evento de grupo de seguridad

Cuando se configura un evento de grupo de seguridad para una máquina virtual de almacenamiento (SVM) y se habilita una auditoría, se generan eventos de auditoría.

Los eventos de los grupos de seguridad con los id de evento 4731, 4732, 4733, 4734 y 4735 se generan cuando se crea o elimina un grupo SMB o NFS local del sistema y se agrega o se elimina el usuario local del grupo. Los eventos de grupo de seguridad se generan cuando se modifica una cuenta de usuario mediante `vserver cifs users-and-groups <local-group>y..vserver services name-service <unix-group>` comandos.

En el ejemplo siguiente se muestra un evento de grupo de seguridad con el ID 4731 generado cuando se crea un grupo de seguridad local UNIX:

```

netapp-clus1::*> vserver services name-service unix-group create -name
testunixgroup -id 20
- System
- Provider
  [ Name]   NetApp-Security-Auditing
  [ Guid]   {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
  EventID  4731
  EventName Local Unix Security Group Created
  ...
  ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
  TargetUserName testunixgroup
  TargetDomainName
  TargetGid 20
  TargetType NFS
  PrivilegeList ~
  GidHistory ~

```

Gestionar evento de cambio de directiva-autorización

Cuando se configura un evento de cambio de política de autorización para una máquina virtual de almacenamiento (SVM) y se habilita una auditoría, se generan eventos de auditoría.

Los eventos de cambio de política de autorización con los id de evento 4704 y 4705 se generan cada vez que se otorgan o revocan los derechos de autorización para un usuario de SMB y un grupo de SMB. Los eventos de cambio de directiva-autorización se generan cuando se asignan o revocan los derechos de autorización utilizando `vserver cifs users-and-groups privilege` comandos relacionados.

En el ejemplo siguiente se muestra un evento de directiva de autorización con el ID 4704 generado cuando se asignan los derechos de autorización para un grupo de usuarios de SMB:

```

netapp-clus1::*> vserver cifs users-and-groups privilege add-privilege
-user-or-group-name testcifslocalgroup -privileges *
- System
- Provider
  [ Name]   NetApp-Security-Auditing
  [ Guid]   {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
  EventID  4704
  EventName User Right Assigned
  ...
  ...
  TargetUserOrGroupName testcifslocalgroup
  TargetUserOrGroupDomainName NETAPP-CLUS1
  TargetUserOrGroupSid S-1-5-21-2447422786-1297661003-4197201688-1004;
  PrivilegeList
  SeTcbPrivilege;SeBackupPrivilege;SeRestorePrivilege;SeTakeOwnershipPrivile
ge;SeSecurityPrivilege;SeChangeNotifyPrivilege;
  TargetType CIFS

```

Gestionar configuraciones de auditoría

Gire manualmente los registros de eventos de auditoría

Para poder ver los registros de eventos de auditoría, los registros deben convertirse en formatos legibles por el usuario. Si desea ver los registros de eventos de una máquina virtual de almacenamiento (SVM) específica antes de que ONTAP gire automáticamente el registro, puede rotar manualmente los registros de eventos de auditoría en una SVM.

Paso

1. Gire los registros de eventos de auditoría mediante `vserver audit rotate-log` comando.

```
vserver audit rotate-log -vserver vs1
```

El registro de eventos de auditoría se guarda en el directorio del registro de eventos de auditoría de SVM con el formato especificado por la configuración de auditoría (XML o. EVT), y se puede ver utilizando la aplicación apropiada.

Habilite y deshabilite la auditoría en las SVM

Puede habilitar o deshabilitar la auditoría en máquinas virtuales de almacenamiento (SVM). Puede que desee detener temporalmente la auditoría de archivos y directorios desactivando la auditoría. Puede habilitar la auditoría en cualquier momento (si existe una configuración de auditoría).

Lo que necesitará

Antes de habilitar la auditoría en la SVM, debe haber ya una configuración de auditoría de la SVM.

"Cree la configuración de auditoría"

Acerca de esta tarea

La desactivación de la auditoría no elimina la configuración de auditoría.

Pasos

1. Ejecute el comando correspondiente:

| Si desea que la auditoría sea... | Introduzca el comando... |
|----------------------------------|--|
| Activado | <code>vserver audit enable -vserver vserver_name</code> |
| Deshabilitado | <code>vserver audit disable -vserver vserver_name</code> |

2. Compruebe que la auditoría está en el estado deseado:

```
vserver audit show -vserver vserver_name
```

Ejemplos

En el siguiente ejemplo, se habilita la auditoría para SVM vs1:

```
cluster1::> vserver audit enable -vserver vs1

cluster1::> vserver audit show -vserver vs1

                Vserver: vs1
            Auditing state: true
      Log Destination Path: /audit_log
Categories of Events to Audit: file-ops, cifs-logon-logoff
                Log Format: evtv
            Log File Size Limit: 100MB
    Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
        Log Rotation Schedule: Day: -
        Log Rotation Schedule: Hour: -
    Log Rotation Schedule: Minute: -
            Rotation Schedules: -
        Log Files Rotation Limit: 10
```

En el siguiente ejemplo, se deshabilita la auditoría para SVM vs1:

```
cluster1::> vserver audit disable -vserver vs1
```

```

Vserver: vs1
Auditing state: false
Log Destination Path: /audit_log
Categories of Events to Audit: file-ops, cifs-logon-logoff
Log Format: evtX
Log File Size Limit: 100MB
Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
Log Rotation Schedule: Day: -
Log Rotation Schedule: Hour: -
Log Rotation Schedule: Minute: -
Rotation Schedules: -
Log Files Rotation Limit: 10
```

Mostrar información acerca de las configuraciones de auditoría

Puede mostrar información acerca de las configuraciones de auditoría. La información puede ayudarle a determinar si la configuración es la que desea aplicar para cada SVM. La información que se muestra también le permite verificar si una configuración de auditoría está habilitada.

Acerca de esta tarea

Puede mostrar información detallada sobre la auditoría de configuraciones en todas las SVM o puede personalizar la información que se muestra en el resultado especificando los parámetros opcionales. Si no especifica ninguno de los parámetros opcionales, se muestra lo siguiente:

- Nombre de SVM a la que se aplica la configuración de auditoría
- El estado de auditoría, que puede ser `true` o `false`

Si el estado de auditoría es `true`, la auditoría está activada. Si el estado de auditoría es `false`, la auditoría está desactivada.

- Las categorías de eventos que se van a auditar
- El formato del registro de auditoría
- El directorio de destino donde el subsistema de auditoría almacena registros de auditoría consolidados y convertidos

Paso

1. Muestra información acerca de la configuración de auditoría mediante `vserver audit show` comando.

Para obtener más información acerca de cómo utilizar el comando, consulte las páginas de manual.

Ejemplos

En el siguiente ejemplo, se muestra un resumen de la configuración de auditoría de todas las SVM:

```
cluster1::> vserver audit show
```

| Vserver | State | Event Types | Log Format | Target Directory |
|---------|-------|-------------|------------|------------------|
| vs1 | false | file-ops | evtx | /audit_log |

En el siguiente ejemplo, se muestra, en el formulario de lista, toda la información de configuración de auditoría de todas las SVM:

```
cluster1::> vserver audit show -instance
```


```

                Vserver: vs1
            Auditing state: true
        Log Destination Path: /audit_log
Categories of Events to Audit: file-ops
            Log Format: evtx
        Log File Size Limit: 100MB
    Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
        Log Rotation Schedule: Day: -
            Log Rotation Schedule: Hour: -
    Log Rotation Schedule: Minute: -
            Rotation Schedules: -
        Log Files Rotation Limit: 0
```

Comandos para modificar configuraciones de auditoría

Si desea cambiar una configuración de auditoría, puede modificar la configuración actual en cualquier momento, incluida la modificación del destino de la ruta de registro y el formato de registro, la modificación de las categorías de eventos que se deben auditar, cómo guardar automáticamente los archivos de registro y la cantidad máxima de archivos de registro que se guardarán.

| Si desea... | Se usa este comando... |
|---|--|
| Modifique la ruta de destino del registro | <code>vserver audit modify</code> con la <code>-destination</code> parámetro |

| | |
|---|--|
| Modifique la categoría de eventos que se van a auditar | vserver audit modify con la -events parámetro <div>  <div> Para auditar los eventos de configuración automática de políticas de acceso central, debe habilitarse la opción de servidor SMB de control de acceso dinámico (DAC) en la máquina virtual de almacenamiento (SVM). </div> </div> |
| Modifique el formato del registro | vserver audit modify con la -format parámetro |
| Activación de los ahorros automáticos en función del tamaño del archivo de registro interno | vserver audit modify con la -rotate-size parámetro |
| Activar los ahorros automáticos en función de un intervalo de tiempo | vserver audit modify con la -rotate -schedule-month, -rotate-schedule -dayofweek, -rotate-schedule-day, -rotate -schedule-hour, y. -rotate-schedule-minute parámetros |
| Especificación del número máximo de archivos de registro guardados | vserver audit modify con la -rotate-limit parámetro |

Eliminar una configuración de auditoría

Si ya no desea auditar los eventos de archivo y directorio en la máquina virtual de almacenamiento (SVM) y no desea mantener una configuración de auditoría en la SVM, puede eliminar la configuración de auditoría.

Pasos

1. Desactive la configuración de auditoría:

```
vserver audit disable -vserver vserver_name
```

```
vserver audit disable -vserver vs1
```

2. Eliminar la configuración de auditoría:

```
vserver audit delete -vserver vserver_name
```

```
vserver audit delete -vserver vs1
```

Comprenda las implicaciones del revertir el clúster

Si tiene pensado revertir el clúster, debe tener en cuenta lo siguiente del proceso de reversión de ONTAP cuando haya en el clúster máquinas virtuales de almacenamiento

(SVM) habilitadas para auditoría. Se deben realizar ciertas acciones antes de revertir.

Revertir a una versión de ONTAP que no admite la auditoría de eventos de inicio de sesión y cierre de sesión de SMB y eventos de almacenamiento provisional de directivas de acceso central

La compatibilidad con la auditoría de eventos de inicio de sesión y cierre de sesión en SMB y para los eventos de configuración de políticas de acceso central comienza con Clustered Data ONTAP 8.3. Si va a revertir a una versión de ONTAP que no admite estos tipos de eventos y tiene configuraciones de auditoría que supervisan estos tipos de eventos, debe cambiar la configuración de auditoría de esas SVM habilitadas para auditoría antes de revertir. Debe modificar la configuración para que sólo se auditen los eventos de operación de archivo.

Solucionar problemas de auditoría y almacenamiento provisional de los problemas de espacio de volumen

Los problemas pueden surgir cuando no hay espacio suficiente en los volúmenes de almacenamiento provisional o en el volumen que contiene los registros de eventos de auditoría. Si no hay espacio suficiente, no se podrán crear nuevos registros de auditoría, lo que impide que los clientes accedan a los datos y las solicitudes de acceso fallen. Se debe saber cómo solucionar los problemas de espacio de estos volúmenes.

Solucione problemas de espacio relacionados con los volúmenes de registro de eventos

Si los volúmenes que contienen archivos de registro de eventos se quedan sin espacio, la auditoría no puede convertir los registros de registro en archivos de registro. Esto provoca errores de acceso de los clientes. Debe saber cómo solucionar problemas de espacio relacionados con los volúmenes de registro de eventos.

- Los administradores de máquinas virtuales de almacenamiento (SVM) y clústeres pueden determinar si no hay espacio en los volúmenes suficiente mostrando información sobre el uso y la configuración de los volúmenes y agregados.
- Si no hay espacio suficiente en los volúmenes que contienen registros de eventos, los administradores de SVM y clúster pueden resolver problemas de espacio eliminando algunos de los archivos de registro de eventos o aumentando el tamaño del volumen.



Si se llena el agregado que contiene el volumen del registro de eventos, se debe aumentar el tamaño del agregado para poder aumentar el tamaño del volumen. Solo un administrador de clúster puede aumentar el tamaño de un agregado.

- La ruta de destino de los archivos de registro de eventos se puede cambiar a un directorio de otro volumen modificando la configuración de auditoría.



En los siguientes casos se deniega el acceso a los datos:

- Si se elimina el directorio de destino.
- Si el límite de archivos de un volumen, que aloja el directorio de destino, alcanza su nivel máximo.

Más información sobre:

- ["Cómo ver información sobre los volúmenes y aumentar el tamaño del volumen"](#).

- ["Cómo ver información sobre los agregados y la gestión de los agregados"](#).

Solucionar problemas de espacio relacionados con los volúmenes de almacenamiento provisional

Si alguno de los volúmenes que contienen archivos staging de la máquina virtual de almacenamiento (SVM) se queda sin espacio, la auditoría no puede escribir registros de registro en archivos staging. Esto provoca errores de acceso de los clientes. Para solucionar este problema, debe determinar si alguno de los volúmenes de almacenamiento provisional utilizados en la SVM está completo mostrando información sobre el uso del volumen.

Si el volumen que contiene los archivos del registro de eventos consolidados tiene espacio suficiente pero siguen existiendo errores de acceso de los clientes debido a que el espacio no es suficiente, es posible que los volúmenes provisional no tengan espacio. El administrador de SVM debe ponerse en contacto con usted para determinar si los volúmenes de almacenamiento provisional que contienen archivos de almacenamiento provisional para la SVM tienen un espacio insuficiente. El subsistema de auditoría genera un evento EMS si no se pueden generar eventos de auditoría debido a la falta de espacio en un volumen provisional. Se muestra el siguiente mensaje: No space left on device. Solo puede ver información sobre la configuración provisional de volúmenes; los administradores de SVM no.

Todos los nombres de volúmenes de almacenamiento provisional comienzan por MDV_aud_ Seguido del UUID del agregado que contiene ese volumen de almacenamiento provisional. El siguiente ejemplo muestra cuatro volúmenes de sistema en la SVM de administrador, que se crearon automáticamente cuando se creó una configuración de auditoría de servicios de archivos para una SVM de datos en el clúster:

```
cluster1::> volume show -vserver cluster1
```

| Vserver | Volume | Aggregate | State | Type | Size | Available |
|----------|--|-----------|--------|------|------|-----------|
| cluster1 | MDV_aud_1d0131843d4811e296fc123478563412 | aggr0 | online | RW | 2GB | 1.90GB |
| cluster1 | MDV_aud_8be27f813d7311e296fc123478563412 | root_vs0 | online | RW | 2GB | 1.90GB |
| cluster1 | MDV_aud_9dc4ad503d7311e296fc123478563412 | aggr1 | online | RW | 2GB | 1.90GB |
| cluster1 | MDV_aud_a4b887ac3d7311e296fc123478563412 | aggr2 | online | RW | 2GB | 1.90GB |

4 entries were displayed.

Si hay espacio insuficiente en los volúmenes de almacenamiento provisional, se pueden resolver los problemas de espacio aumentando el tamaño del volumen.



Si el agregado que contiene el volumen provisional está lleno, se debe aumentar el tamaño del agregado antes de poder aumentar el tamaño del volumen. Solo puede aumentar el tamaño de un agregado, pero los administradores de SVM no.

Si uno o varios agregados tienen un espacio disponible de menos de 2 GB, se produce un error en la creación de la auditoría de SVM. Cuando se produce un error en la creación de la auditoría de SVM, se eliminan los volúmenes de almacenamiento provisional que se crearon.

Utilice FPolicy para supervisar y gestionar archivos en SVM

Comprenda FPolicy

Cuáles son las dos partes de la solución FPolicy

FPolicy es un marco de notificación del acceso a archivos que se utiliza para supervisar y gestionar los eventos de acceso a archivos en máquinas virtuales de almacenamiento (SVM) a través de soluciones de partners. Las soluciones de partners te ayudan a abordar diversos casos de uso, como la gobernanza de datos y el cumplimiento de normativas, la protección frente a ransomware y la movilidad de datos.

Las soluciones para partners incluyen soluciones de 3rd partes compatibles con NetApp y productos de NetApp Workload Security y Cloud Data Sense.

Una solución FPolicy consta de dos partes. El marco de FPolicy de ONTAP gestiona las actividades en el clúster y envía notificaciones a las aplicaciones asociadas (también conocidas como servidores FPolicy externos). Los servidores externos de FPolicy procesan notificaciones que envía FPolicy de ONTAP para cumplir los casos de uso de clientes.

El marco de ONTAP crea y mantiene la configuración de FPolicy, supervisa eventos de archivos y envía notificaciones a servidores de FPolicy externos. FPolicy de ONTAP proporciona la infraestructura que permite la comunicación entre servidores FPolicy externos y nodos de máquinas virtuales de almacenamiento (SVM).

El marco de FPolicy se conecta a servidores de FPolicy externos y envía notificaciones para ciertos eventos del sistema de archivos a los servidores FPolicy cuando estos eventos se producen como resultado del acceso de los clientes. Los servidores FPolicy externos procesan las notificaciones y envían respuestas de nuevo al nodo. Lo que ocurre como resultado del procesamiento de la notificación depende de la aplicación y si la comunicación entre el nodo y los servidores externos es asíncrona o síncrona.

Qué son las notificaciones síncronas y asíncronas

FPolicy envía notificaciones a servidores de FPolicy externos a través de la interfaz de FPolicy. Las notificaciones se envían en modo síncrono o asíncrono. El modo de notificación determina lo que hace ONTAP después de enviar notificaciones a los servidores FPolicy.

- **Notificaciones Asynchronous**

Con notificaciones asíncronas, el nodo no espera una respuesta del servidor FPolicy, lo cual mejora el rendimiento general del sistema. Este tipo de notificación es adecuado para aplicaciones en las que el servidor FPolicy no requiere que se realice ninguna acción como resultado de la evaluación de notificaciones. Por ejemplo, las notificaciones asíncronas se usan cuando el administrador de la máquina virtual de almacenamiento (SVM) desea supervisar y auditar la actividad de acceso a archivos.

Si un servidor de FPolicy que funciona en modo asíncrono experimenta una interrupción de la red, las notificaciones de FPolicy generadas durante la interrupción se almacenan en el nodo de almacenamiento. Cuando el servidor FPolicy vuelve a estar conectado, recibe alertas de las notificaciones almacenadas y

pueden recogerlas del nodo de almacenamiento. El tiempo que las notificaciones se pueden almacenar durante una interrupción se puede configurar hasta 10 minutos.

A partir de ONTAP 9.14.1, FPolicy permite configurar un almacén persistente para capturar eventos de acceso a archivos para políticas asíncronas no obligatorias en la SVM. Los almacenes persistentes pueden ayudar a desacoplar el procesamiento de I/O del cliente del procesamiento de notificaciones de FPolicy para reducir la latencia del cliente. No se admiten las configuraciones síncronas (obligatorias o no obligatorias) y asíncronas obligatorias.

• **Notificaciones sinc**

Cuando se configura para ejecutarse en modo síncrono, el servidor de FPolicy debe reconocer todas las notificaciones antes de permitir que continúe la operación del cliente. Este tipo de notificación se utiliza cuando se requiere una acción basada en los resultados de la evaluación de la notificación. Por ejemplo, las notificaciones síncronas se utilizan cuando el administrador de SVM desea permitir o denegar solicitudes en función de los criterios especificados en el servidor de FPolicy externo.

Aplicaciones síncronas y asíncronas

Existen muchos usos posibles para las aplicaciones de FPolicy, tanto asíncronas como síncronas.

Las aplicaciones asíncronas son aquellas en las que el servidor de FPolicy externo no altera el acceso a los archivos o directorios ni modifica los datos de la máquina virtual de almacenamiento (SVM). Por ejemplo:

- Acceso a archivos y registro de auditorías
- Gestión de recursos de almacenamiento

Las aplicaciones síncronas son aquellas en las que el acceso a los datos se altera o el servidor FPolicy externo modifica los datos. Por ejemplo:

- Gestión de cuotas
- Bloqueo de acceso a archivos
- Archivado de ficheros y gestión del almacenamiento jerárquico
- Servicios de cifrado y descifrado
- Servicios de compresión y descompresión

Almacenes persistentes de FPolicy

A partir de ONTAP 9.14.1, FPolicy permite configurar un almacén persistente para capturar eventos de acceso a archivos para políticas asíncronas no obligatorias en la SVM. Los almacenes persistentes pueden ayudar a desacoplar el procesamiento de I/O del cliente del procesamiento de notificaciones de FPolicy para reducir la latencia del cliente. No se admiten las configuraciones síncronas (obligatorias o no obligatorias) y asíncronas obligatorias.

Esta función solo está disponible en el modo externo de FPolicy. La aplicación asociada que utilice necesita admitir esta función. Debe trabajar con su partner para garantizar que esta configuración de FPolicy sea compatible.

Mejores prácticas

Los administradores de clústeres deben configurar un volumen para el almacén persistente en cada SVM en la que FPolicy esté habilitado. Cuando se configura, un almacén persistente captura todos los eventos de FPolicy que coinciden, que se procesan posteriormente en la canalización de FPolicy y se envían al servidor externo.

El almacén persistente permanece igual que cuando se recibió el último evento cuando se produce un reinicio inesperado o FPolicy se deshabilita y vuelve a habilitar. Tras una operación de toma de control, el nodo asociado almacenará y procesará los nuevos eventos. Tras una operación de devolución, el almacén persistente reanuda el procesamiento de todos los eventos sin procesar que pudieran permanecer desde el momento en que se produjo la toma de control del nodo. Los eventos en directo tendrán prioridad sobre los eventos no procesados.

Si el volumen de almacenamiento persistente se mueve de un nodo a otro en la misma SVM, las notificaciones que aún están por procesar también se moverán al nuevo nodo. Deberá volver a ejecutar el `fpolicy persistent-store create` comando en cualquiera de los nodos después de mover el volumen para garantizar que la notificación pendiente se entregue al servidor externo.

El volumen de almacenamiento persistente se configura por SVM. Para cada SVM con FPolicy, deberá crear un volumen de almacenamiento persistente.

Cree el volumen de almacenamiento persistente en el nodo con LIF que esperan que Fpolicy supervise el tráfico máximo.

Si las notificaciones acumuladas en el almacén persistente superan el tamaño del volumen aprovisionado, FPolicy comenzará a borrar la notificación entrante con los mensajes EMS adecuados.

El nombre del volumen de almacenamiento persistente y la ruta de unión especificada en el momento de la creación del volumen deben coincidir.

Establezca la política de Snapshot en `none` para ese volumen en lugar de `default`. De este modo se garantiza que no haya ninguna restauración accidental de la instantánea que provoque la pérdida de eventos actuales y que se evite un posible procesamiento de eventos duplicados.

Haga que el volumen de almacenamiento persistente no sea accesible para el acceso del protocolo de usuario externo (CIFS/NFS) y evite daños o eliminación accidentales de los registros de eventos persistentes. Para lograr esto, después de habilitar FPolicy, desmonte el volumen en ONTAP para eliminar la ruta de unión, esto hace que sea inaccesible para el acceso al protocolo de usuario.

Para obtener más información, consulte ["Crear almacenes persistentes"](#).

Tipos de configuración de FPolicy

Existen dos tipos de configuración básicos de FPolicy. Una configuración usa servidores FPolicy externos para procesar y actuar según las notificaciones. La otra configuración no utiliza servidores de FPolicy externos; en su lugar, utiliza el servidor FPolicy nativo interno de ONTAP para bloquear archivos fácilmente según extensiones.

- **Configuración del servidor FPolicy externo**

La notificación se envía al servidor FPolicy, que examina la solicitud y aplica reglas para determinar si el nodo debe permitir la operación de archivos solicitada. Para las políticas síncronas, el servidor de FPolicy envía una respuesta al nodo para permitir o bloquear la operación de archivos solicitada.

• Configuración del servidor FPolicy nativo

La notificación se ha seleccionado internamente. La solicitud se permite o se deniega según la configuración de extensión de archivo configurada en el ámbito de FPolicy.

Nota: Las solicitudes de extensión de archivo denegadas no se registran.

Cuándo crear una configuración de FPolicy nativa

Las configuraciones nativas de FPolicy utilizan el motor de FPolicy interno de ONTAP para supervisar y bloquear las operaciones de archivos según la extensión del archivo. Esta solución no requiere servidores FPolicy externos (servidores FPolicy). El uso de una configuración nativa de bloqueo de archivos es apropiado cuando se necesita esta sencilla solución.

El bloqueo de archivos nativo permite supervisar cualquier operación de archivo que coincida con eventos de operación y filtrado configurados y, a continuación, denegar el acceso a archivos con extensiones específicas. Esta es la configuración predeterminada.

Esta configuración proporciona un medio para bloquear el acceso a los archivos basándose únicamente en la extensión del archivo. Por ejemplo, para bloquear los archivos que contienen mp3 extensiones, puede configurar una directiva para proporcionar notificaciones para ciertas operaciones con extensiones de archivo de destino de mp3. La directiva está configurada para denegar mp3 peticiones de archivo para operaciones que generan notificaciones.

Lo siguiente se aplica a las configuraciones nativas de FPolicy:

- También se admite el mismo conjunto de filtros y protocolos compatibles con el tramado de archivos basado en servidor de FPolicy para el bloqueo de archivos nativo.
- El bloqueo de archivos nativo y las aplicaciones de filtrado de archivos basadas en servidor FPolicy se pueden configurar al mismo tiempo.

Para ello, es posible configurar dos políticas de FPolicy independientes para la máquina virtual de almacenamiento (SVM), con una configurada para el bloqueo de archivos nativo y otra para el filtrado de archivos basado en servidor de FPolicy.

- La función nativa de bloqueo de archivos sólo controla los archivos basándose en las extensiones y no en el contenido del archivo.
- En el caso de enlaces simbólicos, el bloqueo de archivos nativos utiliza la extensión de archivo del archivo raíz.

Más información acerca de ["FPolicy: Bloqueo de archivos nativo"](#).

Cuándo crear una configuración que utilice servidores de FPolicy externos

Las configuraciones de FPolicy que utilizan servidores de FPolicy externos para procesar y gestionar notificaciones proporcionan soluciones sólidas para casos de uso, en los que se necesite algo más que un simple bloqueo de archivos según la extensión de archivos.

Debe crear una configuración que utilice servidores de FPolicy externos cuando desee realizar tareas como supervisar y registrar eventos de acceso a archivos, proporcionar servicios de cuotas, realizar bloqueo de archivos según criterios distintos a extensiones de archivos simples, proporcionar servicios de migración de datos mediante aplicaciones de gestión del almacenamiento jerárquicas, O bien ofrece un conjunto detallado de políticas que supervisan solo un subconjunto de datos de la máquina virtual de almacenamiento (SVM).

Las funciones que desempeñan los componentes del clúster con la implementación de FPolicy

El clúster, las máquinas virtuales de almacenamiento (SVM) contenidas y las LIF de datos tienen un rol en una implementación de FPolicy.

- **cluster**

El clúster contiene el marco de gestión de FPolicy y mantiene y gestiona información acerca de todas las configuraciones de FPolicy del clúster.

- **SVM**

Una configuración de FPolicy se define a nivel de SVM. El alcance de la configuración es la SVM, y solo funciona en recursos de SVM. Una configuración de SVM no puede supervisar ni enviar notificaciones para las solicitudes de acceso a los archivos que se realicen para los datos que residen en otra SVM.

Las configuraciones de FPolicy se pueden definir en la SVM de administrador. Después de definir las configuraciones en la SVM de administrador, pueden verse y utilizarse en todas las SVM.

- **LIF de datos**

Las conexiones con los servidores FPolicy se realizan a través de LIF de datos que pertenecen a la SVM con la configuración de FPolicy. Los LIF de datos utilizados para estas conexiones pueden realizar la conmutación al respaldo de la misma manera que los LIF de datos utilizados para el acceso normal de los clientes.

Cómo funciona FPolicy con servidores de FPolicy externos

Una vez que se configura y se habilita FPolicy en la máquina virtual de almacenamiento (SVM), FPolicy se ejecuta en todos los nodos en los que participa la SVM. FPolicy es responsable de establecer y mantener conexiones con servidores FPolicy externos (servidores FPolicy), para el procesamiento de notificaciones y para gestionar mensajes de notificación hacia y desde los servidores FPolicy.

Además, como parte de la gestión de conexiones, FPolicy tiene las siguientes responsabilidades:

- Garantiza que la notificación de archivo fluya a través del LIF correcto hacia el servidor FPolicy.
- Garantiza que cuando varios servidores FPolicy están asociados a una política, el equilibrio de carga se lleva a cabo al enviar notificaciones a los servidores de FPolicy.
- Intenta restablecer la conexión cuando se interrumpe una conexión con un servidor FPolicy.
- Envía las notificaciones a los servidores de FPolicy a través de una sesión autenticada.
- Gestiona la conexión de datos de lectura directa establecida por el servidor FPolicy para atender las solicitudes del cliente cuando está habilitada la lectura de pasarela.

Cómo se utilizan los canales de control para la comunicación de FPolicy

FPolicy inicia una conexión de canal de control a un servidor FPolicy externo desde las LIF de datos de cada nodo que participa en una máquina virtual de almacenamiento (SVM). FPolicy utiliza canales de control para transmitir notificaciones de archivos; por lo tanto, un servidor FPolicy puede ver varias conexiones de canal de control en función de la topología de SVM.

Cómo se utilizan los canales de acceso a datos con privilegios para la comunicación síncrona

Con los casos de uso síncrono, el servidor de FPolicy accede a los datos que residen en la máquina virtual de almacenamiento (SVM) a través de una ruta de acceso a los datos privilegiada. El acceso a través de la ruta privilegiada expone el sistema de archivos completo al servidor FPolicy. Puede acceder a los archivos de datos para recopilar información, para analizar archivos, leer archivos o escribir en archivos.

Debido a que el servidor FPolicy externo puede acceder a todo el sistema de archivos desde la raíz de la SVM a través del canal de datos con privilegios, la conexión de canal de datos con privilegios debe ser segura.

Cómo se utilizan las credenciales de conexión de FPolicy con canales de acceso a datos con privilegios

El servidor FPolicy realiza conexiones de acceso a datos con privilegios a nodos del clúster mediante una credencial de usuario de Windows específica que se guarda con la configuración de FPolicy. SMB es el único protocolo compatible para hacer una conexión con un canal de acceso a datos privilegiado.

Si el servidor FPolicy requiere acceso a datos con privilegios, deben cumplirse las siguientes condiciones:

- Debe habilitarse una licencia para SMB en el clúster.
- El servidor FPolicy debe ejecutarse con las credenciales configuradas en la configuración de FPolicy.

Al realizar una conexión de canal de datos, FPolicy utiliza la credencial para el nombre de usuario de Windows especificado. El acceso a los datos se realiza a través del recurso compartido ONTAP_ADMIN\$ del administrador.

Qué significa otorgar credenciales de superusuario para acceso a datos con privilegios

ONTAP usa la combinación de la dirección IP y las credenciales de usuario configuradas en la configuración de FPolicy para otorgar credenciales de superusuario al servidor FPolicy.

El estado de superusuario otorga los siguientes privilegios cuando el servidor FPolicy acceda a los datos:

- Evite las comprobaciones de permisos

El usuario evita las comprobaciones de los archivos y el acceso al directorio.

- Privilegios especiales de bloqueo

ONTAP permite el acceso de lectura, escritura o modificación a cualquier archivo independientemente de los bloqueos existentes. Si el servidor FPolicy recibe bloqueos de rango de bytes en el archivo, se elimina inmediatamente los bloqueos existentes en el archivo.

- Omitir las comprobaciones de FPolicy

El acceso no genera ninguna notificación de FPolicy.

Cómo gestiona FPolicy el procesamiento de políticas

Es posible que haya varias políticas de FPolicy asignadas a la máquina virtual de almacenamiento (SVM), cada una con una prioridad diferente. Para crear una configuración de FPolicy adecuada en la SVM, es importante comprender la forma en que FPolicy gestiona el procesamiento de políticas.

Cada solicitud de acceso a archivos se evalúa inicialmente para determinar qué directivas están supervisando este evento. Si se trata de un evento supervisado, la información acerca del evento supervisado junto con las políticas interesadas se transfiere a FPolicy donde se evalúa. Cada política se evalúa por orden de prioridad

asignada.

Al configurar las directivas, debe tener en cuenta las siguientes recomendaciones:

- Si desea que una directiva se evalúe siempre antes que otras directivas, configure dicha directiva con una prioridad más alta.
- Si el éxito de la operación de acceso a archivos solicitada en un evento supervisado es un requisito previo para una solicitud de archivo que se evalúa en relación con otra directiva, asigne una prioridad a la directiva que controla el éxito o el fallo de la primera operación de archivo.

Por ejemplo, si una política gestiona la funcionalidad de archivado y restauración de archivos de FPolicy y una segunda política gestiona las operaciones de acceso a archivos en el archivo en línea, la directiva que gestiona la restauración de archivos debe tener una prioridad más alta para que el archivo se restaure antes de que se permita la operación gestionada por la segunda directiva.

- Si desea que se evalúen todas las directivas que puedan aplicarse a una operación de acceso a archivos, dé prioridad a las directivas síncronas.

Puede reorganizar las prioridades de directivas existentes modificando el número de secuencia de directivas. Sin embargo, para que FPolicy evalúe políticas en función del orden de prioridad modificado, debe deshabilitar y volver a habilitar la política con el número de secuencia modificado.

Qué es el proceso de comunicación entre el servidor FPolicy externo y el nodo

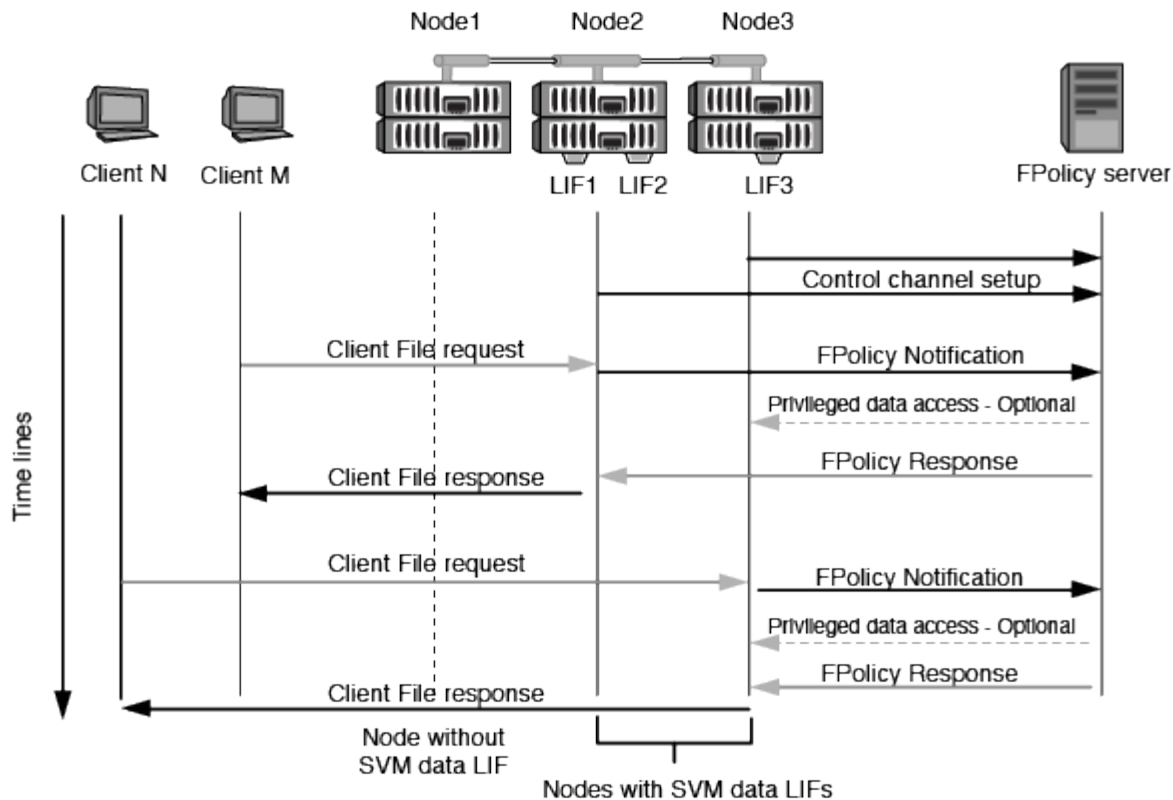
Para planificar correctamente la configuración de FPolicy, debe comprender cuál es el proceso de comunicación entre servidores FPolicy externos.

Cada nodo que participa en cada máquina virtual de almacenamiento (SVM) inicia una conexión con un servidor de FPolicy externo (servidor FPolicy) mediante TCP/IP. Las conexiones con los servidores FPolicy se configuran mediante LIF de datos de nodos; por lo tanto, un nodo participante solo puede configurar una conexión si el nodo tiene una LIF de datos operativa para la SVM.

Cada proceso de FPolicy en los nodos participantes intenta establecer una conexión con el servidor FPolicy cuando se habilite la política. Utiliza la dirección IP y el puerto del motor externo de FPolicy especificado en la configuración de directivas.

La conexión establece un canal de control desde cada uno de los nodos que participan en cada SVM al servidor FPolicy a través de la LIF de datos. Además, si las direcciones LIF de datos IPv4 e IPv6 están presentes en el mismo nodo participante, FPolicy intenta establecer conexiones tanto para IPv4 como IPv6. Por lo tanto, en una situación en la que la SVM se extiende por varios nodos o si hay direcciones IPv4 e IPv6 presentes, el servidor de FPolicy debe estar preparado para varias solicitudes de configuración de canal de control desde el clúster después de habilitar la política FPolicy en la SVM.

Por ejemplo, si un clúster tiene tres nodos (Node1, Node2 y Node3) y los LIF de datos de SVM se distribuyen en Node2 y Node3, los canales de control se inician solo desde Node2 y Node3, independientemente de la distribución de los volúmenes de datos. Supongamos que Node2 tiene dos LIF de datos (LIF1 y LIF2) que pertenecen a la SVM y que la conexión inicial es de LIF1. Si LIF1 falla, FPolicy intenta establecer un canal de control desde LIF2.



Cómo gestiona FPolicy la comunicación externa durante la migración LIF o la conmutación al nodo de respaldo

Los LIF de datos pueden migrarse a puertos de datos del mismo nodo o a puertos de datos de un nodo remoto.

Cuando se produce un error en una LIF de datos o se migra, se establece una nueva conexión de canal de control al servidor de FPolicy. A continuación, FPolicy puede volver a intentar solicitudes de clientes SMB y NFS que agoten el tiempo de espera, con el resultado de enviar nuevas notificaciones a los servidores de FPolicy externos. El nodo rechaza las respuestas del servidor de FPolicy frente a las solicitudes originales de SMB y NFS que han superado el tiempo de espera.

Cómo gestiona FPolicy la comunicación externa durante la conmutación al nodo de respaldo

Si el nodo del clúster que aloja los puertos de datos utilizados para la comunicación de FPolicy falla, ONTAP interrumpe la conexión entre el servidor de FPolicy y el nodo.

El impacto de la conmutación por error de clúster en el servidor FPolicy se puede mitigar configurando la política de conmutación por error para migrar el puerto de datos utilizado en la comunicación de FPolicy a otro nodo activo. Una vez finalizada la migración, se establece una nueva conexión con el nuevo puerto de datos.

Si la política de conmutación por error no está configurada para migrar el puerto de datos, el servidor FPolicy debe esperar a que se active el nodo fallido. Una vez que el nodo está en funcionamiento, se inicia una nueva conexión desde ese nodo con un nuevo ID de sesión.



El servidor FPolicy detecta conexiones rotas con el mensaje de protocolo Keep-alive. El tiempo de espera para purgar el ID de sesión se determina al configurar FPolicy. El tiempo de espera de mantenimiento activo predeterminado es de dos minutos.

Cómo funcionan los servicios de FPolicy en espacios de nombres de SVM

ONTAP proporciona un espacio de nombres de máquina virtual de almacenamiento unificado (SVM). Los volúmenes del clúster se unen entre sí por uniones para proporcionar un único sistema de archivos lógico. El servidor FPolicy conoce la topología de espacio de nombres y proporciona servicios FPolicy en todo el espacio de nombres.

El espacio de nombres es específico de la SVM y está contenido en ella; por lo tanto, solo se puede ver el espacio de nombres desde el contexto de la SVM. Los espacios de nombres tienen las siguientes características:

- Existe un espacio de nombres único en cada SVM, donde la raíz del espacio de nombres es el volumen raíz, representado en el espacio de nombres como barra diagonal (/).
- Todos los demás volúmenes tienen puntos de unión por debajo de la raíz (/).
- Las uniones del volumen son transparentes para los clientes.
- Una única exportación de NFS puede proporcionar acceso al espacio de nombres completo; de lo contrario, las políticas de exportación pueden exportar volúmenes específicos.
- Los recursos compartidos de SMB se pueden crear en el volumen o en qtrees dentro del volumen, o en cualquier directorio dentro del espacio de nombres.
- La arquitectura de espacio de nombres es flexible.

A continuación se muestran ejemplos de arquitecturas de espacios de nombres típicas:

- Un espacio de nombres con una única sucursal fuera de la raíz
- Un espacio de nombres con varias sucursales fuera de la raíz
- Un espacio de nombres con varios volúmenes sin ramificar de la raíz

Cómo la lectura de traspaso de FPolicy mejora la capacidad de uso para la gestión de almacenamiento jerárquica

La lectura de paso a través permite que el servidor FPolicy (funcionando como servidor de gestión de almacenamiento jerárquico (HSM)) proporcione acceso de lectura a archivos sin tener que recuperar el archivo desde el sistema de almacenamiento secundario al sistema de almacenamiento primario.

Cuando un servidor FPolicy se configura para proporcionar HSM a archivos que residen en un servidor SMB, la migración de archivos basada en políticas se produce cuando los archivos se almacenan sin conexión en un almacenamiento secundario y solo queda un archivo stub en el almacenamiento principal. Aunque un archivo stub aparece como un archivo normal para los clientes, en realidad es un archivo sparse que tiene el mismo tamaño del archivo original. El archivo sparse tiene el bit de SMB sin conexión y apunta al archivo real que se ha migrado al almacenamiento secundario.

Normalmente, cuando se recibe una solicitud de lectura de un archivo sin conexión, el contenido solicitado debe volver a recuperarse en el almacenamiento principal y, a continuación, acceder a él a través del almacenamiento principal. La necesidad de recuperar los datos en el almacenamiento primario produce varios efectos no deseados. Entre los efectos no deseados se encuentra el aumento de la latencia a las solicitudes de los clientes, debido a la necesidad de recuperar el contenido antes de responder a la solicitud y al aumento del consumo de espacio necesario para los ficheros recuperados del almacenamiento primario.

La lectura de paso a través de FPolicy permite al servidor HSM (el servidor FPolicy) proporcionar acceso de

lectura a archivos sin tener que recuperar el archivo del sistema de almacenamiento secundario al sistema de almacenamiento principal. En lugar de recuperar los ficheros de nuevo al almacenamiento primario, las solicitudes de lectura se pueden atender directamente desde un almacenamiento secundario.



La operación de lectura pasada de FPolicy no admite la descarga de copias (ODX).

La lectura a través de la contraseña mejora la facilidad de uso, ya que proporciona las siguientes ventajas:

- Se pueden atender las solicitudes de lectura incluso si el almacenamiento primario no tiene espacio suficiente para recuperar los datos solicitados de vuelta al almacenamiento primario.
- Mejor gestión de la capacidad y el rendimiento cuando se puede producir un aumento de la recuperación de datos, como si un script o una solución de backup necesitan acceder a numerosos ficheros sin conexión.
- Se pueden atender las solicitudes de lectura de archivos sin conexión en copias snapshot.

Debido a que las copias Snapshot son de sólo lectura, el servidor FPolicy no puede restaurar el archivo original si el archivo stub se encuentra en una copia snapshot. El uso de la lectura de paso a través elimina este problema.

- Las políticas se pueden configurar para controlar cuándo se atienden las solicitudes de lectura a través del acceso al archivo en el almacenamiento secundario y cuándo debe recuperarse el archivo sin conexión en el almacenamiento primario.

Por ejemplo, se puede crear una directiva en el servidor HSM que especifique el número de veces que se puede acceder al archivo sin conexión en un periodo de tiempo especificado antes de que se vuelva a migrar al almacenamiento primario. Este tipo de directiva evita recuperar archivos a los que rara vez se accede.

Cómo se gestionan las solicitudes de lectura cuando se habilita la lectura de traspaso de FPolicy

Debe comprender cómo se gestionan las solicitudes de lectura cuando se habilita FPolicy de paso a través de lectura para que pueda configurar de forma óptima la conectividad entre la máquina virtual de almacenamiento (SVM) y los servidores FPolicy.

Cuando la lectura de paso a través de FPolicy está habilitada y la SVM recibe una solicitud de archivo sin conexión, FPolicy envía una notificación al servidor FPolicy (servidor HSM) a través del canal de conexión estándar.

Después de recibir la notificación, el servidor FPolicy lee los datos de la ruta de archivo enviada en la notificación y envía los datos solicitados a la SVM a través de la conexión de datos con privilegios de lectura de paso a paso establecida entre la SVM y el servidor FPolicy.

Una vez enviados los datos, el servidor FPolicy responde a la solicitud de lectura como UN PERMISO o DENEGACIÓN. En función de si se permite o deniega la solicitud de lectura, ONTAP enviará la información solicitada o enviará un mensaje de error al cliente.

Planifique la configuración de FPolicy

Requisitos, consideraciones y prácticas recomendadas para configurar FPolicy

Antes de crear y configurar las configuraciones de FPolicy en las SVM, debe tener en cuenta determinados requisitos, consideraciones y prácticas recomendadas para

configurar FPolicy.

Las funciones de FPolicy se configuran mediante la interfaz de línea de comandos (CLI) o mediante las API DE REST.

Requisitos para configurar FPolicy

Antes de configurar y habilitar FPolicy en una máquina virtual de almacenamiento (SVM), debe conocer ciertos requisitos.

- Todos los nodos del clúster deben ejecutar una versión de ONTAP que admita FPolicy.
- Si no utiliza el motor de FPolicy nativo de ONTAP, debe tener instalados servidores de FPolicy externos (servidores FPolicy).
- Los servidores de FPolicy deben instalarse en un servidor al que se pueda acceder desde las LIF de datos de la SVM, donde se habilitaron políticas de FPolicy.



A partir de ONTAP 9.8, ONTAP proporciona un servicio LIF de cliente para conexiones FPolicy de salida con la adición del `data-fpolicy-client` servicio. ["Más información acerca de los LIF y las políticas de servicio"](#).

- La dirección IP del servidor FPolicy debe configurarse como servidor primario o secundario en la configuración del motor externo de directivas de FPolicy.
- Si los servidores FPolicy acceden a los datos a través de un canal de datos con privilegios, se deben cumplir los siguientes requisitos adicionales:
 - Las licencias de SMB deben estar en el clúster.

El acceso a datos con privilegios se logra mediante conexiones SMB.

- Se debe configurar una credencial de usuario para acceder a los archivos a través del canal de datos con privilegios.
- El servidor FPolicy debe ejecutarse con las credenciales configuradas en la configuración de FPolicy.
- Todas las LIF de datos utilizadas para comunicarse con los servidores de FPolicy deben estar configuradas para tener `cifs` como uno de los protocolos permitidos.

Esto incluye los LIF utilizados para conexiones de lectura de paso a través.

- A partir de ONTAP 9.14.1, FPolicy permite configurar un almacén persistente para capturar eventos de acceso a archivos para políticas asíncronas no obligatorias en la SVM. Los almacenes persistentes pueden ayudar a desacoplar el procesamiento de I/O del cliente del procesamiento de notificaciones de FPolicy para reducir la latencia del cliente. No se admiten las configuraciones síncronas (obligatorias o no obligatorias) y asíncronas obligatorias.

Prácticas recomendadas y recomendaciones al configurar FPolicy

Cuando configure FPolicy en máquinas virtuales de almacenamiento (SVM), familiarícese con las mejores prácticas y recomendaciones generales de configuración para garantizar que su configuración de FPolicy ofrece un sólido rendimiento de supervisión y resultados que cumplan con sus requisitos.

Para obtener directrices específicas relacionadas con el rendimiento, el ajuste de tamaño y la configuración, utilice su aplicación de partner de FPolicy.

Configuración de directivas

La configuración del motor externo de FPolicy, los eventos y el alcance de SVM pueden mejorar su experiencia y seguridad en general.

- Configuración del motor externo de FPolicy para SVM:
 - Ofrecer seguridad adicional conlleva un coste en el rendimiento. La activación de la comunicación Secure Sockets Layer (SSL) tiene un efecto de rendimiento en el acceso a recursos compartidos.
 - El motor externo de FPolicy debe configurarse con más de un servidor de FPolicy para proporcionar resiliencia y alta disponibilidad del procesamiento de notificaciones de servidor de FPolicy.
- Configuración de eventos de FPolicy para SVM:

La supervisión de las operaciones de archivos influye en su experiencia general. Por ejemplo, filtrar operaciones de archivos no deseados por el lado del almacenamiento mejora su experiencia. NetApp recomienda configurar la siguiente configuración:

- Supervisión de los tipos mínimos de operaciones de archivo y activación del número máximo de filtros sin romper el caso de uso.
 - Uso de filtros para operaciones getattr, lectura, escritura, apertura y cierre. Los entornos de directorio inicial SMB y NFS tienen un alto porcentaje de estas operaciones.
- Configuración del alcance de FPolicy para SVM:

Restrinja el alcance de las políticas a los objetos de almacenamiento relevantes, como recursos compartidos, volúmenes y exportaciones, en lugar de habilitarlos para toda la SVM. NetApp recomienda comprobar las extensiones del directorio. Si la `is-file-extension-check-on-directories-enabled` el parámetro se establece en `true`, los objetos de directorio están sujetos a las mismas comprobaciones de extensiones que los archivos normales.

Configuración de red

La conectividad de red entre el servidor de FPolicy y la controladora debe ser de baja latencia. NetApp recomienda separar el tráfico de FPolicy del tráfico de cliente mediante una red privada.

Además, debe colocar servidores FPolicy externos (servidores de FPolicy) muy cerca del clúster con una conectividad de ancho de banda elevado para proporcionar una latencia mínima y una conectividad de ancho de banda elevado.



Para una situación en la que el tráfico de LIF para FPolicy está configurado en un puerto diferente a la LIF para el tráfico de cliente, la LIF de FPolicy podría conmutar por error al otro nodo debido a un fallo de puerto. Como resultado, no se puede acceder al servidor FPolicy desde el nodo, lo que provoca que se produzca un error en las notificaciones de FPolicy para las operaciones de archivos en el nodo. Para evitar este problema, compruebe que se pueda acceder al servidor FPolicy a través al menos una LIF del nodo para procesar las solicitudes de FPolicy correspondientes a las operaciones de archivo realizadas en ese nodo.

Configuración de hardware

Puede tener el servidor de FPolicy en un servidor físico o en un servidor virtual. Si el servidor FPolicy se encuentra en un entorno virtual, debe asignar recursos dedicados (CPU, red y memoria) al servidor virtual.

La relación entre el nodo y el servidor FPolicy del clúster debe optimizarse para garantizar que los servidores de FPolicy no estén sobrecargados, lo que puede introducir latencias cuando la SVM responde a las

solicitudes de cliente. El ratio óptimo depende de la aplicación asociada para la que se utilice el servidor FPolicy. NetApp recomienda trabajar con partners para determinar el valor adecuado.

Configuración de múltiples políticas

La política de FPolicy para el bloqueo nativo tiene la prioridad más alta, independientemente del número de secuencia, y las políticas que alteran la decisión tienen una prioridad más alta que otras. La prioridad de la política depende del caso de uso. NetApp recomienda trabajar con los partners para determinar la prioridad adecuada.

Consideraciones de tamaño

FPolicy realiza supervisión en línea de las operaciones SMB y NFS, envía notificaciones al servidor externo y espera una respuesta, según el modo de comunicación del motor externo (síncrona o asíncrona). Este proceso afecta al rendimiento del acceso a SMB y NFS y a los recursos de CPU.

Para mitigar cualquier problema, NetApp recomienda trabajar con los partners para evaluar y dimensionar el entorno antes de habilitar FPolicy. El rendimiento se ve afectado por varios factores, como el número de usuarios, las características de la carga de trabajo, como las operaciones por usuario y el tamaño de los datos, la latencia de la red y los fallos o la lentitud del servidor.

Supervisión del rendimiento

FPolicy es un sistema basado en notificaciones. Las notificaciones se envían a un servidor externo para su procesamiento y para generar una respuesta a ONTAP. Este proceso de ida y vuelta aumenta la latencia de acceso de los clientes.

La supervisión de los contadores de rendimiento en el servidor FPolicy y en ONTAP le permite identificar cuellos de botella en la solución y ajustar los parámetros según sea necesario para obtener una solución óptima. Por ejemplo, un aumento de la latencia de FPolicy tiene un efecto en cascada sobre la latencia de acceso de SMB y NFS. Por lo tanto, debería supervisar tanto la latencia de las cargas de trabajo (SMB y NFS) como la latencia de FPolicy. Además, puede utilizar políticas de calidad de servicio en ONTAP para configurar una carga de trabajo para cada volumen o SVM que esté habilitado para FPolicy.

NetApp recomienda ejecutar el `statistics show -object workload` comando para mostrar las estadísticas de carga de trabajo. Además, debe supervisar los siguientes parámetros:

- Latencias medias, de lectura y de escritura
- Número total de operaciones
- Contadores de lectura y escritura

Puede supervisar el rendimiento de los subsistemas de FPolicy utilizando los siguientes contadores de FPolicy.



Debe estar en modo de diagnóstico para recopilar estadísticas relacionadas con FPolicy.

Pasos

1. Recopilar contadores de FPolicy:

- `statistics start -object fpolicy -instance instance_name -sample-id ID`
- `statistics start -object fpolicy_policy -instance instance_name -sample-id ID`

2. Mostrar contadores de FPolicy:

a. `statistics show -object fpolicy -instance instance_name -sample-id ID`

b. `statistics show -object fpolicy_server -instance instance_name -sample-id ID`

La `fpolicy` y `fpolicy_server` los contadores dan información sobre los diferentes parámetros de rendimiento que se describen en la siguiente tabla.

| Contadores | Descripción |
|---|---|
| • “fpolicy” contadores* | abortated_requests |
| Número de solicitudes de pantalla en las que se ha anulado el procesamiento de la máquina virtual de almacenamiento | event_count |
| Lista de eventos que generan notificaciones | latencia_solicitud_máx |
| Latencia máxima de solicitudes de pantalla | outstanding_requests |
| Número total de solicitudes de pantalla en curso | solicitudes_procesadas |
| Número total de solicitudes de pantalla que han pasado por el procesamiento de fpolicy en la SVM | hist_latencia_solicitud |
| Histograma de latencia para solicitudes de pantalla | requests_dispatched_rate |
| Número de solicitudes de pantalla enviadas por segundo | requests_recepted_rate |
| Número de solicitudes de pantalla recibidas por segundo | • “fpolicy_server” contadores* |
| latencia_solicitud_máx | Latencia máxima para una solicitud de pantalla |
| outstanding_requests | Número total de solicitudes de pantalla en espera de respuesta |
| latencia_solicitud | Latencia media para la solicitud de pantalla |
| hist_latencia_solicitud | Histograma de latencia para solicitudes de pantalla |
| request_sended_rate | Número de solicitudes de pantalla enviadas al servidor FPolicy por segundo |
| response_recepted_rate | Número de respuestas de pantalla recibidas del servidor FPolicy por segundo |

Gestione el flujo de trabajo de FPolicy y la dependencia de otras tecnologías

NetApp recomienda deshabilitar una política de FPolicy antes de realizar cambios de configuración. Por ejemplo, si desea agregar o modificar una dirección IP en el motor externo configurado para la política activada, desactive primero la política.

Si configura FPolicy para supervisar los volúmenes de NetApp FlexCache, NetApp recomienda que no configure FPolicy para que supervise las operaciones de los archivos de lectura y GETATTR. La supervisión de estas operaciones en ONTAP requiere la recuperación de datos de nodo a ruta (I2P). Dado que no pueden recuperarse datos I2P de volúmenes FlexCache, deben recuperarse del volumen de origen. Por lo tanto, la supervisión de estas operaciones elimina los beneficios de rendimiento que puede ofrecer FlexCache.

Cuando se ponen en marcha FPolicy y una solución antivirus externa, primero la solución antivirus recibe notificaciones. El procesamiento de FPolicy se inicia solo después de que se complete el análisis antivirus. Es importante dimensionar correctamente las soluciones antivirus porque un análisis antivirus lento puede afectar al rendimiento general.

Consideraciones sobre la actualización de paso a través y la reversión

Hay ciertas consideraciones de actualización y reversión que debe saber acerca de antes de actualizar a una versión ONTAP que admite lectura previa al paso o antes de revertir a una versión que no admite lectura a través del paso.

Actualizar

Después de actualizar todos los nodos a una versión de ONTAP que admita la lectura PassThrough de FPolicy, el clúster puede usar la funcionalidad de lectura mediante paso a paso; sin embargo, la lectura a través permanece deshabilitada de forma predeterminada en las configuraciones de FPolicy existentes. Para utilizar la lectura de paso a través en las configuraciones de FPolicy existentes, debe deshabilitar la política de FPolicy, modificar la configuración y, a continuación, volver a habilitar la configuración.

Revertir

Antes de revertir a una versión de ONTAP que no sea compatible con la lectura de paso a través de FPolicy, debe cumplir las siguientes condiciones:

- Desactive todas las políticas que utilizan passthrough-read y, a continuación, modifique las configuraciones afectadas para que no utilicen passthrough-read.
- Deshabilite la funcionalidad de FPolicy en el clúster deshabilitando todas las políticas de FPolicy en el clúster.

Antes de volver a una versión de ONTAP que no admita almacenes persistentes, asegúrese de que ninguna de las políticas de FPolicy tenga un almacén persistente configurado. Si se configura un almacén persistente, la reversión fallará.

Cuáles son los pasos para configurar una configuración de FPolicy

Para poder supervisar el acceso a los archivos, debe crearse y habilitarse una configuración de FPolicy en la máquina virtual de almacenamiento (SVM) para la cual se requieren servicios de FPolicy.

Los pasos para configurar y habilitar una configuración de FPolicy en la SVM son los siguientes:

1. Cree un motor externo de FPolicy.

El motor externo de FPolicy identifica los servidores de FPolicy externos (servidores de FPolicy) asociados con una configuración de FPolicy específica. Si se utiliza el motor de FPolicy interno "Native" para crear una configuración nativa de bloqueo de archivos, no será necesario crear un motor externo de FPolicy.

2. Cree un evento FPolicy.

Un evento de FPolicy describe lo que debe supervisar la política de FPolicy. Los eventos consisten en los protocolos y las operaciones de archivos que se deben supervisar y pueden contener una lista de filtros. Los eventos utilizan filtros para limitar la lista de eventos supervisados para los que el motor externo de FPolicy debe enviar notificaciones. Los eventos también especifican si la política supervisa las operaciones de volumen.

3. Cree una política de FPolicy.

La directiva FPolicy es responsable de asociar, con el ámbito apropiado, el conjunto de eventos que se deben supervisar y para los que se deben enviar las notificaciones de eventos supervisados al servidor FPolicy designado (o al motor nativo si no hay servidores FPolicy configurados). La directiva también define si se permite al servidor FPolicy el acceso con privilegios a los datos para los que recibe notificaciones. Un servidor FPolicy necesita acceso con privilegios si el servidor necesita acceder a los datos. Entre los casos de uso típicos en los que se necesita un acceso con privilegios se incluyen el bloqueo de archivos, la gestión de cuotas y la gestión del almacenamiento jerárquico. La directiva es donde se especifica si la configuración de esta directiva utiliza un servidor FPolicy o el servidor FPolicy interno "Native".

Una directiva especifica si la selección es obligatoria. Si el tramado es obligatorio y todos los servidores FPolicy están inactivos o no se recibe ninguna respuesta de los servidores FPolicy dentro de un período de tiempo de espera definido, se deniega el acceso al archivo.

Los límites de una política son la SVM. No es posible aplicar una política a más de una SVM. Sin embargo, una SVM específica puede tener varias políticas de FPolicy, cada una con la misma combinación u otra de configuraciones de alcance, eventos y servidores externos.

4. Configurar el alcance de la directiva.

El alcance de FPolicy determina qué volúmenes, recursos compartidos o políticas de exportación actúa o se excluye de la supervisión. Un ámbito también determina qué extensiones de archivo se deben incluir o excluir de la supervisión de FPolicy.



Las listas de exclusión tienen prioridad sobre las listas de inclusión.

5. Habilite la política de FPolicy.

Cuando la directiva está activada, se conectan los canales de control y, opcionalmente, los canales de datos con privilegios. El proceso de FPolicy en los nodos en los que participa la SVM comienza a supervisar el acceso a archivos y carpetas y, en el caso de eventos que coincidan con los criterios configurados, envía notificaciones a los servidores FPolicy (o al motor nativo si no hay servidores FPolicy configurados).



Si la directiva utiliza el bloqueo de archivos nativo, no se configura ni se asocia un motor externo con la directiva.

Planifique la configuración externa del motor de FPolicy

Planifique la configuración externa del motor de FPolicy

Antes de configurar el motor externo de FPolicy (motor externo), debe comprender lo que significa crear un motor externo y qué parámetros de configuración están disponibles. Esta información le ayuda a determinar qué valores se deben establecer para cada parámetro.

Información que se define al crear el motor externo de FPolicy

La configuración del motor externo define la información que FPolicy necesita para realizar y gestionar conexiones a los servidores FPolicy externos (servidores FPolicy), incluida la siguiente información:

- Nombre de SVM
- Nombre del motor
- Las direcciones IP de los servidores FPolicy primario y secundario y el número de puerto TCP que se utilizarán al establecer la conexión con los servidores FPolicy
- Si el tipo de motor es asíncrono o síncrono
- Cómo autenticar la conexión entre el nodo y el servidor FPolicy

Si decide configurar la autenticación SSL mutua, también debe configurar parámetros que proporcionen información de certificado SSL.

- Cómo administrar la conexión utilizando varias configuraciones avanzadas de privilegios

Esto incluye parámetros que definen elementos como valores de tiempo de espera, valores de reintento, valores de mantenimiento activo, valores máximos de solicitud, valores de tamaño de búfer enviados y de recepción y valores de tiempo de espera de sesión.

La `vserver fpolicy policy external-engine create` El comando se utiliza para crear un motor externo de FPolicy.

Cuáles son los parámetros básicos del motor externo

Es posible usar la siguiente tabla de parámetros de configuración básicos de FPolicy para ayudar a planificar la configuración:

| Tipo de información | Opción |
|--|---|
| <p>SVM</p> <p>Especifica el nombre de SVM que desea asociar a este motor externo.</p> <p>Cada configuración de FPolicy se define dentro de una única SVM. El motor externo, el evento de políticas, el ámbito de políticas y la política que se combinan para crear una configuración de políticas de FPolicy deben estar todos asociados con la misma SVM.</p> | <p><code>-vserver vserver_name</code></p> |

| | |
|--|--|
| <p><i>Nombre del motor</i></p> <p>Especifica el nombre que se asignará a la configuración externa del motor. Debe especificar el nombre del motor externo más tarde al crear la política de FPolicy. Esto asocia el motor externo a la política.</p> <p>El nombre puede tener hasta 256 caracteres.</p> <div data-bbox="164 401 220 457" data-label="Image"> </div> <p>El nombre debe tener hasta 200 caracteres si se configura el nombre del motor externo en una configuración de recuperación ante desastres de MetroCluster o SVM.</p> <p>El nombre puede contener cualquier combinación de los siguientes caracteres de intervalo ASCII:</p> <ul style="list-style-type: none"> • a por z • A por Z • 0 por 9 • " _ " ' - " , and " . " | <p>-engine-name engine_name</p> |
| <p><i>Servidores principales de FPolicy</i></p> <p>Especifica los servidores de FPolicy principales a los que el nodo envía notificaciones para una política de FPolicy determinada. El valor se especifica como una lista delimitada por comas de direcciones IP.</p> <p>Si se especifica más de una dirección IP de servidor principal, cada nodo en el que participa la SVM crea una conexión de control a cada servidor de FPolicy principal especificado en el momento en el que se habilita la política. Si configura varios servidores FPolicy principales, las notificaciones se envían a los servidores FPolicy por turnos.</p> <p>Si el motor externo se usa en una configuración de recuperación ante desastres de MetroCluster o SVM, debe especificar las direcciones IP de los servidores FPolicy en el sitio de origen como servidores principales. Las direcciones IP de los servidores FPolicy del sitio de destino se deben especificar como servidores secundarios.</p> | <p>-primary-servers IP_address,...</p> |
| <p><i>Número de puerto</i></p> <p>Especifica el número de puerto del servicio FPolicy.</p> | <p>-port integer</p> |

| | |
|---|--|
| <p><i>Servidores secundarios de FPolicy</i></p> <p>Especifica los servidores de FPolicy secundarios a los que enviar eventos de acceso a archivos para una política de FPolicy determinada. El valor se especifica como una lista delimitada por comas de direcciones IP.</p> <p>Los servidores secundarios sólo se utilizan cuando no se puede acceder a ninguno de los servidores principales. Las conexiones con servidores secundarios se establecen cuando la directiva está habilitada, pero las notificaciones se envían a servidores secundarios sólo si no se puede acceder a ninguno de los servidores principales. Si configura varios servidores secundarios, las notificaciones se envían a los servidores FPolicy por turnos.</p> | <p><code>-secondary-servers</code> <code>IP_address,...</code></p> |
| <p><i>Tipo de motor externo</i></p> <p>Especifica si el motor externo funciona en modo síncronico o asíncrono. De forma predeterminada, FPolicy funciona en modo síncrono.</p> <p>Cuando se establece en <code>synchronous</code>, El procesamiento de solicitudes de archivo envía una notificación al servidor FPolicy, pero no continúa hasta después de recibir una respuesta del servidor FPolicy. En ese punto, el flujo de solicitudes continúa o procesa los resultados en denegación, dependiendo de si la respuesta del servidor FPolicy permite la acción solicitada.</p> <p>Cuando se establece en <code>asynchronous</code>, El procesamiento de solicitudes de archivo envía una notificación al servidor FPolicy y, a continuación, continúa.</p> | <p><code>-extern-engine-type</code> <code>external_engine_type</code> El valor de este parámetro puede ser uno de los siguientes:</p> <ul style="list-style-type: none"> • <code>synchronous</code> • <code>asynchronous</code> |
| <p><i>Opción SSL para la comunicación con el servidor FPolicy</i></p> <p>Especifica la opción SSL para la comunicación con el servidor FPolicy. Este es un parámetro obligatorio. Puede elegir una de las opciones según la siguiente información:</p> <ul style="list-style-type: none"> • Cuando se establece en <code>no-auth</code>, no se lleva a cabo ninguna autenticación. <p>El enlace de comunicación se establece a través de TCP.</p> <ul style="list-style-type: none"> • Cuando se establece en <code>server-auth</code>, La SVM autentica el servidor FPolicy mediante la autenticación de servidor SSL. • Cuando se establece en <code>mutual-auth</code>, La autenticación mutua se lleva a cabo entre la SVM y el servidor FPolicy; la SVM autentica el servidor FPolicy y el servidor FPolicy autentica la SVM. <p>Si elige configurar la autenticación mutua SSL, también debe configurar el <code>-certificate-common-name</code>, <code>-certificate-serial</code>, y <code>-certificate-ca</code> parámetros.</p> | <p><code>-ssl-option {no-auth</code></p> |
| <p><code>server-auth</code></p> | <p><code>mutual-auth}</code></p> |

| | |
|---|---|
| <p><i>Certificate FQDN o nombre común personalizado</i></p> <p>Especifica el nombre de certificado utilizado si está configurada la autenticación SSL entre la SVM y el servidor FPolicy. Puede especificar el nombre del certificado como un FQDN o como un nombre común personalizado.</p> <p>Si especifica <code>mutual-auth</code> para la <code>-ssl-option</code> parámetro, debe especificar un valor para <code>-certificate-common-name</code> parámetro.</p> | <p><code>-certificate-common-name text</code></p> |
| <p><i>Número de serie del certificado</i></p> <p>Especifica el número de serie del certificado utilizado para la autenticación si se configura la autenticación SSL entre la SVM y el servidor FPolicy.</p> <p>Si especifica <code>mutual-auth</code> para la <code>-ssl-option</code> parámetro, debe especificar un valor para <code>-certificate-serial</code> parámetro.</p> | <p><code>-certificate-serial text</code></p> |
| <p><i>Autoridad del certificado</i></p> <p>Especifica el nombre de CA del certificado utilizado para la autenticación si se configura la autenticación SSL entre la SVM y el servidor FPolicy.</p> <p>Si especifica <code>mutual-auth</code> para la <code>-ssl-option</code> parámetro, debe especificar un valor para <code>-certificate-ca</code> parámetro.</p> | <p><code>-certificate-ca text</code></p> |

Cuáles son las opciones avanzadas del motor externo

Puede usar la siguiente tabla de parámetros de configuración avanzados de FPolicy conforme planifique si desea personalizar la configuración con parámetros avanzados. Estos parámetros se utilizan para modificar el comportamiento de comunicación entre los nodos del clúster y los servidores FPolicy:

| Tipo de información | Opción |
|---|---|
| <p><i>Tiempo de espera para cancelar una solicitud</i></p> <p>Especifica el intervalo de tiempo en horas (h), minutos (m) o segundos (s) Que el nodo espera una respuesta del servidor FPolicy.</p> <p>Si el intervalo de tiempo de espera supera, el nodo envía una solicitud de cancelación al servidor FPolicy. A continuación, el nodo envía la notificación a un servidor FPolicy alternativo. Este tiempo de espera ayuda a gestionar un servidor de FPolicy que no responde, lo que puede mejorar la respuesta del cliente SMB/NFS. Además, cancelar las solicitudes después de un período de tiempo de espera puede ayudar a liberar recursos del sistema, ya que la solicitud de notificación se mueve de un servidor FPolicy inactivo/incorrecto a otro servidor FPolicy alternativo.</p> <p>El intervalo para este valor es 0 por 100. Si el valor se establece en 0, La opción está deshabilitada y los mensajes de solicitud de cancelación no se envían al servidor FPolicy. El valor predeterminado es 20s.</p> | <p><code>-reqs-cancel-timeout integer[h]</code></p> |

| | |
|--|--|
| m | s] |
| <p><i>Tiempo de espera para cancelar una solicitud</i></p> <p>Especifica el tiempo de espera en horas (h), minutos (m) o segundos (s) para cancelar una solicitud.</p> <p>El intervalo para este valor es 0 por 200.</p> | <p>-reqs-abort-timeout `integer[h</p> |
| m | s] |
| <p><i>Intervalo para enviar solicitudes de estado</i></p> <p>Especifica el intervalo en horas (h), minutos (m) o segundos (s) Después de la cual se envía una solicitud de estado al servidor FPolicy.</p> <p>El intervalo para este valor es 0 por 50. Si el valor se establece en 0, La opción está deshabilitada y los mensajes de solicitud de estado no se envían al servidor FPolicy. El valor predeterminado es 10s.</p> | <p>-status-req-interval integer[h</p> |
| m | s] |
| <p><i>Número máximo de solicitudes pendientes en el servidor FPolicy</i></p> <p>Especifica el número máximo de solicitudes pendientes que se pueden poner en cola en el servidor de FPolicy.</p> <p>El intervalo para este valor es 1 por 10000. El valor predeterminado es 500.</p> | <p>-max-server-reqs integer</p> |
| <p><i>Timeout para desconectar un servidor de FPolicy que no responde</i></p> <p>Especifica el intervalo de tiempo en horas (h), minutos (m) o segundos (s) Después de lo cual finaliza la conexión al servidor FPolicy.</p> <p>La conexión finaliza después del período de tiempo de espera sólo si la cola del servidor FPolicy contiene las solicitudes máximas permitidas y no se recibe ninguna respuesta dentro del período de tiempo de espera. El número máximo permitido de solicitudes es cualquiera de las dos 50 (el valor predeterminado) o el número especificado por max-server-reqs-parámetro.</p> <p>El intervalo para este valor es 1 por 100. El valor predeterminado es 60s.</p> | <p>-server-progress -timeout integer[h</p> |
| m | s] |

| | |
|--|--|
| <p><i>Interval para enviar mensajes de mantenimiento activo al servidor de FPolicy</i></p> <p>Especifica el intervalo de tiempo en horas (h), minutos (m) o segundos (s) En los que se envían mensajes de mantenimiento activo al servidor FPolicy.</p> <p>Los mensajes de mantenimiento activo detectan conexiones medio abiertas.</p> <p>El intervalo para este valor es 10 por 600. Si el valor se establece en 0, La opción está deshabilitada y se impide que los mensajes de mantenimiento activo se envíen a los servidores FPolicy. El valor predeterminado es 120s.</p> | <p>-keep-alive-interval-integer[h</p> |
| <p>m</p> | <p>s]</p> |
| <p><i>Intentos máximos de reconexión</i></p> <p>Especifica la cantidad máxima de veces que la SVM intenta volver a conectarse al servidor FPolicy después de haberse roto la conexión.</p> <p>El intervalo para este valor es 0 por 20. El valor predeterminado es 5.</p> | <p>-max-connection-retries integer</p> |
| <p><i>Tamaño de búfer de recepción</i></p> <p>Especifica el tamaño del búfer de recepción del socket conectado para el servidor FPolicy.</p> <p>El valor predeterminado se establece en 256 kilobytes (Kb). Cuando el valor se establece en 0, el tamaño del búfer de recepción se establece en un valor definido por el sistema.</p> <p>Por ejemplo, si el tamaño predeterminado del búfer de recepción del socket es de 65536 bytes, al establecer el valor ajustable en 0, el tamaño del búfer de socket se establece en 65536 bytes. Puede utilizar cualquier valor no predeterminado para establecer el tamaño (en bytes) del búfer de recepción.</p> | <p>-recv-buffer-size integer</p> |
| <p><i>Tamaño del búfer de envío</i></p> <p>Especifica el tamaño del búfer de envío del socket conectado para el servidor FPolicy.</p> <p>El valor predeterminado se establece en 256 kilobytes (Kb). Cuando el valor se establece en 0, el tamaño del búfer de envío se establece en un valor definido por el sistema.</p> <p>Por ejemplo, si el tamaño de búfer de envío predeterminado del socket se establece en 65536 bytes, al establecer el valor ajustable en 0, el tamaño del búfer de socket se establece en 65536 bytes. Puede utilizar cualquier valor no predeterminado para establecer el tamaño (en bytes) del búfer de envío.</p> | <p>-send-buffer-size integer</p> |

| | |
|---|--|
| <p><i>Tiempo de espera para purgar un ID de sesión durante la reconexión</i></p> <p>Especifica el intervalo en horas (h), minutos (m) o segundos (s) Después de lo cual se envía un nuevo ID de sesión al servidor FPolicy durante los intentos de reconexión.</p> <p>Si la conexión entre la controladora de almacenamiento y el servidor FPolicy se completa y se realiza la reconexión dentro de la <code>-session-timeout</code> A intervalos, el ID de sesión antiguo se envía al servidor de FPolicy para poder enviar respuestas a las notificaciones antiguas.</p> <p>El valor predefinido se establece en 10 segundos.</p> | <p><code>-session-timeout</code> <code>[integerh][integerm][integer s]</code></p> |
|---|--|

Información adicional sobre la configuración de motores externos de FPolicy para usar conexiones autenticadas SSL

Debe conocer alguna información adicional si desea configurar el motor externo de FPolicy para usar SSL al conectarse a los servidores de FPolicy.

Autenticación de servidor SSL

Si decide configurar el motor externo de FPolicy para la autenticación del servidor SSL, antes de crear el motor externo, debe instalar el certificado público de la entidad de certificación (CA) que firmó el certificado de servidor FPolicy.

Autenticación mutua

Si configura motores externos de FPolicy para utilizar autenticación mutua de SSL al conectar LIF de datos de máquinas virtuales de almacenamiento (SVM) a servidores FPolicy externos, antes de crear el motor externo, Debe instalar el certificado público de la CA que firmó el certificado de servidor FPolicy junto con el certificado público y el archivo de claves para la autenticación de la SVM. No debe eliminar este certificado mientras ninguna política de FPolicy utilice el certificado instalado.

Si el certificado se elimina mientras FPolicy lo utiliza para autenticación mutua al conectarse a un servidor de FPolicy externo, no podrá volver a habilitar una política de FPolicy deshabilitada que utilice ese certificado. No se puede volver a habilitar la política de FPolicy en esta situación aunque se cree e instale un nuevo certificado con las mismas configuraciones en la SVM.

Si el certificado se ha eliminado, deberá instalar un nuevo certificado, crear nuevos motores externos de FPolicy que utilicen el nuevo certificado y asociar los nuevos motores externos a la política de FPolicy que desee volver a habilitar modificando la directiva de FPolicy.

Instalar certificados para SSL

El certificado público de la CA utilizado para firmar el certificado de servidor FPolicy se instala mediante el `security certificate install` con el `-type` parámetro establecido en `client-ca`. La clave privada y el certificado público requeridos para la autenticación de la SVM se instalan con el `security certificate install` con el `-type` parámetro establecido en `server`.

Los certificados no se replican en las relaciones de recuperación de desastres de la SVM con una configuración que no conserva su ID

Los certificados de seguridad utilizados para la autenticación SSL al realizar conexiones

a servidores FPolicy no replican en destinos de recuperación ante desastres de SVM con configuraciones que no conservan sus ID. Aunque se replica la configuración del motor externo de FPolicy en la SVM, los certificados de seguridad no se replican. Debe instalar manualmente los certificados de seguridad en el destino.

Cuando se configura la relación de recuperación ante desastres de SVM, el valor seleccionado para `-identity-preserve` opción de `snapmirror create` El comando determina los detalles de configuración que se replican en la SVM de destino.

Si establece la `-identity-preserve` opción a `true` (ID-preserve), se replican todos los detalles de configuración de FPolicy, incluida la información de certificados de seguridad. Debe instalar los certificados de seguridad en el destino únicamente si establece la opción en `false` (No conservación por ID).

Restricciones para motores externos de FPolicy con ámbito de clúster con configuraciones de recuperación ante desastres de MetroCluster y SVM

Puede crear un motor externo de FPolicy de ámbito de clúster asignando la máquina virtual de almacenamiento (SVM) del clúster al motor externo. Sin embargo, cuando se crea un motor externo de ámbito de clúster en una configuración de recuperación ante desastres de MetroCluster o SVM, existen ciertas restricciones a la hora de elegir el método de autenticación que la SVM utiliza para la comunicación externa con el servidor de FPolicy.

Puede elegir entre tres opciones de autenticación al crear servidores de FPolicy externos: Sin autenticación, autenticación de servidores SSL y autenticación mutua de SSL. Aunque no existen restricciones al elegir la opción de autenticación si se asigna el servidor FPolicy externo a una SVM de datos, al crear un motor externo de FPolicy con ámbito de clúster:

| Configuración | ¿Permitido? |
|--|-------------|
| Recuperación ante desastres de MetroCluster o SVM y un motor externo de FPolicy de ámbito de clúster sin autenticación (SSL no está configurado) | Sí |
| Recuperación ante desastres de MetroCluster o SVM y un motor externo de FPolicy de ámbito de clúster con servidor SSL o autenticación mutua de SSL | No |

- Si existe un motor externo de FPolicy de ámbito de clúster con autenticación SSL y desea crear una configuración de recuperación ante desastres de MetroCluster o SVM, debe modificar este motor externo para que no utilice ninguna autenticación ni quite el motor externo antes de poder crear la configuración de recuperación ante desastres de SVM o MetroCluster.
- Si ya existe la configuración de recuperación ante desastres de MetroCluster o SVM, ONTAP le impide crear un motor externo de FPolicy con ámbito de clúster con autenticación SSL.

Complete la hoja de trabajo de configuración externa del motor de FPolicy

Puede utilizar esta hoja de trabajo para registrar los valores que necesita durante el proceso de configuración del motor externo de FPolicy. Si es necesario un valor de parámetro, debe determinar qué valor utilizar para esos parámetros antes de configurar el motor externo.

Información para una configuración básica externa del motor

Debe registrar si desea incluir cada parámetro en la configuración externa del motor y, a continuación, registrar el valor de los parámetros que desea incluir.

| Tipo de información | Obligatorio | Incluya | Sus valores |
|---|-------------|---------|-------------|
| El nombre de la máquina virtual de almacenamiento (SVM) | Sí | Sí | |
| Nombre del motor | Sí | Sí | |
| Servidores FPolicy principales | Sí | Sí | |
| Número de puerto | Sí | Sí | |
| Servidores FPolicy secundarios | No | | |
| Tipo de motor externo | No | | |
| Opción SSL para la comunicación con el servidor FPolicy externo | Sí | Sí | |
| Nombre común personalizado o FQDN de certificado | No | | |
| Número de serie del certificado | No | | |
| Entidad de certificación | No | | |

Información para parámetros avanzados del motor externo

Para configurar un motor externo con parámetros avanzados, debe introducir el comando de configuración mientras está en modo de privilegios avanzados.

| Tipo de información | Obligatorio | Incluya | Sus valores |
|---|-------------|---------|-------------|
| Tiempo de espera para cancelar una solicitud | No | | |
| Se ha agotado el tiempo de espera para cancelar una solicitud | No | | |
| Intervalo para enviar solicitudes de estado | No | | |
| Máximo de solicitudes pendientes en el servidor FPolicy | No | | |

| | | | |
|---|----|--|--|
| Se ha agotado el tiempo de espera para desconectar un servidor de FPolicy que no responde | No | | |
| Intervalo para enviar mensajes de mantenimiento activo al servidor FPolicy | No | | |
| Número máximo de intentos de reconexión | No | | |
| Tamaño del búfer de recepción | No | | |
| Tamaño del búfer de envío | No | | |
| Se ha agotado el tiempo de espera para purgar un ID de sesión durante la reconexión | No | | |

Planifique la configuración de eventos de FPolicy

Planifique la información general de la configuración de eventos de FPolicy

Antes de configurar los eventos de FPolicy, debe comprender lo que significa para crear un evento de FPolicy. Debe determinar qué protocolos desea que se supervise el evento, qué eventos debe supervisar y qué filtros de eventos debe utilizar. Esta información le ayuda a planificar los valores que desea establecer.

Qué significa crear un evento FPolicy

Crear el evento FPolicy significa definir información que el proceso de FPolicy debe determinar qué operaciones de acceso a archivos supervisar y para cuáles de las notificaciones de eventos supervisadas deben enviarse al servidor de FPolicy externo. La configuración del evento FPolicy define la siguiente información de configuración:

- El nombre de la máquina virtual de almacenamiento (SVM)
- Nombre del evento
- Qué protocolos supervisar

FPolicy puede supervisar operaciones de acceso a archivos SMB, NFSv3 y NFSv4.

- Qué operaciones de archivos supervisar

No todas las operaciones de archivo son válidas para cada protocolo.

- Qué archivo se filtra a configurar

Sólo son válidas determinadas combinaciones de operaciones de archivos y filtros. Cada protocolo tiene su propio conjunto de combinaciones compatibles.

- Si se supervisan las operaciones de montaje y desmontaje de volúmenes


Hay una dependencia con tres de los parámetros (`-protocol`, `-file-operations`, `-filters`). Las siguientes combinaciones son válidas para los tres parámetros:




- Puede especificar el `-protocol` y.. `-file-operations` parámetros.
- Es posible especificar los tres parámetros.
- No es posible especificar ninguno de los parámetros.

Lo que contiene la configuración del evento FPolicy

Es posible usar la siguiente lista de parámetros de configuración de eventos de FPolicy disponibles para ayudar a planificar la configuración:

| Tipo de información | Opción |
|--|--|
| <p>SVM</p> <p>Especifica el nombre de la SVM que desea asociar a este evento de FPolicy.</p> <p>Cada configuración de FPolicy se define dentro de una única SVM. El motor externo, el evento de políticas, el ámbito de políticas y la política que se combinan para crear una configuración de políticas de FPolicy deben estar todos asociados con la misma SVM.</p> | <p><code>-vserver vserver_name</code></p> |
| <p>Nombre del evento</p> <p>Especifica el nombre que se asignará al evento FPolicy. Cuando crea la política de FPolicy, debe asociar el evento FPolicy con la política mediante el nombre del evento.</p> <p>El nombre puede tener hasta 256 caracteres.</p> <div><p>El nombre debe tener hasta 200 caracteres si configura el evento en una configuración de recuperación ante desastres de MetroCluster o SVM.</p></div> <p>El nombre puede contener cualquier combinación de los siguientes caracteres de intervalo ASCII:</p> <ul style="list-style-type: none">• a por z• A por Z• 0 por 9• " _", "-", and "." | <p><code>-event-name event_name</code></p> |

| | |
|---|--|
| <p><i>Protocolo</i></p> <p>Especifica el protocolo que se configurará para el evento FPolicy. La lista para <code>-protocol</code> puede incluir uno de los siguientes valores:</p> <ul style="list-style-type: none"> • <code>cifs</code> • <code>nfsv3</code> • <code>nfsv4</code> <div data-bbox="167 506 220 562">  </div> <p>Si especifica <code>-protocol</code>, a continuación, debe especificar un valor válido en la <code>-file-operations</code> parámetro. A medida que cambie la versión del protocolo, es posible que los valores válidos cambien.</p> | <p><code>-protocol protocol</code></p> |
|---|--|

Operaciones de archivo

Especifica la lista de operaciones de archivo para el evento FPolicy.

El evento comprueba las operaciones especificadas en esta lista en todas las solicitudes de cliente utilizando el protocolo especificado en la `-protocol` parámetro. Puede enumerar una o varias operaciones de archivo usando una lista delimitada por comas. La lista para `-file-operations` puede incluir uno o varios de los siguientes valores:

- `close` para las operaciones de cierre de archivos
- `create` para operaciones de creación de archivos
- `create-dir` para operaciones de creación de directorios
- `delete` para operaciones de eliminación de archivos
- `delete_dir` para operaciones de eliminación de directorios
- `getattr` para obtener operaciones de atributo
- `link` para operaciones de enlace
- `lookup` para operaciones de búsqueda
- `open` para las operaciones de apertura de archivos
- `read` para las operaciones de lectura de archivos
- `write` para operaciones de escritura de archivos
- `rename` para operaciones de cambio de nombre de archivos
- `rename_dir` para operaciones de cambio de nombre de directorios
- `setattr` para establecer operaciones de atributos
- `symlink` para operaciones de enlace simbólico



Si especifica `-file-operations`, a continuación, debe especificar un protocolo válido en la `-protocol` parámetro.

`-file-operations`
`file_operations,...`

Filtros

`-filters filter, ...`

Especifica la lista de filtros para una operación de archivo determinada para el protocolo especificado. Los valores de la `-filters` el parámetro se utiliza para filtrar solicitudes de cliente. La lista puede incluir una o varias de las siguientes opciones:



Si especifica el `-filters` parámetro, a continuación, también debe especificar valores válidos para `-file` `-operations` y.. `-protocol` parámetros.

- `monitor-ads` opción para filtrar la solicitud del cliente para una corriente de datos alternativa.
- `close-with-modification` opción para filtrar la solicitud de cliente para cerrar con la modificación.
- `close-without-modification` opción para filtrar la solicitud del cliente para cerrar sin modificación.
- `first-read` opción para filtrar la solicitud del cliente para la primera lectura.
- `first-write` opción para filtrar la solicitud del cliente para la primera escritura.
- `offline-bit` opción para filtrar la solicitud de cliente para la definición de bits sin conexión.

Al establecer este filtro, el servidor FPolicy recibe una notificación solo cuando se accede a los archivos sin conexión.

- `open-with-delete-intent` opción para filtrar la solicitud de cliente para abrir con intención de eliminación.

Al establecer este filtro, el servidor FPolicy recibe la notificación sólo cuando se intenta abrir un archivo con la intención de eliminarlo. Los sistemas de archivos utilizan esta función cuando el `FILE_DELETE_ON_CLOSE` se especifica el indicador.

- `open-with-write-intent` opción para filtrar la solicitud de cliente para abrir con intención de escritura.

Al establecer este filtro, el servidor FPolicy recibe la notificación sólo cuando se intenta abrir un archivo con la intención de escribir algo en él.

- `write-with-size-change` opción para filtrar la solicitud del cliente para escritura con cambio de tamaño.

| | |
|--|---|
| <p><i>Filters</i> continuación</p> <ul style="list-style-type: none"> • <code>setattr-with-owner-change</code> opción para filtrar las solicitudes <code>setattr</code> de cliente para cambiar el propietario de un archivo o directorio. • <code>setattr-with-group-change</code> opción para filtrar las solicitudes <code>setattr</code> de cliente para cambiar el grupo de un archivo o directorio. • <code>setattr-with-sacl-change</code> Opción para filtrar las solicitudes <code>setattr</code> de cliente para cambiar el SACL en un archivo o directorio. <p>Este filtro solo está disponible para los protocolos SMB y NFSv4.</p> <ul style="list-style-type: none"> • <code>setattr-with-dacl-change</code> Opción para filtrar las solicitudes de <code>setattr</code> del cliente para cambiar la DACL en un archivo o directorio. <p>Este filtro solo está disponible para los protocolos SMB y NFSv4.</p> <ul style="list-style-type: none"> • <code>setattr-with-modify-time-change</code> opción para filtrar las solicitudes <code>setattr</code> de cliente para cambiar el tiempo de modificación de un archivo o directorio. • <code>setattr-with-access-time-change</code> opción para filtrar las solicitudes <code>setattr</code> de cliente para cambiar el tiempo de acceso de un archivo o directorio. • <code>setattr-with-creation-time-change</code> opción para filtrar las solicitudes <code>setattr</code> de cliente para cambiar el tiempo de creación de un archivo o directorio. <p>Esta opción solo está disponible para el protocolo SMB.</p> <ul style="list-style-type: none"> • <code>setattr-with-mode-change</code> opción para filtrar las solicitudes <code>setattr</code> de cliente para cambiar los bits de modo en un archivo o directorio. • <code>setattr-with-size-change</code> opción para filtrar las solicitudes <code>setattr</code> de cliente para cambiar el tamaño de un archivo. • <code>setattr-with-allocation-size-change</code> opción para filtrar las solicitudes <code>setattr</code> de cliente para cambiar el tamaño de asignación de un archivo. <p>Esta opción solo está disponible para el protocolo SMB.</p> <ul style="list-style-type: none"> • <code>exclude-directory</code> opción para filtrar las solicitudes de cliente para operaciones de directorio. <p>Cuando se especifica este filtro, las operaciones de directorio no se supervisan.</p> | <p><code>-filters filter, ...</code></p> |
| <p><i>Is operación de volumen requerida</i></p> <p>Especifica si se requiere la supervisión para las operaciones de montaje y desmontaje de volúmenes. El valor predeterminado es <code>false</code>.</p> | <p><code>-volume-operation {true</code></p> |

| | |
|--|---|
| <pre>false} -filters filter,...</pre> | <p><i>Notificaciones denegadas de acceso a FPolicy</i></p> <p>A partir de ONTAP 9.13.1, los usuarios pueden recibir notificaciones por operaciones de archivos fallidas debido a la falta de permisos. Estas notificaciones son valiosas para la seguridad, la protección contra el ransomware y la gobernanza. Se generarán notificaciones para la operación de archivo fallida debido a la falta de permiso, que incluye:</p> <ul style="list-style-type: none"> • Fallos debidos a permisos NTFS. • Fallos debidos a bits de modo Unix. • Fallos debidos a NFSv4 ACL. |
| <pre>-monitor-fileop-failure {true</pre> | <pre>false}</pre> |

Combinaciones de operaciones de archivos y filtros compatibles que FPolicy puede supervisar para SMB

Al configurar el evento de FPolicy, debe tener en cuenta que solo ciertas combinaciones de operaciones y filtros de archivos son compatibles para supervisar las operaciones de acceso a archivos SMB.

La lista de operaciones de archivos y combinaciones de filtros admitidas para la supervisión de FPolicy de los eventos de acceso a archivos SMB se proporciona en la siguiente tabla:

| Operaciones de archivos admitidas | Filtros compatibles |
|-----------------------------------|---|
| cierre | anuncios de monitor, bit sin conexión, primer plano con modificación, primer plano sin modificación, primer plano con lectura, excluir directorio |
| cree | anuncios de monitores, bits sin conexión |
| create_dir | Actualmente no hay ningún filtro compatible con esta operación de archivo. |
| eliminar | anuncios de monitores, bits sin conexión |
| delete_dir | Actualmente no hay ningún filtro compatible con esta operación de archivo. |

| | |
|-------------------|---|
| getattr | bit sin conexión, exclude-dir |
| abierto | anuncios de monitores, bits sin conexión, intento de borrado, intento de escritura abierta, dir de exclusión |
| lea | anuncios de monitores, bits sin conexión, primera lectura |
| escritura | anuncios de monitor, bits sin conexión, primera escritura, escritura con cambio de tamaño |
| cambiar el nombre | anuncios de monitores, bits sin conexión |
| dir_renombrar | Actualmente no hay ningún filtro compatible con esta operación de archivo. |
| setattr | anuncios de monitor, offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_sacl_change, setattr_with_dacl_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_time_change, setattr_with_size_change, setattr_with_asition_size_change, exclude_directory |

A partir de ONTAP 9.13.1, los usuarios pueden recibir notificaciones por operaciones de archivos fallidas debido a la falta de permisos. En la siguiente tabla se proporciona la lista de combinaciones de acceso admitido denegado y filtros para la supervisión de FPolicy de los eventos de acceso a archivos SMB:

| | |
|--|---------------------|
| Se admite la operación de archivo denegado de acceso | Filtros compatibles |
| abierto | NA |

Operaciones de archivos admitidas y combinaciones de filtros que FPolicy puede supervisar para NFSv3

Cuando configura su evento de FPolicy, debe tener en cuenta que solo ciertas combinaciones de operaciones y filtros son compatibles para supervisar las operaciones de acceso a archivos NFSv3.

La lista de operaciones de archivos admitidas y combinaciones de filtros para la supervisión de FPolicy de los eventos de acceso a archivos NFSv3 se proporciona en la siguiente tabla:

| | |
|-----------------------------------|--|
| Operaciones de archivos admitidas | Filtros compatibles |
| cree | bit sin conexión |
| create_dir | Actualmente no hay ningún filtro compatible con esta operación de archivo. |
| eliminar | bit sin conexión |

| | |
|-------------------|--|
| delete_dir | Actualmente no hay ningún filtro compatible con esta operación de archivo. |
| enlace | bit sin conexión |
| búsqueda | bit sin conexión, exclude-dir |
| lea | bit sin conexión, primera lectura |
| escritura | sin conexión-bit, primera escritura, escritura-con-cambio de tamaño |
| cambiar el nombre | bit sin conexión |
| dir_renombrar | Actualmente no hay ningún filtro compatible con esta operación de archivo. |
| setattr | offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_size_change, exclude_directory |
| enlace simbólico | bit sin conexión |

A partir de ONTAP 9.13.1, los usuarios pueden recibir notificaciones por operaciones de archivos fallidas debido a la falta de permisos. En la siguiente tabla se proporciona la lista de combinaciones de acceso admitido denegado y filtros para la supervisión de FPolicy de eventos de acceso a archivos NFSv3:

| Se admite la operación de archivo denegado de acceso | Filtros compatibles |
|--|---------------------|
| acceso | NA |
| cree | NA |
| create_dir | NA |
| eliminar | NA |
| delete_dir | NA |
| enlace | NA |
| lea | NA |
| cambiar el nombre | NA |
| dir_renombrar | NA |

| | |
|-----------|----|
| setattr | NA |
| escritura | NA |

Combinaciones de operación de archivos y filtro admitidas que FPolicy puede supervisar para NFSv4

Al configurar el evento de FPolicy, tiene que tener en cuenta que solo admite ciertas combinaciones de operaciones y filtros para supervisar las operaciones de acceso a archivos NFSv4.

La lista de operaciones de archivos y combinaciones de filtros admitidas para la supervisión de FPolicy de los eventos de acceso a archivos NFSv4 se proporciona en la siguiente tabla:

| Operaciones de archivos admitidas | Filtros compatibles |
|-----------------------------------|--|
| cierre | fuera de línea, directorio de exclusión |
| cree | bit sin conexión |
| create_dir | Actualmente no hay ningún filtro compatible con esta operación de archivo. |
| eliminar | bit sin conexión |
| delete_dir | Actualmente no hay ningún filtro compatible con esta operación de archivo. |
| getattr | fuera de línea, directorio de exclusión |
| enlace | bit sin conexión |
| búsqueda | fuera de línea, directorio de exclusión |
| abierto | fuera de línea, directorio de exclusión |
| lea | bit sin conexión, primera lectura |
| escritura | sin conexión-bit, primera escritura, escritura-con-cambio de tamaño |
| cambiar el nombre | bit sin conexión |
| dir_renombrar | Actualmente no hay ningún filtro compatible con esta operación de archivo. |

| | |
|------------------|--|
| setattr | offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_sacl_change, setattr_with_dacl_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_size_change, exclude_directory |
| enlace simbólico | bit sin conexión |

A partir de ONTAP 9.13.1, los usuarios pueden recibir notificaciones por operaciones de archivos fallidas debido a la falta de permisos. En la siguiente tabla se proporciona la lista de combinaciones de acceso admitido denegado y filtros para la supervisión de FPolicy de eventos de acceso a archivos NFSv4:

| Se admite la operación de archivo denegado de acceso | Filtros compatibles |
|--|---------------------|
| acceso | NA |
| cree | NA |
| create_dir | NA |
| eliminar | NA |
| delete_dir | NA |
| enlace | NA |
| abierto | NA |
| lea | NA |
| cambiar el nombre | NA |
| dir_renombrar | NA |
| setattr | NA |
| escritura | NA |

Complete la hoja de trabajo de configuración de eventos de FPolicy

Puede utilizar esta hoja de datos para registrar los valores que necesita durante el proceso de configuración de eventos de FPolicy. Si un valor de parámetro es obligatorio, debe determinar qué valor se debe usar para esos parámetros antes de configurar el evento FPolicy.

Debe registrar si desea incluir cada ajuste de parámetros en la configuración de eventos de FPolicy y, a

continuación, registrar el valor para los parámetros que desea incluir.

| Tipo de información | Obligatorio | Incluya | Sus valores |
|---|-------------|---------|-------------|
| El nombre de la máquina virtual de almacenamiento (SVM) | Sí | Sí | |
| Nombre del evento | Sí | Sí | |
| Protocolo | No | | |
| Operaciones de archivos | No | | |
| Filtros | No | | |
| Operación de volumen | No | | |
| Acceso denegado a eventos (Soporte a partir de ONTAP 9,13) | No | | |

Planifique la configuración de la política de FPolicy

Planifique la información general de configuración de directivas de FPolicy

Antes de configurar la política de FPolicy, debe comprender qué parámetros son necesarios para crear la política y por qué quizás desee configurar determinados parámetros opcionales. Esta información le ayuda a determinar qué valores se deben establecer para cada parámetro.

Al crear una política de FPolicy, debe asociar la política a lo siguiente:


- La máquina virtual de almacenamiento (SVM)
- Uno o más eventos de FPolicy
- Un motor externo de FPolicy

También puede configurar varias opciones de configuración de directivas.

Lo que contiene la configuración de la política de FPolicy

Puede usar la siguiente lista de políticas de FPolicy disponibles y parámetros opcionales para ayudar a planificar la configuración:

| Tipo de información | Opción | Obligatorio | Predeterminado |
|--|--|-------------|----------------|
| SVM name Especifica el nombre de la SVM en la que desea crear una política de FPolicy. | <code>-vserver</code> <code>vserver_name</code> | Sí | Ninguno |

| | | | |
|--|-------------------------------------|-----------|----------------|
| <p>Nombre de directiva</p> <p>Especifica el nombre de la política de FPolicy.</p> <p>El nombre puede tener hasta 256 caracteres.</p> <div data-bbox="167 474 220 527">  </div> <p>El nombre debe tener hasta 200 caracteres si se configura la política en una configuración de recuperación ante desastres de MetroCluster o SVM.</p> <p>El nombre puede contener cualquier combinación de los siguientes caracteres de intervalo ASCII:</p> <ul style="list-style-type: none"> • a por z • A por Z • 0 por 9 • "_", "-", and "." | <p>-policy-name policy_name</p> | <p>Sí</p> | <p>Ninguno</p> |
| <p>Nombres de eventos</p> <p>Especifica una lista de eventos delimitada por comas para asociarlos a la directiva de FPolicy.</p> <ul style="list-style-type: none"> • Puede asociar más de un evento a una directiva. • Un evento es específico de un protocolo. • Puede utilizar una única directiva para supervisar los eventos de acceso a archivos de más de un protocolo creando un evento para cada protocolo que desee supervisar la directiva y asociando los eventos a la directiva. • Los eventos deben existir previamente. | <p>-events event_name, ...</p> | <p>Sí</p> | <p>Ninguno</p> |

| | | | |
|--|--|--|----------------------------|
| <p><i>Nombre externo del motor</i></p> <p>Especifica el nombre del motor externo que se va a asociar a la directiva de FPolicy.</p> <ul style="list-style-type: none"> • Un motor externo contiene información que el nodo necesita para enviar notificaciones a un servidor FPolicy. • Es posible configurar FPolicy para usar el motor externo nativo de ONTAP para bloquear archivos fácilmente o para usar un motor externo que esté configurado para utilizar servidores de FPolicy externos (servidores FPolicy) a fin de ofrecer un bloqueo de archivos y una gestión de archivos más sofisticados. • Si desea usar el motor externo nativo, puede no especificar un valor para este parámetro o bien puede especificar <code>native</code> como valor. • Si desea utilizar servidores FPolicy, la configuración del motor externo ya debe existir. | <p><code>-engine</code> <code>engine_name</code></p> | <p>Sí (a menos que la política utilice el motor nativo de ONTAP interno)</p> | <p><code>native</code></p> |
| <p><i>Es obligatoria la selección requerida</i></p> <p>Especifica si es necesario realizar un análisis de acceso a archivos obligatorio.</p> <ul style="list-style-type: none"> • La configuración de tramado obligatoria determina qué acción se realiza en un evento de acceso a archivos en un caso en que todos los servidores principales y secundarios están inactivos o no se recibe respuesta de los servidores FPolicy dentro de un período de tiempo de espera determinado. • Cuando se establece en <code>true</code>, se deniegan los eventos de acceso a archivos. • Cuando se establece en <code>false</code>, se permiten eventos de acceso a archivos. | <p><code>-is-mandatory</code> <code>{true</code></p> | <p><code>false}</code></p> | <p>No</p> |

| | | | |
|------|--|--|-----|
| true | <p>Permitir acceso privilegiado</p> <p>Especifica si desea que el servidor FPolicy tenga acceso privilegiado a los archivos y carpetas supervisados mediante una conexión de datos con privilegios.</p> <p>Si se configura, los servidores FPolicy pueden acceder a archivos desde la raíz de la SVM que contiene los datos supervisados mediante la conexión de datos con privilegios.</p> <p>Para obtener un acceso a datos con privilegios, debe tener una licencia para SMB en el clúster y todas las LIF de datos utilizadas para conectarse con los servidores de FPolicy se deben configurar para que tengan <code>cifs</code> como uno de los protocolos permitidos.</p> <p>Si desea configurar la directiva para permitir el acceso con privilegios, también debe especificar el nombre de usuario de la cuenta que desea que el servidor FPolicy utilice para obtener acceso con privilegios.</p> | <p>-allow -privileged -access {yes</p> | no} |
|------|--|--|-----|

| | | | |
|--|-----------|---|---|
| <p>No (a menos que la lectura directa esté habilitada)</p> | <p>no</p> | <p><i>Nombre de usuario privilegiado</i></p> <p>Especifica el nombre de usuario de la cuenta que utilizan los servidores FPolicy para el acceso a datos con privilegios.</p> <ul style="list-style-type: none"> • El valor de este parámetro debe utilizar el formato "dain\user name". • Si -allow -privileged -access se establece en no, cualquier valor establecido para este parámetro se omite. | <p>-privileged -user-name user_name</p> |
|--|-----------|---|---|

| | | | |
|---|----------------|---|--|
| <p>No (a menos que el acceso con privilegios esté activado)</p> | <p>Ninguno</p> | <p><i>Permitir passThrough-read</i></p> <p>Especifica si los servidores FPolicy pueden proporcionar servicios de lectura de paso a través para los archivos que los servidores FPolicy han archivado en almacenamiento secundario (archivos sin conexión):</p> <ul style="list-style-type: none"> • La lectura mediante paso es una forma de leer datos de archivos sin conexión sin restaurar los datos en el almacenamiento primario. <p>La lectura tras paso reduce las latencias de respuesta, ya que no es necesario recuperar los archivos en el almacenamiento principal antes de responder a la solicitud de lectura. Además, la lectura tras paso optimiza la eficiencia del almacenamiento , ya que elimina la necesidad de consumir espacio de almacenamiento primario con archivos que se recuperan únicamente para satisfacer las solicitudes de lectura.</p> | <pre>-is-passthrough -read-enabled {true</pre> |
|---|----------------|---|--|

Requisito para las configuraciones de alcance de FPolicy si la política de FPolicy utiliza el motor nativo

Si configura la política de FPolicy para utilizar el motor nativo, hay un requisito específico para definir el ámbito de FPolicy configurado para la política.

El alcance de FPolicy define los límites en los que se aplica la política de FPolicy. Por ejemplo, si se aplica a volúmenes o recursos compartidos especificados. Hay una serie de parámetros que restringen aún más el ámbito al que se aplica la política de FPolicy. Uno de estos parámetros es `-is-file-extension-check-on-directories-enabled`, especifica si se comprueban las extensiones de archivo privilegiado en los directorios. El valor predeterminado es `false`, lo que significa que las extensiones de archivo de los directorios no están marcadas.

Cuando se habilita una política de FPolicy que utilice el motor nativo en una estructura de partición o volumen y en la `-is-file-extension-check-on-directories-enabled` el parámetro establece en `false` para el ámbito de la directiva, se deniega el acceso al directorio. Con esta configuración, dado que las extensiones de archivo no se comprueban en busca de directorios, cualquier operación de directorio se deniega si está dentro del ámbito de la directiva.

Para garantizar que el acceso al directorio se realice correctamente al utilizar el motor nativo, debe configurar el `-is-file-extension-check-on-directories-enabled` parámetro para `true` al crear el ámbito.

Con este parámetro establecido en `true`, Las comprobaciones de extensión se realizan para las operaciones de directorio y la decisión de permitir o denegar el acceso se toma en función de las extensiones incluidas o excluidas en la configuración del ámbito de FPolicy.

Complete la hoja de trabajo de la política de FPolicy

Puede utilizar esta hoja de trabajo para registrar los valores que necesita durante el proceso de configuración de directivas de FPolicy. Debe registrar si desea incluir cada configuración de parámetros en la configuración de políticas de FPolicy y, a continuación, registrar el valor para los parámetros que desea incluir.

| Tipo de información | Incluya | Sus valores |
|---|---------|-------------|
| El nombre de la máquina virtual de almacenamiento (SVM) | Sí | |
| Nombre de la política | Sí | |
| Nombres de eventos | Sí | |
| Nombre del motor externo | | |
| ¿Es obligatorio realizar pruebas de detección? | | |
| Permitir acceso privilegiado | | |
| Nombre de usuario privilegiado | | |
| ¿Está habilitada la lectura PassThrough? | | |

Planifique la configuración del alcance de FPolicy

Planifique la información general de configuración del alcance de FPolicy

Antes de configurar el ámbito de FPolicy, debe comprender qué significa para crear un ámbito. Debe comprender qué contiene la configuración del ámbito. También debe comprender cuáles son las reglas de alcance de prioridad. Esta información puede ayudarle a planificar los valores que desea establecer.

Qué significa crear un alcance de FPolicy

Crear el ámbito de FPolicy significa definir los límites en los que se aplica la política de FPolicy. La máquina virtual de almacenamiento (SVM) es el límite básico. Cuando se crea un alcance para una política de FPolicy, debe definir la política de FPolicy a la que se aplicará y debe designar a las SVM que desee aplicar el alcance.

Hay una serie de parámetros que restringen aún más el ámbito dentro de la SVM especificada. Puede restringir el ámbito especificando qué incluir en el ámbito o especificando qué excluir del ámbito. Después de aplicar un ámbito a una política habilitada, las comprobaciones de eventos de política se aplican al ámbito definido por este comando.

Se generan notificaciones para eventos de acceso a archivos en los que se encuentran coincidencias en las opciones de «incluir». No se generan notificaciones para eventos de acceso a archivos en los que se encuentran coincidencias en las opciones "exclude".

La configuración del alcance de FPolicy define la siguiente información de configuración:

- Nombre de SVM
- Nombre de la política
- Los recursos compartidos que se van a incluir o excluir de lo que se supervisa
- Las políticas de exportación que se van a incluir o excluir de lo que se supervise
- Los volúmenes que se van a incluir o excluir de lo que se supervise
- Extensiones de archivo que se van a incluir o excluir de lo que se supervisa
- Si se realizan comprobaciones de extensión de archivo en objetos de directorio



Existen consideraciones especiales para el ámbito de una política de FPolicy de clúster. La política de FPolicy del clúster es una política que el administrador de clúster crea para la SVM de administrador. Si el administrador de clúster también crea el ámbito para esa política de FPolicy de clúster, el administrador de SVM no puede crear un ámbito para esa misma política. Sin embargo, si el administrador de clúster no crea un ámbito para la política de FPolicy de clúster, todos los administradores de SVM pueden crear el ámbito para esa política de clúster. Si el administrador de SVM crea un ámbito para esa política de FPolicy de clúster, el administrador de clúster no podrá crear posteriormente un alcance de clúster para esa misma política de clúster. Esto se debe a que el administrador de clúster no puede anular el ámbito de la misma política de clúster.

Cuáles son las reglas de alcance de prioridad

Las siguientes reglas de prioridad se aplican a las configuraciones del ámbito:

- Cuando se incluye un recurso compartido en la `-shares-to-include` el parámetro y el volumen principal del recurso compartido se incluyen en la `-volumes-to-exclude` parámetro, `-volumes-to`

-exclude tiene precedencia -shares-to-include.

- Cuando se incluye una política de exportación en la -export-policies-to-include el parámetro y el volumen principal de la política de exportación se incluyen en la -volumes-to-exclude parámetro, -volumes-to-exclude tiene precedencia -export-policies-to-include.
- Un administrador puede especificar ambas opciones -file-extensions-to-include y.. -file -extensions-to-exclude listas.

La -file-extensions-to-exclude el parámetro se comprueba antes de la -file-extensions-to-include el parámetro está seleccionado.

Lo que contiene la configuración del alcance de FPolicy

Es posible usar la siguiente lista de parámetros de configuración del ámbito de FPolicy disponibles para ayudar a planificar la configuración:



Al configurar qué recursos compartidos, políticas de exportación, volúmenes y extensiones de archivo incluir o excluir del ámbito, los parámetros incluir y excluir pueden incluir metacaracteres como ""?" and ""*"". No se admite el uso de expresiones regulares.

| Tipo de información | Opción |
|---|---|
| SVM Especifica el nombre de la SVM donde desea crear un alcance de FPolicy. Cada configuración de FPolicy se define dentro de una única SVM. El motor externo, el evento de políticas, el ámbito de políticas y la política que se combinan para crear una configuración de políticas de FPolicy deben estar todos asociados con la misma SVM. | -vserver vserver_name |
| Nombre de directiva Especifica el nombre de la política de FPolicy a la que desea asociar el ámbito. Debe haber la política de FPolicy. | -policy-name policy_name |
| Acciones a incluir Especifica una lista de recursos compartidos delimitados por comas que se van a supervisar la política de FPolicy a la que se aplica el ámbito. | -shares-to-include share_name, ... |
| Acciones para excluir Especifica una lista de recursos compartidos delimitados por comas que se van a excluir de la supervisión de la política de FPolicy a la que se aplica el ámbito. | -shares-to-exclude share_name, ... |
| Volumes to include especifica una lista de volúmenes delimitada por comas que supervisar la política de FPolicy a la que se aplica el ámbito. | -volumes-to-include volume_name, ... |

| | |
|---|--|
| <p><i>Volúmenes para excluir</i></p> <p>Especifica una lista delimitada por comas de volúmenes que se van a excluir de la supervisión de la política de FPolicy a la que se aplica el ámbito.</p> | <pre>-volumes-to-exclude volume_name, ...</pre> |
| <p><i>Export Policies to include</i></p> <p>Especifica una lista delimitada por comas de políticas de exportación que se deben supervisar para la directiva de FPolicy a la que se aplica el ámbito.</p> | <pre>-export-policies-to -include export_policy_name, ...</pre> |
| <p><i>Exportar directivas para excluir</i></p> <p>Especifica una lista delimitada por comas de políticas de exportación que se van a excluir de la supervisión de la directiva de FPolicy a la que se aplica el ámbito.</p> | <pre>-export-policies-to -exclude export_policy_name, ...</pre> |
| <p><i>Extensiones de archivo para incluir</i></p> <p>Especifica una lista delimitada por comas de extensiones de archivo que se va a supervisar para la directiva de FPolicy a la que se aplica el ámbito.</p> | <pre>-file-extensions-to -include file_extensions, ...</pre> |
| <p><i>Extensión de archivo para excluir</i></p> <p>Especifica una lista delimitada por comas de extensiones de archivo que se van a excluir de la supervisión de la directiva de FPolicy a la que se aplica el ámbito.</p> | <pre>-file-extensions-to -exclude file_extensions, ...</pre> |
| <p><i>Es la comprobación de la extensión del archivo en el directorio activado ?</i></p> <p>Especifica si las comprobaciones de extensión de nombre de archivo también se aplican a los objetos de directorio. Si este parámetro se establece en <code>true</code>, los objetos de directorio están sujetos a las mismas comprobaciones de extensión que los archivos normales. Si este parámetro se establece en <code>false</code>, los nombres de directorio no coinciden para las extensiones y las notificaciones se envían para los directorios aunque sus extensiones de nombre no coincidan.</p> <p>Si la política de FPolicy a la que se asigna el ámbito está configurada para usar el motor nativo, este parámetro debe configurarse en <code>true</code>.</p> | <pre>-is-file-extension -check-on-directories -enabled {true</pre> |
| <p><code>false</code></p> | <pre>}</pre> |

Complete la hoja de cálculo del alcance de FPolicy

Esta hoja de trabajo se puede usar para registrar los valores necesarios durante el proceso de configuración del ámbito de FPolicy. Si es necesario un valor de parámetro, debe determinar qué valor se debe usar para esos parámetros antes de configurar el alcance de FPolicy.

Debe registrar si desea incluir cada configuración de parámetros en la configuración del ámbito de FPolicy y, a

continuación, registrar el valor para los parámetros que desea incluir.

| Tipo de información | Obligatorio | Incluya | Sus valores |
|--|-------------|---------|-------------|
| El nombre de la máquina virtual de almacenamiento (SVM) | Sí | Sí | |
| Nombre de la política | Sí | Sí | |
| Recursos compartidos que incluir | No | | |
| Recursos compartidos para excluir | No | | |
| Volúmenes que incluir | No | | |
| Volúmenes para excluir | No | | |
| Las políticas de exportación que se incluirán | No | | |
| Directivas de exportación para excluir | No | | |
| Extensiones de archivo que se incluirán | No | | |
| Extensión de archivo para excluir | No | | |
| ¿Está activada la comprobación de extensión de archivo en el directorio? | No | | |

Cree la configuración de FPolicy

Cree el motor externo FPolicy

Debe crear un motor externo para comenzar a crear una configuración de FPolicy. El motor externo define el modo en que FPolicy realiza y gestiona conexiones a servidores FPolicy externos. Si su configuración utiliza el motor interno de ONTAP (el motor externo nativo) para bloquear archivos de forma sencilla, no tendrá que configurar un motor externo de FPolicy independiente y no tenga que llevar a cabo este paso.

Lo que necesitará

La ["motor externo"](#) debe rellenar la hoja de trabajo.

Acerca de esta tarea

Si el motor externo se utiliza en una configuración de MetroCluster, debe especificar las direcciones IP de los servidores FPolicy del sitio de origen como servidores principales. Las direcciones IP de los servidores FPolicy del sitio de destino se deben especificar como servidores secundarios.

Pasos

1. Cree el motor externo FPolicy mediante `vserver fpolicy policy external-engine create` comando.

El siguiente comando crea un motor externo en una máquina virtual de almacenamiento (SVM) `vs1.example.com`. No se requiere autenticación para las comunicaciones externas con el servidor FPolicy.

```
vserver fpolicy policy external-engine create -vserver-name vs1.example.com
-engine-name engine1 -primary-servers 10.1.1.2,10.1.1.3 -port 6789 -ssl-option
no-auth
```

2. Verifique la configuración del motor externo de FPolicy mediante `vserver fpolicy policy external-engine show` comando.

El siguiente comando muestra información acerca de todos los motores externos configurados en SVM `vs1.example.com`:

```
vserver fpolicy policy external-engine show -vserver vs1.example.com
```

| | | Primary | Secondary | | |
|-----------------|---------|-----------|-----------|-------|--------|
| External | | | | | |
| Vserver | Engine | Servers | Servers | Port | Engine |
| Type | | | | | |
| ----- | ----- | ----- | ----- | ----- | |
| ----- | | | | | |
| vs1.example.com | engine1 | 10.1.1.2, | - | 6789 | |
| synchronous | | 10.1.1.3 | | | |

El siguiente comando muestra información detallada sobre el motor externo denominado «'motor1'» en la SVM `vs1.example.com`:

```
vserver fpolicy policy external-engine show -vserver vs1.example.com -engine
-name engine1
```

| | |
|--|--------------------|
| Vserver: | vs1.example.com |
| Engine: | engine1 |
| Primary FPolicy Servers: | 10.1.1.2, 10.1.1.3 |
| Port Number of FPolicy Service: | 6789 |
| Secondary FPolicy Servers: | - |
| External Engine Type: | synchronous |
| SSL Option for External Communication: | no-auth |
| FQDN or Custom Common Name: | - |
| Serial Number of Certificate: | - |
| Certificate Authority: | - |

Cree el evento FPolicy

Como parte de la creación de una configuración de políticas de FPolicy, debe crear un evento FPolicy. El evento se asocia a la política de FPolicy cuando se cree. Un evento define qué protocolo supervisar y qué eventos de acceso a archivos supervisar y filtrar.

Antes de empezar

Debe completar el evento de FPolicy "hoja de trabajo".

Cree el evento FPolicy

- 1. Cree el evento FPolicy mediante `vserver fpolicy policy event create` comando.

```
vserver fpolicy policy event create -vserver vs1.example.com -event-name event1 -protocol cifs -file-operations open,close,read,write
```

- 2. Verifique la configuración del evento FPolicy mediante `vserver fpolicy policy event show` comando.

```
vserver fpolicy policy event show -vserver vs1.example.com
```

| Vserver | Event | File | | Filters | Is Volume Operation |
|-----------------|--------|-----------|--------------------------|---------|---------------------|
| | Name | Protocols | Operations | | |
| ----- | ----- | ----- | ----- | ----- | |
| ----- | | | | | |
| vs1.example.com | event1 | cifs | open, close, read, write | - | false |

Cree los eventos de acceso denegado a FPolicy

A partir de ONTAP 9.13.1, los usuarios pueden recibir notificaciones por operaciones de archivos fallidas debido a la falta de permisos. Estas notificaciones son valiosas para la seguridad, la protección contra el ransomware y la gobernanza.

- 1. Cree el evento FPolicy mediante `vserver fpolicy policy event create` comando.

```
vserver fpolicy policy event create -vserver vs1.example.com -event-name event1 -protocol cifs -monitor-fileop-failure true -file-operations open
```

Crear almacenes persistentes

A partir de ONTAP 9.14.1, FPolicy le permite configurar un "Almacenes persistentes" Para capturar eventos de acceso a archivos para políticas asíncronas no obligatorias en la SVM. Los almacenes persistentes pueden ayudar a desacoplar el procesamiento de I/O del cliente del procesamiento de notificaciones de FPolicy para reducir la latencia del cliente. No se admiten las configuraciones síncronas (obligatorias o no obligatorias) y asíncronas obligatorias.

Mejores prácticas

- Antes de utilizar la funcionalidad de almacén persistente, asegúrese de que sus aplicaciones asociadas admiten esta configuración.
- El volumen de almacenamiento persistente se configura por SVM. Para cada SVM con FPolicy necesitará un volumen de almacenamiento persistente.
- El nombre del volumen de almacenamiento persistente y la ruta de unión especificada en el momento de la creación del volumen deben coincidir.
- Cree el volumen de almacenamiento persistente en el nodo con LIF que esperan que Fpolicy supervise el tráfico máximo.
- Establezca la política de Snapshot en `none` para ese volumen en lugar de `default`. De este modo se garantiza que no haya ninguna restauración accidental de la instantánea que provoque la pérdida de eventos actuales y que se evite un posible procesamiento de eventos duplicados.
- Haga que el volumen de almacenamiento persistente no sea accesible para el acceso del protocolo de usuario externo (CIFS/NFS) y evite daños o eliminación accidentales de los registros de eventos persistentes. Para lograr esto, después de habilitar FPolicy, desmonte el volumen en ONTAP para eliminar la ruta de unión, esto hace que sea inaccesible para el acceso al protocolo de usuario.

Pasos

1. Cree un volumen vacío en la SVM que se pueda aprovisionar para el almacén persistente:

```
volume create -vserver <SVM Name> -volume <volume> -state <online> -junction  
-path <path> -policy <default> -unix-permissions <777> -size <value>  
-aggregate <aggregate name> -snapshot-policy <none>
```

- El tamaño del volumen de almacenamiento persistente se basa en la duración del tiempo durante el cual desea continuar los eventos que no se entregan al servidor externo (aplicación asociada).

Por ejemplo, si desea que 30 minutos de eventos persistan en un clúster con una capacidad de 30K notificaciones por segundo:

Tamaño de volumen requerido = 30000 x 30 x 60 x 0,6KB (tamaño medio de registro de notificación) = 32400000 KB = ~32 GB

Para encontrar la tasa de notificación aproximada, puede contactar con su aplicación de partner de FPolicy o utilizar el contador de FPolicy `requests_dispatched_rate`.

- Se espera que un usuario administrador con suficientes privilegios de RBAC (para crear un volumen) cree un volumen (con los comandos de la cli del volumen o la API de REST) del tamaño deseado y proporcione el nombre de ese volumen como el `-volume`. En el almacén persistente cree el comando de la CLI o la API de REST.

2. Cree el almacén persistente:

```
vserver fpolicy persistent store create -vserver <SVM> -persistent-store  
<PS_name> -volume <volume>
```

- Persistent-store: Nombre del almacén persistente
- Volume: El volumen de almacenamiento persistente

3. Una vez creado el almacén persistente, puede crear la política de FPolicy y agregar el nombre del almacén persistente a esa política.

Para obtener más información, consulte ["Cree la política FPolicy"](#).

Cree la política FPolicy

Cuando crea la política de FPolicy, debe asociar un motor externo y uno o varios eventos a la política. La directiva también especifica si es necesario realizar un tramado obligatorio, si los servidores FPolicy tienen un acceso privilegiado a los datos en la máquina virtual de almacenamiento (SVM) y si está habilitada la lectura paso a través para archivos sin conexión.

Lo que necesitará

- Debe rellenar la hoja de trabajo de la política FPolicy.
- Si planea configurar la directiva para que utilice servidores FPolicy, el motor externo debe existir.
- Debe existir al menos un evento FPolicy que planifique para asociar a la política de FPolicy.
- Si desea configurar el acceso a datos con privilegios, debe existir un servidor SMB en la SVM.
- Para configurar un almacén persistente para una política, el tipo de motor debe ser **asincrónico** y la política debe ser **no obligatoria**.

Para obtener más información, consulte ["Crear almacenes persistentes"](#).

Pasos

1. Cree la política de FPolicy:

```
vserver fpolicy policy create -vserver-name vserver_name -policy-name
policy_name -engine engine_name -events event_name, [-persistent-store
PS_name] [-is-mandatory {true|false}] [-allow-privileged-access {yes|no}] [-
privileged-user-name domain\user_name] [-is-passthrough-read-enabled
{true|false}]
```

- Puede añadir uno o varios eventos a la política de FPolicy.
- De forma predeterminada, la selección obligatoria está activada.
- Si desea permitir el acceso con privilegios mediante la configuración del `-allow-privileged-access` parámetro a. `yes`, también debe configurar un nombre de usuario con privilegios para el acceso con privilegios.
- Si desea configurar `passthrough-read` mediante el ajuste `-is-passthrough-read-enabled` parámetro a. `true`, también debe configurar el acceso a datos con privilegios.

El siguiente comando crea una política denominada «'poly1'» que tiene asociado el evento denominado «'event1'» y el motor externo denominado «'motor1'». Esta directiva utiliza valores predeterminados en la configuración de directivas:

```
vserver fpolicy policy create -vserver vs1.example.com -policy-name policy1
-events event1 -engine engine1
```

El siguiente comando crea una política denominada «'policy 2'» que tiene asociado el evento denominado «'event2'» y el motor externo denominado «'motor2'». Esta directiva está configurada para utilizar acceso privilegiado utilizando el nombre de usuario especificado. La lectura PassThrough está habilitada:

```
vserver fpolicy policy create -vserver vs1.example.com -policy-name policy2
-events event2 -engine engine2 -allow-privileged-access yes -privileged-
user-name example\archive_acct -is-passthrough-read-enabled true
```

El siguiente comando crea una política denominada «'native1'» que tiene asociado el evento denominado «'event3'». Esta directiva utiliza el motor nativo y utiliza valores predeterminados en la configuración de directivas:

```
vserver fpolicy policy create -vserver vs1.example.com -policy-name native1
-events event3 -engine native
```

- 2. Compruebe la configuración de la política de FPolicy mediante la `vserver fpolicy policy show` comando.

El siguiente comando muestra información acerca de las tres políticas de FPolicy configuradas, incluida la siguiente información:

- La SVM asociada a la política
 - El motor externo asociado a la directiva
 - Los eventos asociados a la política
 - Si es necesario realizar una selección obligatoria
 - Si se requiere un acceso privilegiado
- ```
vserver fpolicy policy show
```

| Vserver         | Policy Name | Events | Engine  | Is Mandatory | Privileged Access |
|-----------------|-------------|--------|---------|--------------|-------------------|
| -----           | -----       | -----  | -----   | -----        |                   |
| vs1.example.com | policy1     | event1 | engine1 | true         | no                |
| vs1.example.com | policy2     | event2 | engine2 | true         | yes               |
| vs1.example.com | native1     | event3 | native  | true         | no                |

Cree el alcance de FPolicy

Después de crear la política de FPolicy, debe crear un alcance de FPolicy. Al crear el ámbito, debe asociar el ámbito a una política de FPolicy. Un ámbito define los límites en los que se aplica la política de FPolicy. Los ámbitos pueden incluir o excluir archivos basados en recursos compartidos, políticas de exportación, volúmenes y extensiones de archivo.

Lo que necesitará

Se debe completar la hoja de cálculo del alcance de FPolicy. La política de FPolicy debe existir con un motor externo asociado (si la política se configura para utilizar servidores de FPolicy externos) y debe tener al menos un evento de FPolicy asociado.

Pasos

- 1. Cree el alcance de FPolicy mediante `vserver fpolicy policy scope create` comando.

```
vserver fpolicy policy scope create -vserver-name vs1.example.com -policy-name
policy1 -volumes-to-include datavol1,datavol2
```

2. Compruebe la configuración del alcance de FPolicy mediante `vserver fpolicy policy scope show` comando.

```
vserver fpolicy policy scope show -vserver vs1.example.com -instance
```

```
Vserver: vs1.example.com
Policy: policy1
Shares to Include: -
Shares to Exclude: -
Volumes to Include: datavol1, datavol2
Volumes to Exclude: -
Export Policies to Include: -
Export Policies to Exclude: -
File Extensions to Include: -
File Extensions to Exclude: -
```

### Habilite la política de FPolicy

Después de configurar una configuración de políticas de FPolicy, debe habilitar la política de FPolicy. Al habilitar la directiva, se establece su prioridad e inicia la supervisión del acceso a los archivos de la directiva.

#### Lo que necesitará

La política de FPolicy debe existir con un motor externo asociado (si la política se configura para utilizar servidores de FPolicy externos) y debe tener al menos un evento de FPolicy asociado. El alcance de la política de FPolicy debe existir y debe asignarse a la política de FPolicy.

#### Acerca de esta tarea

La prioridad se utiliza cuando se habilitan varias políticas en la máquina virtual de almacenamiento (SVM) y se ha suscrito más de una directiva al mismo evento de acceso a archivos. Las directivas que utilizan la configuración del motor nativo tienen una prioridad mayor que las directivas para cualquier otro motor, independientemente del número de secuencia que se les haya asignado al habilitar la política.



No se puede habilitar una política en la SVM de administrador.

### Pasos

1. Habilite la política de FPolicy mediante `vserver fpolicy enable` comando.

```
vserver fpolicy enable -vserver-name vs1.example.com -policy-name policy1
-sequence-number 1
```

2. Compruebe que la política de FPolicy esté habilitada mediante el `vserver fpolicy show` comando.

```
vserver fpolicy show -vserver vs1.example.com
```



|                 |             | Sequence |        |         |
|-----------------|-------------|----------|--------|---------|
| Vserver         | Policy Name | Number   | Status | Engine  |
| -----           | -----       | -----    | -----  | -----   |
| vs1.example.com | policy1     | 1        | on     | engine1 |

## Gestione las configuraciones de FPolicy

### Modifique las configuraciones de FPolicy

#### Comandos para modificar las configuraciones de FPolicy

Puede modificar las configuraciones de FPolicy modificando los elementos que componen la configuración. Puede modificar motores externos, eventos de FPolicy, ámbitos de FPolicy y políticas de FPolicy. También es posible habilitar o deshabilitar las políticas de FPolicy. Al deshabilitar la política de FPolicy, la supervisión de archivos se interrumpirá para esa política.

Se recomienda deshabilitar la política de FPolicy antes de modificar la configuración.

| Si desea modificar... | Se usa este comando...                                     |
|-----------------------|------------------------------------------------------------|
| Motores externos      | <code>vserver fpolicy policy external-engine modify</code> |
| Eventos               | <code>vserver fpolicy policy event modify</code>           |
| Ámbitos               | <code>vserver fpolicy policy scope modify</code>           |
| Normativas            | <code>vserver fpolicy policy modify</code>                 |

Consulte las páginas de manual de los comandos para obtener más información.

#### Habilite o deshabilite políticas de FPolicy

Es posible habilitar las políticas de FPolicy una vez completada la configuración. Al habilitar la directiva, se establece su prioridad e inicia la supervisión del acceso a los archivos de la directiva. Puede deshabilitar las políticas de FPolicy si desea detener la supervisión de acceso a los archivos para la política.

#### Lo que necesitará

Antes de habilitar las políticas de FPolicy, debe completar la configuración de FPolicy.

#### Acerca de esta tarea

- La prioridad se utiliza cuando se habilitan varias políticas en la máquina virtual de almacenamiento (SVM) y se ha suscrito más de una directiva al mismo evento de acceso a archivos.
- Las directivas que utilizan la configuración del motor nativo tienen una prioridad mayor que las directivas para cualquier otro motor, independientemente del número de secuencia que se les haya asignado al

habilitar la política.

- Si desea cambiar la prioridad de una política de FPolicy, debe deshabilitar la política y volver a habilitarla mediante el nuevo número de secuencia.

## Paso

1. Ejecute la acción adecuada:

| Si desea...                         | Introduzca el siguiente comando...                                                                               |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Habilite una política de FPolicy    | <code>vserver fpolicy enable -vserver-name vserver_name -policy-name policy_name -sequence-number integer</code> |
| Deshabilite una política de FPolicy | <code>vserver fpolicy disable -vserver-name vserver_name -policy-name policy_name</code>                         |

## Mostrar información acerca de las configuraciones de FPolicy

### Cómo funcionan los comandos show

Es útil cuando se muestra información acerca de la configuración de FPolicy para comprender cómo `show` funcionan los comandos.

1. `show` comando sin parámetros adicionales muestra información en un formulario de resumen. Además, cada uno `show` el comando tiene los mismos dos parámetros opcionales que se excluyen mutuamente, `-instance` y `-fields`.

Cuando utilice la `-instance` parámetro con a `show` el resultado del comando muestra información detallada en formato de lista. En algunos casos, el resultado detallado puede ser largo e incluir más información de la que usted necesita. Puede utilizar el `-fields fieldname[,fieldname...]` parámetro para personalizar la salida de modo que solo muestre información sobre los campos especificados. Puede identificar los campos que puede especificar introduciendo `?` después del `-fields` parámetro.



El resultado de un `show` con el `-fields` el parámetro puede mostrar otros campos relevantes y necesarios relacionados con los campos solicitados.

Cada `show` el comando tiene uno o varios parámetros opcionales que filtran la salida y le permiten limitar el alcance de la información que se muestra en la salida del comando. Puede identificar qué parámetros opcionales están disponibles para un comando, introduzca `?` después del `show` comando.

La `show` El comando admite patrones de estilo UNIX y comodines para permitir que coincida con varios valores en argumentos de parámetros de comandos. Por ejemplo, puede utilizar el operador comodín (`*`), EL operador NOT (`!`), EL operador OR (`|`), el operador Range (`integer...integer`), el operador menor que (`<`), el operador mayor que (`>`), el operador menor o igual que (`<=`) y el operador mayor que o igual a (`>=`) cuando especifique valores.

Para obtener más información acerca del uso de patrones de estilo UNIX y comodines, consulte [Mediante la interfaz de línea de comandos de la ONTAP](#).

## Comandos para mostrar información acerca de las configuraciones de FPolicy

Utilice la `fpolicy show` Comandos para mostrar información acerca de la configuración de FPolicy, incluida información acerca de motores, eventos, ámbitos y políticas externos de FPolicy.

| Si desea mostrar información acerca de FPolicy... | Se usa este comando...                                   |
|---------------------------------------------------|----------------------------------------------------------|
| Motores externos                                  | <code>vserver fpolicy policy external-engine show</code> |
| Eventos                                           | <code>vserver fpolicy policy event show</code>           |
| Ámbitos                                           | <code>vserver fpolicy policy scope show</code>           |
| Normativas                                        | <code>vserver fpolicy policy show</code>                 |

Consulte las páginas de manual de los comandos para obtener más información.

### Muestra información acerca del estado de la política de FPolicy

Puede mostrar información acerca del estado de las políticas de FPolicy para determinar si una política está habilitada, qué motor externo está configurado para usar, qué número de secuencia corresponde a la política y a qué máquina virtual de almacenamiento (SVM) está asociada la política de FPolicy.

#### Acerca de esta tarea

Si no especifica ningún parámetro, el comando muestra la siguiente información:

- Nombre de SVM
- Nombre de la política
- Número de secuencia de directivas
- Estado de la política

Además de mostrar información sobre el estado de política para las políticas de FPolicy configuradas en el clúster o una SVM específica, puede usar parámetros de comandos para filtrar el resultado del comando por otros criterios.

Puede especificar el `-instance` parámetro para mostrar información detallada de las políticas mostradas. De forma alternativa, puede utilizar la `-fields` parámetro para mostrar solamente los campos indicados en el resultado del comando, o `-fields ?` para determinar qué campos se pueden utilizar.

#### Paso

1. Mostrar información filtrada acerca del estado de política de FPolicy mediante el comando correspondiente:

|                                                               |                          |
|---------------------------------------------------------------|--------------------------|
| Si desea mostrar información de estado acerca de políticas... | Introduzca el comando... |
|---------------------------------------------------------------|--------------------------|

|                                                                |                                                |
|----------------------------------------------------------------|------------------------------------------------|
| En el clúster                                                  | <code>vserver fpolicy show</code>              |
| Que tienen el estado especificado                              | <code>`vserver fpolicy show -status {on</code> |
| <code>off}`</code>                                             | En una SVM especificada                        |
| <code>vserver fpolicy show<br/>-vserver vserver_name</code>    | Con el nombre de la política especificada      |
| <code>vserver fpolicy show<br/>-policy-name policy_name</code> | Que utilizan el motor externo especificado     |

### Ejemplo

En el siguiente ejemplo se muestra la información acerca de las políticas de FPolicy en el clúster:

```
cluster1::> vserver fpolicy show
```

| Vserver         | Policy Name    | Sequence<br>Number | Status | Engine |
|-----------------|----------------|--------------------|--------|--------|
| -----           | -----          | -----              | -----  | -----  |
| FPolicy         | cserver_policy | -                  | off    | eng1   |
| vs1.example.com | v1p1           | -                  | off    | eng2   |
| vs1.example.com | v1p2           | -                  | off    | native |
| vs1.example.com | v1p3           | -                  | off    | native |
| vs1.example.com | cserver_policy | -                  | off    | eng1   |
| vs2.example.com | v1p1           | 3                  | on     | native |
| vs2.example.com | v1p2           | 1                  | on     | eng3   |
| vs2.example.com | cserver_policy | 2                  | on     | eng1   |

### Muestra información acerca de las políticas de FPolicy habilitadas

Puede mostrar información acerca de las políticas de FPolicy habilitadas para determinar qué motor externo de FPolicy se ha configurado para utilizar, cuál es la prioridad de la política y a qué máquina virtual de almacenamiento (SVM) está asociada la política de FPolicy.

### Acerca de esta tarea

Si no especifica ningún parámetro, el comando muestra la siguiente información:

- Nombre de SVM
- Nombre de la política
- Prioridad en materia de políticas

Puede utilizar parámetros de comando para filtrar el resultado del comando por criterios especificados.

### Paso

1. Muestre información sobre las políticas de FPolicy habilitadas mediante el comando correspondiente:

|                                                                 |                                                                    |
|-----------------------------------------------------------------|--------------------------------------------------------------------|
| Si desea mostrar información sobre las políticas habilitadas... | Introduzca el comando...                                           |
| En el clúster                                                   | <code>vserver fpolicy show-enabled</code>                          |
| En una SVM especificada                                         | <code>vserver fpolicy show-enabled -vserver vserver_name</code>    |
| Con el nombre de la política especificada                       | <code>vserver fpolicy show-enabled -policy-name policy_name</code> |
| Con el número de secuencia especificado                         | <code>vserver fpolicy show-enabled -priority integer</code>        |

### Ejemplo

En el siguiente ejemplo se muestra la información acerca de las políticas de FPolicy habilitadas en el clúster:

```
cluster1::> vserver fpolicy show-enabled
Vserver Policy Name Priority

vs1.example.com pol_native native
vs1.example.com pol_native2 native
vs1.example.com pol1 2
vs1.example.com pol2 4
```

## Gestione las conexiones del servidor FPolicy

### Conéctese a servidores de FPolicy externos

Para habilitar el procesamiento de archivos, es posible que deba conectarse manualmente a un servidor FPolicy externo si la conexión ha finalizado previamente. Una conexión se completa después de alcanzar el tiempo de espera del servidor o debido a algún error. Como alternativa, el administrador podría terminar manualmente una conexión.

### Acerca de esta tarea

Si se produce un error grave, es posible finalizar la conexión con el servidor FPolicy. Después de resolver el problema que provocó el error grave, debe volver a conectarse manualmente al servidor FPolicy.

### Pasos

1. Conéctese al servidor de FPolicy externo mediante `vserver fpolicy engine-connect` comando.

Para obtener más información acerca del comando, consulte las páginas de manual.

2. Compruebe que el servidor FPolicy externo esté conectado mediante el `vserver fpolicy show-engine` comando.

Para obtener más información acerca del comando, consulte las páginas de manual.

#### **Desconectarse de servidores de FPolicy externos**

Es posible que deba desconectarse manualmente de un servidor de FPolicy externo. Esto puede ser aconsejable si el servidor FPolicy tiene problemas con el procesamiento de solicitudes de notificación o si necesita realizar tareas de mantenimiento en el servidor FPolicy.

#### **Pasos**

1. Desconecte del servidor FPolicy externo mediante `vserver fpolicy engine-disconnect` comando.

Para obtener más información acerca del comando, consulte las páginas de manual.

2. Compruebe que el servidor FPolicy externo esté desconectado mediante el `vserver fpolicy show-engine` comando.

Para obtener más información acerca del comando, consulte las páginas de manual.

#### **Muestra información acerca de las conexiones con servidores FPolicy externos**

Es posible mostrar información de estado acerca de las conexiones a servidores FPolicy externos (servidores FPolicy) para el clúster o para una máquina virtual de almacenamiento (SVM) especificada. Esta información puede ayudarle a determinar qué servidores de FPolicy están conectados.

#### **Acerca de esta tarea**

Si no especifica ningún parámetro, el comando muestra la siguiente información:

- Nombre de SVM
- Nombre del nodo
- Nombre de la política de FPolicy
- Dirección IP del servidor FPolicy
- Estado del servidor FPolicy
- Tipo de servidor FPolicy

Además de mostrar información acerca de las conexiones de FPolicy en el clúster o una SVM específica, puede usar parámetros de comandos para filtrar el resultado del comando según otros criterios.

Puede especificar el `-instance` parámetro para mostrar información detallada de las políticas mostradas. De forma alternativa, puede utilizar la `-fields` parámetro para mostrar solo los campos indicados en el resultado del comando. Puede entrar ? después del `-fields` parámetro para averiguar qué campos se pueden utilizar.

#### **Paso**

1. Mostrar información filtrada acerca del estado de conexión entre el nodo y el servidor FPolicy mediante el comando correspondiente:

|                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Si desea mostrar información de estado de conexión acerca de los servidores FPolicy... | Introduzca...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Que especifique                                                                        | <code>vserver fpolicy show-engine -server IP_address</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Para una SVM especificada                                                              | <code>vserver fpolicy show-engine -vserver vserver_name</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Que se adjuntan con una directiva específica                                           | <code>vserver fpolicy show-engine -policy-name policy_name</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Con el estado del servidor que especifique                                             | <code>vserver fpolicy show-engine -server-status status</code><br><br>El estado del servidor puede ser uno de los siguientes: <ul style="list-style-type: none"> <li>• <code>connected</code></li> <li>• <code>disconnected</code></li> <li>• <code>connecting</code></li> <li>• <code>disconnecting</code></li> </ul>                                                                                                                                                                                                                                                                                                                                       |
| Con el tipo especificado                                                               | <code>vserver fpolicy show-engine -server-type type</code><br><br>El tipo de servidor FPolicy puede ser uno de los siguientes: <ul style="list-style-type: none"> <li>• <code>primary</code></li> <li>• <code>secondary</code></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Que se desconectaron con el motivo especificado                                        | <code>vserver fpolicy show-engine -disconnect-reason text</code><br><br>La desconexión puede deberse a varias razones. Los siguientes son motivos comunes para la desconexión: <ul style="list-style-type: none"> <li>• <code>Disconnect command received from CLI.</code></li> <li>• <code>Error encountered while parsing notification response from FPolicy server.</code></li> <li>• <code>FPolicy Handshake failed.</code></li> <li>• <code>SSL handshake failed.</code></li> <li>• <code>TCP Connection to FPolicy server failed.</code></li> <li>• <code>The screen response message received from the FPolicy server is not valid.</code></li> </ul> |

## Ejemplo

Este ejemplo muestra información acerca de las conexiones del motor externo a los servidores FPolicy en

SVM vs1.example.com:

```
cluster1::> vsserver fpolicy show-engine -vsserver vs1.example.com
FPolicy
Vserver Policy Node Server Server- Server-
----- -
vs1.example.com policy1 node1 10.1.1.2 connected primary
vs1.example.com policy1 node1 10.1.1.3 disconnected primary
vs1.example.com policy1 node2 10.1.1.2 connected primary
vs1.example.com policy1 node2 10.1.1.3 disconnected primary
```

Este ejemplo solo muestra información acerca de los servidores FPolicy conectados:

```
cluster1::> vsserver fpolicy show-engine -fields server -server-status
connected
node vsserver policy-name server

node1 vs1.example.com policy1 10.1.1.2
node2 vs1.example.com policy1 10.1.1.2
```

**Muestra información acerca del estado de conexión de lectura de paso a través de FPolicy**

Es posible mostrar información acerca del estado de conexión de lectura directa de FPolicy en los servidores FPolicy externos (servidores FPolicy) para el clúster o para una máquina virtual de almacenamiento (SVM) especificada. Esta información puede ayudarle a determinar qué servidores de FPolicy tienen conexiones de datos de lectura directa y para los que se ha desconectado los servidores de FPolicy.

**Acerca de esta tarea**

Si no especifica ningún parámetro, el comando muestra la siguiente información:

- Nombre de SVM
- Nombre de la política de FPolicy
- Nombre del nodo
- Dirección IP del servidor FPolicy
- Estado de conexión de lectura directa de FPolicy

Además de mostrar información acerca de las conexiones de FPolicy en el clúster o una SVM específica, puede usar parámetros de comandos para filtrar el resultado del comando según otros criterios.

Puede especificar el `-instance` parámetro para mostrar información detallada de las políticas mostradas. De forma alternativa, puede utilizar la `-fields` parámetro para mostrar solo los campos indicados en el resultado del comando. Puede entrar `?` después del `-fields` parámetro para averiguar qué campos se pueden utilizar.

**Paso**



1. Mostrar información filtrada acerca del estado de conexión entre el nodo y el servidor FPolicy mediante el comando correspondiente:

|                                                                                              |                                                                                                                                                                                                                                                                                   |
|----------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Si desea mostrar información sobre el estado de la conexión acerca de...                     | Introduzca el comando...                                                                                                                                                                                                                                                          |
| El estado de la conexión de lectura directa de FPolicy para el clúster                       | <code>vserver fpolicy show-passthrough-read-connection</code>                                                                                                                                                                                                                     |
| El estado de conexión de lectura directa de FPolicy para una SVM especificada                | <code>vserver fpolicy show-passthrough-read-connection -vserver vserver_name</code>                                                                                                                                                                                               |
| Estado de conexión de lectura directa de FPolicy para una política especificada              | <code>vserver fpolicy show-passthrough-read-connection -policy-name policy_name</code>                                                                                                                                                                                            |
| El estado de conexión de lectura directa de FPolicy detallado para una política especificada | <code>vserver fpolicy show-passthrough-read-connection -policy-name policy_name -instance</code>                                                                                                                                                                                  |
| El estado de conexión de lectura directa de FPolicy correspondiente al estado especificado   | <code>vserver fpolicy show-passthrough-read-connection -policy-name policy_name -server-status status</code> El estado del servidor puede ser uno de los siguientes: <ul style="list-style-type: none"><li>• <code>connected</code></li><li>• <code>disconnected</code></li></ul> |

Ejemplo

El siguiente comando muestra información acerca de las conexiones de lectura de paso a través de todos los servidores FPolicy del clúster:

```
cluster1::> vserver fpolicy show-passthrough-read-connection
```

| Vserver         | Policy Name | Node       | FPolicy Server | Server Status |
|-----------------|-------------|------------|----------------|---------------|
| vs2.example.com | pol_cifs_2  | FPolicy-01 | 2.2.2.2        | disconnected  |
| vs1.example.com | pol_cifs_1  | FPolicy-01 | 1.1.1.1        | connected     |

El siguiente comando muestra información detallada acerca de las conexiones de lectura a través de paso desde los servidores FPolicy configurados en la política "pol\_cifs\_1":

```
cluster1::> vserver fpolicy show-passthrough-read-connection -policy-name
pol_cifs_1 -instance
```

Node: FPolicy-01

Vserver: vs1.example.com

Policy: pol\_cifs\_1

Server: 1.1.1.1

Session ID of the Control Channel: 8cef052e-2502-11e3-  
88d4-123478563412

Server Status: connected

Time Passthrough Read Channel was Connected: 9/24/2013 10:17:45

Time Passthrough Read Channel was Disconnected: -

Reason for Passthrough Read Channel Disconnection: none

## Verifique el acceso mediante el seguimiento de seguridad

### Cómo funcionan los seguimientos de seguridad

Puede añadir filtros de seguimiento de permisos para indicarle a ONTAP que registre la información sobre por qué los servidores SMB y NFS de una máquina virtual de almacenamiento (SVM) permiten o deniega la solicitud de un cliente o usuario para realizar una operación. Esto puede ser útil si desea verificar que el esquema de seguridad de acceso a archivos es adecuado o si desea solucionar problemas de acceso a archivos.

Los seguimientos de seguridad permiten configurar un filtro que detecta las operaciones del cliente en SMB y NFS en la SVM, y realizar el seguimiento de todas las comprobaciones de acceso que coinciden con ese filtro. A continuación, puede ver los resultados de la traza, lo que proporciona un resumen práctico de la razón por la que se permitió o denegó el acceso.

Cuando desee verificar la configuración de seguridad para el acceso SMB o NFS en los archivos y carpetas de la SVM o si tiene algún problema de acceso, puede añadir rápidamente un filtro para activar el seguimiento de permisos.

En la siguiente lista, se describen aspectos importantes sobre el funcionamiento de los seguimientos de seguridad:

- ONTAP aplica seguimientos de seguridad a nivel de SVM.
- Cada solicitud entrante se realiza un análisis para ver si coincide con los criterios de filtrado de cualquier seguimiento de seguridad activado.
- Los seguimientos se realizan tanto para solicitudes de acceso a archivos como a carpetas.
- Los seguimientos pueden filtrarse según los criterios siguientes:
  - IP del cliente
  - Ruta SMB o NFS
  - Nombre de Windows

- Nombre UNIX

- Las solicitudes se someten a un análisis de los resultados de respuesta de acceso *Allowed* y *denied*.
- Cada solicitud que coincide con los criterios de filtrado de trazas activadas se registra en el registro de resultados de seguimiento.
- El administrador de almacenamiento puede configurar un tiempo de espera en un filtro para deshabilitarlo automáticamente.
- Si una solicitud coincide con varios filtros, se registran los resultados del filtro con el número de índice más alto.
- El administrador de almacenamiento puede imprimir los resultados del registro de resultados de rastreo para determinar por qué se permitió o denegó una solicitud de acceso.

## **Tipos de acceso comprueba el monitor de seguimiento de seguridad**

Las comprobaciones de acceso de un archivo o una carpeta se realizan según varios criterios. Los seguimientos de seguridad supervisan las operaciones con todos estos criterios.

Los tipos de comprobaciones de acceso que supervisa el seguimiento de seguridad incluyen los siguientes:

- Estilo de seguridad del volumen y del qtree
- Seguridad efectiva del sistema de archivos que contiene los archivos y carpetas en los que se solicitan operaciones
- Asignación de usuarios
- Permisos a nivel de recurso compartido
- Permisos a nivel de exportación
- Permisos a nivel de archivo
- Seguridad para proteger el acceso al nivel de almacenamiento

## **Consideraciones que tener en cuenta al crear seguimientos de seguridad**

Debe tener en cuenta diferentes consideraciones cuando cree seguimientos de seguridad en máquinas virtuales de almacenamiento (SVM). Por ejemplo, debe saber en qué protocolos puede crear una traza, qué estilos de seguridad son compatibles y cuál es el número máximo de trazas activas.

- Solo puede crear seguimientos de seguridad en las SVM.
- Cada entrada del filtro de seguimiento de seguridad es específica para la SVM.

Debe especificar la SVM donde desee ejecutar el seguimiento.

- Puede agregar filtros de seguimiento de permisos para solicitudes SMB y NFS.
- Debe configurar el servidor SMB o NFS en la SVM donde desee crear filtros de seguimiento.
- Puede crear seguimientos de seguridad para archivos y carpetas que residen en volúmenes y qtrees de estilo de seguridad NTFS, UNIX y mixtos.
- Puede añadir un máximo de 10 filtros de seguimiento de permisos por SVM.

- Debe especificar un número de índice de filtro al crear o modificar un filtro.

Los filtros se tienen en cuenta por orden del número de índice. Los criterios de un filtro con un número de índice más alto se tienen en cuenta antes que los criterios con un número de índice más bajo. Si la solicitud que se realiza el seguimiento coincide con los criterios de varios filtros habilitados, sólo se activa el filtro con el número de índice más alto.

- Una vez creado y habilitado un filtro de seguimiento de seguridad, debe realizar algunas solicitudes de archivo o carpeta en un sistema cliente para generar la actividad que el filtro de seguimiento pueda capturar e iniciar sesión en el registro de resultados de seguimiento.
- Debe agregar filtros de seguimiento de permisos sólo para fines de verificación de acceso a archivos o solución de problemas.

La adición de filtros de seguimiento de permisos tiene un efecto secundario en el rendimiento de la controladora.

Cuando haya terminado con la actividad de verificación o solución de problemas, deberá desactivar o quitar todos los filtros de seguimiento de permisos. Además, los criterios de filtrado que seleccione deben ser lo más específicos posible para que ONTAP no envíe un gran número de resultados de seguimiento al registro.

## Realizar seguimientos de seguridad

### Realice información general sobre los seguimientos de seguridad

La realización de un seguimiento de seguridad implica la creación de un filtro de seguimiento de seguridad, la verificación de los criterios de filtro, la generación de solicitudes de acceso en un cliente SMB o NFS que coincida con los criterios de filtro y la visualización de los resultados.

Una vez que haya terminado de utilizar un filtro de seguridad para capturar información de seguimiento, puede modificar el filtro y reutilizarlo, o bien deshabilitarlo si ya no lo necesita. Después de ver y analizar los resultados de la traza del filtro, puede eliminarlos si ya no son necesarios.

### Cree filtros de seguimiento de seguridad

Es posible crear filtros de seguimiento de seguridad que detecten operaciones de cliente SMB y NFS en máquinas virtuales de almacenamiento (SVM) y realizar un seguimiento de todas las comprobaciones de acceso que coincidan con el filtro. Puede utilizar los resultados de los seguimientos de seguridad para validar la configuración o solucionar problemas de acceso.


#### Acerca de esta tarea

Hay dos parámetros necesarios para el comando `vserver Security trace filter create`:

| Parámetros necesarios | Descripción |
|-----------------------|-------------|
|-----------------------|-------------|

|                                    |                                                                                                                                                                                                                            |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-vserver vserver_name</code> | <p><i>SVM name</i></p> <p>El nombre de la SVM que contiene los archivos o las carpetas en los que se desea aplicar el filtro de seguimiento de seguridad.</p>                                                              |
| <code>-index index_number</code>   | <p><i>Número de índice de filtro</i></p> <p>El número de índice que desea aplicar al filtro. Está limitado a un máximo de 10 filtros de seguimiento por SVM. Los valores permitidos para este parámetro son de 1 a 10.</p> |

Varios parámetros de filtro opcionales le permiten personalizar el filtro de seguimiento de seguridad para limitar los resultados generados por el seguimiento de seguridad:

| Parámetro de filtro                                                                                    | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-client-ip IP_Address</code>                                                                     | Este filtro especifica la dirección IP desde la cual el usuario accede a la SVM.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <code>-path path</code>                                                                                | <p>Este filtro especifica la ruta en la que se aplicará el filtro de seguimiento de permisos. Valor para <code>-path</code> puede utilizar cualquiera de los siguientes formatos:</p> <ul style="list-style-type: none"> <li>• La ruta de acceso completa, que comienza desde la raíz del recurso compartido o la exportación</li> <li>• Una ruta parcial, relativa a la raíz del recurso compartido</li> </ul> <p>Debe usar los separadores de directorios de estilo UNIX del directorio de estilo NFS en el valor de la ruta.</p>                                                                                                                                                         |
| <code>-windows-name win_user_name</code><br>O. <code>-unix</code><br><code>-name`unix_user_name</code> | <p>Puede especificar el nombre de usuario de Windows o el nombre de usuario de UNIX cuyas solicitudes de acceso desea rastrear. La variable de nombre de usuario no distingue mayúsculas y minúsculas. No puede especificar tanto un nombre de usuario de Windows como un nombre de usuario de UNIX en el mismo filtro.</p> <div>  <p>Aunque se pueden realizar el seguimiento de eventos de acceso SMB y NFS, es posible que se utilicen el usuario UNIX asignado y los grupos de usuarios UNIX asignados al realizar comprobaciones de acceso a datos de estilo de seguridad mixtos o UNIX.</p> </div> |
| <code>-trace-allow {yes</code>                                                                         | <code>no}</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

|                                                                                                                                                                                                                                                                                            |                                                                                                                                                             |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| El seguimiento de los eventos Denegar siempre está habilitado para un filtro de seguimiento de seguridad. Opcionalmente, es posible realizar el seguimiento de los eventos de permitir. Para realizar el seguimiento de los eventos de permitir, este parámetro se debe establecer en yes. | -enabled {enabled                                                                                                                                           |
| disabled}                                                                                                                                                                                                                                                                                  | Es posible habilitar o deshabilitar el filtro de seguimiento de seguridad. De manera predeterminada, el filtro de seguimiento de seguridad está habilitado. |
| -time-enabled integer                                                                                                                                                                                                                                                                      | Puede especificar un tiempo de espera para el filtro, después del cual se deshabilita.                                                                      |

### Pasos

1. Cree un filtro de seguimiento de seguridad:

```
vserver security trace filter create -vserver vserver_name -index
index_numberfilter_parameters
```

filter\_parameters es una lista de parámetros de filtro opcionales.

Para obtener más información, consulte las páginas de manual del comando.

2. Compruebe la entrada del filtro de seguimiento de seguridad:

```
vserver security trace filter show -vserver vserver_name -index index_number
```

### Ejemplos

El siguiente comando crea un filtro de seguimiento de seguridad para cualquier usuario que acceda a un archivo con una ruta de acceso compartida \\server\share1\dir1\dir2\file.txt Desde la dirección IP 10.10.10.7. El filtro utiliza una ruta completa para el -path opción. La dirección IP del cliente utilizada para acceder a los datos es 10.10.10.7. El filtro se agota el tiempo de espera después de 30 minutos:

```
cluster1::> vserver security trace filter create -vserver vs1 -index 1
-path /dir1/dir2/file.txt -time-enabled 30 -client-ip 10.10.10.7
cluster1::> vserver security trace filter show -index 1
Vserver Index Client-IP Path Trace-Allow
Windows-Name
----- -
vs1 1 10.10.10.7 /dir1/dir2/file.txt no -
```

El siguiente comando crea un filtro de seguimiento de seguridad mediante una ruta relativa para -path opción. El filtro rastrea el acceso de un usuario de Windows llamado "joe". Joe está accediendo a un archivo

con una ruta de acceso compartido \\server\share1\dir1\dir2\file.txt. Los seguimientos de filtro permiten y niegan eventos:

```
cluster1::> vserver security trace filter create -vserver vs1 -index 2
-path /dir1/dir2/file.txt -trace-allow yes -windows-name mydomain\joe

cluster1::> vserver security trace filter show -vserver vs1 -index 2
 Vserver: vs1
 Filter Index: 2
 Client IP Address to Match: -
 Path: /dir1/dir2/file.txt
 Windows User Name: mydomain\joe
 UNIX User Name: -
 Trace Allow Events: yes
 Filter Enabled: enabled
 Minutes Filter is Enabled: 60
```

**Muestra información acerca de los filtros de seguimiento de seguridad**

Es posible ver información sobre los filtros de seguimiento de seguridad configurados en la máquina virtual de almacenamiento (SVM). Esto le permite ver qué tipos de eventos de acceso tienen cada seguimiento de filtro.

**Paso**

- 1. Muestra información acerca de las entradas del filtro de seguimiento de seguridad mediante `vserver security trace filter show` comando.
- Para obtener más información acerca de cómo utilizar este comando, consulte las páginas man.

**Ejemplos**

El siguiente comando muestra información sobre todos los filtros de seguimiento de seguridad en la SVM vs1:

```
cluster1::> vserver security trace filter show -vserver vs1
Vserver Index Client-IP Path Trace-Allow
Windows-Name
----- -
vs1 1 - /dir1/dir2/file.txt yes -
vs1 2 - /dir3/dir4/ no
mydomain\joe
```

**Mostrar resultados de rastreo de seguridad**

Puede mostrar los resultados de seguimiento de seguridad generados para las operaciones de archivo que coinciden con los filtros de seguimiento de seguridad. Puede

utilizar los resultados para validar la configuración de seguridad del acceso a los archivos o para solucionar problemas de acceso a los archivos SMB y NFS.

**Lo que necesitará**

Debe existir un filtro de seguimiento de seguridad habilitado y las operaciones deben haberse realizado desde un cliente SMB o NFS que coincida con el filtro de seguimiento de seguridad para generar los resultados de seguimiento de seguridad.

**Acerca de esta tarea**

Puede mostrar un resumen de todos los resultados de seguimiento de seguridad o puede personalizar la información que se muestra en el resultado especificando parámetros opcionales. Esto puede ser útil cuando los resultados de la traza de seguridad contienen un gran número de registros.

Si no especifica ninguno de los parámetros opcionales, se muestra lo siguiente:

- El nombre de la máquina virtual de almacenamiento (SVM)
- Nombre del nodo
- Número de índice de seguimiento de seguridad
- Estilo de seguridad
- Ruta
- Razón
- Nombre de usuario

El nombre de usuario se mostrará en función de la configuración del filtro de seguimiento:

|                                     |                                                                                |
|-------------------------------------|--------------------------------------------------------------------------------|
| Si el filtro está configurado...    | Realice lo siguiente...                                                        |
| Con un nombre de usuario UNIX       | El resultado de la traza de seguridad muestra el nombre de usuario de UNIX.    |
| Con un nombre de usuario de Windows | El resultado de la traza de seguridad muestra el nombre de usuario de Windows. |
| Sin un nombre de usuario            | El resultado de la traza de seguridad muestra el nombre de usuario de Windows. |

Puede personalizar la salida utilizando parámetros opcionales. Algunos de los parámetros opcionales que se pueden utilizar para refinar los resultados devueltos en el resultado del comando son los siguientes:

|                         |                                                                                                                                                  |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| Parámetro opcional      | Descripción                                                                                                                                      |
| -fields field_name, ... | Muestra el resultado en los campos que elija. Es posible usar este parámetro de forma independiente o combinada con otros parámetros opcionales. |



|                                |                                                                                                                                                                                                                     |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -instance                      | Muestra información detallada acerca de los eventos de seguimiento de seguridad. Use este parámetro con otros parámetros opcionales para mostrar información detallada sobre los resultados específicos del filtro. |
| -node node_name                | Muestra información solo sobre eventos en el nodo especificado.                                                                                                                                                     |
| -vserver vserver_name          | Muestra información solo sobre eventos en la SVM especificada.                                                                                                                                                      |
| -index integer                 | Muestra información sobre los eventos que ocurrieron como resultado del filtro correspondiente al número de índice especificado.                                                                                    |
| -client-ip IP_address          | Muestra información sobre los eventos ocurridos como resultado del acceso a archivos desde la dirección IP del cliente especificada.                                                                                |
| -path path                     | Muestra información sobre los eventos producidos como resultado del acceso a archivos a la ruta especificada.                                                                                                       |
| -user-name user_name           | Muestra información acerca de los eventos que ocurrieron como resultado del acceso a archivos por parte del usuario de Windows o UNIX especificado.                                                                 |
| -security-style security_style | Muestra información sobre los eventos que ocurrieron en sistemas de archivos con el estilo de seguridad especificado.                                                                                               |

Consulte la página man para obtener información sobre otros parámetros opcionales que puede utilizar con el comando.

## Paso

1. Mostrar los resultados del filtro de seguimiento de seguridad mediante la `vserver security trace trace-result show` comando.

```
vserver security trace trace-result show -user-name domain\user
```

```
Vserver: vs1
```

| Node  | Index | Filter Details                                               | Reason                        |
|-------|-------|--------------------------------------------------------------|-------------------------------|
| ----- | ----- | -----                                                        | -----                         |
| node1 | 3     | User:domain\user<br>Security Style:mixed<br>Path:/dir1/dir2/ | Access denied by explicit ACE |
| node1 | 5     | User:domain\user<br>Security Style:unix<br>Path:/dir1/       | Access denied by explicit ACE |

## Modificar filtros de seguimiento de seguridad

Si desea cambiar los parámetros de filtro opcionales utilizados para determinar qué eventos de acceso se rastrean, puede modificar los filtros de seguimiento de seguridad existentes.

### Acerca de esta tarea

Debe identificar el filtro de seguimiento de seguridad que desea modificar especificando el nombre de la máquina virtual de almacenamiento (SVM) en la que se aplica el filtro y el número de índice del filtro. Puede modificar todos los parámetros de filtro opcionales.

### Pasos

1. Modificar un filtro de seguimiento de seguridad:

```
vserver security trace filter modify -vserver vserver_name -index
index_numberfilter_parameters
```

- ° `vserver_name` Es el nombre de la SVM en la que desea aplicar un filtro de seguimiento de seguridad.
- ° `index_number` es el número de índice que desea aplicar al filtro. Los valores permitidos para este parámetro son de 1 a 10.
- ° `filter_parameters` es una lista de parámetros de filtro opcionales.

2. Compruebe la entrada del filtro de seguimiento de seguridad:

```
vserver security trace filter show -vserver vserver_name -index index_number
```

### Ejemplo

El siguiente comando modifica el filtro de seguimiento de seguridad con el número de índice 1. El filtro realiza un seguimiento de los eventos de cualquier usuario que acceda a un archivo con una ruta de acceso compartido `\\server\share1\dir1\dir2\file.txt` Desde cualquier dirección IP. El filtro utiliza una ruta completa para el `-path` opción. Los seguimientos de filtro permiten y niegan eventos:

```
cluster1::> vserver security trace filter modify -vserver vs1 -index 1
-path /dir1/dir2/file.txt -trace-allow yes

cluster1::> vserver security trace filter show -vserver vs1 -index 1
Vserver: vs1
Filter Index: 1
Client IP Address to Match: -
Path: /dir1/dir2/file.txt
Windows User Name: -
UNIX User Name: -
Trace Allow Events: yes
Filter Enabled: enabled
Minutes Filter is Enabled: 60
```

**Elimine filtros de seguimiento de seguridad**

Si ya no necesita una entrada de filtro de seguimiento de seguridad, puede eliminarla. Debido a que puede tener un máximo de 10 filtros de seguimiento de seguridad por máquina virtual de almacenamiento (SVM), al eliminar filtros innecesarios, podrá crear nuevos filtros si llegó al máximo.

**Acerca de esta tarea**

Para identificar de forma única el filtro de seguimiento de seguridad que desea eliminar, debe especificar lo siguiente:

- Nombre de la SVM a la que se aplica el filtro de seguimiento
- El número de índice del filtro de seguimiento

**Pasos**

1. Identifique el número de índice de filtro de la entrada del filtro de seguimiento de seguridad que desea eliminar:

```
vserver security trace filter show -vserver vserver_name

vserver security trace filter show -vserver vs1
```

| Vserver      | Index | Client-IP | Path                | Trace-Allow |
|--------------|-------|-----------|---------------------|-------------|
| Windows-Name |       |           |                     |             |
| -----        | ----- | -----     | -----               | -----       |
| vs1          | 1     | -         | /dir1/dir2/file.txt | yes         |
| vs1          | 2     | -         | /dir3/dir4/         | no          |
| mydomain\joe |       |           |                     |             |

2. Utilizando la información del número de índice de filtro del paso anterior, elimine la entrada de filtro:

```
vserver security trace filter delete -vserver vserver_name -index index_number

vserver security trace filter delete -vserver vs1 -index 1
```

3. Compruebe que la entrada del filtro de seguimiento de seguridad se ha eliminado:

```
vserver security trace filter show -vserver vserver_name

vserver security trace filter show -vserver vs1
```

| Vserver      | Index | Client-IP | Path        | Trace-Allow |
|--------------|-------|-----------|-------------|-------------|
| Windows-Name |       |           |             |             |
| -----        | ----- | -----     | -----       | -----       |
| vs1          | 2     | -         | /dir3/dir4/ | no          |
| mydomain\joe |       |           |             |             |

## Eliminar registros de rastreo de seguridad

Después de terminar de utilizar un registro de seguimiento de filtro para verificar la seguridad de acceso a archivos o para solucionar problemas de acceso de clientes SMB o NFS, puede eliminar el registro de seguimiento de seguridad del registro de seguimiento de seguridad.

### Acerca de esta tarea

Para poder eliminar un registro de seguimiento de seguridad, debe conocer el número de secuencia del registro.



Cada máquina virtual de almacenamiento (SVM) puede almacenar un máximo de 128 registros de seguimiento. Si se alcanza el máximo en la SVM, los registros de seguimiento más antiguos se eliminan automáticamente a medida que se añaden otros nuevos. Si no desea eliminar manualmente los registros de seguimiento de esta SVM, es posible eliminar automáticamente ONTAP los resultados de rastros más antiguos después de alcanzar el máximo para hacer espacio para nuevos resultados.

### Pasos

1. Identifique el número de secuencia del registro que desea eliminar:

```
vserver security trace trace-result show -vserver vserver_name -instance
```

2. Elimine el registro de seguimiento de seguridad:

```
vserver security trace trace-result delete -node node_name -vserver
vserver_name -seqnum integer
```

```
vserver security trace trace-result delete -vserver vs1 -node node1 -seqnum
999
```

- `-node node_name` es el nombre del nodo de clúster en el que se produjo el evento de seguimiento de permisos que desea eliminar.

Este es un parámetro obligatorio.

- `-vserver vserver_name` Es el nombre de la SVM donde se produjo el evento de seguimiento de permisos que desea eliminar.

Este es un parámetro obligatorio.

- `-seqnum integer` es el número de secuencia del evento de registro que se desea eliminar.

Este es un parámetro obligatorio.

## Elimine todos los registros de rastreo de seguridad

Si no desea conservar ninguno de los registros de seguimiento de seguridad existentes, puede eliminar todos los registros de un nodo con un único comando.

### Paso

1. Eliminar todos los registros de rastreo de seguridad:

```
vserver security trace trace-result delete -node node_name -vserver
vserver_name *
```

- ° `-node node_name` es el nombre del nodo de clúster en el que se produjo el evento de seguimiento de permisos que desea eliminar.
- ° `-vserver vserver_name` Es el nombre de la máquina virtual de almacenamiento (SVM) donde se produjo el evento de seguimiento de permisos que desea eliminar.

## Interpretar los resultados de las trazas de seguridad

Los resultados del seguimiento de seguridad proporcionan el motivo por el que se permitía o denegaba una solicitud. Salida muestra el resultado como una combinación de la razón por la que se permite o deniega el acceso y la ubicación dentro de la ruta de comprobación de acceso en la que se permite o se deniega el acceso. Puede utilizar los resultados para aislar e identificar por qué se permiten o no acciones.

### Búsqueda de información acerca de las listas de tipos de resultados y detalles de filtro

Puede encontrar las listas de tipos de resultados y detalles de filtro que se pueden incluir en los resultados del rastreo de seguridad en las páginas man de `vserver security trace trace-result show` comando.

### Ejemplo de resultado de la Reason en un Allow tipo de resultado

A continuación se muestra un ejemplo del resultado de la Reason campo que aparece en el registro de resultados de seguimiento en un Allow tipo de resultado:

```
Access is allowed because SMB implicit permission grants requested
access while opening existing file or directory.
```

```
Access is allowed because NFS implicit permission grants requested
access while opening existing file or directory.
```

### Ejemplo de resultado de la Reason en un Deny tipo de resultado

A continuación se muestra un ejemplo del resultado de la Reason campo que aparece en el registro de resultados de seguimiento en un Deny tipo de resultado:

```
Access is denied. The requested permissions are not granted by the
ACE while checking for child-delete access on the parent.
```

### Ejemplo de resultado de la `Filter details` campo

A continuación se muestra un ejemplo del resultado de la `Filter details` campo del registro de resultados de seguimiento, que enumera el estilo de seguridad efectivo del sistema de archivos que contiene archivos y carpetas que coinciden con los criterios de filtro:

```
Security Style: MIXED and ACL
```

## Dónde encontrar información adicional

Una vez que haya probado correctamente el acceso al cliente SMB, puede ejecutar la configuración avanzada de SMB o añadir acceso SAN. Una vez que haya probado correctamente el acceso al cliente NFS, puede ejecutar una configuración de NFS avanzada o añadir acceso SAN. Una vez completado el acceso al protocolo, debe proteger el volumen raíz de la SVM.

### Configuración de SMB

Puede configurar el acceso SMB además utilizando lo siguiente:

- ["Gestión de SMB"](#)

Describe cómo configurar y gestionar el acceso a archivos mediante el protocolo SMB.

- ["Informe técnico de NetApp 4191: Guía de mejores prácticas para servicios de archivos de Windows para Clustered Data ONTAP 8.2"](#)

Proporciona una breve descripción general de la implementación de SMB y otras funciones de servicios de archivos Windows con recomendaciones e información básica sobre solución de problemas para ONTAP.

- ["Informe técnico de NetApp 3740: Protocolo CIFS de última generación de SMB 2 en Data ONTAP"](#)

Describe las funciones de SMB 2, los detalles de configuración y su implementación en ONTAP.

### Configuración de NFS

Puede configurar el acceso NFS de forma adicional utilizando lo siguiente:

- ["Gestión de NFS"](#)

Describe cómo configurar y gestionar el acceso a archivos mediante el protocolo NFS.

- ["Informe técnico de NetApp 4067: Guía de prácticas recomendadas e implementación de NFS"](#)

Sirve de guía de funcionamiento de NFSv3 y NFSv4 y ofrece una descripción general del sistema operativo de ONTAP haciendo hincapié en NFSv4.

- ["Informe técnico de NetApp 4668: Guía de prácticas recomendadas de servicios de nombres"](#)

Proporciona una lista completa de prácticas recomendadas, límites, recomendaciones y consideraciones a la hora de configurar archivos de LDAP, NIS, DNS y usuarios locales y de grupos para fines de autenticación.

- ["Informe técnico de NetApp 4616: Kerberos de NFS en ONTAP con Microsoft Active Directory"](#)
- ["Informe técnico de NetApp 4835: Cómo configurar LDAP en ONTAP"](#)
- ["Informe técnico de NetApp 3580: Guía de mejoras y prácticas recomendadas de NFSv4: Implementación de Data ONTAP"](#)

Describe las prácticas recomendadas que se deben seguir mientras implementa componentes de NFSv4 en clientes AIX, Linux o Solaris conectados a sistemas que ejecutan ONTAP.

## Protección de volúmenes raíz

Después de configurar los protocolos en la SVM, debe asegurarse de que su volumen raíz esté protegido:

- ["Protección de datos"](#)

Describe cómo crear un reflejo de uso compartido de carga para proteger el volumen raíz de SVM, que es una práctica recomendada por NetApp para SVM habilitadas para NAS. También describe cómo recuperarse rápidamente de fallos o pérdidas de volúmenes mediante la promoción del volumen raíz de SVM desde un reflejo de uso compartido de carga.

# Gestione el cifrado con System Manager



## Cifre los datos almacenados mediante el cifrado basado en software

Use el cifrado de volúmenes para garantizar que los datos de volúmenes no se puedan leer si el dispositivo subyacente se reasigna, se devuelve, se pierde o es robado. El cifrado de volúmenes no requiere discos especiales; funciona con todos los HDD y SSD.

El cifrado de volúmenes requiere un gestor de claves. Puede configurar el gestor de claves incorporado con System Manager. También puede usar un administrador de claves externo, pero primero debe configurarlo mediante la CLI de ONTAP.

Una vez que se configura el gestor de claves, los nuevos volúmenes se cifran de forma predeterminada.

### Pasos

1. Haga clic en **clúster > Configuración**.
2. En **cifrado**, haga clic en  Para configurar el gestor de claves incorporado por primera vez.
3. Para cifrar los volúmenes existentes, haga clic en **almacenamiento > volúmenes**.
4. En el volumen deseado, haga clic en  Y, a continuación, haga clic en **Editar**.
5. Seleccione **Activar cifrado**.

## Cifre los datos almacenados mediante unidades de autocifrado



Use el cifrado de discos para garantizar que no se puedan leer todos los datos de un

nivel local si el dispositivo subyacente se reasigna, se devuelve, se pierde o es robado. El cifrado de discos requiere discos duros o SSD de cifrado automático especiales.

El cifrado de discos requiere un gestor de claves. Puede configurar el gestor de claves incorporado mediante System Manager. También puede usar un administrador de claves externo, pero primero debe configurarlo mediante la CLI de ONTAP.

Si ONTAP detecta discos de autocifrado, se le solicita que configure el gestor de claves incorporado al crear el nivel local.

### Pasos

1. En **cifrado**, haga clic en  para configurar el gestor de claves incorporado.
2. Si aparece un mensaje que indica que es necesario volver a asignar la clave a los discos, haga clic en  Y, a continuación, haga clic en **Rekey Disks**.

## Gestione el cifrado con la interfaz de línea de comandos

### Información general de cifrado NetApp

NetApp ofrece tecnologías de cifrado basadas en software y hardware para garantizar que los datos en reposo no se puedan leer en caso de reasignación, devolución, pérdida o robo del medio de almacenamiento.

- El cifrado basado en software con el cifrado de volúmenes de NetApp (NVE) admite el cifrado de datos de un volumen por vez
- El cifrado basado en hardware con el cifrado del almacenamiento de NetApp (NSE) admite el cifrado de disco completo (FDE) de los datos a medida que se escriben.

### Configure el cifrado de volúmenes de NetApp

#### Configure la información general de cifrado de volúmenes de NetApp

El cifrado de volúmenes de NetApp (NVE) es una tecnología basada en software para cifrar datos en reposo un volumen por vez. Una clave de cifrado a la que solo se puede acceder el sistema de almacenamiento garantiza que los datos de volumen no se puedan leer si el dispositivo subyacente se reasigna, se devuelve, se pierde o es robado.

#### Comprender NVE

Con NVE, tanto los metadatos como los datos (incluidas las copias Snapshot) están cifrados. El acceso a los datos se proporciona mediante una clave XTS-AES-256 exclusiva, una por volumen. Un servidor de gestión de claves externo o un gestor de claves incorporado (OKM) proporciona claves a los nodos:

- El servidor de gestión de claves externo es un sistema de terceros en el entorno de almacenamiento que proporciona claves a los nodos mediante el protocolo de interoperabilidad de gestión de claves (KMIP). Se recomienda configurar servidores de gestión de claves externos a partir de sus datos en un sistema de almacenamiento diferente.
- El gestor de claves incorporado es una herramienta integrada que proporciona claves para nodos desde el mismo sistema de almacenamiento que los datos.



A partir de ONTAP 9.7, el cifrado de volúmenes y agregados se habilita de forma predeterminada si se dispone de una licencia de cifrado de volúmenes (ve) y se usa un gestor de claves incorporado o externo. La licencia VE se incluye con "ONTAP One". Siempre que se configure un gestor de claves externo o incorporado, habrá un cambio en el modo en que la configuración del cifrado de datos en reposo está establecida para los agregados y volúmenes totalmente nuevos. Los nuevos agregados tendrán activado de forma predeterminada el cifrado de agregados de NetApp (NAE). Los volúmenes nuevos que no forman parte de un agregado de NAE tendrán habilitado el cifrado de volúmenes de NetApp (NVE), de forma predeterminada. Si una máquina virtual de almacenamiento de datos (SVM) está configurada con su propio gestor de claves mediante la gestión de claves multi-tenant, el volumen creado para esa SVM se configura automáticamente con NVE.

Puede habilitar el cifrado en un volumen nuevo o existente. NVE es compatible con toda la gama de funciones de eficiencia del almacenamiento, incluidas la deduplicación y la compresión. A partir de ONTAP 9.14.1, puede hacerlo [Habilite NVE en los volúmenes raíz de la SVM existentes](#).



Si utiliza SnapLock, puede habilitar el cifrado solo en volúmenes de SnapLock nuevos y vacíos. No puede habilitar el cifrado en un volumen de SnapLock existente.

Es posible utilizar el NVE en cualquier tipo de agregado (HDD, SSD, híbrido, LUN de cabina), con cualquier tipo de RAID y en cualquier implementación de ONTAP compatible, incluido ONTAP Select. También puede utilizar NVE con cifrado basado en hardware para «doble cifrado» de datos en unidades con autocifrado.

Cuando NVE está habilitado, el volcado de memoria también se cifra.

#### **Cifrado a nivel de agregado**

Normalmente, a cada volumen cifrado se le asigna una clave única. Cuando se elimina el volumen, la clave se elimina con él.

A partir de ONTAP 9.6, puede usar *NetApp Aggregate Encryption (NAE)* para asignar claves al agregado que contiene los volúmenes que se van a cifrar. Cuando se elimina un volumen cifrado, se conservan las claves del agregado. Las claves se eliminan si se elimina todo el agregado.

Debe utilizar el cifrado a nivel de agregado si tiene pensado realizar deduplicación en línea o en segundo plano a nivel de agregado. De lo contrario, NVE no admite la deduplicación a nivel de agregado.

A partir de ONTAP 9.7, el cifrado de volúmenes y agregados se habilita de forma predeterminada si se dispone de una licencia de cifrado de volúmenes (ve) y se usa un gestor de claves incorporado o externo.

Los volúmenes NVE y NAE pueden coexistir en el mismo agregado. Los volúmenes cifrados con el cifrado a nivel de agregado son, de forma predeterminada, los volúmenes NAE. Puede anular el valor predeterminado al cifrar el volumen.

Puede utilizar el `volume move` Comando para convertir un volumen NVE en un volumen NAE y viceversa. Es posible replicar un volumen NAE en un volumen NVE.

No puede utilizar `secure purge` Comandos en un volumen NAE.

#### **Cuándo usar servidores de gestión de claves externos**

Aunque es menos caro y, en general, más práctico para usar el gestor de claves incorporado, debe configurar los servidores KMIP si se da alguna de las siguientes situaciones:

- Su solución de gestión de claves de cifrado debe cumplir con el estándar de procesamiento de información federal (FIPS) 140-2 o el estándar KMIP DE OASIS.

- Necesita una solución de varios clústeres con gestión centralizada de las claves de cifrado.
- Su empresa requiere una seguridad añadida para almacenar claves de autenticación en un sistema o en una ubicación distinta de los datos.

### Ámbito de la gestión de claves externas

El alcance de la gestión de claves externas determina si los servidores de gestión de claves protegen todas las SVM del clúster o solo las SVM seleccionadas:

- Puede usar un *cluster scope* a fin de configurar la gestión de claves externas para todas las SVM del clúster. El administrador de clúster tiene acceso a todas las claves almacenadas en los servidores.
- A partir de ONTAP 9.6, se puede usar un *SVM Scope* para configurar la gestión de claves externas para una SVM con nombre en el clúster. Esto es mejor para entornos multi-tenant en los que cada inquilino usa una SVM (o un conjunto de SVM) diferente para servir datos. Solo el administrador de SVM para un inquilino determinado tiene acceso a las claves de ese inquilino.
- A partir de ONTAP 9.10.1, se puede utilizar [Azure Key Vault](#) y [Google Cloud KMS](#) Para proteger las claves NVE solo para SVM de datos. Está disponible para el KMS de AWS a partir de 9.12.0.

Puede utilizar ambos ámbitos en el mismo clúster. Si se configuraron servidores de gestión de claves para una SVM, ONTAP solo usa esos servidores para proteger las claves. De lo contrario, ONTAP protege las claves con los servidores de gestión de claves configurados para el clúster.

Hay disponible una lista de los gestores de claves externos validados en la "[Herramienta de matriz de interoperabilidad de NetApp \(IMT\)](#)". Puede encontrar esta lista introduciendo el término «gestores clave» en la función de búsqueda de IMT.

### Detalles de soporte

En la siguiente tabla se muestran los detalles de soporte de NVE:

| Recurso o característica | Detalles de soporte                                                                                                                           |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| Plataformas              | Se requiere capacidad de descarga de AES-ni. Consulte Hardware Universe (HWU) para verificar que NVE y NAE son compatibles con su plataforma. |

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cifrado                     | <p>A partir de ONTAP 9.7, los agregados y volúmenes recién creados se cifran de forma predeterminada cuando se añade una licencia de cifrado de volúmenes (ve) y se configura un gestor de claves externo o integrado. Si necesita crear un agregado no cifrado, utilice el siguiente comando:</p> <pre>storage aggregate create -encrypt-with-aggr-key false</pre> <p>Si necesita crear un volumen de texto sin formato, utilice el siguiente comando:</p> <pre>volume create -encrypt false</pre> <p>El cifrado no está activado de forma predeterminada si:</p> <ul style="list-style-type: none"> <li>• LA licencia VE no está instalada.</li> <li>• El gestor de claves no está configurado.</li> <li>• La plataforma o el software no admiten el cifrado.</li> <li>• El cifrado de hardware está activado.</li> </ul> |
| ONTAP                       | Todas las implementaciones de ONTAP. La compatibilidad con ONTAP Cloud está disponible en ONTAP 9.5 y versiones posteriores.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Dispositivos                | HDD, SSD, híbrido, LUN de cabina.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| RAID                        | RAID0, RAID4, RAID-DP, RAID-TEC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Volúmenes                   | Volúmenes de datos y volúmenes raíz de SVM existentes. No se pueden cifrar datos en volúmenes de metadatos de MetroCluster. En versiones de ONTAP anteriores a 9.14.1, no se pueden cifrar datos en el volumen raíz de la SVM con NVE. A partir de ONTAP 9.14.1, ONTAP admite <a href="#">NVE en volúmenes raíz de SVM</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Cifrado a nivel de agregado | <p>A partir de ONTAP 9.6, NVE admite el cifrado a nivel de agregado (NAE):</p> <ul style="list-style-type: none"> <li>• Debe utilizar el cifrado a nivel de agregado si tiene pensado realizar deduplicación en línea o en segundo plano a nivel de agregado.</li> <li>• No se puede volver a introducir la clave de un volumen de cifrado en el nivel de un agregado.</li> <li>• La opción de purga segura no es compatible con los volúmenes de cifrado a nivel de agregado.</li> <li>• Además de los volúmenes de datos, NAE admite el cifrado de volúmenes raíz de SVM y el volumen de metadatos de MetroCluster. NAE no admite el cifrado del volumen raíz.</li> </ul>                                                                                                                                                 |
| Alcance de SVM              | A partir de ONTAP 9.6, NVE admite el ámbito de SVM solo para la gestión de claves externas, no para el gestor de claves incorporado. MetroCluster es compatible a partir de ONTAP 9.8.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

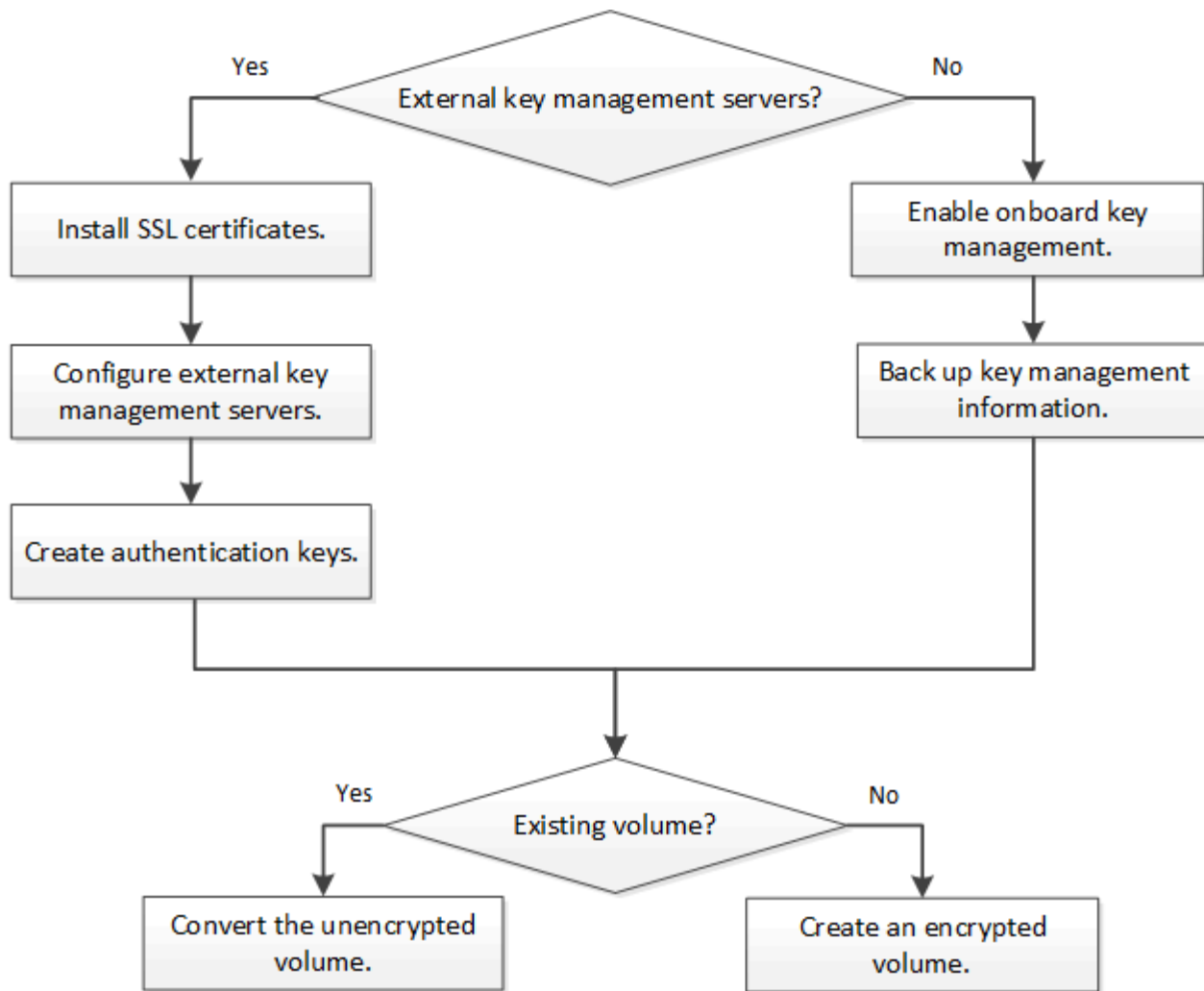
|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Eficiencia del almacenamiento | <p>Deduplicación, compresión, compactación, FlexClone.</p> <p>Los clones utilizan la misma clave que el elemento principal, incluso después de dividir el clon del elemento principal. Debe realizar un <code>volume move</code> en un clon dividido, después del cual el clon dividido tendrá una clave diferente.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Replicación                   | <ul style="list-style-type: none"> <li>• Para la replicación de volúmenes, los volúmenes de origen y destino pueden tener diferentes configuraciones de cifrado. El cifrado se puede configurar para el origen y sin configurar para el destino, y viceversa.</li> <li>• Para la replicación de SVM, el volumen de destino se cifra automáticamente, a menos que el destino no contenga un nodo compatible con el cifrado de volúmenes, en cuyo caso la replicación se realice correctamente, pero el volumen de destino no está cifrado.</li> <li>• Para las configuraciones de MetroCluster, cada clúster extrae claves de gestión de claves externas de sus servidores de claves configurados. El servicio de replicación de configuración replica las claves de OKM al sitio del partner.</li> </ul> |
| Cumplimiento de normativas    | A partir de ONTAP 9.2, SnapLock es compatible en los modos Compliance y Enterprise, sólo para nuevos volúmenes. No puede habilitar el cifrado en un volumen de SnapLock existente.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| FlexGroups                    | A partir de ONTAP 9.2, los FlexGroup son compatibles. Los agregados de destino deben tener el mismo tipo que los agregados de origen, ya sea a nivel de volumen o de agregado. A partir de ONTAP 9.5, se admite la reclave sin movimiento de volúmenes FlexGroup.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Transición de 7-Mode          | A partir de 7-Mode Transition Tool 3.3, puede utilizar la CLI de 7-Mode Transition Tool para realizar una transición basada en copias a los volúmenes de destino habilitados para NVE en el sistema en clúster.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

#### Información relacionada

["Preguntas más frecuentes: Cifrado de volúmenes de NetApp y cifrado de agregados de NetApp"](#)

#### Flujo de trabajo de cifrado de volúmenes de NetApp

Es necesario configurar servicios de gestión de claves para poder habilitar el cifrado de volúmenes. Puede habilitar el cifrado en un volumen nuevo o en uno existente.



"[Debe instalar la licencia VE](#)" Y configure los servicios de gestión de claves antes de poder cifrar datos con NVE. Antes de instalar la licencia, debería "[Determine si la versión de ONTAP es compatible con NVE](#)".

## Configure NVE

### Determine si la versión del clúster es compatible con NVE

Debe determinar si la versión de clúster es compatible con NVE antes de instalar la licencia. Puede utilizar el `version` comando para determinar la versión del clúster.

### Acerca de esta tarea

La versión del clúster es la versión más baja de ONTAP que se ejecuta en cualquier nodo del clúster.

### Paso

1. Determine si la versión de clúster es compatible con NVE:

```
version -v
```

NVE no es compatible si el resultado del comando muestra el texto «'1Ono-DARE» (del cifrado «no de datos en reposo») o si utiliza una plataforma que no aparezca en la "[Detalles de soporte](#)".

El siguiente comando determina si se admite NVE a. `cluster1`.

```
cluster1::> version -v
NetApp Release 9.1.0: Tue May 10 19:30:23 UTC 2016 <1Ono-DARE>
```

El resultado de 1Ono-DARE Indica que la versión del clúster no es compatible con NVE.

## Instale la licencia

Una licencia ve le permite usar la función en todos los nodos del clúster. Esta licencia es necesaria para poder cifrar datos con NVE. Se incluye con ["ONTAP One"](#).

Antes de ONTAP One, la licencia VE se incluía con el paquete de cifrado. El bundle de cifrado ya no se ofrece, pero sigue siendo válido. Aunque actualmente no es obligatorio, los clientes existentes pueden optar por hacerlo ["Actualice a ONTAP One"](#).

## Antes de empezar

- Para realizar esta tarea, debe ser un administrador de clústeres.
- Debe haber recibido la clave de licencia de VE de su representante de ventas o tener instalado ONTAP One.

## Pasos

1. ["Compruebe que la licencia VE está instalada"](#).

El nombre del paquete de licencia de VE es `VE`.

2. Si la licencia no está instalada, ["Use System Manager o la interfaz de línea de comandos de ONTAP para instalarlo"](#).

## Configure la gestión de claves externas

### Configure información general sobre la gestión de claves externas

Puede usar uno o varios servidores de gestión de claves externos para proteger las claves que utiliza el clúster para acceder a los datos cifrados. Un servidor de gestión de claves externo es un sistema de terceros en el entorno de almacenamiento que proporciona claves a los nodos mediante el protocolo de interoperabilidad de gestión de claves (KMIP).



Para ONTAP 9.1 y versiones anteriores, las LIF de gestión de nodos se deben asignar a los puertos que están configurados con el rol de gestión de nodos antes de poder usar el gestor de claves externo.

El cifrado de volúmenes de NetApp (NVE) es compatible con el gestor de claves incorporado en ONTAP 9.1 y versiones posteriores. A partir de ONTAP 9.3, NVE admite la gestión de claves externas (KMIP) y el gestor de claves incorporado. A partir de ONTAP 9.10.1, puede utilizar [Azure Key Vault o el servicio de Google Cloud Key Manager](#) Para proteger las claves NVE. A partir de ONTAP 9.11.1, es posible configurar varios administradores de claves externos en un clúster de. Consulte [Configurar servidores de claves en cluster](#).

## Gestione los administradores de claves externos con System Manager

A partir de ONTAP 9,7, puede almacenar y administrar claves de autenticación y cifrado con el Administrador de claves integrado. A partir de ONTAP 9.13.1, también es posible usar gestores de claves externos para almacenar y gestionar estas claves.

El gestor de claves incorporado almacena y gestiona claves en una base de datos segura interna del clúster. Su alcance es el cluster. Un gestor de claves externo almacena y gestiona claves fuera del clúster. Su alcance puede ser el clúster o el equipo virtual de almacenamiento. Pueden usarse uno o más administradores de claves externos. Se aplican las siguientes condiciones:

- Si se habilita el gestor de claves incorporado, no es posible habilitar un gestor de claves externo en el nivel del clúster, pero se puede habilitar en el nivel de máquina virtual de almacenamiento.
- Si se habilita un gestor de claves externo en el nivel de clúster, no se puede habilitar el administrador de claves incorporado.

Al usar administradores de claves externos, puede registrar hasta cuatro servidores de claves primarios por máquina virtual y clúster de almacenamiento. Cada servidor de claves primario se puede agrupar en clúster con hasta tres servidores de claves secundarios.

### Configure un gestor de claves externo


Para añadir un administrador de claves externo para una máquina virtual de almacenamiento, debe añadir una puerta de enlace opcional al configurar la interfaz de red para la máquina virtual de almacenamiento. Si la máquina virtual de almacenamiento se creó sin la ruta de red, deberá crear la ruta explícitamente para el gestor de claves externo. Consulte "[Crear una LIF \(interfaz de red\)](#)".



### Pasos

Es posible configurar un administrador de claves externo comenzando desde distintas ubicaciones de System Manager.

1. Para configurar un gestor de claves externo, realice uno de los siguientes pasos de inicio.

| Flujo de trabajo                     | Navegación                         | Paso inicial                                                                                                                                                                                              |
|--------------------------------------|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configure el Administrador de claves | <b>Clúster &gt; Ajustes</b>        | Desplácese a la sección <b>Seguridad</b> . En <b>Cifrado</b> , seleccione  . Seleccione <b>External Key Manager</b> . |
| Agregar nivel local                  | <b>Almacenamiento &gt; Niveles</b> | Seleccione <b>+ Agregar nivel local</b> . Marque la casilla de verificación denominada Configurar Administrador de claves. Seleccione <b>External Key Manager</b> .                                       |
| Prepare el almacenamiento            | <b>Tablero</b>                     | En la sección <b>Capacidad</b> , selecciona <b>Preparar almacenamiento</b> . A continuación, seleccione Configure Key Manager. Seleccione <b>External Key Manager</b> .                                   |

|                                                                                          |                                                 |                                                                                                                                                                                                                                             |
|------------------------------------------------------------------------------------------|-------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configurar cifrado (gestor de claves únicamente en el ámbito de la VM de almacenamiento) | <b>Almacenamiento &gt; VM de almacenamiento</b> | Seleccione la máquina virtual de almacenamiento. Seleccione la pestaña <b>Ajustes</b> . En la sección <b>Cifrado</b> en <b>Seguridad</b> , seleccione  . |
|------------------------------------------------------------------------------------------|-------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|



- Para agregar un servidor de claves primario, seleccione  **Add**, Y complete los campos **IP Address** o **Host Name** y **Port**.
- Los certificados instalados existentes se enumeran en los campos **Certificados de CA de servidor KMIP** y **Certificado de cliente KMIP**. Puede realizar cualquiera de las siguientes acciones:
  - Seleccione  para seleccionar los certificados instalados que desea asignar al gestor de claves. (Se pueden seleccionar varios certificados de CA de servicio, pero solo se puede seleccionar un certificado de cliente).
  - Seleccione **Añadir nuevo certificado** para agregar un certificado que aún no se haya instalado y asignarlo al administrador de claves externo.
  - Seleccione  junto al nombre del certificado para eliminar los certificados instalados que no desea asignar al gestor de claves externo.
- Para agregar un servidor de claves secundario, seleccione **Agregar** en la columna **Servidores de claves secundarios** y proporcione sus detalles.
- Seleccione **Guardar** para completar la configuración.



### Edite un gestor de claves externo existente

Si ya configuró un administrador de claves externo, es posible modificar su configuración.

#### Pasos

- Para editar la configuración de un gestor de claves externo, realice uno de los siguientes pasos de inicio.

| Ámbito                                           | Navegación                                      | Paso inicial                                                                                                                                                                                                                                                                                                  |
|--------------------------------------------------|-------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Gestor de claves externo de ámbito del clúster   | <b>Clúster &gt; Ajustes</b>                     | Desplácese a la sección <b>Seguridad</b> . En <b>Cifrado</b> , seleccione  . A continuación, seleccione <b>Editar External Key Manager</b> .                                                                              |
| Gestor de claves externo de ámbito de Storage VM | <b>Almacenamiento &gt; VM de almacenamiento</b> | Seleccione la máquina virtual de almacenamiento. Seleccione la pestaña <b>Ajustes</b> . En la sección <b>Cifrado</b> en <b>Seguridad</b> , seleccione  . A continuación, seleccione <b>Editar External Key Manager</b> . |

- Los servidores de claves existentes se enumeran en la tabla **Servidores de claves**. Es posible realizar las siguientes operaciones:
  - Para agregar un nuevo servidor de claves, seleccione  **Add**.
  - Para suprimir un servidor de claves, seleccione  al final de la celda de la tabla que contiene el nombre del servidor de claves. Los servidores de claves secundarios asociados con ese servidor de claves primario también se eliminan de la configuración.



## Elimine un gestor de claves externo

Es posible eliminar un gestor de claves externo si los volúmenes no están cifrados.

### Pasos

1. Para eliminar un gestor de claves externo, realice uno de los siguientes pasos.

| Ámbito                                           | Navegación                                      | Paso inicial                                                                                                                                                                                                              |
|--------------------------------------------------|-------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Gestor de claves externo de ámbito del clúster   | <b>Clúster &gt; Ajustes</b>                     | Desplácese a la sección <b>Seguridad</b> . En <b>Cifrado</b> , selecciona <b>Seleccionar</b> , A continuación, seleccione <b>Eliminar External Key Manager</b> .                                                          |
| Gestor de claves externo de ámbito de Storage VM | <b>Almacenamiento &gt; VM de almacenamiento</b> | Seleccione la máquina virtual de almacenamiento. Seleccione la pestaña <b>Ajustes</b> . En la sección <b>Cifrado</b> en <b>Seguridad</b> , selecciona , A continuación, seleccione <b>Eliminar External Key Manager</b> . |

## Migrar claves entre gestores de claves

Cuando se habilitan varios administradores de claves en un clúster, las claves deben migrarse de un administrador de claves a otro. Este proceso se completa automáticamente con System Manager.

- Si se habilita el administrador de claves incorporado o un gestor de claves externo en el nivel del clúster y algunos volúmenes están cifrados, A continuación, cuando se configura un administrador de claves externo en el nivel de la máquina virtual de almacenamiento, las claves se deben migrar desde el administrador de claves incorporado o el administrador de claves externo en el nivel del clúster al administrador de claves externo en el nivel de la máquina virtual de almacenamiento. System Manager completa automáticamente este proceso.
- Si se crearon volúmenes sin cifrado en una máquina virtual de almacenamiento, no es necesario migrar las claves.

## Instale los certificados SSL en el clúster

El clúster y el servidor KMIP utilizan certificados SSL KMIP para verificar la identidad de las otras y establecer una conexión SSL. Antes de configurar la conexión SSL con el servidor KMIP, debe instalar los certificados SSL de cliente KMIP para el clúster y el certificado público SSL para la entidad de certificación (CA) raíz del servidor KMIP.

### Acerca de esta tarea

En una pareja de alta disponibilidad, ambos nodos deben usar los mismos certificados KMIP públicos y privados. Si conecta varias parejas de alta disponibilidad con el mismo servidor KMIP, todos los nodos de las parejas de alta disponibilidad deben utilizar los mismos certificados KMIP públicos y privados.

### Antes de empezar

- La hora debe sincronizarse en el servidor que crea los certificados, el servidor KMIP y el clúster.
- Debe haber obtenido el certificado de cliente SSL KMIP público para el clúster.
- Debe haber obtenido la clave privada asociada con el certificado de cliente SSL KMIP para el clúster.

- El certificado de cliente SSL KMIP no debe estar protegido por contraseña.
- Debe haber obtenido el certificado público de SSL para la entidad de certificación (CA) raíz del servidor KMIP.
- En un entorno de MetroCluster, debe instalar los mismos certificados SSL KMIP en ambos clústeres.



Es posible instalar los certificados de cliente y de servidor en el servidor KMIP antes o después de instalar los certificados en el clúster.

## Pasos

1. Instale los certificados de cliente SSL KMIP para el clúster:

```
security certificate install -vserver admin_svm_name -type client
```

Se le solicita que introduzca los certificados públicos y privados de SSL KMIP.

```
cluster1::> security certificate install -vserver cluster1 -type client
```

2. Instale el certificado público SSL para la entidad de certificación (CA) raíz del servidor KMIP:

```
security certificate install -vserver admin_svm_name -type server-ca
```

```
cluster1::> security certificate install -vserver cluster1 -type server-ca
```

## Habilitar gestión de claves externas en ONTAP 9.6 y versiones posteriores (NVE)

Puede utilizar uno o varios servidores KMIP para proteger las claves que utiliza el clúster para acceder a los datos cifrados. A partir de ONTAP 9.6, tiene la opción de configurar un gestor de claves externo independiente para proteger las claves que utiliza una SVM de datos para acceder a los datos cifrados.

A partir de ONTAP 9.11.1, puede agregar hasta 3 servidores de claves secundarios por servidor de claves primario para crear un servidor de claves en clúster. Para obtener más información, consulte [Configurar servidores de claves externas en cluster](#).

### Acerca de esta tarea

Se pueden conectar hasta cuatro servidores KMIP a un clúster o una SVM. Se recomienda un mínimo de dos servidores para la redundancia y la recuperación ante desastres.

El alcance de la gestión de claves externas determina si los servidores de gestión de claves protegen todas las SVM del clúster o solo las SVM seleccionadas:

- Puede usar un *cluster scope* a fin de configurar la gestión de claves externas para todas las SVM del clúster. El administrador de clúster tiene acceso a todas las claves almacenadas en los servidores.
- A partir de ONTAP 9.6, puede usar un *SVM Scope* para configurar la gestión de claves externa para una SVM de datos en el clúster. Esto es mejor para entornos multi-tenant en los que cada inquilino usa una SVM (o un conjunto de SVM) diferente para servir datos. Solo el administrador de SVM para un inquilino determinado tiene acceso a las claves de ese inquilino.
- Para entornos multi-tenant, instale una licencia para *MT\_EK\_MGMT* mediante el siguiente comando:

```
system license add -license-code <MT_EK_MGMT license code>
```

Para obtener una sintaxis de comando completa, consulte la página de manual del comando.

Puede utilizar ambos ámbitos en el mismo clúster. Si se configuraron servidores de gestión de claves para una SVM, ONTAP solo usa esos servidores para proteger las claves. De lo contrario, ONTAP protege las claves con los servidores de gestión de claves configurados para el clúster.

Puede configurar la gestión de claves incorporada en el ámbito del clúster y la gestión de claves externas en el ámbito de la SVM. Puede utilizar el `security key-manager key migrate` Comando para migrar claves de la gestión de claves integrada en el ámbito del clúster a administradores de claves externos en el ámbito de la SVM.

### Antes de empezar

- Deben haberse instalado el cliente KMIP SSL y los certificados de servidor.
- Debe ser un administrador de clúster o de SVM para ejecutar esta tarea.
- Si desea habilitar la gestión de claves externas para un entorno de MetroCluster, MetroCluster debe estar completamente configurado para poder habilitar la gestión de claves externas.
- En un entorno de MetroCluster, debe instalar el certificado SSL KMIP en ambos clústeres.

### Pasos

1. Configure la conectividad del gestor de claves para el clúster:

```
security key-manager external enable -vserver admin_SVM -key-servers
host_name|IP_address:port,... -client-cert client_certificate -server-ca-cert
server_CA_certificates
```



- La `security key-manager external enable` el comando sustituye al `security key-manager setup` comando. Si ejecuta el comando en la solicitud de inicio de sesión del clúster, `admin_SVM` Los valores predeterminados en la SVM de administrador del clúster actual. Para poder configurar el ámbito del clúster, debe ser el administrador del clúster. Puede ejecutar el `security key-manager external modify` comando para cambiar la configuración de gestión de claves externas.
- En un entorno de MetroCluster, si va a configurar la gestión de claves externa para la SVM de administrador, debe repetir el `security key-manager external enable` en el clúster de partners.

El siguiente comando habilita la gestión de claves externas para `cluster1` con tres servidores de claves externas. El primer servidor de claves se especifica mediante su nombre de host y puerto, el segundo se especifica mediante una dirección IP y el puerto predeterminado, y el tercero se especifica mediante una dirección IPv6 y un puerto:

```
cluster1::> security key-manager external enable -vserver cluster1 -key
-servers
ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
-client-cert AdminVserverClientCert -server-ca-certs
AdminVserverServerCaCert
```

2. Configure un administrador de claves una SVM:

```
security key-manager external enable -vserver SVM -key-servers
host_name|IP_address:port,... -client-cert client_certificate -server-ca-cert
server_CA_certificates
```



- Si ejecuta el comando en la solicitud de inicio de sesión de SVM, SVM El valor predeterminado es la SVM actual. Para configurar el ámbito de SVM, debe ser un administrador de clústeres o de SVM. Puede ejecutar el `security key-manager external modify` comando para cambiar la configuración de gestión de claves externas.
- En un entorno de MetroCluster, si va a configurar la gestión de claves externas para una SVM de datos, no es necesario repetir el `security key-manager external enable` en el clúster de partners.

El siguiente comando habilita la gestión de claves externas para `svm1` con un único servidor de claves escuchando en el puerto predeterminado 5696:

```
svm11::> security key-manager external enable -vserver svm1 -key-servers
keyserver.svm1.com -client-cert SVM1ClientCert -server-ca-certs
SVM1ServerCaCert
```

### 3. Repita el último paso para todas las SVM adicionales.



También puede utilizar el `security key-manager external add-servers` Comando para configurar SVM adicionales. La `security key-manager external add-servers` el comando sustituye al `security key-manager add` comando. Para obtener una sintaxis de comando completa, consulte la página `man`.

### 4. Compruebe que todos los servidores KMIP configurados están conectados:

```
security key-manager external show-status -node node_name
```



La `security key-manager external show-status` el comando sustituye al `security key-manager show -status` comando. Para obtener una sintaxis de comando completa, consulte la página `man`.

```
cluster1::> security key-manager external show-status
```

| Node  | Vserver  | Key Server                                   | Status    |
|-------|----------|----------------------------------------------|-----------|
| ----- |          |                                              |           |
| node1 |          |                                              |           |
|       | svm1     | keyserver.svm1.com:5696                      | available |
|       | cluster1 | 10.0.0.10:5696                               | available |
|       |          | fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234 | available |
|       |          | ks1.local:15696                              | available |
| node2 |          |                                              |           |
|       | svm1     | keyserver.svm1.com:5696                      | available |
|       | cluster1 | 10.0.0.10:5696                               | available |
|       |          | fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234 | available |
|       |          | ks1.local:15696                              | available |

```
8 entries were displayed.
```

5. Opcionalmente, convierta volúmenes de texto sin formato en volúmenes cifrados.

```
volume encryption conversion start
```

Debe haber configurado completamente un gestor de claves externo para poder convertir los volúmenes. En un entorno MetroCluster, debe configurarse un gestor de claves externo en ambos sitios.

## Habilite la gestión de claves externas en ONTAP 9.5 y versiones anteriores

Puede utilizar uno o varios servidores KMIP para proteger las claves que utiliza el clúster para acceder a los datos cifrados. Se pueden conectar hasta cuatro servidores KMIP a un nodo. Se recomienda un mínimo de dos servidores para la redundancia y la recuperación ante desastres.

### Acerca de esta tarea

ONTAP configura la conectividad de los servidores KMIP para todos los nodos del clúster.

### Antes de empezar

- Deben haberse instalado el cliente KMIP SSL y los certificados de servidor.
- Para realizar esta tarea, debe ser un administrador de clústeres.
- Debe configurar el entorno de MetroCluster antes de configurar un gestor de claves externo.
- En un entorno de MetroCluster, debe instalar el certificado SSL KMIP en ambos clústeres.

### Pasos

1. Configure la conectividad de Key Manager para los nodos del clúster:

```
security key-manager setup
```

Se inicia la configuración del gestor de claves.



En un entorno de MetroCluster, debe ejecutar este comando en ambos clústeres.

2. Introduzca la respuesta adecuada en cada solicitud.

3. Añadir un servidor KMIP:

```
security key-manager add -address key_management_server_ipaddress
```

```
cluster1::> security key-manager add -address 20.1.1.1
```



En un entorno de MetroCluster, debe ejecutar este comando en ambos clústeres.

4. Añada un servidor KMIP adicional para redundancia:

```
security key-manager add -address key_management_server_ipaddress
```

```
cluster1::> security key-manager add -address 20.1.1.2
```



En un entorno de MetroCluster, debe ejecutar este comando en ambos clústeres.

5. Compruebe que todos los servidores KMIP configurados están conectados:

```
security key-manager show -status
```

Para obtener una sintaxis de comando completa, consulte la página man.

```
cluster1::> security key-manager show -status
```

| Node        | Port | Registered Key Manager | Status    |
|-------------|------|------------------------|-----------|
| -----       | ---- | -----                  | -----     |
| cluster1-01 | 5696 | 20.1.1.1               | available |
| cluster1-01 | 5696 | 20.1.1.2               | available |
| cluster1-02 | 5696 | 20.1.1.1               | available |
| cluster1-02 | 5696 | 20.1.1.2               | available |

6. Opcionalmente, convierta volúmenes de texto sin formato en volúmenes cifrados.

```
volume encryption conversion start
```

Debe haber configurado completamente un gestor de claves externo para poder convertir los volúmenes. En un entorno MetroCluster, debe configurarse un gestor de claves externo en ambos sitios.

## Gestione claves con un proveedor de cloud

A partir de ONTAP 9.10.1, puede utilizar ["Azure Key Vault \(AKV\)"](#) y.. ["Servicio de gestión de claves de Google Cloud Platform \(Cloud KMS\)"](#) Para proteger sus claves de cifrado de ONTAP en una aplicación alojada en el cloud. A partir de ONTAP 9.12.0, también puede proteger las claves de NVE con ["KMS DE AWS"](#).

AWS KMS, AKV y Cloud KMS se pueden utilizar para proteger ["Claves de cifrado de volúmenes de NetApp \(NVE\)"](#) Solo para SVM de datos.

### Acerca de esta tarea

La gestión de claves con un proveedor de cloud se puede habilitar con la interfaz de línea de comandos o la API DE REST DE ONTAP.

Al usar un proveedor de cloud para proteger las claves, tiene en cuenta que de forma predeterminada se usa un LIF SVM de datos para comunicarse con el punto final de gestión de claves de cloud. Una red de gestión de nodos se usa para comunicarse con los servicios de autenticación del proveedor de cloud (login.microsoftonline.com para Azure; oauth2.googleapis.com para Cloud KMS). Si la red de clúster no está configurada correctamente, el clúster no utilizará correctamente el servicio de gestión de claves.

Al utilizar el servicio de gestión de claves de un proveedor de cloud, debe tener en cuenta las siguientes limitaciones:

- La gestión de claves para proveedores de cloud no está disponible para el cifrado del almacenamiento de NetApp (NSE) y el cifrado de agregados de NetApp (NAE). ["KMIP externos"](#) se puede utilizar en su lugar.
- La gestión de claves para proveedores de cloud no está disponible para las configuraciones de MetroCluster.
- La gestión de claves del proveedor de cloud solo puede configurarse en una SVM de datos.

### Antes de empezar

- Debe haber configurado el KMS en el proveedor de nube correspondiente.
- Los nodos del clúster ONTAP deben admitir NVE.
- ["Debe haber instalado las licencias de cifrado de volúmenes \(VE\) y de gestión de claves de cifrado multi-tenant \(MTEKM\)"](#). Estas licencias se incluyen con ["ONTAP One"](#).
- Debe ser un administrador de clúster o de SVM.
- Las SVM de datos no deben incluir ningún volumen cifrado ni emplear un gestor de claves. Si la SVM de datos incluye volúmenes cifrados, debe migrarlos antes de configurar el KMS.

### Habilite la gestión de claves externas

La habilitación de la gestión de claves externas depende del administrador de claves específico que se use. Elija la pestaña del gestor de claves y el entorno adecuados.

## AWS

### Antes de empezar

- Debe crear un permiso para la clave KMS de AWS que utilizará el rol de IAM que gestiona el cifrado. El rol de IAM debe incluir una política que permita las siguientes operaciones:
  - DescribeKey
  - Encrypt
  - Decrypt

Para obtener más información, consulte la documentación de AWS para ["subvenciones"](#).

### Habilite AWS KMS en una SVM de ONTAP

1. Antes de comenzar, obtenga tanto el ID de clave de acceso como la clave secreta de su KMS de AWS.
2. Configure el nivel de privilegio en Advanced:  
`set -priv advanced`
3. Habilitar AWS KMS:  
`security key-manager external aws enable -vserver svm_name -region AWS_region -key-id key_ID -encryption-context encryption_context`
4. Cuando se le solicite, introduzca la clave secreta.
5. Confirme que el KMS de AWS se ha configurado correctamente:  
`security key-manager external aws show -vserver svm_name`

## Azure

### Habilite Azure Key Vault en una SVM de ONTAP

1. Antes de empezar, debe obtener las credenciales de autenticación adecuadas de su cuenta de Azure, ya sea un secreto de cliente o un certificado. También debe asegurarse de que todos los nodos del clúster estén en buen estado. Puede comprobarlo con el comando `cluster show`.
2. Establezca el nivel privilegiado en avanzado  
`set -priv advanced`
3. Habilite AKV en el SVM  
`security key-manager external azure enable -client-id client_id -tenant-id tenant_id -name -key-id key_id -authentication-method {certificate|client-secret}`  
Cuando se le solicite, introduzca el certificado de cliente o el secreto de cliente desde la cuenta de Azure.
4. Compruebe que AKV está activado correctamente:  
`security key-manager external azure show vserver svm_name`  
Si la accesibilidad del servicio no es correcta, establezca la conectividad con el servicio de gestión de claves AKV a través del LIF de Data SVM.

## Google Cloud

### Habilite Cloud KMS en una SVM de ONTAP

1. Antes de comenzar, obtenga la clave privada para el archivo de claves de cuenta de Google Cloud KMS en formato JSON. Se puede encontrar en su cuenta de GCP.



También debe asegurarse de que todos los nodos del clúster estén en buen estado. Puede comprobarlo con el comando `cluster show`.

2. Defina el nivel con privilegios en avanzado:

```
set -priv advanced
```

3. Habilite Cloud KMS en la SVM

```
security key-manager external gcp enable -vserver svm_name -project-id
project_id-key-ring-name key_ring_name -key-ring-location key_ring_location
-key-name key_name
```

Cuando se le solicite, introduzca el contenido del archivo JSON con la clave privada de cuenta de servicio

4. Compruebe que Cloud KMS está configurado con los parámetros correctos:

```
security key-manager external gcp show vservers svm_name
```

El estado de `kms_wrapped_key_status` será "UNKNOWN" si no se crearon volúmenes cifrados.

Si la accesibilidad del servicio no es correcta, establezca la conectividad con el servicio de gestión de claves de GCP a través de la LIF de SVM de datos.

Si ya hay uno o más volúmenes cifrados configurados para una SVM de datos y el administrador de claves incorporado de la SVM de administrador gestiona las claves NVE correspondientes, esas claves se deben migrar al servicio de gestión de claves externa. Para hacerlo con la CLI, ejecute el comando:

```
security key-manager key migrate -from-Vserver admin_SVM -to-Vserver data_SVM
```

No se pueden crear nuevos volúmenes cifrados para la SVM de datos del inquilino hasta que todas las claves NVE de la SVM de datos se migren correctamente.

#### Información relacionada

- ["Cifrar volúmenes con las soluciones de cifrado de NetApp para Cloud Volumes ONTAP"](#)

#### Habilitar la gestión de claves incorporada en ONTAP 9.6 y versiones posteriores (NVE)

Puede usar el administrador de claves incorporado para proteger las claves que el clúster utiliza para acceder a los datos cifrados. Debe habilitar el administrador de claves incorporado en cada clúster que tenga acceso a un volumen cifrado o a un disco de autocifrado.

#### Acerca de esta tarea

Debe ejecutar el `security key-manager onboard sync` cada vez que añada un nodo al clúster.

Si tiene una configuración MetroCluster, debe ejecutar el `security key-manager onboard enable` primero en el clúster local y, a continuación, ejecute el `security key-manager onboard sync` en el clúster remoto, utilizando la misma clave de acceso en cada uno. Cuando ejecute el `security key-manager onboard enable` del clúster local y, a continuación, sincronice en el clúster remoto, no es necesario ejecutar el `enable` comando de nuevo desde el clúster remoto.

De forma predeterminada, no es necesario introducir la clave de acceso del administrador de claves cuando se reinicia un nodo. Puede utilizar el `cc-mode-enabled=yes` opción para solicitar que los usuarios introduzcan la frase de contraseña después de un reinicio.

Para NVE, si estableció `cc-mode-enabled=yes`, volúmenes creados con `volume create y.. volume move start` los comandos se cifran automáticamente. Para `volume create`, no es necesario especificar `-encrypt true`. Para `volume move start`, no es necesario especificar `-encrypt-destination true`.

Al configurar el cifrado de datos de ONTAP en reposo, para cumplir los requisitos de las soluciones comerciales para la clasificación (CSfC), debe usar NSE con NVE y asegurarse de que el gestor de claves incorporado esté habilitado en modo de criterios comunes. Consulte la ["Breve descripción de la solución CSfC"](#) Para obtener más información sobre CSfC.

Cuando el gestor de claves incorporado se habilita en el modo de criterios comunes (`cc-mode-enabled=yes`), el comportamiento del sistema se cambia de las siguientes formas:

- El sistema supervisa los intentos fallidos consecutivos de acceso al clúster cuando funciona en modo de criterios comunes.

Si no puede introducir la clave de acceso del clúster correcta en el arranque, los volúmenes cifrados no se montan. Para corregir esto, debe reiniciar el nodo e introducir la clave de acceso del clúster correcta. Una vez arrancado, el sistema permite 5 introducir correctamente la clave de acceso del clúster en un periodo de 24 horas para cualquier comando que requiera la clave de acceso del clúster como parámetro. Si se alcanza el límite (por ejemplo, no ha podido introducir correctamente la clave de acceso del clúster 5 veces en una fila), debe esperar al tiempo de espera de 24 horas o reiniciar el nodo para restablecer el límite.

- Las actualizaciones de imágenes del sistema utilizan el certificado de firma de código RSA-3072 de NetApp junto con los resúmenes firmados con código SHA-384 para comprobar la integridad de la imagen en lugar del certificado de firma de código RSA-2048 de NetApp habitual y los resúmenes firmados con código SHA-256.

El comando `upgrade` verifica que el contenido de la imagen no se ha alterado o dañado comprobando varias firmas digitales. El proceso de actualización de imágenes continúa con el paso siguiente si la validación se realiza correctamente; de lo contrario, la actualización de la imagen falla. Consulte `cluster image` página del comando `man` para obtener información sobre las actualizaciones del sistema.

El gestor de claves incorporado almacena claves en la memoria volátil. El contenido de la memoria volátil se borra al reiniciar o detener el sistema. En condiciones normales de funcionamiento, el contenido de la memoria volátil se borrará en un plazo de 30 segundos cuando se pare un sistema.

### Antes de empezar

- Para realizar esta tarea, debe ser un administrador de clústeres.
- Debe configurar el entorno de MetroCluster antes de configurar el gestor de claves incorporado.

### Pasos

1. Inicie la configuración del gestor de claves:

```
security key-manager onboard enable -cc-mode-enabled yes|no
```

Configurado `cc-mode-enabled=yes` para solicitar que los usuarios introduzcan la frase de acceso del administrador de claves después de un reinicio. Para NVE, si estableció `cc-mode-enabled=yes`, volúmenes creados con `volume create y..volume move start` los comandos se cifran automáticamente. La `- cc-mode-enabled` La opción no es compatible con las configuraciones de MetroCluster. La `security key-manager onboard enable` el comando sustituye al `security key-manager setup` comando.

En el siguiente ejemplo, se inicia el comando key Manager setup en cluster1 sin necesidad de introducir la frase de contraseña después de cada reinicio:

```
cluster1::> security key-manager onboard enable
```

```
Enter the cluster-wide passphrase for onboard key management in Vserver
"cluster1":: <32..256 ASCII characters long text>
Reenter the cluster-wide passphrase: <32..256 ASCII characters long
text>
```

2. En el indicador de frase de contraseña, introduzca una frase de paso entre 32 y 256 caracteres, o bien, para "cc-mode", una frase de paso entre 64 y 256 caracteres.



Si la frase de paso "cc-mode" especificada es menor de 64 caracteres, hay un retraso de cinco segundos antes de que la operación de configuración del gestor de claves vuelva a mostrar la indicación de contraseña.

3. En la solicitud de confirmación de contraseña, vuelva a introducir la frase de contraseña.
4. Compruebe que se han creado las claves de autenticación:

```
security key-manager key query -key-type NSE-AK
```



La `security key-manager key query` el comando sustituye al `security key-manager query key` comando. Para obtener una sintaxis de comando completa, consulte la página `man`.

El ejemplo siguiente verifica para qué se han creado claves de autenticación `cluster1`:

```
cluster1::> security key-manager key query -key-type NSE-AK
Node: node1
Vserver: cluster1
Key Manager: onboard
Key Manager Type: OKM
Key Manager Policy: -
```

| Key Tag                                                                                         | Key Type | Encryption | Restored |
|-------------------------------------------------------------------------------------------------|----------|------------|----------|
| node1                                                                                           | NSE-AK   | AES-256    | true     |
| Key ID:<br>00000000000000000200000000000100056178fc6ace6d91472df8a9286daacc00000000<br>00000000 |          |            |          |
| node1                                                                                           | NSE-AK   | AES-256    | true     |
| Key ID:<br>00000000000000000200000000000100df1689a148fdfbf9c2b198ef974d0baa00000000<br>00000000 |          |            |          |

2 entries were displayed.

5. Opcionalmente, convierta volúmenes de texto sin formato en volúmenes cifrados.

```
volume encryption conversion start
```

El gestor de claves incorporado debe estar completamente configurado antes de convertir los volúmenes. En un entorno MetroCluster, el gestor de claves incorporado debe configurarse en ambos sitios.

### Después de terminar

Copie la clave de acceso en una ubicación segura fuera del sistema de almacenamiento para usarla en el futuro.

Siempre que configure la clave de acceso de Onboard Key Manager, también debe realizar un backup manual de la información en una ubicación segura fuera del sistema de almacenamiento para usarla en caso de desastre. Consulte ["Realice un backup manual de la información de gestión de claves incorporada"](#).

### Habilitar la gestión de claves incorporada en ONTAP 9.5 y versiones anteriores (NVE)

Puede usar el administrador de claves incorporado para proteger las claves que el clúster utiliza para acceder a los datos cifrados. Debe habilitar el gestor de claves incorporado en cada clúster que acceda a un volumen cifrado o un disco de autocifrado.

### Acerca de esta tarea

Debe ejecutar el `security key-manager setup` cada vez que añada un nodo al clúster.

Si tiene una configuración de MetroCluster, revise las siguientes directrices:

- En ONTAP 9.5, debe ejecutar `security key-manager setup` en el clúster local y `security key-manager setup -sync-metrocluster-config yes` en el clúster remoto, utilizando la misma clave de acceso en cada uno.
- Antes de ONTAP 9.5, debe ejecutar `security key-manager setup` en el clúster local, espere aproximadamente 20 segundos y después ejecute `security key-manager setup` en el clúster remoto, utilizando la misma clave de acceso en cada uno.

De forma predeterminada, no es necesario introducir la clave de acceso del administrador de claves cuando se reinicia un nodo. A partir de ONTAP 9.4, puede utilizar el `-enable-cc-mode yes` opción para solicitar que los usuarios introduzcan la frase de contraseña después de un reinicio.

Para NVE, si estableció `-enable-cc-mode yes`, volúmenes creados con `volume create y.. volume move start` los comandos se cifran automáticamente. Para `volume create`, no es necesario especificar `-encrypt true`. Para `volume move start`, no es necesario especificar `-encrypt-destination true`.



Después de un intento de clave de acceso con errores, debe reiniciar el nodo de nuevo.

#### Antes de empezar

- Si utiliza NSE o NVE con un servidor de gestión de claves externa (KMIP), debe haber eliminado la base de datos del gestor de claves externo.

["Transición a la gestión de claves incorporada desde la gestión de claves externas"](#)

- Para realizar esta tarea, debe ser un administrador de clústeres.
- Debe configurar el entorno de MetroCluster antes de configurar el gestor de claves incorporado.

#### Pasos

1. Inicie la configuración del gestor de claves:

```
security key-manager setup -enable-cc-mode yes|no
```



A partir de ONTAP 9.4, puede utilizar el `-enable-cc-mode yes` opción para solicitar que los usuarios introduzcan la frase de contraseña del administrador de claves después de un reinicio. Para NVE, si estableció `-enable-cc-mode yes`, volúmenes creados con `volume create y.. volume move start` los comandos se cifran automáticamente.

En el siguiente ejemplo, se inicia la configuración del gestor de claves en cluster1 sin necesidad de introducir la clave de acceso después de cada reinicio:

• • •

- 



- 



6. Opcionalmente, convierta volúmenes de texto sin formato en volúmenes cifrados.

```
volume encryption conversion start
```

El gestor de claves incorporado debe estar completamente configurado antes de convertir los volúmenes. En un entorno MetroCluster, el gestor de claves incorporado debe configurarse en ambos sitios.

### Después de terminar

Copie la clave de acceso en una ubicación segura fuera del sistema de almacenamiento para usarla en el futuro.

Siempre que configure la clave de acceso de Onboard Key Manager, también debe realizar un backup manual de la información en una ubicación segura fuera del sistema de almacenamiento para usarla en caso de desastre. Consulte ["Realice un backup manual de la información de gestión de claves incorporada"](#).

### Habilite la gestión de claves incorporada en los nodos recién añadidos

Puede usar el administrador de claves incorporado para proteger las claves que el clúster utiliza para acceder a los datos cifrados. Debe habilitar el gestor de claves incorporado en cada clúster que acceda a un volumen cifrado o un disco de autocifrado.



Para ONTAP 9.5 y versiones anteriores, debe ejecutar el `security key-manager setup` cada vez que añada un nodo al clúster.

Para ONTAP 9.6 y versiones posteriores, debe ejecutar el `security key-manager sync` cada vez que añada un nodo al clúster.

Si añade un nodo a un clúster que tiene configurada la gestión de claves integrada, este comando se ejecutará para actualizar las claves que faltan.

Si tiene una configuración de MetroCluster, revise las siguientes directrices:

- A partir de ONTAP 9.6, debe ejecutar `security key-manager onboard enable` en el clúster local primero y después ejecute `security key-manager onboard sync` en el clúster remoto, utilizando la misma clave de acceso en cada uno.
- En ONTAP 9.5, debe ejecutar `security key-manager setup` en el clúster local y `security key-manager setup -sync-metrocluster-config yes` en el clúster remoto, utilizando la misma clave de acceso en cada uno.
- Antes de ONTAP 9.5, debe ejecutar `security key-manager setup` en el clúster local, espere aproximadamente 20 segundos y después ejecute `security key-manager setup` en el clúster remoto, utilizando la misma clave de acceso en cada uno.

De forma predeterminada, no es necesario introducir la clave de acceso del administrador de claves cuando se reinicia un nodo. A partir de ONTAP 9.4, puede utilizar el `-enable-cc-mode yes` opción para solicitar que los usuarios introduzcan la frase de contraseña después de un reinicio.

Para NVE, si estableció `-enable-cc-mode yes`, volúmenes creados con `volume create y.. volume move start` los comandos se cifran automáticamente. Para `volume create`, no es necesario especificar `-encrypt true`. Para `volume move start`, no es necesario especificar `-encrypt-destination true`.



Después de un intento de clave de acceso con errores, debe reiniciar el nodo de nuevo.

## Cifre datos de volúmenes con NVE

### Cifre datos de volúmenes con la información general de NVE

A partir de ONTAP 9.7, el cifrado de volúmenes y agregados se habilita de forma predeterminada cuando se dispone de la licencia *ve* y la gestión de claves interna o externa. Para ONTAP 9.6 y versiones anteriores, es posible habilitar el cifrado en un volumen nuevo o en uno existente. Debe haber instalado la licencia *ve* y haber habilitado la gestión de claves para poder habilitar el cifrado de volúmenes. NVE es conforme a la normativa FIPS-140-2 de nivel 1.

### Habilite el cifrado a nivel de agregado con la licencia *ve*

A partir de ONTAP 9.7, los agregados y volúmenes recién creados se cifran de forma predeterminada cuando tenga el "**LICENCIA VE**" o la gestión de claves externas o incorporadas. A partir de ONTAP 9.6, puede utilizar el cifrado a nivel de agregado para asignar claves al agregado que contiene para los volúmenes que se van a cifrar.

### Acerca de esta tarea

Debe utilizar el cifrado a nivel de agregado si tiene pensado realizar deduplicación en línea o en segundo plano a nivel de agregado. De lo contrario, NVE no admite la deduplicación a nivel de agregado.

Un agregado habilitado para el cifrado a nivel de agregado se denomina agregado *NAE* (para el cifrado de agregados de NetApp). Todos los volúmenes de un agregado de *NAE* deben estar cifrados con *NAE* o *NVE*. Con el cifrado a nivel de agregado, los volúmenes que cree en el agregado se cifran de forma predeterminada con el cifrado *NAE*. Puede anular el valor predeterminado para utilizar el cifrado *NVE* en su lugar.

No se admiten volúmenes de texto sin formato en los agregados de la *NAE*.

### Antes de empezar

Para realizar esta tarea, debe ser un administrador de clústeres.

### Pasos

1. Habilite o deshabilite el cifrado de nivel de agregado:

| Para...                                                                  | Se usa este comando...                                                                                       |
|--------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| Cree un agregado de <i>NAE</i> con ONTAP 9.7 o posterior                 | <code>storage aggregate create -aggregate aggregate_name -node node_name</code>                              |
| Cree un agregado de <i>NAE</i> con ONTAP 9.6                             | <code>storage aggregate create -aggregate aggregate_name -node node_name -encrypt-with -aggr-key true</code> |
| Convertir un agregado que no sea <i>NAE</i> en un agregado de <i>NAE</i> | <code>storage aggregate modify -aggregate aggregate_name -node node_name -encrypt-with -aggr-key true</code> |



Convertir un agregado de NAE en un agregado que no sea NAE

```
storage aggregate modify -aggregate
aggregate_name -node node_name -encrypt-with
-aggr-key false
```

Para obtener una sintaxis de comando completa, consulte las páginas man.

El siguiente comando habilita el cifrado a nivel de agregado para `aggr1`:

- ONTAP 9.7 o posterior:

```
cluster1::> storage aggregate create -aggregate aggr1
```

- ONTAP 9.6 o anterior:

```
cluster1::> storage aggregate create -aggregate aggr1 -encrypt-with
-aggr-key true
```

## 2. Compruebe que el agregado está habilitado para el cifrado:

```
storage aggregate show -fields encrypt-with-aggr-key
```

Para obtener una sintaxis de comando completa, consulte la página man.

El siguiente comando lo verifica `aggr1` está habilitado para el cifrado:

```
cluster1::> storage aggregate show -fields encrypt-with-aggr-key
aggregate encrypt-aggr-key

aggr0_vsim4 false
aggr1 true
2 entries were displayed.
```

## Después de terminar

Ejecute el `volume create` comando para crear los volúmenes cifrados.

Si utiliza un servidor KMIP para almacenar las claves de cifrado de un nodo, ONTAP inserta automáticamente una clave de cifrado en el servidor al cifrar un volumen.

## Habilite el cifrado en un nuevo volumen

Puede utilizar el `volume create` comando para habilitar el cifrado en un volumen nuevo.

## Acerca de esta tarea

Puede cifrar volúmenes con el cifrado de volúmenes de NetApp (NVE) y, para comenzar con ONTAP 9.6, el

cifrado de agregados de NetApp (NAE). Para obtener más información sobre NAE y NVE, consulte [información general de cifrado de volúmenes](#).

El procedimiento para habilitar el cifrado en un nuevo volumen en ONTAP varía en función de la versión de ONTAP que esté usando y su configuración específica:


- A partir de ONTAP 9.4, si se habilita `cc-mode` Cuando se configura el gestor de claves incorporado, los volúmenes que se crean con el `volume create` el comando se cifra automáticamente, tanto si se especifica como si no `-encrypt true`.
- En ONTAP 9.6 y versiones anteriores, es necesario utilizar `-encrypt true` con `volume create` comandos para habilitar el cifrado (siempre que no se haya habilitar `cc-mode`).
- Si desea crear un volumen NAE en ONTAP 9.6, debe habilitar NAE en el nivel de agregado. Consulte [Habilite el cifrado a nivel de agregado con la licencia ve](#) para obtener más detalles sobre esta tarea.
- A partir de ONTAP 9.7, los volúmenes recién creados se cifran de forma predeterminada cuando el "LICENCIA VE" o la gestión de claves externas o incorporadas. De forma predeterminada, los nuevos volúmenes que se crean en un agregado de NAE serán del tipo NAE en lugar de NVE.
  - Si añade, en ONTAP 9.7 y versiones posteriores `-encrypt true` para la `volume create` Comando para crear un volumen en un agregado de NAE, el volumen tendrá el cifrado NVE en lugar de NAE. Todos los volúmenes de un agregado de NAE deben estar cifrados con NVE o NAE.



No se admiten los volúmenes de texto sin formato en los agregados de NAE.

Pasos

1. Cree un volumen nuevo y especifique si el cifrado está habilitado en el volumen. Si el nuevo volumen se encuentra en un agregado de NAE, de forma predeterminada el volumen será un volumen de NAE:

| Para crear...                   | Se usa este comando...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Un volumen NAE                  | <code>volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Un volumen de NVE               | <div><code>volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name -encrypt true +</code><div><p>En ONTAP 9.6 y versiones anteriores en las que NAE no es compatible, <code>-encrypt true</code> Especifica que el volumen se debe cifrar con NVE. En ONTAP 9.7 y posteriores, donde se crean volúmenes en agregados de NAE, <code>-encrypt true</code> Reemplaza el tipo de cifrado predeterminado de NAE para crear un volumen NVE en su lugar.</p></div></div> |
| Un volumen de texto sin formato | <code>volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name -encrypt false</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

Para obtener la sintaxis completa del comando, consulte la página de referencia de comandos de LINK:[https://docs.netapp.com/us-en/ontap-cli-9141/volume-create.html#volume create#](https://docs.netapp.com/us-en/ontap-cli-9141/volume-create.html#volume_create#).

2. Compruebe que los volúmenes estén habilitados para el cifrado:

```
volume show -is-encrypted true
```

Para obtener una sintaxis completa del comando, consulte ["referencia de comandos"](#).

## Resultado

Si utiliza un servidor KMIP para almacenar las claves de cifrado de un nodo, ONTAP "inserta automáticamente" una clave de cifrado en el servidor cuando se cifra un volumen.

=

:allow-uri-read:

## Habilite el cifrado en un volumen existente

Puede utilizar cualquiera de los dos `volume move start` o `la volume encryption conversion start` comando para habilitar el cifrado en un volumen existente.

## Acerca de esta tarea

- A partir de ONTAP 9.3, puede utilizar la `volume encryption conversion start` comando para habilitar el cifrado de un volumen existente «in situ», sin necesidad de mover el volumen a otra ubicación. Como alternativa, puede utilizar el `volume move start` comando.
- Para ONTAP 9,2 y versiones anteriores, solo puede utilizar el `volume move start` comando para habilitar el cifrado mediante el movimiento de un volumen existente.

## Habilite el cifrado en un volumen existente con el comando `volume Encryption conversion start`

A partir de ONTAP 9.3, puede utilizar la `volume encryption conversion start` comando para habilitar el cifrado de un volumen existente «in situ», sin necesidad de mover el volumen a otra ubicación.

Después de iniciar una operación de conversión, debe completarse. Si se encuentra con un problema de rendimiento durante la operación, puede ejecutar el `volume encryption conversion pause` para pausar la operación y el `volume encryption conversion resume` comando para reanudar la operación.



No puede utilizar `volume encryption conversion start` Para convertir un volumen de SnapLock.

## Pasos

1. Habilitar el cifrado en un volumen existente:

```
volume encryption conversion start -vserver SVM_name -volume volume_name
```

Para obtener información sobre la sintaxis de toda el comando, consulte la página man del comando.

El siguiente comando habilita el cifrado en el volumen existente `vol1`:

```
cluster1::> volume encryption conversion start -vserver vs1 -volume vol1
```

El sistema crea una clave de cifrado para el volumen. Los datos del volumen se cifran.

2. Compruebe el estado de la operación de conversión:

```
volume encryption conversion show
```

Para obtener información sobre la sintaxis de toda el comando, consulte la página man del comando.

El siguiente comando muestra el estado de la operación de conversión:

```
cluster1::> volume encryption conversion show
```

| Vserver | Volume | Start Time         | Status                       |
|---------|--------|--------------------|------------------------------|
| -----   | -----  | -----              | -----                        |
| vs1     | vol1   | 9/18/2017 17:51:41 | Phase 2 of 2 is in progress. |

3. Cuando finalice la operación de conversión, compruebe que el volumen esté habilitado para el cifrado:

```
volume show -is-encrypted true
```

Para obtener información sobre la sintaxis de toda el comando, consulte la página man del comando.

El siguiente comando muestra los volúmenes cifrados en cluster1:

```
cluster1::> volume show -is-encrypted true
```

| Vserver | Volume | Aggregate | State  | Type  | Size  | Available | Used  |
|---------|--------|-----------|--------|-------|-------|-----------|-------|
| -----   | -----  | -----     | -----  | ----- | ----- | -----     | ----- |
| vs1     | vol1   | aggr2     | online | RW    | 200GB | 160.0GB   | 20%   |

## Resultado

Si utiliza un servidor KMIP para almacenar las claves de cifrado de un nodo, ONTAP inserta automáticamente una clave de cifrado en el servidor al cifrar un volumen.

## Habilite el cifrado en un volumen existente con el comando volume Move start

Puede utilizar el `volume move start` comando para habilitar el cifrado mediante el movimiento de un volumen existente. Debe usar `volume move start` En ONTAP 9.2 y anteriores. Se puede usar el mismo agregado o uno diferente.

## Acerca de esta tarea

- A partir de ONTAP 9.8, se puede utilizar `volume move start` Para habilitar el cifrado en un volumen de SnapLock o FlexGroup.
- A partir de ONTAP 9.4, si activa `"cc-mode"` cuando configura el Administrador de claves incorporado, los volúmenes que crea con el `volume move start` el comando se cifra automáticamente. No es necesario que especifique `-encrypt-destination true`.
- A partir de ONTAP 9.6, puede utilizar el cifrado a nivel de agregado con el fin de asignar claves al agregado que contiene para mover los volúmenes. Un volumen cifrado con una clave única se denomina *NVE volume* (lo que significa que utiliza cifrado de volúmenes de NetApp). Un volumen cifrado con una clave de nivel de agregado se denomina *NAE volume* (para el cifrado de agregados de NetApp). No se admiten los volúmenes de texto sin formato en los agregados de NAE.

- A partir de ONTAP 9.14.1, se puede cifrar un volumen raíz de SVM con NVE. Para obtener más información, consulte [Configure el cifrado de volúmenes NetApp en un volumen raíz de SVM](#).

### Antes de empezar

Debe ser un administrador de clústeres para realizar esta tarea o un administrador de SVM a quien el administrador de clúster haya delegado esta autoridad.

"Delegar la autoridad para ejecutar el comando `volume move`"

### Pasos

1. Mueva un volumen existente y especifique si el cifrado está habilitado en el volumen:

| Para convertir...                                                                                                                 | Se usa este comando...                                                                                                                                                                  |
|-----------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Un volumen de texto sin formato a un volumen NVE                                                                                  | <code>volume move start -vserver <i>SVM_name</i> -volume <i>volume_name</i> -destination-aggregate <i>aggregate_name</i> -encrypt-destination true</code>                               |
| Un volumen NVE o un volumen sin texto en un volumen NAE (suponiendo que se habilite el cifrado a nivel de agregado en el destino) | <code>volume move start -vserver <i>SVM_name</i> -volume <i>volume_name</i> -destination-aggregate <i>aggregate_name</i> -encrypt-with-aggr-key true</code>                             |
| Un volumen NAE a un volumen NVE                                                                                                   | <code>volume move start -vserver <i>SVM_name</i> -volume <i>volume_name</i> -destination-aggregate <i>aggregate_name</i> -encrypt-with-aggr-key false</code>                            |
| Volumen NAE a un volumen de texto sin formato                                                                                     | <code>volume move start -vserver <i>SVM_name</i> -volume <i>volume_name</i> -destination-aggregate <i>aggregate_name</i> -encrypt-destination false -encrypt-with-aggr-key false</code> |
| Un volumen NVE a un volumen de texto sin texto                                                                                    | <code>volume move start -vserver <i>SVM_name</i> -volume <i>volume_name</i> -destination-aggregate <i>aggregate_name</i> -encrypt-destination false</code>                              |

Para obtener información sobre la sintaxis de toda el comando, consulte la página man del comando.

El siguiente comando convierte un volumen de texto sin formato denominado `vol1` Para un volumen NVE:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-destination true
```

Si asumimos que el cifrado a nivel de agregado está habilitado en el destino, el siguiente comando convierte un volumen NVE o de texto sin formato denominado `vol1` A un volumen de NAE:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-with-aggr-key true
```

El siguiente comando convierte un volumen NAE llamado `vol2` Para un volumen NVE:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-with-aggr-key false
```

El siguiente comando convierte un volumen NAE llamado `vol2` a un volumen de texto sin formato:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false -encrypt-with-aggr-key false
```

El siguiente comando convierte un volumen de NVE llamado `vol2` a un volumen de texto sin formato:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false
```

## 2. Vea el tipo de cifrado de volúmenes de clúster:

```
volume show -fields encryption-type none|volume|aggregate
```

La `encryption-type` Campo está disponible en ONTAP 9.6 y versiones posteriores.

Para obtener información sobre la sintaxis de toda el comando, consulte la página man del comando.

El siguiente comando muestra el tipo de cifrado de volúmenes en `cluster2`:

```
cluster2::> volume show -fields encryption-type
```

| vserver | volume | encryption-type |
|---------|--------|-----------------|
| -----   | -----  | -----           |
| vs1     | vol1   | none            |
| vs2     | vol2   | volume          |
| vs3     | vol3   | aggregate       |

## 3. Compruebe que los volúmenes estén habilitados para el cifrado:

```
volume show -is-encrypted true
```

Para obtener información sobre la sintaxis de toda el comando, consulte la página man del comando.

El siguiente comando muestra los volúmenes cifrados en `cluster2`:

```
cluster2::> volume show -is-encrypted true
```

| Vserver | Volume | Aggregate | State  | Type  | Size  | Available | Used  |
|---------|--------|-----------|--------|-------|-------|-----------|-------|
| -----   | -----  | -----     | -----  | ----- | ----- | -----     | ----- |
| vs1     | vol1   | aggr2     | online | RW    | 200GB | 160.0GB   | 20%   |

## Resultado

Si utiliza un servidor KMIP para almacenar las claves de cifrado de un nodo, ONTAP inserta automáticamente una clave de cifrado en el servidor cuando se cifra un volumen.

## Configure el cifrado de volúmenes NetApp en un volumen raíz de SVM

A partir de ONTAP 9.14.1, puede habilitar el cifrado de volúmenes de NetApp (NVE) en un volumen raíz de una máquina virtual de almacenamiento (SVM). Con NVE, el volumen raíz se cifra con una clave única, lo que permite una mayor seguridad en la SVM.

## Acerca de esta tarea

NVE en un volumen raíz de SVM solo se puede habilitar una vez que se creó la SVM.

## Antes de empezar

- El volumen raíz de SVM no debe estar en un agregado cifrado con el cifrado de agregados de NetApp (NAE).
- Debe haber habilitado el cifrado con el administrador de claves incorporado o un gestor de claves externo.
- Debe ejecutar ONTAP 9.14.1 o una versión posterior.
- Para migrar una SVM que contiene un volumen raíz cifrado con NVE, debe convertir el volumen raíz de la SVM en un volumen de texto sin formato una vez finalizada la migración y, luego, volver a cifrar el volumen raíz de la SVM.
  - Si el agregado de destino de la migración de SVM utiliza NAE, el volumen raíz hereda NAE de manera predeterminada.
- Si la SVM está en una relación de recuperación ante desastres de SVM:
  - La configuración de cifrado en una SVM reflejada no se copia en el destino. Si habilita NVE en el origen o destino, debe habilitar por separado NVE en el volumen raíz de la SVM reflejada.
  - Si todos los agregados del clúster de destino utilizan NAE, el volumen raíz de SVM utilizará NAE.

## Pasos

Puede habilitar NVE en un volumen raíz de SVM con la interfaz de línea de comandos de ONTAP o System Manager.

## CLI

Puede habilitar NVE en el volumen raíz de la SVM sin movimiento o mediante el movimiento del volumen entre agregados.

### Cifre el volumen raíz en su lugar

1. Convierta el volumen raíz en un volumen de cifrado:

```
volume encryption conversion start -vserver svm_name -volume volume
```

2. Confirme que el cifrado se ha realizado correctamente. La `volume show -encryption-type volume` Muestra una lista de todos los volúmenes con NVE.

### Cifre el volumen raíz de la SVM al moverlo


1. Inicie un movimiento de volumen:

```
volume move start -vserver svm_name -volume volume -destination-aggregate aggregate -encrypt-with-aggr-key false -encrypt-destination true
```

Para obtener más información acerca de `volume move`, consulte [Mover un volumen](#).

2. Confirme el `volume move` la operación se ha realizado correctamente con el `volume move show` comando. La `volume show -encryption-type volume` Muestra una lista de todos los volúmenes con NVE.

## System Manager

1. Navegue hasta **Almacenamiento > Volúmenes**.
2. Junto al nombre del volumen raíz de la SVM que desea cifrar, seleccione  Luego **Editar**.
3. En el encabezado **Almacenamiento y optimización**, seleccione **Activar cifrado**.
4. Seleccione **Guardar**.

## Habilite el cifrado de volumen raíz del nodo

A partir de ONTAP 9.8, puede usar el cifrado de volúmenes de NetApp para proteger el volumen raíz del nodo.



### Acerca de esta tarea

Este procedimiento se aplica al volumen raíz del nodo. No se aplica a los volúmenes raíz de SVM. Los volúmenes raíz de SVM se pueden proteger mediante cifrado a nivel de agregado y [A partir de ONTAP 9.14.1, NVE](#).

Una vez que se inicia el cifrado del volumen raíz, se debe completar. No puede pausar la operación. Una vez completado el cifrado, no puede asignar una nueva clave al volumen raíz y no puede ejecutar una operación de purga segura.

### Antes de empezar

- Su sistema debe utilizar una configuración de alta disponibilidad.
- Se debe crear el volumen raíz del nodo.



- El sistema debe tener un administrador de claves incorporado o un servidor de gestión de claves externo mediante el protocolo de interoperabilidad de gestión de claves (KMIP).

## Pasos

1. Cifre el volumen raíz:

```
volume encryption conversion start -vserver SVM_name -volume root_vol_name
```

2. Compruebe el estado de la operación de conversión:

```
volume encryption conversion show
```

3. Una vez completada la operación de conversión, compruebe que el volumen esté cifrado:

```
volume show -fields
```

El siguiente ejemplo muestra el resultado de un volumen cifrado.

```
::> volume show -vserver xyz -volume vol0 -fields is-encrypted
vserver volume is-encrypted

xyz vol0 true
```

## Configuración del cifrado basado en hardware de NetApp

### Información general sobre el cifrado basado en hardware de NetApp

El cifrado basado en hardware de NetApp admite el cifrado de disco completo (FDE) de los datos mientras se escriben. No se pueden leer los datos sin una clave de cifrado almacenada en el firmware. La clave de cifrado, a su vez, sólo es accesible a un nodo autenticado.

#### Cifrado basado en hardware de NetApp

Un nodo se autentica a una unidad de autocifrado mediante una clave de autenticación recuperada de un servidor de gestión de claves externo o Onboard Key Manager:

- El servidor de gestión de claves externo es un sistema de terceros en el entorno de almacenamiento que proporciona claves a los nodos mediante el protocolo de interoperabilidad de gestión de claves (KMIP). Se recomienda configurar servidores de gestión de claves externos a partir de sus datos en un sistema de almacenamiento diferente.
- El gestor de claves incorporado es una herramienta integrada que proporciona claves de autenticación a nodos del mismo sistema de almacenamiento que los datos.

Puede utilizar el cifrado de volúmenes de NetApp con cifrado basado en hardware para «cifrar doble» los datos de unidades con autocifrado.

Cuando se habilitan unidades de autocifrado, también se cifra el volcado de memoria.



Si una pareja de alta disponibilidad utiliza unidades SAS o NVMe cifradas (SED, NSE, FIPS), debe seguir las instrucciones del tema [Devolver una unidad FIPS o SED al modo sin protección](#). Para todas las unidades dentro de la pareja de alta disponibilidad antes de inicializar el sistema (opciones de arranque 4 o 9). Si las unidades se reasignan, es posible que no se produzcan pérdidas de datos futuras.

### Tipos de unidades de autocifrado compatibles

Se admiten dos tipos de unidades de autocifrado:

- Las unidades SAS o NVMe con certificación FIPS de autocifrado son compatibles con todos los sistemas FAS y AFF. Estas unidades, denominadas **\_unidades FIPS**, cumplen con los requisitos del nivel 2 de la publicación estándar de procesamiento de información federal 140-2. Las capacidades certificadas ofrecen protecciones además del cifrado, como la prevención de ataques de denegación de servicio en la unidad. Las unidades FIPS no pueden combinarse con otros tipos de unidades en el mismo nodo o en la pareja de alta disponibilidad.
- A partir de ONTAP 9.6, las unidades NVMe de autocifrado que no se han sometido a pruebas FIPS son compatibles con los sistemas AFF A800, A320 y posteriores. Estas unidades, denominadas **SED**, ofrecen las mismas funcionalidades de cifrado que las unidades FIPS, pero se pueden combinar con unidades sin cifrado en el mismo nodo o par de alta disponibilidad.
- Todas las unidades validadas con FIPS utilizan un módulo criptográfico de firmware que se ha realizado mediante la validación FIPS. El módulo criptográfico de la unidad FIPS no utiliza ninguna clave generada fuera de la unidad (el módulo criptográfico del firmware de la unidad utiliza la frase de acceso de autenticación que se introduce en la unidad para obtener una clave de cifrado).



Las unidades sin cifrado son unidades que no están de SED o FIPS.



Si utiliza NSE en un sistema con un módulo Flash Cache, también debe habilitar NVE o NAE. NSE no cifra los datos que residen en el módulo de Flash Cache.

### Cuándo utilizar la gestión de claves externas

Aunque resulta menos caro y, por lo general, más práctico, utilizar el gestor de claves incorporado, se debe utilizar la gestión de claves externa si se da alguna de las siguientes situaciones:

- La política de su organización requiere una solución de gestión de claves que utilice un módulo criptográfico FIPS 140-2 de nivel 2 (o superior).
- Necesita una solución de varios clústeres con gestión centralizada de las claves de cifrado.
- Su empresa requiere una seguridad añadida para almacenar claves de autenticación en un sistema o en una ubicación distinta de los datos.

### Detalles de soporte

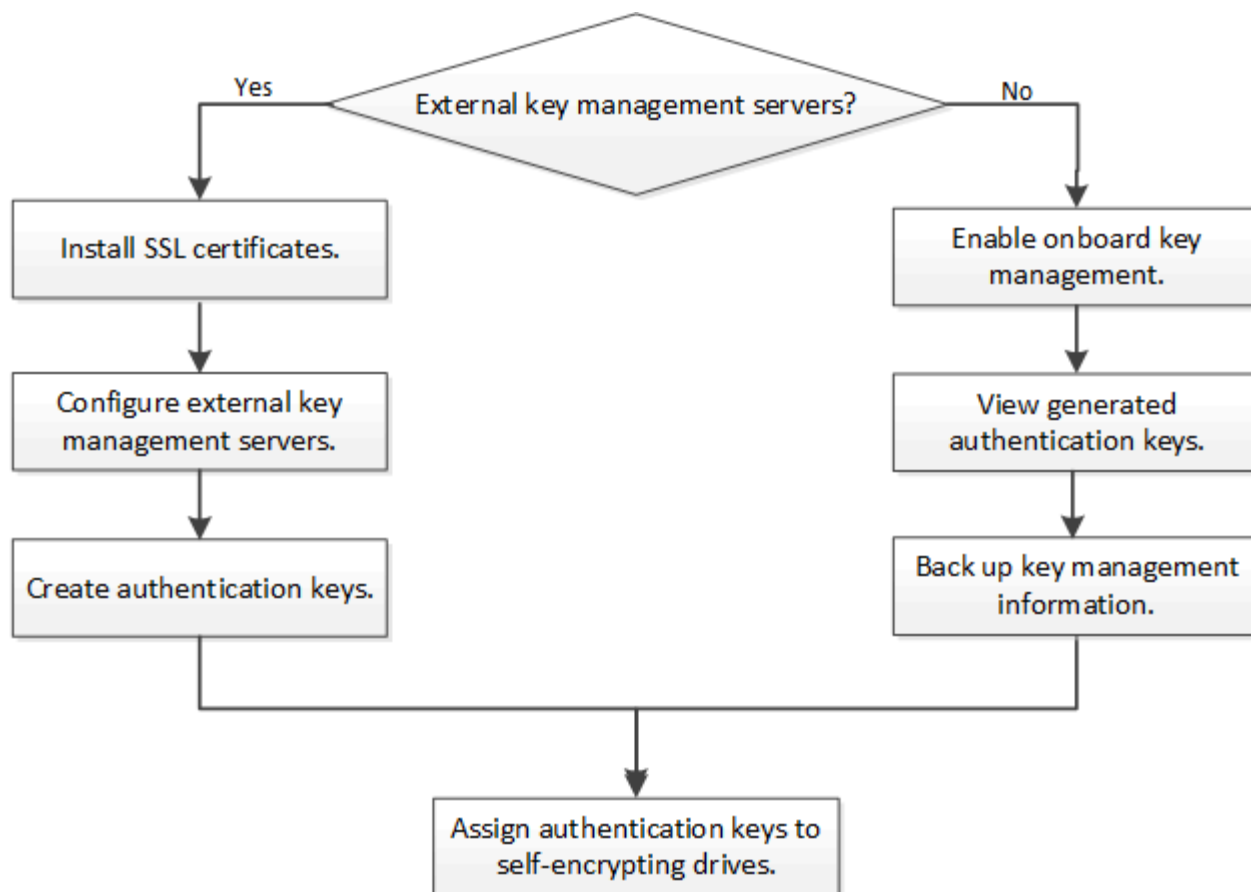
En la siguiente tabla se muestran detalles importantes de compatibilidad con el cifrado de hardware. Consulte la matriz de interoperabilidad para obtener la información más reciente sobre servidores KMIP, sistemas de almacenamiento y bandejas de discos compatibles.

| Recurso o característica | Detalles de soporte |
|--------------------------|---------------------|
|--------------------------|---------------------|

|                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Conjuntos de discos no homogéneos                                 | <ul style="list-style-type: none"> <li>• Las unidades FIPS no pueden combinarse con otros tipos de unidades en el mismo nodo o en la pareja de alta disponibilidad. Las parejas de alta disponibilidad conformes pueden coexistir con parejas de alta disponibilidad no conformes en el mismo clúster.</li> <li>• SEDS puede combinarse con unidades sin cifrado en el mismo nodo o en la pareja de alta disponibilidad.</li> </ul>                                                         |
| Tipo de unidad                                                    | <ul style="list-style-type: none"> <li>• Las unidades FIPS pueden ser SAS o NVMe.</li> <li>• SEDS debe ser unidades NVMe.</li> </ul>                                                                                                                                                                                                                                                                                                                                                        |
| Interfaces de red de 10 GB                                        | A partir de ONTAP 9.3, las configuraciones de gestión de claves KMIP admiten interfaces de red de 10 GB para las comunicaciones con servidores de gestión de claves externos.                                                                                                                                                                                                                                                                                                               |
| Puertos para la comunicación con el servidor de gestión de claves | A partir de ONTAP 9.3, es posible usar cualquier puerto de la controladora de almacenamiento para la comunicación con el servidor de gestión de claves. De lo contrario, debe utilizar el puerto e0M para la comunicación con los servidores de gestión de claves. Según el modelo de controladora de almacenamiento, es posible que ciertas interfaces de red no estén disponibles durante el proceso de arranque para establecer la comunicación con los servidores de gestión de claves. |
| MetroCluster (MCC) (en inglés)                                    | <ul style="list-style-type: none"> <li>• Las unidades NVMe admiten MCC.</li> <li>• Las unidades SAS no son compatibles con MCC.</li> </ul>                                                                                                                                                                                                                                                                                                                                                  |

#### Flujo de trabajo de cifrado basado en hardware

Debe configurar los servicios de gestión de claves para que el clúster pueda autenticarse en la unidad de autocifrado. Es posible usar un servidor de gestión de claves externo o un administrador de claves incorporado.



#### Información relacionada

- ["Hardware Universe de NetApp"](#)
- ["Cifrado de volúmenes de NetApp y cifrado de agregados de NetApp"](#)

### Configure la gestión de claves externas

#### Configure información general sobre la gestión de claves externas

Puede usar uno o varios servidores de gestión de claves externos para proteger las claves que utiliza el clúster para acceder a los datos cifrados. Un servidor de gestión de claves externo es un sistema de terceros en el entorno de almacenamiento que proporciona claves a los nodos mediante el protocolo de interoperabilidad de gestión de claves (KMIP).

Para ONTAP 9.1 y versiones anteriores, las LIF de gestión de nodos se deben asignar a los puertos que están configurados con el rol de gestión de nodos antes de poder usar el gestor de claves externo.

El cifrado de volúmenes de NetApp (NVE) se puede implementar con el administrador de claves incorporado en ONTAP 9.1 y versiones posteriores. En ONTAP 9.3 y versiones posteriores, el NVE puede implementarse con gestión de claves externa (KMIP) y el gestor de claves incorporado. A partir de ONTAP 9.11.1, es posible configurar varios administradores de claves externos en un clúster de. Consulte [Configurar servidores de claves en cluster](#).

Si utiliza ONTAP 9.2 o una versión anterior, debe rellenar la hoja de datos de configuración de red antes de habilitar la gestión de claves externas.



A partir de ONTAP 9.3, el sistema detecta automáticamente toda la información de red necesaria.

| Elemento                                                                    | Notas                                                                                                                                                                                                                                                     | Valor |
|-----------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| Nombre de la interfaz de red de gestión de claves                           |                                                                                                                                                                                                                                                           |       |
| Dirección IP de la interfaz de red de gestión de claves                     | Dirección IP de LIF de gestión de nodos, en formato IPv4 o IPv6                                                                                                                                                                                           |       |
| Longitud del prefijo de red IPv6 de la interfaz de red de gestión de claves | Si utiliza IPv6, la longitud del prefijo de red IPv6                                                                                                                                                                                                      |       |
| Máscara de subred de la interfaz de red de gestión de claves                |                                                                                                                                                                                                                                                           |       |
| Dirección IP de puerta de enlace de la interfaz de red de gestión de claves |                                                                                                                                                                                                                                                           |       |
| La dirección IPv6 de la interfaz de red del clúster                         | Solo es obligatorio si se utiliza IPv6 para la interfaz de red de gestión de claves                                                                                                                                                                       |       |
| Número de puerto para cada servidor KMIP                                    | Opcional. El número de puerto debe ser el mismo para todos los servidores KMIP. Si no proporciona un número de puerto, se establece de forma predeterminada en el puerto 5696, que es el puerto asignado por Internet Numbers Authority (IANA) para KMIP. |       |
| Nombre de etiqueta de clave                                                 | Opcional. El nombre de etiqueta de clave se utiliza para identificar todas las claves que pertenecen a un nodo. El nombre de etiqueta de clave predeterminado es el nombre del nodo.                                                                      |       |

#### Información relacionada

["Informe técnico de NetApp 3954: Requisitos y procedimientos previos a la instalación de cifrado del almacenamiento de NetApp para IBM Tivoli Lifetime Key Manager"](#)

## Instale los certificados SSL en el clúster

El clúster y el servidor KMIP utilizan certificados SSL KMIP para verificar la identidad de las otras y establecer una conexión SSL. Antes de configurar la conexión SSL con el servidor KMIP, debe instalar los certificados SSL de cliente KMIP para el clúster y el certificado público SSL para la entidad de certificación (CA) raíz del servidor KMIP.

### Acerca de esta tarea

En una pareja de alta disponibilidad, ambos nodos deben usar los mismos certificados KMIP públicos y privados. Si conecta varias parejas de alta disponibilidad con el mismo servidor KMIP, todos los nodos de las parejas de alta disponibilidad deben utilizar los mismos certificados KMIP públicos y privados.

### Antes de empezar

- La hora debe sincronizarse en el servidor que crea los certificados, el servidor KMIP y el clúster.
- Debe haber obtenido el certificado de cliente SSL KMIP público para el clúster.
- Debe haber obtenido la clave privada asociada con el certificado de cliente SSL KMIP para el clúster.
- El certificado de cliente SSL KMIP no debe estar protegido por contraseña.
- Debe haber obtenido el certificado público de SSL para la entidad de certificación (CA) raíz del servidor KMIP.
- En un entorno de MetroCluster, debe instalar los mismos certificados SSL KMIP en ambos clústeres.



Es posible instalar los certificados de cliente y de servidor en el servidor KMIP antes o después de instalar los certificados en el clúster.

### Pasos

1. Instale los certificados de cliente SSL KMIP para el clúster:

```
security certificate install -vserver admin_svm_name -type client
```

Se le solicita que introduzca los certificados públicos y privados de SSL KMIP.

```
cluster1::> security certificate install -vserver cluster1 -type client
```

2. Instale el certificado público SSL para la entidad de certificación (CA) raíz del servidor KMIP:

```
security certificate install -vserver admin_svm_name -type server-ca
```

```
cluster1::> security certificate install -vserver cluster1 -type server-ca
```

## Habilitar gestión de claves externa en ONTAP 9.6 y posterior (basada en hardware)

Puede utilizar uno o varios servidores KMIP para proteger las claves que utiliza el clúster para acceder a los datos cifrados. Se pueden conectar hasta cuatro servidores KMIP a un nodo. Se recomienda un mínimo de dos servidores para la redundancia y la recuperación ante desastres.

A partir de ONTAP 9.11.1, puede agregar hasta 3 servidores de claves secundarios por servidor de claves primario para crear un servidor de claves en clúster. Para obtener más información, consulte [Configurar servidores de claves externas en cluster](#).

### Antes de empezar

- Deben haberse instalado el cliente KMIP SSL y los certificados de servidor.
- Para realizar esta tarea, debe ser un administrador de clústeres.
- Debe configurar el entorno de MetroCluster antes de configurar un gestor de claves externo.
- En un entorno de MetroCluster, debe instalar el certificado SSL KMIP en ambos clústeres.

### Pasos

1. Configure la conectividad del gestor de claves para el clúster:

```
security key-manager external enable -vserver admin_SVM -key-servers
host_name|IP_address:port,... -client-cert client_certificate -server-ca-cert
server_CA_certificates
```



- La `security key-manager external enable` el comando sustituye al `security key-manager setup` comando. Puede ejecutar el `security key-manager external modify` comando para cambiar la configuración de gestión de claves externas. Para obtener una sintaxis de comando completa, consulte las páginas man.
- En un entorno de MetroCluster, si va a configurar la gestión de claves externa para la SVM de administrador, debe repetir el `security key-manager external enable` en el clúster de partners.

El siguiente comando habilita la gestión de claves externas para `cluster1` con tres servidores de claves externas. El primer servidor de claves se especifica mediante su nombre de host y puerto, el segundo se especifica mediante una dirección IP y el puerto predeterminado, y el tercero se especifica mediante una dirección IPv6 y un puerto:

```
cluster1::> security key-manager external enable -key-servers
ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
-client-cert AdminVserverClientCert -server-ca-certs
AdminVserverServerCaCert
```

2. Compruebe que todos los servidores KMIP configurados están conectados:

```
security key-manager external show-status -node node_name -vserver SVM -key
-server host_name|IP_address:port -key-server-status available|not-
responding|unknown
```



La `security key-manager external show-status` el comando sustituye al `security key-manager show -status` comando. Para obtener una sintaxis de comando completa, consulte la página man.

```
cluster1::> security key-manager external show-status
```

| Node  | Vserver  | Key Server                                   | Status    |
|-------|----------|----------------------------------------------|-----------|
| ----- |          |                                              |           |
| ----- |          |                                              |           |
| node1 |          |                                              |           |
|       | cluster1 |                                              |           |
|       |          | 10.0.0.10:5696                               | available |
|       |          | fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234 | available |
|       |          | ks1.local:15696                              | available |
| node2 |          |                                              |           |
|       | cluster1 |                                              |           |
|       |          | 10.0.0.10:5696                               | available |
|       |          | fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234 | available |
|       |          | ks1.local:15696                              | available |

6 entries were displayed.

#### Habilite la gestión de claves externas en ONTAP 9.5 y versiones anteriores

Puede utilizar uno o varios servidores KMIP para proteger las claves que utiliza el clúster para acceder a los datos cifrados. Se pueden conectar hasta cuatro servidores KMIP a un nodo. Se recomienda un mínimo de dos servidores para la redundancia y la recuperación ante desastres.

#### Acerca de esta tarea

ONTAP configura la conectividad de los servidores KMIP para todos los nodos del clúster.

#### Antes de empezar

- Deben haberse instalado el cliente KMIP SSL y los certificados de servidor.
- Para realizar esta tarea, debe ser un administrador de clústeres.
- Debe configurar el entorno de MetroCluster antes de configurar un gestor de claves externo.
- En un entorno de MetroCluster, debe instalar el certificado SSL KMIP en ambos clústeres.

#### Pasos

1. Configure la conectividad de Key Manager para los nodos del clúster:

```
security key-manager setup
```

Se inicia la configuración del gestor de claves.



En un entorno de MetroCluster, debe ejecutar este comando en ambos clústeres.

2. Introduzca la respuesta adecuada en cada solicitud.
3. Añadir un servidor KMIP:



```
security key-manager add -address key_management_server_ipaddress
```

```
cluster1::> security key-manager add -address 20.1.1.1
```



En un entorno de MetroCluster, debe ejecutar este comando en ambos clústeres.

#### 4. Añada un servidor KMIP adicional para redundancia:

```
security key-manager add -address key_management_server_ipaddress
```

```
cluster1::> security key-manager add -address 20.1.1.2
```



En un entorno de MetroCluster, debe ejecutar este comando en ambos clústeres.

#### 5. Compruebe que todos los servidores KMIP configurados están conectados:

```
security key-manager show -status
```

Para obtener una sintaxis de comando completa, consulte la página [man](#).

```
cluster1::> security key-manager show -status
```

| Node        | Port | Registered Key Manager | Status    |
|-------------|------|------------------------|-----------|
| -----       | ---- | -----                  | -----     |
| cluster1-01 | 5696 | 20.1.1.1               | available |
| cluster1-01 | 5696 | 20.1.1.2               | available |
| cluster1-02 | 5696 | 20.1.1.1               | available |
| cluster1-02 | 5696 | 20.1.1.2               | available |

#### 6. Opcionalmente, convierta volúmenes de texto sin formato en volúmenes cifrados.

```
volume encryption conversion start
```

Debe haber configurado completamente un gestor de claves externo para poder convertir los volúmenes. En un entorno MetroCluster, debe configurarse un gestor de claves externo en ambos sitios.

#### Configurar servidores de claves externas en cluster

A partir de ONTAP 9.11.1, se puede configurar la conectividad a los servidores de gestión de claves externos en clúster en una SVM. Con los servidores de claves en clúster, puede designar servidores de claves principales y secundarios en una SVM. Al registrar claves, ONTAP primero intentará acceder a un servidor de claves primario antes de intentar acceder secuencialmente a los servidores secundarios hasta que la operación se complete correctamente, lo que evita la duplicación de claves.

Los servidores de claves externos pueden utilizarse para las claves NSE, NVE, NAE y SED. Una SVM puede admitir hasta cuatro servidores KMIP externos principales. Cada servidor primario puede admitir hasta tres servidores de claves secundarios.

## Antes de empezar

- ["La gestión de claves KMIP debe estar habilitada para la SVM"](#).
- Este proceso solo admite servidores de claves que utilizan KMIP. Para obtener una lista de los servidores de claves compatibles, consulte ["Herramienta de matriz de interoperabilidad de NetApp"](#).
- Todos los nodos del clúster deben ejecutar ONTAP 9.11.1 o una versión posterior.
- El orden de los servidores enumera los argumentos en la `-secondary-key-servers` El parámetro refleja el orden de acceso de los servidores de gestión de claves externas (KMIP).

## Cree un servidor de claves en clúster

El procedimiento de configuración depende de si se ha configurado o no un servidor de claves primario.

### Añada servidores de claves primarios y secundarios a una SVM

1. Confirme que no se ha habilitado ninguna gestión de claves para el clúster:  

```
security key-manager external show -vserver svm_name
```

Si la SVM ya tiene el máximo de cuatro servidores de claves primarias habilitados, debe eliminar uno de los servidores de claves primarios existentes antes de añadir uno nuevo.
2. Habilite el gestor de claves principal:  

```
security key-manager external enable -vserver svm_name -key-servers
server_ip -client-cert client_cert_name -server-ca-certs
server_ca_cert_names
```
3. Modifique el servidor de claves primario para añadir servidores de claves secundarios. La `-secondary-key-servers` el parámetro acepta una lista de hasta tres servidores de claves separados por coma.  

```
security key-manager external modify-server -vserver svm_name -key-servers
primary_key_server -secondary-key-servers list_of_key_servers
```

### Añadir servidores de claves secundarios a un servidor de claves primario existente

1. Modifique el servidor de claves primario para añadir servidores de claves secundarios. La `-secondary-key-servers` el parámetro acepta una lista de hasta tres servidores de claves separados por coma.  

```
security key-manager external modify-server -vserver svm_name -key-servers
primary_key_server -secondary-key-servers list_of_key_servers
```

Para obtener más información sobre los servidores de claves secundarios, consulte [\[mod-secondary\]](#).

## Modifique los servidores de claves en cluster

Para modificar clústeres de servidores de claves externos, cambie el estado (principal o secundario) de servidores de claves específicos, añada o elimine servidores de claves secundarios, o cambie el orden de acceso de los servidores de claves secundarios.

## Convertir servidores de claves primarios y secundarios

Para convertir un servidor de claves primario en un servidor de claves secundario, primero debe eliminarlo de

la SVM con el `security key-manager external remove-servers` comando.

Para convertir un servidor de claves secundario en un servidor de claves primario, primero se debe quitar el servidor de claves secundario de su servidor de claves primario existente. Consulte [\[mod-secondary\]](#). Si convierte un servidor de claves secundario en un servidor primario mientras elimina una clave existente, intentar agregar un servidor nuevo antes de completar la eliminación y conversión puede provocar la duplicación de claves.

## Modificar servidores de claves secundarios

Los servidores de claves secundarios se gestionan con el `-secondary-key-servers` parámetro de `security key-manager external modify-server` comando. La `-secondary-key-servers` el parámetro acepta una lista separada por comas. El orden especificado de los servidores de claves secundarios de la lista determina la secuencia de acceso de los servidores de claves secundarios. El orden de acceso se puede modificar ejecutando el comando `security key-manager external modify-server` con los servidores de claves secundarios introducidos en un orden diferente.

Para eliminar un servidor de claves secundario, el `-secondary-key-servers` los argumentos deben incluir los servidores de claves que desea guardar mientras omite el que se va a quitar. Para quitar todos los servidores de claves secundarios, use el argumento `-`, significando ninguno.

Para obtener más información, consulte `security key-manager external` en la ["Referencia de comandos de la ONTAP"](#).

## Cree claves de autenticación en ONTAP 9.6 y versiones posteriores

Puede utilizar el `security key-manager key create` Comando para crear las claves de autenticación de un nodo y almacenarlas en los servidores KMIP configurados.

### Acerca de esta tarea

Si la configuración de seguridad requiere el uso de claves diferentes para la autenticación de datos y la autenticación FIPS 140-2-2, debe crear una clave independiente para cada una. Si este no es el caso, puede usar la misma clave de autenticación para el cumplimiento de FIPS que utiliza para el acceso a los datos.

ONTAP crea claves de autenticación para todos los nodos del clúster.

- Este comando no es compatible cuando el gestor de claves incorporado está habilitado. Sin embargo, se crean automáticamente dos claves de autenticación cuando se habilita el gestor de claves incorporado. Las teclas se pueden ver con el siguiente comando:

```
security key-manager key query -key-type NSE-AK
```

- Recibe una advertencia si los servidores de gestión de claves configurados ya almacenan más de 128 claves de autenticación.
- Puede utilizar el `security key-manager key delete` comando para eliminar las claves no utilizadas. La `security key-manager key delete` El comando falla si ONTAP utiliza actualmente la clave proporcionada. (Debe tener privilegios superiores a «'admin'» para utilizar este comando).



En un entorno de MetroCluster, antes de eliminar una clave, debe asegurarse de que la clave no se esté utilizando en el clúster de partners. Puede utilizar los siguientes comandos en el clúster de partners para comprobar que la clave no esté en uso:

- ° `storage encryption disk show -data-key-id key-id`
- ° `storage encryption disk show -fips-key-id key-id`

## Antes de empezar

Para realizar esta tarea, debe ser un administrador de clústeres.

## Pasos

1. Cree las claves de autenticación para los nodos del clúster:

```
security key-manager key create -key-tag passphrase_label -prompt-for-key
true|false
```



Ajuste `prompt-for-key=true` hace que el sistema solicite al administrador del clúster la clave de acceso que se usará en la autenticación de unidades cifradas. De lo contrario, el sistema genera automáticamente una frase de acceso de 32 bytes. La `security key-manager key create` el comando sustituye al `security key-manager create-key` comando. Para obtener una sintaxis de comando completa, consulte la página man.

En el siguiente ejemplo se crean las claves de autenticación para `cluster1`, generar automáticamente una frase de paso de 32 bytes:

```
cluster1::> security key-manager key create
Key ID:
000000000000000000002000000000001006268333f870860128fbe17d393e5083b00000000
00000000
```

2. Compruebe que se han creado las claves de autenticación:

```
security key-manager key query -node node
```



La `security key-manager key query` el comando sustituye al `security key-manager query key` comando. Para obtener una sintaxis de comando completa, consulte la página man. El ID de clave que se muestra en el resultado es un identificador que se utiliza para hacer referencia a la clave de autenticación. No es la clave de autenticación real ni la clave de cifrado de datos.

El ejemplo siguiente verifica para qué se han creado claves de autenticación `cluster1`:

```
cluster1::> security key-manager key query
 Vserver: cluster1
 Key Manager: external
 Node: node1
```

| Key Tag                                                                             | Key Type | Restored |
|-------------------------------------------------------------------------------------|----------|----------|
| node1                                                                               | NSE-AK   | yes      |
| Key ID:                                                                             |          |          |
| 000000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e0000000000000000 |          |          |
| node1                                                                               | NSE-AK   | yes      |
| Key ID:                                                                             |          |          |
| 000000000000000000002000000000001006f4e2513353a674305872a4c9f3bf7970000000000000000 |          |          |

```
 Vserver: cluster1
 Key Manager: external
 Node: node2
```

| Key Tag                                                                             | Key Type | Restored |
|-------------------------------------------------------------------------------------|----------|----------|
| node2                                                                               | NSE-AK   | yes      |
| Key ID:                                                                             |          |          |
| 000000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e0000000000000000 |          |          |
| node2                                                                               | NSE-AK   | yes      |
| Key ID:                                                                             |          |          |
| 000000000000000000002000000000001006f4e2513353a674305872a4c9f3bf7970000000000000000 |          |          |

## Cree claves de autenticación en ONTAP 9.5 y versiones anteriores

Puede utilizar el `security key-manager create-key` Comando para crear las claves de autenticación de un nodo y almacenarlas en los servidores KMIP configurados.

### Acerca de esta tarea

Si la configuración de seguridad requiere el uso de claves diferentes para la autenticación de datos y la autenticación FIPS 140-2-2, debe crear una clave independiente para cada una. Si no es así, puede usar la misma clave de autenticación para el cumplimiento de FIPS que se usa para acceder a los datos.

ONTAP crea claves de autenticación para todos los nodos del clúster.

- Este comando no es compatible cuando la gestión de claves incorporada está habilitada.
- Recibe una advertencia si los servidores de gestión de claves configurados ya almacenan más de 128 claves de autenticación.

Se puede usar el software del servidor de gestión de claves para eliminar las claves sin usar y, a continuación, ejecutar el comando de nuevo.

### Antes de empezar

Para realizar esta tarea, debe ser un administrador de clústeres.

### Pasos

1. Cree las claves de autenticación para los nodos del clúster:

```
security key-manager create-key
```

Para obtener una sintaxis de comando completa, consulte la página de manual del comando.



El ID de clave que se muestra en el resultado es un identificador que se utiliza para hacer referencia a la clave de autenticación. No es la clave de autenticación real ni la clave de cifrado de datos.

En el siguiente ejemplo se crean las claves de autenticación para `cluster1`:

```
cluster1::> security key-manager create-key
(security key-manager create-key)
Verifying requirements...

Node: cluster1-01
Creating authentication key...
Authentication key creation successful.
Key ID: F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C

Node: cluster1-01
Key manager restore operation initialized.
Successfully restored key information.

Node: cluster1-02
Key manager restore operation initialized.
Successfully restored key information.
```

2. Compruebe que se han creado las claves de autenticación:

```
security key-manager query
```

Para obtener una sintaxis de comando completa, consulte la página `man`.

El ejemplo siguiente verifica para qué se han creado claves de autenticación `cluster1`:

```
cluster1::> security key-manager query

(security key-manager query)

Node: cluster1-01
Key Manager: 20.1.1.1
Server Status: available

Key Tag Key Type Restored

cluster1-01 NSE-AK yes
Key ID:
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C

Node: cluster1-02
Key Manager: 20.1.1.1
Server Status: available

Key Tag Key Type Restored

cluster1-02 NSE-AK yes
Key ID:
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
```

#### Asignar una clave de autenticación de datos a una unidad FIPS o SED (gestión de claves externa)

Puede utilizar el `storage encryption disk modify` Para asignar una clave de autenticación de datos a una unidad FIPS o SED. Los nodos de clúster utilizan esta clave para bloquear o desbloquear los datos cifrados en la unidad.

#### Acerca de esta tarea

Una unidad de autocifrado está protegida contra el acceso no autorizado solo si su ID de clave de autenticación se configura como un valor no predeterminado. El ID seguro del fabricante (MSID), que tiene el ID de clave 0x0, es el valor predeterminado estándar para las unidades SAS. Para las unidades NVMe, el valor predeterminado estándar es una clave nula, que se representa como un ID de clave en blanco. Cuando se asigna el ID de clave a una unidad de autocifrado, el sistema cambia el ID de clave de autenticación por un valor no predeterminado.

Este procedimiento no causa interrupciones.

#### Antes de empezar

Para realizar esta tarea, debe ser un administrador de clústeres.

#### Pasos

1. Asigne una clave de autenticación de datos a una unidad FIPS o SED:

```
storage encryption disk modify -disk disk_ID -data-key-id key_ID
```

Para obtener una sintaxis de comando completa, consulte la página de manual del comando.



Puede utilizar el `security key-manager query -key-type NSE-AK` Comando para ver los ID clave.

```
cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
```

```
Info: Starting modify on 14 disks.
View the status of the operation by using the
storage encryption disk show-status command.
```

## 2. Compruebe que se han asignado las claves de autenticación:

```
storage encryption disk show
```

Para obtener una sintaxis de comando completa, consulte la página man.

```
cluster1::> storage encryption disk show
Disk Mode Data Key ID

0.0.0 data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
0.0.1 data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
[...]
```

## Configure la gestión de claves incorporada

Habilite la gestión de claves incorporada en ONTAP 9.6 y versiones posteriores

Puede usar el gestor de claves incorporado para autenticar nodos de clúster en una unidad FIPS o SED. El gestor de claves incorporado es una herramienta integrada que proporciona claves de autenticación a nodos del mismo sistema de almacenamiento que los datos. El gestor de claves incorporado es conforme a la normativa FIPS-140-2 de nivel 1.

Puede usar el administrador de claves incorporado para proteger las claves que el clúster utiliza para acceder a los datos cifrados. Debe habilitar el gestor de claves incorporado en cada clúster que acceda a un volumen cifrado o un disco de autocifrado.

### Acerca de esta tarea

Debe ejecutar el `security key-manager onboard enable` cada vez que añada un nodo al clúster. En



las configuraciones de MetroCluster, debe ejecutar `security key-manager onboard enable` en el clúster local primero y después ejecute `security key-manager onboard sync` en el clúster remoto, utilizando la misma clave de acceso en cada uno.

De forma predeterminada, no es necesario introducir la clave de acceso del administrador de claves cuando se reinicia un nodo. Excepto en MetroCluster, puede utilizar el `cc-mode-enabled=yes` opción para solicitar que los usuarios introduzcan la frase de contraseña después de un reinicio.

Cuando el gestor de claves incorporado se habilita en el modo de criterios comunes (`cc-mode-enabled=yes`), el comportamiento del sistema se cambia de las siguientes formas:

- El sistema supervisa los intentos fallidos consecutivos de acceso al clúster cuando funciona en modo de criterios comunes.

Si se habilitó el cifrado en almacenamiento de NetApp (NSE) y no se puede introducir la clave de acceso del clúster correcta en el arranque, el sistema no puede autenticarse en sus unidades y se reinicia automáticamente. Para corregir esto, debe introducir la clave de acceso correcta del clúster en el símbolo del sistema de arranque. Una vez arrancado, el sistema permite 5 introducir correctamente la clave de acceso del clúster en un periodo de 24 horas para cualquier comando que requiera la clave de acceso del clúster como parámetro. Si se alcanza el límite (por ejemplo, no ha podido introducir correctamente la clave de acceso del clúster 5 veces en una fila), debe esperar al tiempo de espera de 24 horas o reiniciar el nodo para restablecer el límite.

- Las actualizaciones de imágenes del sistema utilizan el certificado de firma de código RSA-3072 de NetApp junto con los resúmenes firmados con código SHA-384 para comprobar la integridad de la imagen en lugar del certificado de firma de código RSA-2048 de NetApp habitual y los resúmenes firmados con código SHA-256.

El comando `upgrade` verifica que el contenido de la imagen no se ha alterado o dañado comprobando varias firmas digitales. El proceso de actualización de imágenes continúa con el paso siguiente si la validación se realiza correctamente; de lo contrario, la actualización de la imagen falla. Consulte la página del manual «cluster image» para obtener información sobre las actualizaciones del sistema.

El gestor de claves incorporado almacena claves en la memoria volátil. El contenido de la memoria volátil se borra al reiniciar o detener el sistema. En condiciones normales de funcionamiento, el contenido de la memoria volátil se borrará en un plazo de 30 segundos cuando se pare un sistema.

### Antes de empezar

- Si utiliza NSE con un servidor de gestión de claves externa (KMIP), debe haber eliminado la base de datos de gestor de claves externo.

#### "Transición a la gestión de claves incorporada desde la gestión de claves externas"

- Para realizar esta tarea, debe ser un administrador de clústeres.
- Debe configurar el entorno de MetroCluster para poder configurar el gestor de claves incorporado.

### Pasos

1. Inicie el comando de configuración del gestor de claves:

```
security key-manager onboard enable -cc-mode-enabled yes|no
```



Configurado `cc-mode-enabled=yes` para solicitar que los usuarios introduzcan la frase de acceso del administrador de claves después de un reinicio. La `-cc-mode-enabled` La opción no es compatible con las configuraciones de MetroCluster. La `security key-manager onboard enable` el comando sustituye al `security key-manager setup` comando.

En el siguiente ejemplo, se inicia el comando key Manager setup en cluster1 sin necesidad de introducir la frase de contraseña después de cada reinicio:

```
cluster1::> security key-manager onboard enable
```

```
Enter the cluster-wide passphrase for onboard key management in Vserver
"cluster1":<32..256 ASCII characters long text>
Reenter the cluster-wide passphrase: <32..256 ASCII characters long
text>
```

2. En el indicador de frase de contraseña, introduzca una frase de paso entre 32 y 256 caracteres, o bien, para "cc-mode", una frase de paso entre 64 y 256 caracteres.



Si la frase de paso "cc-mode" especificada es menor de 64 caracteres, hay un retraso de cinco segundos antes de que la operación de configuración del gestor de claves vuelva a mostrar la indicación de contraseña.

3. En la solicitud de confirmación de contraseña, vuelva a introducir la frase de contraseña.
4. Compruebe que se han creado las claves de autenticación:

```
security key-manager key query -node node
```



La `security key-manager key query` el comando sustituye al `security key-manager query key` comando. Para obtener una sintaxis de comando completa, consulte la página man.

El ejemplo siguiente verifica para qué se han creado claves de autenticación cluster1:

```
cluster1::> security key-manager key query
```

```
Vserver: cluster1
```

```
Key Manager: onboard
```

```
Node: node1
```

| Key Tag                                                                             | Key Type | Restored |
|-------------------------------------------------------------------------------------|----------|----------|
| -----                                                                               | -----    | -----    |
| node1                                                                               | NSE-AK   | yes      |
| Key ID:                                                                             |          |          |
| 000000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e0000000000000000 |          |          |
| node1                                                                               | NSE-AK   | yes      |
| Key ID:                                                                             |          |          |
| 000000000000000000002000000000001006f4e2513353a674305872a4c9f3bf7970000000000000000 |          |          |

```
Vserver: cluster1
```

```
Key Manager: onboard
```

```
Node: node2
```

| Key Tag                                                                             | Key Type | Restored |
|-------------------------------------------------------------------------------------|----------|----------|
| -----                                                                               | -----    | -----    |
| node1                                                                               | NSE-AK   | yes      |
| Key ID:                                                                             |          |          |
| 000000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e0000000000000000 |          |          |
| node2                                                                               | NSE-AK   | yes      |
| Key ID:                                                                             |          |          |
| 000000000000000000002000000000001006f4e2513353a674305872a4c9f3bf7970000000000000000 |          |          |

## Después de terminar

Copie la clave de acceso en una ubicación segura fuera del sistema de almacenamiento para usarla en el futuro.

Se realiza automáticamente un backup de toda la información de gestión de claves en la base de datos replicada (RDB) del clúster. También es necesario realizar una copia de seguridad de la información manualmente para su uso en caso de desastre.

## Habilite la gestión de claves incorporada en ONTAP 9.5 y versiones anteriores

Puede usar el gestor de claves incorporado para autenticar nodos de clúster en una unidad FIPS o SED. El gestor de claves incorporado es una herramienta integrada que proporciona claves de autenticación a nodos del mismo sistema de almacenamiento que los datos. El gestor de claves incorporado es conforme a la normativa FIPS-140-2 de nivel 1.

Puede usar el administrador de claves incorporado para proteger las claves que el clúster utiliza para acceder a los datos cifrados. Debe habilitar el gestor de claves incorporado en cada clúster que acceda a un volumen cifrado o un disco de autocifrado.

### Acerca de esta tarea

Debe ejecutar el `security key-manager setup` cada vez que añada un nodo al clúster.

Si tiene una configuración de MetroCluster, revise las siguientes directrices:

- En ONTAP 9.5, debe ejecutar `security key-manager setup` en el clúster local y `security key-manager setup -sync-metrocluster-config yes` en el clúster remoto, utilizando la misma clave de acceso en cada uno.
- Antes de ONTAP 9.5, debe ejecutar `security key-manager setup` en el clúster local, espere aproximadamente 20 segundos y después ejecute `security key-manager setup` en el clúster remoto, utilizando la misma clave de acceso en cada uno.

De forma predeterminada, no es necesario introducir la clave de acceso del administrador de claves cuando se reinicia un nodo. A partir de ONTAP 9.4, puede utilizar el `-enable-cc-mode yes` opción para solicitar que los usuarios introduzcan la frase de contraseña después de un reinicio.

Para NVE, si estableció `-enable-cc-mode yes`, volúmenes creados con `volume create` y `volume move start` los comandos se cifran automáticamente. Para `volume create`, no es necesario especificar `-encrypt true`. Para `volume move start`, no es necesario especificar `-encrypt-destination true`.



Después de un intento de clave de acceso con errores, debe reiniciar el nodo de nuevo.

### Antes de empezar

- Si utiliza NSE con un servidor de gestión de claves externa (KMIP), debe haber eliminado la base de datos de gestor de claves externo.

["Transición a la gestión de claves incorporada desde la gestión de claves externas"](#)

- Para realizar esta tarea, debe ser un administrador de clústeres.
- Debe configurar el entorno de MetroCluster para poder configurar el gestor de claves incorporado.

### Pasos

1. Inicie la configuración del gestor de claves:

```
security key-manager setup -enable-cc-mode yes|no
```



A partir de ONTAP 9.4, puede utilizar el `-enable-cc-mode yes` opción para solicitar que los usuarios introduzcan la frase de contraseña del administrador de claves después de un reinicio. Para NVE, si estableció `-enable-cc-mode yes`, volúmenes creados con `volume create` y `volume move start` los comandos se cifran automáticamente.

En el siguiente ejemplo, se inicia la configuración del gestor de claves en cluster1 sin necesidad de introducir la clave de acceso después de cada reinicio:

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

...

Would you like to use onboard key-management? {yes, no} [yes]:
Enter the cluster-wide passphrase: <32..256 ASCII characters long
text>
Reenter the cluster-wide passphrase: <32..256 ASCII characters long
text>
```

2. Introduzca `yes` en el símbolo del sistema de para configurar la gestión integrada de claves.
3. En el indicador de frase de contraseña, introduzca una frase de paso entre 32 y 256 caracteres, o bien, para `"cc-mode"`, una frase de paso entre 64 y 256 caracteres.



Si la frase de paso `"cc-mode"` especificada es menor de 64 caracteres, hay un retraso de cinco segundos antes de que la operación de configuración del gestor de claves vuelva a mostrar la indicación de contraseña.

4. En la solicitud de confirmación de contraseña, vuelva a introducir la frase de contraseña.
5. Compruebe que las claves estén configuradas para todos los nodos:

```
security key-manager key show
```

Para obtener la sintaxis completa del comando, consulte la página `man`.

```
cluster1::> security key-manager key show

Node: node1
Key Store: onboard
Key ID Used By

0000000000000000020000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK

Node: node2
Key Store: onboard
Key ID Used By

0000000000000000020000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK
```

## Después de terminar

Se realiza automáticamente un backup de toda la información de gestión de claves en la base de datos replicada (RDB) del clúster.

Siempre que configure la clave de acceso de Onboard Key Manager, también debe realizar un backup manual de la información en una ubicación segura fuera del sistema de almacenamiento para usarla en caso de desastre. Consulte ["Realice un backup manual de la información de gestión de claves incorporada"](#).

## Asignar una clave de autenticación de datos a una unidad FIPS o SED (gestión de claves incorporada)

Puede utilizar el `storage encryption disk modify` Para asignar una clave de autenticación de datos a una unidad FIPS o SED. Los nodos de clúster usan esta clave para acceder a los datos de la unidad.

## Acerca de esta tarea

Una unidad de autocifrado está protegida contra el acceso no autorizado solo si su ID de clave de autenticación se configura como un valor no predeterminado. El ID seguro del fabricante (MSID), que tiene el ID de clave 0x0, es el valor predeterminado estándar para las unidades SAS. Para las unidades NVMe, el valor predeterminado estándar es una clave nula, que se representa como un ID de clave en blanco. Cuando se asigna el ID de clave a una unidad de autocifrado, el sistema cambia el ID de clave de autenticación por un valor no predeterminado.

## Antes de empezar

Para realizar esta tarea, debe ser un administrador de clústeres.

## Pasos

1. Asigne una clave de autenticación de datos a una unidad FIPS o SED:

```
storage encryption disk modify -disk disk_ID -data-key-id key_ID
```

Para obtener una sintaxis de comando completa, consulte la página de manual del comando.



Puede utilizar el `security key-manager key query -key-type NSE-AK` Comando para ver los ID clave.

```
cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
0000000000000000000020000000000010019215b9738bc7b43d4698c80246db1f4
```

```
Info: Starting modify on 14 disks.
View the status of the operation by using the
storage encryption disk show-status command.
```

2. Compruebe que se han asignado las claves de autenticación:

```
storage encryption disk show
```

Para obtener una sintaxis de comando completa, consulte la página `man`.

```
cluster1::> storage encryption disk show
Disk Mode Data Key ID

0.0.0 data
00000000000000000000200000000000010019215b9738bc7b43d4698c80246db1f4
0.0.1 data
00000000000000000000200000000000010059851742AF2703FC91369B7DB47C4722
[...]
```

## Asigne una clave de autenticación FIPS 140-2 a una unidad FIPS

Puede utilizar el `storage encryption disk modify` con el `-fips-key-id` Opción para asignar una clave de autenticación FIPS 140-2 a una unidad FIPS. Los nodos de clúster utilizan esta clave para las operaciones de unidad distintas del acceso a los datos, como evitar ataques de denegación de servicio en la unidad.

### Acerca de esta tarea

Es posible que la configuración de seguridad requiera el uso de claves diferentes para la autenticación de datos y la autenticación FIPS 140-2-2. Si no es así, puede usar la misma clave de autenticación para el cumplimiento de FIPS que se usa para acceder a los datos.

Este procedimiento no causa interrupciones.

### Antes de empezar

El firmware de la unidad debe ser compatible con el cumplimiento de normativas FIPS 140-2-2. La ["Herramienta de matriz de interoperabilidad de NetApp"](#) contiene información sobre las versiones de firmware de la unidad admitidas.

### Pasos

1. Primero debe asegurarse de que ha asignado una clave de autenticación de datos. Esto se puede hacer utilizando un [gestor de claves externas](#) o una [gestión de claves incorporada](#). Compruebe que la clave está asignada con el comando `storage encryption disk show`.
2. Asigne una clave de autenticación FIPS 140-2 a SED:

```
storage encryption disk modify -disk disk_id -fips-key-id
fips_authentication_key_id
```

Puede utilizar el `security key-manager query` Comando para ver los ID clave.

```
cluster1::> storage encryption disk modify -disk 2.10.* -fips-key-id
6A1E21D80000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
```

```
Info: Starting modify on 14 disks.
 View the status of the operation by using the
 storage encryption disk show-status command.
```

### 3. Compruebe que se ha asignado la clave de autenticación:

```
storage encryption disk show -fips
```

Para obtener una sintaxis de comando completa, consulte la página man.

```
cluster1::> storage encryption disk show -fips
Disk Mode FIPS-Compliance Key ID

2.10.0 full
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
2.10.1 full
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
[...]
```

### Habilite el modo compatible con FIPS en todo el clúster para conexiones de servidor KMIP

Puede utilizar el `security config modify` con el `-is-fips-enabled` Opción de habilitar el modo compatible con FIPS en todo el clúster para los datos que están en movimiento. Al hacerlo, obliga al clúster a usar OpenSSL en modo FIPS al conectarse a servidores KMIP.

#### Acerca de esta tarea

Cuando habilita el modo compatible con FIPS en todo el clúster, el clúster utilizará únicamente paquetes de cifrado validados TLS1.2 y FIPS. El modo compatible con FIPS para todo el clúster está deshabilitado de forma predeterminada.

Debe reiniciar los nodos del clúster de forma manual después de modificar la configuración de seguridad de todo el clúster.

#### Antes de empezar

- La controladora de almacenamiento debe configurarse en modo conforme a FIPS.
- Todos los servidores KMIP deben ser compatibles con TLSv1.2. El sistema requiere TLSv1.2 para completar la conexión con el servidor KMIP cuando se habilita el modo compatible con FIPS en todo el clúster.

#### Pasos

1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Compruebe que TLSv1.2 es compatible:

```
security config show -supported-protocols
```

Para obtener una sintaxis de comando completa, consulte la página man.



```
cluster1::> security config show
```

|           | Cluster   |                         | Cluster                             |
|-----------|-----------|-------------------------|-------------------------------------|
| Security  |           |                         |                                     |
| Interface | FIPS Mode | Supported Protocols     | Supported Ciphers Config            |
| Ready     |           |                         |                                     |
| -----     | -----     | -----                   | -----                               |
| -----     |           |                         |                                     |
| SSL       | false     | TLSv1.2, TLSv1.1, TLSv1 | ALL:!LOW:<br>!aNULL:!EXP:<br>!eNULL |
|           |           |                         | yes                                 |

### 3. Habilite el modo compatible con FIPS para todo el clúster:

```
security config modify -is-fips-enabled true -interface SSL
```

Para obtener una sintaxis de comando completa, consulte la página man.

### 4. Reiniciar nodos del clúster de forma manual.

### 5. Compruebe que el modo compatible con FIPS en todo el clúster esté habilitado:

```
security config show
```

```
cluster1::> security config show
```

|           | Cluster   |                     | Cluster                                  |
|-----------|-----------|---------------------|------------------------------------------|
| Security  |           |                     |                                          |
| Interface | FIPS Mode | Supported Protocols | Supported Ciphers Config                 |
| Ready     |           |                     |                                          |
| -----     | -----     | -----               | -----                                    |
| -----     |           |                     |                                          |
| SSL       | true      | TLSv1.2, TLSv1.1    | ALL:!LOW:<br>!aNULL:!EXP:<br>!eNULL:!RC4 |
|           |           |                     | yes                                      |

## Gestione el cifrado de NetApp

### Descifrar datos de volumen

Puede utilizar el `volume move start` comando para mover y anular el cifrado de datos de volúmenes.

#### Antes de empezar

Para realizar esta tarea, debe ser un administrador de clústeres. Como alternativa, puede ser un administrador de SVM al que el administrador del clúster haya delegado autoridad. Para obtener más información, consulte ["Delegue la autoridad para ejecutar el comando volume move"](#).

#### Pasos

1. Mueva un volumen de cifrado existente y descifre los datos en el volumen:

```
volume move start -vserver SVM_name -volume volume_name -destination-aggregate
aggregate_name -encrypt-destination false
```

Para obtener una sintaxis de comando completa, consulte la página de manual del comando.

El siguiente comando mueve un volumen existente llamado `vol1` al agregado de destino `aggr3` y descifra los datos del volumen:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr3 -encrypt-destination false
```

El sistema elimina la clave de cifrado del volumen. Los datos del volumen no están cifrados.

2. Compruebe que el volumen esté deshabilitado para el cifrado:

```
volume show -encryption
```

Para obtener una sintaxis de comando completa, consulte la página de manual del comando.

El siguiente comando muestra si los volúmenes están activados `cluster1` están cifrados:

```
cluster1::> volume show -encryption
```

| Vserver | Volume | Aggregate | State  | Encryption State |
|---------|--------|-----------|--------|------------------|
| -----   | -----  | -----     | -----  | -----            |
| vs1     | vol1   | aggr1     | online | none             |

## Mueva un volumen cifrado

Puede utilizar el `volume move start` comando para mover un volumen cifrado. El volumen movido puede residir en el mismo agregado o en otra diferente.

### Acerca de esta tarea

El movimiento generará un error si el nodo de destino o el volumen de destino no admiten el cifrado de volúmenes.

La `-encrypt-destination` opción para `volume move start` el valor predeterminado es `true` para los volúmenes cifrados. El requisito para especificar que no desea que el volumen de destino cifrado garantice que no se descifren de forma accidental los datos del volumen.

### Antes de empezar

Para realizar esta tarea, debe ser un administrador de clústeres. Como alternativa, puede ser un administrador de SVM al que el administrador del clúster haya delegado autoridad. Para obtener más información, consulte ["delegue la autoridad para ejecutar el comando volume move"](#).

### Pasos

## 1. Mueva un volumen de cifrado existente y deje los datos en el volumen cifrado:

```
volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name
```

Para obtener una sintaxis de comando completa, consulte la página de manual del comando.

El siguiente comando mueve un volumen existente llamado `vol1` al agregado de destino `aggr3` y deja los datos del volumen cifrados:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr3
```

## 2. Compruebe que el volumen esté habilitado para el cifrado:

```
volume show -is-encrypted true
```

Para obtener una sintaxis de comando completa, consulte la página de manual del comando.

El siguiente comando muestra los volúmenes cifrados en `cluster1`:

```
cluster1::> volume show -is-encrypted true
```

| Vserver | Volume | Aggregate | State  | Type  | Size  | Available | Used  |
|---------|--------|-----------|--------|-------|-------|-----------|-------|
| -----   | -----  | -----     | -----  | ----- | ----- | -----     | ----- |
| vs1     | vol1   | aggr3     | online | RW    | 200GB | 160.0GB   | 20%   |

## Delegue la autoridad para ejecutar el comando `volume move`

Puede utilizar el `volume move` comando para cifrar un volumen existente, mover un volumen cifrado o descifrar un volumen. Los administradores del clúster pueden ejecutar `volume move` Command propiamente dichos o pueden delegar la autoridad para ejecutar el comando a los administradores de SVM.

### Acerca de esta tarea

De manera predeterminada, los administradores de SVM asignan el `vsadmin` rol, que no incluye la autoridad para mover volúmenes. Debe asignar el `vsadmin-volume` Rol a administradores de SVM para permitirles ejecutar el `volume move` comando.

### Paso

#### 1. Delegue la autoridad para ejecutar `volume move` comando:

```
security login modify -vserver SVM_name -user-or-group-name user_or_group_name
-application application -authmethod authentication_method -role vsadmin-
volume
```

Para obtener una sintaxis de comando completa, consulte la página de manual del comando.

El siguiente comando concede la autoridad de administrador de SVM para ejecutar el `volume move` comando.

```
cluster1::>security login modify -vserver engData -user-or-group-name
SVM-admin -application ssh -authmethod domain -role vsadmin-volume
```

### Cambie la clave de cifrado de un volumen con el comando `volume Encryption rekey start`

Es una práctica recomendada para cambiar la clave de cifrado de un volumen periódicamente. A partir de ONTAP 9.3, puede utilizar la `volume encryption rekey start` para cambiar la clave de cifrado.

#### Acerca de esta tarea

Una vez que se inicia una operación de reclave, ésta debe completarse. No hay vuelta a la llave antigua. Si se encuentra con un problema de rendimiento durante la operación, puede ejecutar el `volume encryption rekey pause` para pausar la operación y el `volume encryption rekey resume` comando para reanudar la operación.

Hasta que finalice la operación de reclave, el volumen tendrá dos teclas. Las nuevas escrituras y sus lecturas correspondientes utilizarán la nueva clave. De lo contrario, las lecturas utilizarán la clave antigua.



No puede utilizar `volume encryption rekey start` Para volver a introducir un volumen de SnapLock.

#### Pasos

1. Cambiar una clave de cifrado:

```
volume encryption rekey start -vserver SVM_name -volume volume_name
```

El comando siguiente cambia la clave de cifrado de `vol1` En `SVMvs1`:

```
cluster1::> volume encryption rekey start -vserver vs1 -volume vol1
```

2. Verificar el estado de la operación de rellave:

```
volume encryption rekey show
```

Para obtener una sintaxis de comando completa, consulte la página de manual del comando.

El siguiente comando muestra el estado de la operación de nueva clave:

```
cluster1::> volume encryption rekey show
```

| Vserver | Volume | Start Time         | Status                       |
|---------|--------|--------------------|------------------------------|
| -----   | -----  | -----              | -----                        |
| vs1     | vol1   | 9/18/2017 17:51:41 | Phase 2 of 2 is in progress. |

3. Una vez finalizada la operación de nueva clave, compruebe que el volumen esté habilitado para el cifrado:

```
volume show -is-encrypted true
```

Para obtener una sintaxis de comando completa, consulte la página de manual del comando.

El siguiente comando muestra los volúmenes cifrados en `cluster1`:

```
cluster1::> volume show -is-encrypted true
```

| Vserver | Volume | Aggregate | State  | Type  | Size  | Available | Used  |
|---------|--------|-----------|--------|-------|-------|-----------|-------|
| -----   | -----  | -----     | -----  | ----- | ----- | -----     | ----- |
| vs1     | vol1   | aggr2     | online | RW    | 200GB | 160.0GB   | 20%   |

### Cambie la clave de cifrado de un volumen con el comando `volume move start`

Es una práctica recomendada para cambiar la clave de cifrado de un volumen periódicamente. Puede utilizar el `volume move start` para cambiar la clave de cifrado. Debe usar `volume move start` En ONTAP 9.2 y anteriores. El volumen movido puede residir en el mismo agregado o en otra diferente.

#### Acerca de esta tarea

No puede utilizar `volume move start` Para volver a introducir los datos en un volumen SnapLock o FlexGroup.

#### Antes de empezar

Para realizar esta tarea, debe ser un administrador de clústeres. Como alternativa, puede ser un administrador de SVM al que el administrador del clúster haya delegado autoridad. Para obtener más información, consulte ["delegue la autoridad para ejecutar el comando volume move"](#).

#### Pasos

1. Mueva un volumen existente y cambie la clave de cifrado:

```
volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -generate-destination-key true
```

Para obtener una sintaxis de comando completa, consulte la página de manual del comando.

El siguiente comando mueve un volumen existente llamado **vol1** al agregado de destino **aggr2** y cambia la clave de cifrado:

```
cluster1::> volume move start -vserver vs1 -volume voll1 -destination
-aggregate aggr2 -generate-destination-key true
```

Se crea una nueva clave de cifrado para el volumen. Los datos del volumen permanecen cifrados.

## 2. Compruebe que el volumen esté habilitado para el cifrado:

```
volume show -is-encrypted true
```

Para obtener una sintaxis de comando completa, consulte la página de manual del comando.

El siguiente comando muestra los volúmenes cifrados en cluster1:

```
cluster1::> volume show -is-encrypted true
```

| Vserver | Volume | Aggregate | State  | Type  | Size  | Available | Used  |
|---------|--------|-----------|--------|-------|-------|-----------|-------|
| -----   | -----  | -----     | -----  | ----- | ----- | -----     | ----- |
| vs1     | voll1  | aggr2     | online | RW    | 200GB | 160.0GB   | 20%   |

## Gire las claves de autenticación para el cifrado del almacenamiento de NetApp

Puede rotar las claves de autenticación cuando utiliza Storage Encryption (NSE) de NetApp.

### Acerca de esta tarea

La rotación de claves de autenticación en un entorno de NSE es compatible si se utiliza External Key Manager (KMIP).



No se admite la rotación de claves de autenticación en un entorno de NSE en el gestor de claves incorporado (OKM).

### Pasos

1. Utilice la `security key-manager create-key` comando para generar nuevas claves de autenticación.

Debe generar nuevas claves de autenticación para poder cambiar las claves de autenticación.

2. Utilice la `storage encryption disk modify -disk * -data-key-id` comando para cambiar las claves de autenticación.

## Elimine un volumen cifrado

Puede utilizar el `volume delete` comando para eliminar un volumen cifrado.

### Antes de empezar

- Para realizar esta tarea, debe ser un administrador de clústeres. Como alternativa, puede ser un administrador de SVM al que el administrador del clúster haya delegado autoridad. Para obtener más

información, consulte ["delegue la autoridad para ejecutar el comando volume move"](#).

- El volumen debe estar fuera de línea.

## Paso

1. Elimine un volumen cifrado:

```
volume delete -vserver SVM_name -volume volume_name
```

Para obtener una sintaxis de comando completa, consulte la página de manual del comando.

El siguiente comando elimina un volumen cifrado denominado vol1:

```
cluster1::> volume delete -vserver vs1 -volume vol1
```

Introduzca *yes* cuando se le solicite que confirme la eliminación.

El sistema elimina la clave de cifrado del volumen después de 24 horas.

Uso `volume delete` con la `-force true` opción para eliminar un volumen y destruir inmediatamente la clave de cifrado correspondiente. Este comando requiere privilegios avanzados. Para obtener más información, consulte la página `man`.

## Después de terminar

Puede utilizar el `volume recovery-queue` comando para recuperar un volumen eliminado durante el período de retención después de emitir el `volume delete` comando:

```
volume recovery-queue SVM_name -volume volume_name
```

## "Cómo usar la función Volume Recovery"

### Eliminar datos de forma segura en un volumen cifrado

**Purgue los datos de forma segura en una información general de los volúmenes cifrados**

A partir de ONTAP 9.4, puede utilizar la purga segura para eliminar datos sin interrupciones en volúmenes con la función NVE habilitada. La depuración de datos en un volumen cifrado garantiza que no pueda recuperarse de los medios físicos, por ejemplo, en casos de "eliminación de columnas", donde los seguimientos de datos pueden haberse quedado atrás cuando se sobrescriben los bloques o cuando se eliminan de forma segura los datos de un inquilino que están vaciando.

La purga segura solo funciona con los archivos eliminados previamente en volúmenes habilitados para NVE. No puede limpiar un volumen no cifrado. Debe usar los servidores KMIP para suministrar claves, no el gestor de claves incorporado.

### Consideraciones que tener en cuenta al utilizar la purga segura

- Los volúmenes creados en un agregado habilitado para el cifrado de agregados de NetApp (NAE) no admiten la purga segura.

- La purga segura solo funciona con los archivos eliminados previamente en volúmenes habilitados para NVE.
- No puede limpiar un volumen no cifrado.
- Debe usar los servidores KMIP para suministrar claves, no el gestor de claves incorporado.

Las funciones de purga segura varían dependiendo de su versión de ONTAP.

#### ONTAP 9,8 y versiones posteriores

- MetroCluster y FlexGroup admiten la purga segura.
- Si el volumen que se purga es el origen de una relación de SnapMirror, no es necesario interrumpir la relación de SnapMirror para realizar una purga segura.
- El método de recifrado es diferente para los volúmenes que utilizan protección de datos SnapMirror frente a los volúmenes que no utilizan protección de datos de SnapMirror (DP) o los que utilizan protección de datos ampliada de SnapMirror.
  - De forma predeterminada, los volúmenes que utilizan el modo de protección de datos de SnapMirror (DP) vuelven a cifrar los datos con el método de recifrado del volumen.
  - De forma predeterminada, los volúmenes que no utilizan la protección de datos de SnapMirror o volúmenes mediante el modo de protección de datos ampliada (XDP) de SnapMirror utilizan el método de recifrado in situ.
  - Estos valores predeterminados se pueden cambiar con `secure purge re-encryption-method [volume-move|in-place-rekey]` comando.
- De manera predeterminada, todas las copias de Snapshot de los volúmenes FlexVol se eliminan automáticamente durante la operación de purga segura. De manera predeterminada, las snapshots en volúmenes de FlexGroup y los volúmenes que utilizan la protección de datos de SnapMirror no se eliminan automáticamente durante la operación de purga segura. Estos valores predeterminados se pueden cambiar con `secure purge delete-all-snapshots [true|false]` comando.

#### ONTAP 9.7 y anteriores:

- La purga segura no admite lo siguiente:
  - FlexClone
  - SnapVault
  - FabricPool
- Si el volumen que se purga es el origen de una relación de SnapMirror, debe interrumpir la relación de SnapMirror para poder purgar el volumen.

Si hay copias Snapshot ocupadas en el volumen, debe liberar las copias Snapshot antes de poder purgar el volumen. Por ejemplo, es posible que deba dividir un volumen FlexClone de su principal.

- Al invocar correctamente la función de purga de seguridad, se activa un movimiento de volúmenes que se vuelve a cifrar los datos restantes sin purgar con una clave nueva.

El volumen movido permanece en el agregado actual. La clave antigua se destruye automáticamente, lo que garantiza que los datos purgados no puedan recuperarse del medio de almacenamiento.



A partir de ONTAP 9.4, puede utilizar la purga segura para obtener datos «crub» sin interrupciones en volúmenes con NVE habilitado.

### Acerca de esta tarea

La purga segura puede tardar de varios minutos a varias horas en completarse, dependiendo de la cantidad de datos de los archivos eliminados. Puede utilizar el `volume encryption secure-purge show` comando para ver el estado de la operación. Puede utilizar el `volume encryption secure-purge abort` comando para finalizar la operación.



Para realizar una purga segura en un host SAN, debe eliminar todo el LUN que contiene los archivos que desea purgar, o debe poder perforar agujeros en la LUN para los bloques que pertenecen a los archivos que desea purgar. Si no puede eliminar la LUN, o el sistema operativo del host no admite orificios de perforación en la LUN, no puede realizar una purga segura.

### Antes de empezar

- Para realizar esta tarea, debe ser un administrador de clústeres.
- Se requieren privilegios avanzados para esta tarea.

### Pasos

1. Elimine los archivos o la LUN que desea purgar de forma segura.
  - En un cliente NAS, elimine los archivos que desea purgar de forma segura.
  - En un host SAN, elimine la LUN que desea purgar o perforar agujeros en la LUN de los bloques que pertenecen a los archivos que desea purgar.
2. En el sistema de almacenamiento, cambie al nivel de privilegio avanzado:

```
set -privilege advanced
```

3. Si los archivos que desea purgar de forma segura están en instantáneas, elimine las instantáneas:

```
snapshot delete -vserver SVM_name -volume volume_name -snapshot
```

4. Elimine de forma segura los archivos eliminados:

```
volume encryption secure-purge start -vserver SVM_name -volume volume_name
```

El siguiente comando purga de manera segura los archivos eliminados de `vol1` En `SVMvs1`:

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume
vol1
```

5. Compruebe el estado de la operación de purga segura:

```
volume encryption secure-purge show
```

## Purgue los datos de forma segura en un volumen cifrado con una relación de SnapMirror asíncrono

A partir de ONTAP 9.8, puede utilizar una purga segura para datos «crub» sin interrupciones en volúmenes habilitados para NVE con una relación asíncrona de SnapMirror.

### Antes de empezar

- Para realizar esta tarea, debe ser un administrador de clústeres.
- Se requieren privilegios avanzados para esta tarea.

### Acerca de esta tarea

La purga segura puede tardar de varios minutos a varias horas en completarse, dependiendo de la cantidad de datos de los archivos eliminados. Puede utilizar el `volume encryption secure-purge show` comando para ver el estado de la operación. Puede utilizar el `volume encryption secure-purge abort` comando para finalizar la operación.



Para realizar una purga segura en un host SAN, debe eliminar todo el LUN que contiene los archivos que desea purgar, o debe poder perforar agujeros en la LUN para los bloques que pertenecen a los archivos que desea purgar. Si no puede eliminar la LUN, o el sistema operativo del host no admite orificios de perforación en la LUN, no puede realizar una purga segura.

### Pasos

1. En el sistema de almacenamiento, cambie al nivel de privilegio avanzado:

```
set -privilege advanced
```

2. Elimine los archivos o la LUN que desea purgar de forma segura.
  - En un cliente NAS, elimine los archivos que desea purgar de forma segura.
  - En un host SAN, elimine la LUN que desea purgar o perforar agujeros en la LUN de los bloques que pertenecen a los archivos que desea purgar.
3. Prepare el volumen de destino en la relación asíncrona para que se purgue de forma segura:

```
volume encryption secure-purge start -vserver SVM_name -volume volume_name
-prepare true
```

Repita este paso con cada volumen de la relación de SnapMirror asíncrono.

4. Si los archivos que desea purgar de forma segura están en las copias snapshot, elimine las copias snapshot:

```
snapshot delete -vserver SVM_name -volume volume_name -snapshot
```

5. Si los archivos que desea purgar de forma segura están en las copias snapshot básicas, haga lo siguiente:
  - a. Cree una copia Snapshot en el volumen de destino en la relación de SnapMirror asíncrono:

```
volume snapshot create -snapshot snapshot_name -vserver SVM_name -volume
volume_name
```

- b. Actualización de SnapMirror para hacer avanzar la copia snapshot básica:

```
snapmirror update -source-snapshot snapshot_name -destination-path
destination_path
```

Repita este paso con cada volumen de la relación de SnapMirror asíncrono.

- a. Repita los pasos (a) y (b) igual al número de copias Snapshot base y una.

Por ejemplo, si tiene dos copias Snapshot base, deberá repetir los pasos (a) y (b) tres veces.

- b. Compruebe que la copia Snapshot básica está presente:

```
snapshot show -vserver SVM_name -volume volume_name
```

- c. Elimine la copia Snapshot básica:

```
snapshot delete -vserver svm_name -volume volume_name -snapshot snapshot
```

#### 6. Elimine de forma segura los archivos eliminados:

```
volume encryption secure-purge start -vserver svm_name -volume volume_name
```

Repita este paso con cada volumen de la relación de SnapMirror asíncrono.

El siguiente comando purga de forma segura los archivos eliminados de «'vol1'» de la SVM «'vs1'»:

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume
vol1
```

#### 7. Compruebe el estado de la operación de purga segura:

```
volume encryption secure-purge show
```

### Limpie los datos en un volumen cifrado con una relación de SnapMirror síncrono

A partir de ONTAP 9,8, puede utilizar una purga segura para «depurar» datos sin interrupciones en los volúmenes con NVE habilitados con una relación de SnapMirror síncrono.

#### Acerca de esta tarea

Una purga segura puede tardar de varios minutos a varias horas en completarse, dependiendo de la cantidad de datos de los archivos eliminados. Puede utilizar el `volume encryption secure-purge show` comando para ver el estado de la operación. Puede utilizar el `volume encryption secure-purge abort` comando para finalizar la operación.



Para realizar una purga segura en un host SAN, debe eliminar todo el LUN que contiene los archivos que desea purgar, o debe poder perforar agujeros en la LUN para los bloques que pertenecen a los archivos que desea purgar. Si no puede eliminar la LUN, o el sistema operativo del host no admite orificios de perforación en la LUN, no puede realizar una purga segura.

#### Antes de empezar

- Para realizar esta tarea, debe ser un administrador de clústeres.
- Se requieren privilegios avanzados para esta tarea.

## Pasos

1. En el sistema de almacenamiento, cambie al nivel de privilegio avanzado:

```
set -privilege advanced
```

2. Elimine los archivos o la LUN que desea purgar de forma segura.
  - En un cliente NAS, elimine los archivos que desea purgar de forma segura.
  - En un host SAN, elimine la LUN que desea purgar o perforar agujeros en la LUN de los bloques que pertenecen a los archivos que desea purgar.
3. Prepare el volumen de destino en la relación asíncrona para que se purgue de forma segura:

```
volume encryption secure-purge start -vserver SVM_name -volume volume_name
-prepare true
```

Repita este paso con el otro volumen de la relación de SnapMirror síncrono.

4. Si los archivos que desea purgar de forma segura están en las copias snapshot, elimine las copias snapshot:

```
snapshot delete -vserver SVM_name -volume volume_name -snapshot snapshot
```

5. Si el archivo de purga segura está en la base o en copias snapshot comunes, actualice SnapMirror para mover la copia snapshot común hacia delante:

```
snapmirror update -source-snapshot snapshot_name -destination-path
destination_path
```

Existen dos copias Snapshot comunes, por lo que este comando debe emitirse dos veces.

6. Si el archivo de purga segura está en la copia Snapshot coherente con las aplicaciones, elimine la copia Snapshot en ambos volúmenes de la relación de SnapMirror síncrono:

```
snapshot delete -vserver SVM_name -volume volume_name -snapshot snapshot
```

Ejecute este paso en ambos volúmenes.

7. Elimine de forma segura los archivos eliminados:

```
volume encryption secure-purge start -vserver SVM_name -volume volume_name
```

Repita este paso con cada volumen de la relación de SnapMirror síncrono.

El siguiente comando purga de forma segura los archivos eliminados en «'vol1'» en la SMV «'vs1'».

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume
vol1
```

## 8. Compruebe el estado de la operación de purga segura:

```
volume encryption secure-purge show
```

### Cambie la clave de acceso de gestión de claves incorporada

Una práctica recomendada para la seguridad es cambiar periódicamente la clave de acceso de gestión de claves incorporada. Debe copiar la nueva clave de gestión integrada en una ubicación segura fuera del sistema de almacenamiento para usarla en el futuro.

#### Antes de empezar

- Debe ser un administrador de clúster o de SVM para ejecutar esta tarea.
- Se requieren privilegios avanzados para esta tarea.

#### Pasos

##### 1. Cambie al nivel de privilegio avanzado:

```
set -privilege advanced
```

##### 2. Cambie la clave de acceso de gestión de claves incorporada:

| Para esta versión de ONTAP... | Se usa este comando...                                      |
|-------------------------------|-------------------------------------------------------------|
| ONTAP 9.6 y posteriores       | <code>security key-manager onboard update-passphrase</code> |
| ONTAP 9,5 y anteriores        | <code>security key-manager update-passphrase</code>         |

Para obtener una sintaxis de comando completa, consulte las páginas `man`.

El siguiente comando ONTAP 9.6 permite cambiar la clave de acceso de gestión de claves incorporada para `cluster1`:

```
cluster1::> security key-manager onboard update-passphrase
Warning: This command will reconfigure the cluster passphrase for
onboard key management for Vserver "cluster1".
Do you want to continue? {y|n}: y
Enter current passphrase:
Enter new passphrase:
```

3. Introduzca `y` en el símbolo del sistema de para cambiar la clave de acceso de gestión de claves incorporada.
4. Introduzca la frase de contraseña actual en la solicitud de contraseña actual.
5. En la nueva solicitud de frase de contraseña, introduzca una frase de paso entre 32 y 256 caracteres, o bien, para `"cc-mode"`, una frase de paso entre 64 y 256 caracteres.

Si la frase de paso "cc-mode" especificada es menor de 64 caracteres, hay un retraso de cinco segundos antes de que la operación de configuración del gestor de claves vuelva a mostrar la indicación de contraseña.

6. En la solicitud de confirmación de contraseña, vuelva a introducir la frase de contraseña.

### Después de terminar

En un entorno de MetroCluster, debe actualizar la clave de acceso en el clúster de partners:

- En ONTAP 9.5 y versiones anteriores, debe ejecutar `security key-manager update-passphrase` con la misma clave de acceso en el clúster del partner.
- A partir de la versión 9.6 de ONTAP, se le solicitará que se ejecute `security key-manager onboard sync` con la misma clave de acceso en el clúster del partner.

Debe copiar la clave de gestión integrada en una ubicación segura fuera del sistema de almacenamiento para usarla en el futuro.

Debe realizar un backup manual de la información de gestión de claves siempre que se cambie la clave de acceso de gestión de claves incorporada.

["Realizar un backup manual de la información de gestión de claves incorporada"](#)

### Realice un backup manual de la información de gestión de claves incorporada

Se debe copiar la información de gestión de claves incorporada en una ubicación segura fuera del sistema de almacenamiento siempre que se configure la clave de acceso de Onboard Key Manager.

### Lo que necesitará

- Para realizar esta tarea, debe ser un administrador de clústeres.
- Se requieren privilegios avanzados para esta tarea.

### Acerca de esta tarea

Se realiza automáticamente un backup de toda la información de gestión de claves en la base de datos replicada (RDB) del clúster. También debe realizar un backup de la información de gestión de claves manualmente para su uso en caso de desastre.

### Pasos

1. Cambie al nivel de privilegio avanzado:

```
set -privilege advanced
```

2. Muestre la información de backup de gestión de claves para el clúster:

| Para esta versión de ONTAP... | Se usa este comando...                                |
|-------------------------------|-------------------------------------------------------|
| ONTAP 9.6 y posteriores       | <code>security key-manager onboard show-backup</code> |
| ONTAP 9,5 y anteriores        | <code>security key-manager backup show</code>         |

+  
El siguiente comando 9,6 muestra la información del backup de gestión de claves para `cluster1`:  
+

1. Copie la información del backup en una ubicación segura fuera del sistema de almacenamiento para usarla en caso de desastre.

El procedimiento que siga para restaurar las claves de cifrado de gestión de claves incorporada varía en función de su versión de ONTAP.

## Antes de empezar

- Si utiliza NSE con un servidor de gestión de claves externa (KMIP), debe haber eliminado la base de datos de gestor de claves externo. Para obtener más información, consulte ["transición a la gestión de claves incorporada desde la gestión de claves externa"](#)
- Para realizar esta tarea, debe ser un administrador de clústeres.



Si utiliza NSE en un sistema con un módulo Flash Cache, también debe habilitar NVE o NAE. NSe no cifra los datos que residen en el módulo de Flash Cache.

## ONTAP 9,8 y versiones posteriores con volumen raíz cifrado



Si ejecuta ONTAP 9,8 o una versión posterior y el volumen raíz no está cifrado, siga el procedimiento para ONTAP 9,6 o una versión posterior.

Si ejecuta ONTAP 9.8 y versiones posteriores y el volumen raíz está cifrado, debe configurar una clave de recuperación de gestión de claves incorporada con el menú de arranque. Este proceso también es necesario si realiza un reemplazo del soporte de arranque.

1. Arranque el nodo en el menú de arranque y seleccione opción (10) Set onboard key management recovery secrets.
2. Introduzca `y` para utilizar esta opción.
3. En el aviso de, introduzca la clave de acceso de gestión de claves incorporada para el clúster.
4. En el aviso, introduzca los datos de la clave de backup.

El nodo vuelve al menú de arranque.

5. En el menú de inicio, seleccione opción (1) Normal Boot.

## ONTAP 9.6 y posteriores

1. Compruebe que es necesario restaurar la clave:  
`security key-manager key query -node node`
2. Restaure la clave:  
`security key-manager onboard sync`

Para obtener una sintaxis de comando completa, consulte las páginas man.

El siguiente comando de ONTAP 9.6 sincroniza las claves de la jerarquía de claves integradas:

```
cluster1::> security key-manager onboard sync
```

```
Enter the cluster-wide passphrase for onboard key management in Vserver
"cluster1":> <32..256 ASCII characters long text>
```

3. En la solicitud de contraseña, introduzca la clave de acceso de gestión de claves incorporada para el clúster.



## ONTAP 9,5 y anteriores

1. Compruebe que es necesario restaurar la clave:

```
security key-manager key show
```

2. Si ejecuta ONTAP 9.8 y versiones posteriores y se cifra el volumen raíz, complete los siguientes pasos:

Si ejecuta ONTAP 9.6 o 9.7, o si está ejecutando ONTAP 9.8 o una versión posterior y el volumen raíz no está cifrado, omita este paso.

3. Restaure la clave:

```
security key-manager setup -node node
```

Para obtener una sintaxis de comando completa, consulte las páginas man.

4. En la solicitud de contraseña, introduzca la clave de acceso de gestión de claves incorporada para el clúster.

## Restaure las claves de cifrado de gestión de claves externas

Puede restaurar manualmente claves de cifrado de gestión de claves externas e insertarlas en otro nodo. Tal vez desee hacer esto si va a reiniciar un nodo que estaba inactivo temporalmente cuando creó las claves para el clúster.

### Acerca de esta tarea

A partir de la versión 9.6 de ONTAP, se puede utilizar el `security key-manager key query -node node_name` comando para comprobar si es necesario restaurar la clave.

En ONTAP 9.5 y versiones anteriores, se puede utilizar `security key-manager key show` comando para comprobar si es necesario restaurar la clave.



Si utiliza NSE en un sistema con un módulo Flash Cache, también debe habilitar NVE o NAE. NSe no cifra los datos que residen en el módulo de Flash Cache.

### Antes de empezar

Debe ser un administrador de clúster o de SVM para ejecutar esta tarea.

### Pasos

1. Si ejecuta ONTAP 9.8 o una versión posterior y el volumen raíz está cifrado, haga lo siguiente:

Si está ejecutando ONTAP 9.7 o una versión anterior, o si está ejecutando ONTAP 9.8 o una versión posterior y el volumen raíz no está cifrado, omita este paso.

- a. Establezca los arranques:

```
setenv kmip.init.ipaddr <ip-address>
```

```
setenv kmip.init.netmask <netmask>
```

```
setenv kmip.init.gateway <gateway>
```

```
setenv kmip.init.interface e0M
```

boot\_ontap

- b. Arranque el nodo en el menú de arranque y seleccione opción (11) `Configure node for external key management`.
- c. Siga las instrucciones para introducir el certificado de gestión.

Una vez introducida toda la información del certificado de gestión, el sistema vuelve al menú de arranque.

- d. En el menú de inicio, seleccione opción (1) `Normal Boot`.

## 2. Restaure la clave:

| Para esta versión de ONTAP...                                  | Se usa este comando...                                                                            |
|----------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| ONTAP 9.6 y posteriores                                        | <code>`security key-manager external restore -vserver SVM -node node -key-server host_name</code> |
| <code>IP_address:port -key-id key_id -key -tag key_tag`</code> | ONTAP 9,5 y anteriores                                                                            |



`node` el valor predeterminado es todos los nodos. Para obtener una sintaxis de comando completa, consulte las páginas man. Este comando no es compatible cuando la gestión de claves incorporada está habilitada.

El siguiente comando ONTAP 9.6 restaura claves de autenticación de gestión de claves externas a todos los nodos en `cluster1`:

```
cluster1::> security key-manager external restore
```

## Reemplace los certificados SSL

Todos los certificados SSL tienen una fecha de vencimiento. Debe actualizar los certificados antes de que caduquen para evitar la pérdida de acceso a las claves de autenticación.

### Antes de empezar

- Debe haber obtenido el certificado público de reemplazo y la clave privada para el clúster (certificado de cliente KMIP).
- Debe haber obtenido el certificado público de reemplazo para el servidor KMIP (certificado de servidor KMIP).
- Debe ser un administrador de clúster o de SVM para ejecutar esta tarea.
- En un entorno de MetroCluster, debe reemplazar el certificado SSL KMIP en ambos clústeres.



Puede instalar los certificados de cliente y servidor de repuesto en el servidor KMIP antes o después de instalar los certificados en el clúster.

## Pasos

1. Instale el nuevo certificado de CA de servidor KMIP:

```
security certificate install -type server-ca -vserver <>
```

2. Instale el nuevo certificado de cliente KMIP:

```
security certificate install -type client -vserver <>
```

3. Actualice la configuración del gestor de claves para usar los certificados recién instalados:

```
security key-manager external modify -vserver <> -client-cert <> -server-ca
-certs <>
```

Si ejecuta ONTAP 9.6 o una versión posterior en un entorno MetroCluster y desea modificar la configuración de gestor de claves en la SVM de administrador, debe ejecutar el comando en ambos clústeres de la configuración.



La actualización de la configuración del gestor de claves para usar los certificados recién instalados devolverá un error si las claves públicas/privadas del nuevo certificado de cliente son diferentes de las instaladas previamente. Consulte el artículo de la base de conocimientos ["Las claves privadas o públicas del nuevo certificado de cliente son diferentes del certificado de cliente existente"](#) para obtener instrucciones sobre cómo anular este error.

## Sustituya una unidad FIPS o SED

Puede reemplazar una unidad FIPS o SED de la misma manera que reemplaza un disco normal. Asegúrese de asignar nuevas claves de autenticación de datos a la unidad de reemplazo. Para una unidad FIPS, puede asignar también una nueva clave de autenticación FIPS 140-2.



Si un par de alta disponibilidad está usando ["Cifrar unidades SAS o NVMe \(SED, NSE, FIPS\)"](#), debe seguir las instrucciones del tema ["Devolver una unidad FIPS o SED al modo sin protección"](#) Para todas las unidades dentro de la pareja de ha antes de inicializar el sistema (opciones de arranque 4 o 9). Si las unidades se reasignan, es posible que no se produzcan pérdidas de datos futuras.

### Antes de empezar

- Debe conocer el ID de clave de la clave de autenticación que utiliza la unidad.
- Para realizar esta tarea, debe ser un administrador de clústeres.

### Pasos

1. Asegúrese de que el disco se ha marcado como erróneo:

```
storage disk show -broken
```

Para obtener una sintaxis de comando completa, consulte la página man.

```
cluster1::> storage disk show -broken
```

```
Original Owner: cluster1-01
```

```
Checksum Compatibility: block
```

|          |        |         |      |       |     |      |       |       |       |         | Usable |
|----------|--------|---------|------|-------|-----|------|-------|-------|-------|---------|--------|
| Physical |        |         |      |       |     |      |       |       |       |         |        |
| Disk     | Outage | Reason  | HA   | Shelf | Bay | Chan | Pool  | Type  | RPM   | Size    |        |
| Size     |        |         |      |       |     |      |       |       |       |         |        |
| -----    | ----   | -----   | ---- | ----  | --- | ---- | ----- | ----- | ----- | -----   | -----  |
| 0.0.0    | admin  | failed  | 0b   | 1     | 0   | A    | Pool0 | FCAL  | 10000 | 132.8GB |        |
| 133.9GB  |        |         |      |       |     |      |       |       |       |         |        |
| 0.0.7    | admin  | removed | 0b   | 2     | 6   | A    | Pool1 | FCAL  | 10000 | 132.8GB |        |
| 134.2GB  |        |         |      |       |     |      |       |       |       |         |        |
| [...]    |        |         |      |       |     |      |       |       |       |         |        |

2. Quite el disco con error y sustitúyalo por una nueva unidad FIPS o SED siguiendo las instrucciones de la guía de hardware para su modelo de bandeja de discos.
3. Asigne la propiedad del disco recién sustituido:

```
storage disk assign -disk disk_name -owner node
```

Para obtener una sintaxis de comando completa, consulte la página man.

```
cluster1::> storage disk assign -disk 2.1.1 -owner cluster1-01
```

4. Confirme que se ha asignado el disco nuevo:

```
storage encryption disk show
```

Para obtener una sintaxis de comando completa, consulte la página man.

```
cluster1::> storage encryption disk show
Disk Mode Data Key ID

0.0.0 data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
0.0.1 data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
1.10.0 data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
1.10.1 data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
2.1.1 open 0x0
[...]
```

5. Asigne las claves de autenticación de datos a la unidad FIPS o SED.

"Asignar una clave de autenticación de datos a una unidad FIPS o SED (gestión de claves externa)"

6. Si es necesario, asigne una clave de autenticación FIPS 140-2 a la unidad FIPS.

"Asignar una clave de autenticación FIPS 140-2 a una unidad FIPS"

## Haga que los datos en una unidad FIPS o SED sean inaccesibles

### Hacer datos en una unidad FIPS o información general inaccesible de SED

Si desea que los datos de una unidad FIPS o SED sean inaccesibles permanentemente, pero mantenga el espacio no utilizado de la unidad disponible para los nuevos datos, puede desinfectar el disco. Si desea que los datos no se puedan acceder a ellos de forma permanente y no es necesario volver a utilizar la unidad, es posible destruirlos.

- El saneamiento de disco

Cuando se limpia una unidad de autocifrado, el sistema cambia la clave de cifrado de disco a un nuevo valor aleatorio, restablece el estado de bloqueo de encendido a FALSE y establece el ID de clave en un valor predeterminado, es decir, el ID seguro de fabricante 0x0 (unidades SAS) o una clave nula (unidades NVMe). Si lo hace, los datos del disco son inaccesibles y es imposible recuperarlos. Puede reutilizar discos sanitizados como discos de repuesto no ceros.

- Destrucción de discos

Cuando destruye una unidad FIPS o SED, el sistema establece la clave de cifrado del disco en un valor aleatorio desconocido y bloquea el disco de forma irreversible. De este modo, el disco se vuelve inutilizable de forma permanente y los datos del mismo no se podrán acceder de forma permanente.

Puede desinfectar o destruir unidades de autocifrado individuales o todas las unidades de autocifrado de un nodo.

## Desinfecte una unidad FIPS o SED

Si desea hacer que los datos en una unidad FIPS o SED sean inaccesibles de forma permanente y utilizar la unidad para datos nuevos, puede utilizar la `storage encryption disk sanitize` comando para desinfectar la unidad.

### Acerca de esta tarea

Cuando se limpia una unidad de autocifrado, el sistema cambia la clave de cifrado de disco a un nuevo valor aleatorio, restablece el estado de bloqueo de encendido a FALSE y establece el ID de clave en un valor predeterminado, es decir, el ID seguro de fabricante 0x0 (unidades SAS) o una clave nula (unidades NVMe). Si lo hace, los datos del disco son inaccesibles y es imposible recuperarlos. Puede reutilizar discos sanitizados como discos de repuesto no ceros.

### Antes de empezar

Para realizar esta tarea, debe ser un administrador de clústeres.

### Pasos

1. Migre los datos que se deben conservar a un agregado en otro disco.
2. Elimine el agregado de la unidad FIPS o SED para que se sanean:

```
storage aggregate delete -aggregate aggregate_name
```

Para obtener una sintaxis de comando completa, consulte la página man.

```
cluster1::> storage aggregate delete -aggregate aggr1
```

3. Identifique el ID de disco para la unidad FIPS o SED para sanitización:

```
storage encryption disk show -fields data-key-id,fips-key-id,owner
```

Para obtener una sintaxis de comando completa, consulte la página man.

```
cluster1::> storage encryption disk show
Disk Mode Data Key ID

0.0.0 data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
0.0.1 data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
1.10.2 data
F1CB30AFF1CB30B0010100000000000CF0EFD81EA9F6324EA97B369351C56AC
[...]
```

4. Si una unidad FIPS se ejecuta en el modo de cumplimiento de normativas FIPS, establezca el ID de clave de autenticación FIPS del nodo nuevamente en el ID de MSID 0x0 predeterminado:

```
storage encryption disk modify -disk disk_id -fips-key-id 0x0
```

Puede utilizar el `security key-manager query` Comando para ver los ID clave.

```
cluster1::> storage encryption disk modify -disk 1.10.2 -fips-key-id 0x0
```

Info: Starting modify on 1 disk.

View the status of the operation by using the  
storage encryption disk show-status command.

## 5. Desinfecte la unidad:

```
storage encryption disk sanitize -disk disk_id
```

Puede utilizar este comando para desinfectar solo los discos duros o los discos rotos. Para desinfectar todos los discos independientemente del tipo, utilice `-force-all-state` opción. Para obtener una sintaxis de comando completa, consulte la página [man](#).



ONTAP le pedirá que introduzca una frase de confirmación antes de continuar. Introduzca la frase exactamente como se muestra en la pantalla.

```
cluster1::> storage encryption disk sanitize -disk 1.10.2
```

Warning: This operation will cryptographically sanitize 1 spare or  
broken self-encrypting disk on 1 node.

To continue, enter sanitize disk: sanitize disk

Info: Starting sanitize on 1 disk.

View the status of the operation using the  
storage encryption disk show-status command.

## Destruir una unidad FIPS o SED

Si desea que los datos en una unidad FIPS o SED sean inaccesibles de forma permanente y no necesita reutilizar la unidad, puede utilizar la `storage encryption disk destroy` comando para destruir el disco.

### Acerca de esta tarea

Cuando destruye una unidad FIPS o SED, el sistema configura la clave de cifrado de disco para tener un valor aleatorio desconocido y bloquea la unidad de forma irreversible. De este modo, el disco se vuelve prácticamente inutilizable y los datos del disco se dejan permanentemente inaccesibles. No obstante, puede restablecer el disco a su configuración de fábrica mediante el ID seguro físico (PSID) impreso en la etiqueta del disco. Para obtener más información, consulte ["Devolver una unidad FIPS o SED al servicio cuando se pierden las claves de autenticación"](#).



No debe destruir una unidad FIPS o SED a menos que tenga el servicio no retornable Disk Plus (NRD Plus). La destrucción de un disco anula su garantía.

## Antes de empezar

Para realizar esta tarea, debe ser un administrador de clústeres.

## Pasos

1. Migre los datos que se deben conservar a un agregado en otro disco diferente.
2. Elimine el agregado en la unidad FIPS o SED para destruirse:

```
storage aggregate delete -aggregate aggregate_name
```

Para obtener una sintaxis de comando completa, consulte la página man.

```
cluster1::> storage aggregate delete -aggregate aggr1
```

3. Identifique el ID de disco de la unidad FIPS o SED que se van a destruir:

```
storage encryption disk show
```

Para obtener una sintaxis de comando completa, consulte la página man.

```
cluster1::> storage encryption disk show
Disk Mode Data Key ID

0.0.0 data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
0.0.1 data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
1.10.2 data
F1CB30AFF1CB30B0010100000000000CF0EFD81EA9F6324EA97B369351C56AC
[...]
```

4. Destruir el disco:

```
storage encryption disk destroy -disk disk_id
```

Para obtener una sintaxis de comando completa, consulte la página man.



Se le pedirá que introduzca una frase de confirmación antes de continuar. Introduzca la frase exactamente como se muestra en la pantalla.



```
cluster1::> storage encryption disk destroy -disk 1.10.2
```

Warning: This operation will cryptographically destroy 1 spare or broken self-encrypting disks on 1 node.

You cannot reuse destroyed disks unless you revert them to their original state using the PSID value.

To continue, enter

```
destroy disk
```

```
:destroy disk
```

Info: Starting destroy on 1 disk.

View the status of the operation by using the "storage encryption disk show-status" command.

#### Datos de trituración de emergencia en una unidad FIPS o SED

En caso de una emergencia de seguridad, puede evitar al instante el acceso a una unidad FIPS o SED, incluso si no hay alimentación disponible para el sistema de almacenamiento o el servidor KMIP.

#### Antes de empezar

- Si utiliza un servidor KMIP que no tiene alimentación disponible, el servidor KMIP debe configurarse con un elemento de autenticación fácilmente destruido (por ejemplo, una tarjeta inteligente o una unidad USB).
- Para realizar esta tarea, debe ser un administrador de clústeres.

#### Paso

1. Lleve a cabo la destrucción de datos de emergencia en una unidad FIPS o SED:

|       |                         |
|-------|-------------------------|
| Si... | Realice lo siguiente... |
|-------|-------------------------|

|                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                               |
|---------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| <p>Hay alimentación disponible en el sistema de almacenamiento y hay tiempo para desconectar el sistema de almacenamiento sin problemas</p> | <p>a. Si el sistema de almacenamiento está configurado como un par de alta disponibilidad, deshabilite el respaldo.</p> <p>b. Desconectar y eliminar todos los agregados.</p> <p>c. Configure el nivel de privilegio en Advanced:</p> <pre>set -privilege advanced</pre> <p>d. Si la unidad está en modo de cumplimiento de normativas FIPS, establezca el identificador de clave de autenticación FIPS del nodo nuevamente en el MSID predeterminado:</p> <pre>storage encryption disk modify -disk * -fips-key-id 0x0</pre> <p>e. Detenga el sistema de almacenamiento.</p> <p>f. Arranque en modo de mantenimiento.</p> <p>g. Desinfecte o destruya los discos:</p> <ul style="list-style-type: none"> <li>◦ Si desea que los datos de los discos sean inaccesibles y aún así pueda volver a utilizarlos, desinfecte los discos:</li> </ul> <pre>disk encrypt sanitize -all</pre> <ul style="list-style-type: none"> <li>◦ Si desea que los datos de los discos sean inaccesibles y no necesita guardar los discos, destruya los discos:</li> </ul> <pre>disk encrypt destroy disk_id1 disk_id2 ...</pre> | <p>El sistema de almacenamiento dispone de energía y debe purgar los datos inmediatamente</p> |
|---------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>a. <b>Si desea que los datos de los discos sean inaccesibles y todavía puedan reutilizar los discos, desinfecte los discos:</b></p> <p>b. Si el sistema de almacenamiento está configurado como un par de alta disponibilidad, deshabilite el respaldo.</p> <p>c. Configure el nivel de privilegio en Advanced:</p> <pre>set -privilege advanced</pre> <p>d. Si la unidad está en modo de cumplimiento de normativas FIPS, establezca el identificador de clave de autenticación FIPS del nodo nuevamente en el MSID predeterminado:</p> <pre>storage encryption disk modify -disk * -fips-key-id 0x0</pre> <p>e. Desinfecte el disco:</p> <pre>storage encryption disk sanitize -disk * -force-all-states true</pre> | <p>a. <b>Si desea que los datos en los discos sean inaccesibles y no necesita guardar los discos, destruya los discos:</b></p> <p>b. Si el sistema de almacenamiento está configurado como un par de alta disponibilidad, deshabilite el respaldo.</p> <p>c. Configure el nivel de privilegio en Advanced:</p> <pre>set -privilege advanced</pre> <p>d. Destruya los discos:</p> <pre>storage encryption disk destroy -disk * -force-all-states true</pre> | <p>El sistema de almacenamiento produce una alarma y deja el sistema en un estado de desactivación permanente con todos los datos borrados. Para volver a utilizar el sistema, debe volver a configurarlo.</p> |
| <p>La alimentación está disponible en el servidor KMIP, pero no en el sistema de almacenamiento</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <p>a. Inicie sesión en el servidor KMIP.</p> <p>b. Destruya todas las claves asociadas con las unidades FIPS o SED que contengan los datos a los que desea impedir el acceso. De este modo se evita que el sistema de almacenamiento tenga acceso a las claves de cifrado de disco.</p>                                                                                                                                                                    | <p>No hay alimentación disponible para el servidor KMIP o el sistema de almacenamiento</p>                                                                                                                     |

Para obtener una sintaxis de comando completa, consulte las páginas man.

**Devuelva una unidad FIPS o SED a servicio cuando se pierdan las claves de autenticación**

El sistema trata una unidad FIPS o SED como rota si se pierden las claves de autenticación de ella de forma permanente y no pueden recuperarla del servidor KMIP. Aunque no puede acceder o recuperar los datos en el disco, puede tomar medidas para que el espacio sin usar del SED esté disponible de nuevo para los datos.

**Antes de empezar**

Para realizar esta tarea, debe ser un administrador de clústeres.

**Acerca de esta tarea**

Debe utilizar este proceso solo si tiene la seguridad de que las claves de autenticación de la unidad FIPS o SED se pierden de forma permanente y que no puede recuperarlos.

Si los discos se particionan, primero deben desparticionarse para poder iniciar este proceso.



El comando para anular la partición de un disco solo está disponible a nivel de diagnóstico y solo se debe realizar bajo la supervisión del soporte de NetApp. **Es muy recomendable que se ponga en contacto con el servicio de asistencia de NetApp antes de continuar.** También puede consultar el artículo de la base de conocimientos ["Cómo desparticionar una unidad de reserva en ONTAP"](#).

**Pasos**

- 1. Devolver una unidad FIPS o SED a servicio:

|                  |                        |
|------------------|------------------------|
| Si el SEDS es... | Utilice estos pasos... |
|------------------|------------------------|

|                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>No en el modo de cumplimiento de FIPS ni en el modo de cumplimiento de FIPS y la clave FIPS está disponible</p> | <ol style="list-style-type: none"> <li>a. Configure el nivel de privilegio en Advanced:<br/> <code>set -privilege advanced</code></li> <li>b. Restablezca la clave FIPS al ID seguro de fabricación predeterminado 0x0:<br/> <code>storage encryption disk modify -fips-key-id 0x0 -disk <i>disk_id</i></code></li> <li>c. Compruebe que la operación se ha realizado correctamente:<br/> <code>storage encryption disk show-status</code><br/> Si la operación falló, use el proceso de PSID en este tema.</li> <li>d. Desinfecte el disco roto:<br/> <code>storage encryption disk sanitize -disk <i>disk_id</i></code><br/> Compruebe que la operación se ha realizado correctamente con el comando <code>storage encryption disk show-status</code> antes de continuar con el siguiente paso.</li> <li>e. Elimine el error del disco sanitizado:<br/> <code>storage disk unfail -spare true -disk <i>disk_id</i></code></li> <li>f. Compruebe si el disco tiene un propietario:<br/> <code>storage disk show -disk <i>disk_id</i></code><br/><br/> Si el disco no tiene un propietario, asigne uno.<br/> <code>storage disk assign -owner node -disk <i>disk_id</i></code><br/><br/> <ol style="list-style-type: none"> <li>i. Introduzca el nodo que posee los discos que desea desinfectar:<br/><br/> <code>system node run -node <i>node_name</i></code><br/><br/> Ejecute el <code>disk sanitize release</code> comando.</li> </ol> </li> <li>g. Salga del infierno. Elimine el error del disco de nuevo:<br/> <code>storage disk unfail -spare true -disk <i>disk_id</i></code></li> <li>h. Compruebe que el disco se ha convertido en un repuesto y que está listo para su uso en un agregado:<br/> <code>storage disk show -disk <i>disk_id</i></code></li> </ol> |
|--------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>En el modo de cumplimiento de normativas FIPS, la clave FIPS no está disponible y el SED tiene un PSID impreso en la etiqueta</p> | <ol style="list-style-type: none"> <li>Obtenga el PSID del disco de la etiqueta del disco.</li> <li>Configure el nivel de privilegio en Advanced:<br/> <pre>set -privilege advanced</pre> </li> <li>Restablezca el disco a sus ajustes configurados de fábrica:<br/> <pre>storage encryption disk revert-to-original-state -disk <i>disk_id</i> -psid <i>disk_physical_secure_id</i></pre> Compruebe que la operación se ha realizado correctamente con el comando <code>storage encryption disk show-status</code> antes de continuar con el siguiente paso. </li> <li>Si está ejecutando ONTAP 9.8P5 o anterior, vaya al siguiente paso. Si su sistema ejecuta ONTAP 9.8P6 o una versión posterior, anule el error del disco saneado.<br/> <pre>storage disk unfaill -disk <i>disk_id</i></pre> </li> <li>Compruebe si el disco tiene un propietario:<br/> <pre>storage disk show -disk <i>disk_id</i></pre> <p>Si el disco no tiene un propietario, asigne uno.<br/> <pre>storage disk assign -owner node -disk <i>disk_id</i></pre> </p></li> <li>Introduzca el nodo que posee los discos que desea desinfectar:<br/> <pre>system node run -node <i>node_name</i></pre> <p>Ejecute el <code>disk sanitize release</code> comando.</p> </li> <li>Salir del infierno.. Elimine el error del disco de nuevo:<br/> <pre>storage disk unfaill -spare true -disk <i>disk_id</i></pre> </li> <li>Compruebe que el disco se ha convertido en un repuesto y que está listo para su uso en un agregado:<br/> <pre>storage disk show -disk <i>disk_id</i></pre> </li> </ol> |
|--------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Para obtener una sintaxis completa del comando, consulte ["referencia de comandos"](#).

### Devolver una unidad FIPS o SED al modo sin protección

Una unidad FIPS o SED está protegida del acceso no autorizado solo si el ID de clave de autenticación del nodo está establecido en un valor distinto del predeterminado. Puede devolver una unidad FIPS o SED al modo sin protección mediante el `storage encryption disk modify` Comando para establecer el ID de clave en el valor predeterminado.

Si una pareja de alta disponibilidad utiliza unidades SAS o NVMe cifradas (SED, NSE, FIPS), debe seguir este proceso para todas las unidades de la pareja de alta disponibilidad antes de inicializar el sistema (opciones de arranque 4 o 9). Si las unidades se reasignan, es posible que no se produzcan pérdidas de datos futuras.

### Antes de empezar

Para realizar esta tarea, debe ser un administrador de clústeres.

## Pasos

1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Si una unidad FIPS se ejecuta en el modo de cumplimiento de normativas FIPS, establezca el ID de clave de autenticación FIPS del nodo nuevamente en el ID de MSID 0x0 predeterminado:

```
storage encryption disk modify -disk disk_id -fips-key-id 0x0
```

Puede utilizar el `security key-manager query` Comando para ver los ID clave.

```
cluster1::> storage encryption disk modify -disk 2.10.11 -fips-key-id 0x0
```

```
Info: Starting modify on 14 disks.
View the status of the operation by using the
storage encryption disk show-status command.
```

Confirme que la operación se ha realizado correctamente con el comando:

```
storage encryption disk show-status
```

Repita el comando `show-status` hasta que los números en “Disks comenzada” y “Disks Done” sean los mismos.

```
cluster1:: storage encryption disk show-status
```

|          | FIPS       | Latest  | Start              |       | Execution  | Disks |
|----------|------------|---------|--------------------|-------|------------|-------|
| Disks    | Disks      |         |                    |       |            |       |
| Node     | Support    | Request | Timestamp          |       | Time (sec) | Begun |
| Done     | Successful |         |                    |       |            |       |
| -----    | -----      | -----   | -----              | ----- | -----      | ----- |
| -----    | -----      |         |                    |       |            |       |
| cluster1 | true       | modify  | 1/18/2022 15:29:38 | 3     | 14         | 5     |
| 5        |            |         |                    |       |            |       |

1 entry was displayed.

3. Vuelva a establecer el ID de clave de autenticación de datos del nodo en el MSID 0x0 predeterminado:

```
storage encryption disk modify -disk disk_id -data-key-id 0x0
```

Valor de `-data-key-id` Debe configurarse en 0x0 si devuelve una unidad SAS o NVMe al modo sin protección.

Puede utilizar el `security key-manager query` Comando para ver los ID clave.

```
cluster1::> storage encryption disk modify -disk 2.10.11 -data-key-id 0x0
```

Info: Starting modify on 14 disks.  
View the status of the operation by using the  
storage encryption disk show-status command.

Confirme que la operación se ha realizado correctamente con el comando:

```
storage encryption disk show-status
```

Repita el comando show-status hasta que los números sean iguales. La operación se completa cuando los números de «discos iniciados» y «discos realizados» son los mismos.

### Modo de mantenimiento

A partir de ONTAP 9.7, es posible volver a introducir una unidad FIPS en modo de mantenimiento. Solo debe utilizar el modo de mantenimiento si no puede utilizar las instrucciones de la CLI de ONTAP de la sección anterior.

### Pasos

1. Establezca el ID de clave de autenticación FIPS del nodo de nuevo en el MSID 0x0 predeterminado:

```
disk encrypt rekey_fips 0x0 disklist
```

2. Vuelva a establecer el ID de clave de autenticación de datos del nodo en el MSID 0x0 predeterminado:

```
disk encrypt rekey 0x0 disklist
```

3. Confirme que la clave de autenticación FIPS se ha recodificado correctamente:

```
disk encrypt show_fips
```

4. Confirmar que la clave de autenticación de datos se ha recodificado correctamente con:

```
disk encrypt show
```

Es probable que la salida muestre el ID de clave predeterminado de MSID 0x0 o el valor de 64 caracteres que contiene el servidor de claves. La Locked? el campo hace referencia al bloqueo de datos.

| Disk    | FIPS Key ID | Locked? |
|---------|-------------|---------|
| 0a.01.0 | 0x0         | Yes     |

### Quite una conexión de administrador de claves externo

Es posible desconectar un servidor KMIP de un nodo cuando ya no se necesita el servidor. Por ejemplo, es posible que se desconecte un servidor KMIP cuando se realiza



la transición al cifrado de volúmenes.

**Acerca de esta tarea**

Cuando desconecta un servidor KMIP de un nodo en un par de alta disponibilidad, el sistema desconecta automáticamente el servidor de todos los nodos del clúster.



Si planea continuar utilizando la gestión de claves externas después de desconectar un servidor KMIP, asegúrese de que haya otro servidor KMIP disponible para servir claves de autenticación.

**Antes de empezar**

Debe ser un administrador de clúster o de SVM para ejecutar esta tarea.

**Paso**

- 1. Desconecte un servidor KMIP del nodo actual:

| Para esta versión de ONTAP... | Se usa este comando...                                                                           |
|-------------------------------|--------------------------------------------------------------------------------------------------|
| ONTAP 9.6 y posteriores       | <code>`security key-manager external remove-servers -vserver SVM -key -servers host_name`</code> |
| IP_address:port,...`          | ONTAP 9,5 y anteriores                                                                           |

En un entorno de MetroCluster, debe repetir estos comandos en ambos clústeres para la SVM de administrador.

Para obtener una sintaxis de comando completa, consulte las páginas man.

El siguiente comando ONTAP 9.6 deshabilita las conexiones a dos servidores de gestión de claves externos para `cluster1`, el primero denominado `ks1`, Escuchando en el puerto predeterminado 5696, el segundo con la dirección IP 10.0.0.20, escuchando en el puerto 24482:

```
cluster1::> security key-manager external remove-servers -vserver
cluster-1 -key-servers ks1,10.0.0.20:24482
```

**Modifique las propiedades del servidor de gestión de claves externo**

A partir de ONTAP 9,6, puede utilizar el `security key-manager external modify-server` Comando para cambiar el tiempo de espera de I/O y el nombre de usuario de un servidor de gestión de claves externo.

**Antes de empezar**

- Debe ser un administrador de clúster o de SVM para ejecutar esta tarea.
- Se requieren privilegios avanzados para esta tarea.
- En un entorno de MetroCluster, debe repetir estos pasos en ambos clústeres para la SVM de administrador.

**Pasos**

1. En el sistema de almacenamiento, cambie al nivel de privilegio avanzado:

```
set -privilege advanced
```

2. Modifique las propiedades del servidor de administración de claves externo para el clúster:

```
security key-manager external modify-server -vserver admin_SVM -key-server
host_name|IP_address:port,... -timeout 1...60 -username user_name
```



El valor del tiempo de espera se expresa en segundos. Si modifica el nombre de usuario, se le solicitará que introduzca una nueva contraseña. Si ejecuta el comando en la solicitud de inicio de sesión del clúster, *admin\_SVM* Los valores predeterminados en la SVM de administrador del clúster actual. Debe ser el administrador de clústeres para modificar las propiedades del servidor de administrador de claves externo.

El comando siguiente cambia el valor de tiempo de espera a 45 segundos para el *cluster1* el servidor de gestión de claves externo escucha en el puerto predeterminado 5696:

```
cluster1::> security key-manager external modify-server -vserver
cluster1 -key-server ks1.local -timeout 45
```

3. Modificar las propiedades del servidor de gestor de claves externo para una SVM (solo NVE):

```
security key-manager external modify-server -vserver SVM -key-server
host_name|IP_address:port,... -timeout 1...60 -username user_name
```



El valor del tiempo de espera se expresa en segundos. Si modifica el nombre de usuario, se le solicitará que introduzca una nueva contraseña. Si ejecuta el comando en la solicitud de inicio de sesión de SVM, *SVM* El valor predeterminado es la SVM actual. Debe ser el administrador de clúster o de SVM para modificar las propiedades del servidor de administrador de claves externo.

El siguiente comando cambia el nombre de usuario y la contraseña del *svm1* el servidor de gestión de claves externo escucha en el puerto predeterminado 5696:

```
svm1::> security key-manager external modify-server -vserver svm11 -key
-server ks1.local -username svm1user
Enter the password:
Reenter the password:
```

4. Repita el último paso para todas las SVM adicionales.

### Transición a la gestión de claves externas desde la gestión de claves incorporada

Si desea cambiar a la gestión de claves externas desde la gestión de claves incorporada, debe eliminar la configuración de gestión de claves incorporada para poder habilitar la gestión de claves externas.

### Antes de empezar

- Para el cifrado basado en hardware, debe restablecer las claves de datos de todas las unidades FIPS o SED a su valor predeterminado.

["Devolver una unidad FIPS o SED al modo sin protección"](#)

- Para el cifrado basado en software, debe descifrar todos los volúmenes.

["Descifrar los datos de volúmenes"](#)

- Para realizar esta tarea, debe ser un administrador de clústeres.

### Paso

1. Elimine la configuración integrada de gestión de claves para un clúster:

| Para esta versión de ONTAP... | Se usa este comando...                                         |
|-------------------------------|----------------------------------------------------------------|
| ONTAP 9.6 y posteriores       | <code>security key-manager onboard disable -vserver SVM</code> |
| ONTAP 9,5 y anteriores        | <code>security key-manager delete-key-database</code>          |

Para obtener una sintaxis completa del comando, consulte ["Páginas de manual de ONTAP"](#).

### Transición a la gestión de claves incorporada desde la gestión de claves externas

Si desea cambiar a la gestión de claves incorporada desde la gestión de claves externas, debe eliminar la configuración de gestión de claves externa para poder habilitar la gestión de claves incorporada.

### Antes de empezar

- Para el cifrado basado en hardware, debe restablecer las claves de datos de todas las unidades FIPS o SED a su valor predeterminado.

["Devolver una unidad FIPS o SED al modo sin protección"](#)

- Eliminó todas las conexiones del administrador de claves externo.

["Eliminación de una conexión de administrador de claves externo"](#)

- Para realizar esta tarea, debe ser un administrador de clústeres.

### Procedimiento

Los pasos para realizar la transición de la gestión de claves dependen de la versión de ONTAP que esté utilizando.

### ONTAP 9.6 y posteriores

1. Cambie al nivel de privilegio avanzado:

```
set -privilege advanced
```

2. Utilizar el comando:

```
security key-manager external disable -vserver admin_SVM
```



En un entorno de MetroCluster, debe repetir el comando en ambos clústeres para la SVM de administrador.

### ONTAP 9,5 y anteriores

Utilizar el comando:

```
security key-manager delete-kmip-config
```

## Qué sucede cuando no se puede acceder a los servidores de gestión de claves durante el proceso de arranque

ONTAP toma ciertas precauciones para evitar un comportamiento no deseado en el caso de que un sistema de almacenamiento configurado para NSE no pueda alcanzar ninguno de los servidores de gestión de claves especificados durante el proceso de arranque.

Si el sistema de almacenamiento está configurado para NSE, el SED está recodificado y bloqueado y el SED está encendido, el sistema de almacenamiento debe recuperar las claves de autenticación necesarias de los servidores de gestión de claves para autenticarse en el SED antes de poder acceder a los datos.

El sistema de almacenamiento intenta contactar con los servidores de gestión de claves especificados durante tres horas. Si el sistema de almacenamiento no puede alcanzar ninguna de ellas después de esa hora, el proceso de arranque se detiene y el sistema de almacenamiento se detiene.

Si el sistema de almacenamiento se contacta correctamente con el servidor de gestión de claves especificado, se intenta establecer una conexión SSL hasta 15 minutos. Si el sistema de almacenamiento no puede establecer una conexión SSL con cualquier servidor de gestión de claves especificado, el proceso de arranque se detiene y el sistema de almacenamiento se detiene.

Mientras el sistema de almacenamiento intenta comunicarse y conectarse a servidores de gestión de claves, muestra información detallada sobre los intentos fallidos en la CLI. Puede interrumpir los intentos de contacto en cualquier momento con Ctrl-C.

Como medida de seguridad, el cifrado de disco automático permite únicamente un número limitado de intentos de acceso no autorizados, tras los cuales se deshabilita el acceso a los datos existentes. Si el sistema de almacenamiento no puede ponerse en contacto con ningún servidor de gestión de claves especificado para obtener las claves de autenticación adecuadas, solo puede intentar autenticarse con la clave predeterminada, lo que provoca un intento fallido y una alarma. Si el sistema de almacenamiento está configurado para reiniciarse automáticamente en caso de producirse una alarma, entra en un bucle de arranque, lo que da como resultado intentos de autenticación con errores constantes en el SED.

Detener el sistema de almacenamiento en estas situaciones es mediante un diseño para evitar que el sistema de almacenamiento entre en un bucle de arranque y posible pérdida de datos involuntaria como resultado del cifrado de disco de forma permanente debido a que se supera el límite de seguridad de un cierto número de

intentos de autenticación fallidos consecutivos. El límite y el tipo de protección de bloqueo dependen de las especificaciones de fabricación y del tipo de SED:

| Tipo SED                                                                  | Número de intentos fallidos consecutivos de autenticación que provocan el bloqueo | Tipo de protección de bloqueo cuando se alcanza el límite de seguridad                                                     |
|---------------------------------------------------------------------------|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| HDD                                                                       | 1024                                                                              | Permanente. No se pueden recuperar los datos, incluso cuando la clave de autenticación correcta vuelva a estar disponible. |
| X440_PHM2800MCTO SSD NSE de 800 GB con revisiones de firmware NA00 o NA01 | 5                                                                                 | Temporal. El bloqueo solo está activo hasta que se somete al disco a un ciclo de encendido y apagado.                      |
| SSD X577_PHM2800MCTO 800GB NSE con revisiones de firmware NA00 o NA01     | 5                                                                                 | Temporal. El bloqueo solo está activo hasta que se somete al disco a un ciclo de encendido y apagado.                      |
| X440_PHM2800MCTO SSD NSE de 800 GB con revisiones de firmware superiores  | 1024                                                                              | Permanente. No se pueden recuperar los datos, incluso cuando la clave de autenticación correcta vuelva a estar disponible. |
| SSD X577_PHM2800MCTO 800GB NSE con revisiones de firmware superiores      | 1024                                                                              | Permanente. No se pueden recuperar los datos, incluso cuando la clave de autenticación correcta vuelva a estar disponible. |
| El resto de modelos de SSD                                                | 1024                                                                              | Permanente. No se pueden recuperar los datos, incluso cuando la clave de autenticación correcta vuelva a estar disponible. |

Para todos los tipos de SED, una autenticación correcta restablece el recuento de prueba a cero.

Si encuentra esta situación en la que se detiene el sistema de almacenamiento debido a un error en el cual se llega a los servidores de gestión de claves especificados, primero debe identificar y corregir la causa del error de comunicación antes de intentar seguir arrancando el sistema de almacenamiento.

### **Desactive el cifrado de forma predeterminada**

A partir de ONTAP 9.7, el cifrado de volúmenes y agregados se habilita de forma predeterminada si se dispone de una licencia de cifrado de volúmenes (ve) y se usa un gestor de claves incorporado o externo. Si es necesario, puede deshabilitar el cifrado de forma predeterminada en todo el clúster.

### **Antes de empezar**

Debe ser un administrador de clústeres para realizar esta tarea o un administrador de SVM a quien el administrador de clúster haya delegado esta autoridad.

## Paso

1. Para deshabilitar el cifrado de forma predeterminada para todo el clúster en ONTAP 9.7 o posterior, ejecute el siguiente comando:

```
options -option-name encryption.data_at_rest_encryption.disable_by_default
-option-value on
```

# Protección de datos y recuperación ante desastres

## Protección de datos con System Manager

### Información general sobre la protección de datos con System Manager

Los temas de esta sección muestran cómo configurar y gestionar la protección de datos con System Manager en ONTAP 9.7 y versiones posteriores.

Si utiliza System Manager en ONTAP 9.7 o una versión anterior, consulte ["Documentación clásica de System Manager de ONTAP"](#)

Proteja sus datos mediante la creación y la gestión de copias Snapshot, reflejos, almacenes y relaciones de mirroring y almacén.

*SnapMirror* es la tecnología de recuperación ante desastres diseñada para la conmutación al nodo de respaldo del almacenamiento principal al secundario en un sitio geográficamente remoto. Como su nombre indica, SnapMirror crea una réplica, o réplica, de sus datos de trabajo en almacenamiento secundario desde la cual puede seguir proporcionando datos en caso de catástrofe en el centro principal.

Un *vault* está diseñado para la replicación de copias snapshot disco a disco con el fin de cumplir con los estándares y otros fines relacionados con la gobernanza. A diferencia de la relación de SnapMirror, en la que el destino normalmente solo contiene las copias Snapshot que actualmente se encuentran en el volumen de origen, un destino de almacén normalmente conserva las copias Snapshot puntuales creadas durante un período mucho más largo.



A partir de ONTAP 9.10.1, se pueden crear relaciones de protección de datos entre bloques de S3 mediante SnapMirror S3. Los bloques de destino pueden estar en sistemas ONTAP locales o remotos, o en sistemas que no sean ONTAP, como StorageGRID y AWS. Para obtener más información, consulte ["Información general de SnapMirror de S3"](#).

### Cree políticas de protección de datos personalizadas

Puede crear políticas de protección de datos personalizadas con System Manager cuando las políticas de protección existentes no son apropiadas para sus necesidades. A partir de ONTAP 9.11.1, puede usar System Manager para crear políticas de mirroring y almacén personalizadas para mostrar y seleccionar políticas heredadas. Esta función también está disponible en ONTAP 9.8P12 y en parches posteriores de ONTAP 9.8.

Cree políticas de protección personalizadas en los clústeres de origen y destino.

#### Pasos

1. Haga clic en **Protección > Configuración de directiva local**.
2. En **Directivas de protección**, haga clic en .
3. En el panel **Directivas de protección**, haga clic en .
4. Escriba el nombre de la nueva política y seleccione el alcance de la misma.
5. Elija un tipo de política. Para agregar una directiva sólo de almacén o sólo de duplicación, seleccione

**asíncrona** y haga clic en **utilizar un tipo de directiva heredada**.




6. Complete los campos obligatorios.
7. Haga clic en **Guardar**.
8. Repita estos pasos en el otro clúster.

## Configure las copias Snapshot

Puede crear políticas de copia de Snapshot para especificar el número máximo de copias de Snapshot que se crean automáticamente y la frecuencia con la que se crean. La política especifica cuándo crear copias Snapshot, cuántas copias se retendrán y cómo nombrarlas.

Este procedimiento crea una política de copias de Snapshot únicamente en el clúster local.

### Pasos

1. Haga clic en **Protección > Descripción general > Configuración de directivas locales**.
2. En **Directivas de instantánea**, haga clic en , a continuación, haga clic en .
3. Escriba el nombre de la directiva, seleccione el ámbito de la directiva y, en **programaciones**, haga clic en  para introducir los detalles de la programación.

## Calcule el espacio que se puede reclamar antes de eliminar las copias snapshot

A partir de ONTAP 9.10.1, puede usar System Manager para seleccionar las copias de Snapshot que desea eliminar y calcular el espacio que puede reclamarse antes de eliminarlas.

### Pasos

1. Haga clic en **almacenamiento > volúmenes**.
2. Seleccione el volumen desde el que desea eliminar copias de Snapshot.
3. Haga clic en **copias Snapshot**.
4. Seleccione una o más copias de Snapshot.
5. Haga clic en **calcular espacio recuperable**.

## Habilitar o deshabilitar el acceso de los clientes al directorio de copia Snapshot

A partir de ONTAP 9.10.1, se puede usar System Manager para habilitar o deshabilitar los sistemas cliente para acceder a un directorio de copia de Snapshot en un volumen. Al habilitar el acceso, el directorio de copia Snapshot resulta visible para los clientes y permite que los clientes de Windows asignen una unidad al directorio de copias Snapshot para ver y acceder a su contenido.

Puede habilitar o deshabilitar el acceso al directorio de copias Snapshot de un volumen mediante la edición de la configuración del volumen o la edición de la configuración de recursos compartidos del volumen.



## Habilitar o deshabilitar el acceso de los clientes al directorio de copia de Snapshot mediante la edición de un volumen

De forma predeterminada, los clientes pueden acceder al directorio de copia Snapshot de un volumen.

### Pasos

1. Haga clic en **almacenamiento > volúmenes**.
2. Seleccione el volumen que contiene el directorio copias de Snapshot que desea mostrar u ocultar.
3. Haga clic en **:** Y seleccione **Editar**.
4. En la sección **Configuración de copias Snapshot (local)**, seleccione o anule la selección de **Mostrar el directorio de copias Snapshot a clientes**.
5. Haga clic en **Guardar**.

## Habilitar o deshabilitar el acceso de los clientes al directorio de copia de Snapshot mediante la edición de un recurso compartido

De forma predeterminada, los clientes pueden acceder al directorio de copia Snapshot de un volumen.

### Pasos

1. Haga clic en **almacenamiento > Recursos compartidos**.
2. Seleccione el volumen que contiene el directorio copias de Snapshot que desea mostrar u ocultar.
3. Haga clic en **:** Y seleccione **Editar**.
4. En la sección **Propiedades de recurso compartido**, seleccione o anule la selección de **permitir a los clientes acceder al directorio copias Snapshot**.
5. Haga clic en **Guardar**.

## Prepare el mirroring y el almacenamiento

Puede proteger los datos replicando en un clúster remoto con fines de recuperación ante desastres y backup de datos.




Existen varias políticas de protección predeterminadas disponibles. Debe haber creado las políticas de protección si desea usar políticas personalizadas.



### Pasos

1. En el clúster local, haga clic en **Protección > Descripción general**.
2. Expanda **Configuración de interconexión de clústeres**. Haga clic en **Add Network interfaces** y añada interfaces de red de interconexión de clústeres para el clúster.

Repita este paso en el clúster remoto.

3. En el clúster remoto, haga clic en **Protección > Descripción general**. Haga clic en  En la sección Cluster peers y haga clic en **Generate Passphrase**.
  4. Copie la clave de acceso generada y péguela en el clúster local.
  5. En el clúster local, en Cluster peers, haga clic en **Peer Clusters** y pare los clústeres locales y remotos.
  6. De manera opcional, en Storage VM peers, haga clic en  Posteriormente **Peer Storage VMs** para poner en la misma conexión los equipos virtuales de almacenamiento.
  7. Haga clic en **proteger volúmenes** para proteger sus volúmenes. Para proteger sus LUN, haga clic en **almacenamiento > LUN**, seleccione una LUN que proteger y, a continuación, haga clic en  **Protect**.
- Seleccione la política de protección según el tipo de protección de datos que necesite.
8. Para comprobar que los volúmenes y LUN están protegidos correctamente desde el clúster local, haga clic en **almacenamiento > volúmenes** o **almacenamiento > LUN** y expanda la vista volumen/LUN.

## Otras maneras de hacerlo en ONTAP

| Para ejecutar estas tareas con...                                        | Ver este contenido...                                                                                 |
|--------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| System Manager Classic (disponible con ONTAP 9.7 y versiones anteriores) | <a href="#">"Información general de preparación para la recuperación ante desastres de volúmenes"</a> |
| La interfaz de línea de comandos de ONTAP                                | <a href="#">"Cree una relación de paridad entre clústeres"</a>                                        |

## Configure los reflejos y almacenes

Cree un mirror y almacén de un volumen para proteger los datos en caso de desastre y disponer de varias versiones archivadas de los datos a las que se puede revertir. A partir de ONTAP 9.11.1, se puede usar System Manager para seleccionar políticas de mirroring y almacén predefinidas y personalizadas, para mostrar y seleccionar políticas heredadas, y para anular las programaciones de transferencia definidas en una política de protección al proteger volúmenes y máquinas virtuales de almacenamiento. Esta función también está disponible en ONTAP 9.8P12 y en parches posteriores de ONTAP 9.8.




Si utiliza la versión de revisión de ONTAP 9.8P12 o posterior de ONTAP 9.8 y configuró SnapMirror con System Manager, debe utilizar ONTAP 9.9.1P13 o posterior y ONTAP 9.10.1P10 o versiones de revisión posteriores si tiene pensado actualizar a las versiones de ONTAP 9.9.1 o ONTAP 9.10.1.

Este procedimiento crea una política de protección de datos en un clúster remoto. Los clústeres de origen y destino utilizan interfaces de red de interconexión de clústeres para intercambiar datos. En el procedimiento se asume el ["se crean interfaces de red de interconexión de clústeres y los clústeres que contienen los volúmenes tienen una relación entre iguales"](#) (emparejado). También es posible establecer una relación entre iguales de máquinas virtuales de almacenamiento para la protección de datos; sin embargo, si las máquinas virtuales de almacenamiento no tienen una relación entre iguales, pero los permisos están habilitados, las máquinas virtuales de almacenamiento se establecen una relación entre iguales automáticamente cuando se crea la relación de protección.



## Pasos

1. Seleccione el volumen o LUN que desea proteger: Haga clic en **almacenamiento > volúmenes** o **almacenamiento > LUN** y, a continuación, haga clic en el volumen o nombre de LUN que desee.
2. Haga clic en  **Protect**.
3. Seleccione el clúster de destino y la máquina virtual de almacenamiento.
4. De forma predeterminada, la política asíncrona está seleccionada. Para seleccionar una directiva síncrona, haga clic en **más opciones**.
5. Haga clic en **proteger**.
6. Haga clic en la ficha **SnapMirror (local o remoto)** del volumen o LUN seleccionados para verificar que la protección está configurada correctamente.

## Información relacionada

- ["Crear y eliminar volúmenes de prueba de conmutación al nodo de respaldo de SnapMirror"](#).

## Otras maneras de hacerlo en ONTAP


| Para ejecutar estas tareas con...                                        | Ver este contenido...                                                              |
|--------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| System Manager Classic (disponible con ONTAP 9.7 y versiones anteriores) | <a href="#">"Información general sobre backup de volúmenes mediante SnapVault"</a> |
| La interfaz de línea de comandos de ONTAP                                | <a href="#">"Cree una relación de replicación"</a>                                 |

## Resincronice una relación de protección

Cuando el volumen de origen original vuelva a estar disponible después de un desastre, puede volver a sincronizar los datos del volumen de destino y restablecer la relación de protección.

Este procedimiento reemplaza los datos del volumen de origen original en una relación asíncrona para poder empezar a proporcionar datos del volumen de origen original de nuevo y reanudar la relación de protección original.

## Pasos


1. Haga clic en **Protección > Relaciones** y, a continuación, haga clic en la relación de desconexión que desea volver a sincronizar.
2. Haga clic en  Y, a continuación, seleccione **Resync**.
3. En **Relaciones**, supervise el progreso de la resincronización comprobando el estado de la relación. El estado cambia a "reflejado" cuando se completa la resincronización.

## Restaurar un volumen de una copia de Snapshot anterior

Si se pierden o se dañan datos de un volumen, es posible revertir los datos mediante la restauración a partir de una copia de Snapshot anterior.

Este procedimiento reemplaza los datos actuales del volumen de origen con datos de una versión de copia Snapshot anterior. Debe realizar esta tarea en el clúster de destino.

**Pasos**

1. Haga clic en **Protección > Relaciones** y, a continuación, haga clic en el nombre del volumen de origen.
2. Haga clic en  Y, a continuación, seleccione **Restaurar**.
3. En **Fuente**, el volumen de origen está seleccionado de forma predeterminada. Haga clic en **otro volumen** si desea elegir un volumen distinto al de origen.
4. En **destino**, elija la copia Snapshot que desea restaurar.
5. Si su origen y destino se encuentran en diferentes clústeres, en el clúster remoto, haga clic en **Protección > Relaciones** para supervisar el progreso de la restauración.

**Otras maneras de hacerlo en ONTAP**


| Para ejecutar estas tareas con...                                        | Ver este contenido...                                                                       |
|--------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| System Manager Classic (disponible con ONTAP 9.7 y versiones anteriores) | <a href="#">"Información general sobre la restauración de volúmenes mediante SnapVault"</a> |
| La interfaz de línea de comandos de ONTAP                                | <a href="#">"Restaure el contenido de un volumen a partir de un destino de SnapMirror"</a>  |

**Recuperar desde copias Snapshot**

Es posible recuperar un volumen a un momento específico anterior mediante la restauración desde una copia Snapshot.

Este procedimiento restaura un volumen a partir de una copia Snapshot.

**Pasos**


1. Haga clic en **almacenamiento** y seleccione un volumen.
2. En **copias Snapshot**, haga clic en  Junto a la copia Snapshot que desea restaurar y seleccione **Restaurar**.

**Restaurar en un nuevo volumen**

A partir de ONTAP 9.8, se puede usar System Manager para restaurar los datos de los que se ha realizado un backup en el volumen de destino a un volumen distinto al de origen.

Cuando se restaura a otro volumen, es posible seleccionar un volumen existente o crear un volumen nuevo.

**Pasos**

1. Seleccione la relación de protección deseada: Haga clic en **Protección > Relaciones**.
2. Haga clic en  Y haga clic en **Restaurar**.
3. En la sección **Fuente**, seleccione **otro volumen** y seleccione el clúster y Storage VM.
4. Seleccione **volumen existente** o **Crear un nuevo volumen**.
5. Si va a crear un volumen nuevo, introduzca el nombre del volumen.

6. En la sección **destino**, seleccione la copia Snapshot que desea restaurar.
7. Haga clic en **Guardar**.
8. En **Relaciones**, supervise el progreso de la restauración visualizando **Estado de transferencia** para la relación.

## Resincronización inversa de una relación de protección

A partir de ONTAP 9.8, es posible usar System Manager para realizar una operación de resincronización inversa a fin de eliminar una relación de protección existente y revertir las funciones de los volúmenes de origen y de destino. A continuación, se utilizará el volumen de destino para suministrar datos mientras se repara o se sustituye el origen, se actualiza el origen y se establece la configuración original de los sistemas.



System Manager no admite la resincronización inversa con relaciones dentro del clúster. Puede usar la CLI de ONTAP para realizar operaciones de resincronización inversa con relaciones entre clústeres.

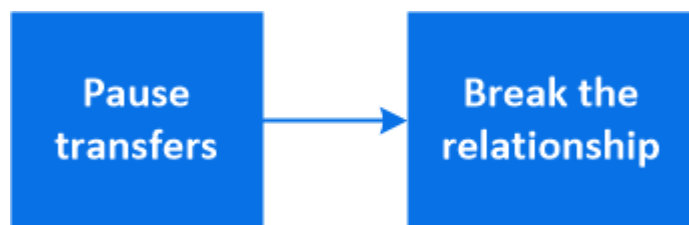
Cuando se realiza una operación de resynch inversa, se eliminan todos los datos del volumen de origen más recientes que los datos de la copia Snapshot común.

### Pasos

1. Seleccione la relación de protección deseada: Haga clic en **Protección > Relaciones**.
2. Haga clic en **:** Y haga clic en **Reverse Resync**.
3. En **Relaciones**, supervise el progreso de la resincronización inversa visualizando **Estado de transferencia** para la relación.

## Sirva datos desde un destino de SnapMirror

Para servir datos desde un destino de mirroring cuando un origen deja de estar disponible, detenga las transferencias programadas hacia el destino y, a continuación, rompa la relación de SnapMirror para hacer que el destino sea editable.



### Pasos

1. Seleccione la relación de protección deseada: Haga clic en **Protección > Relaciones** y, a continuación, haga clic en el nombre de volumen deseado.
2. Haga clic en **:**.
3. Detener transferencias programadas : haga clic en **Pausa**.
4. Haga que el destino sea editable: Haga clic en **romper**.
5. Vaya a la página principal **Relaciones** para verificar que el estado de la relación se muestra como "roto".

### Siguientes pasos:

Cuando el volumen de origen deshabilitado se vuelve a disponibilidad, debe volver a sincronizar la relación para copiar los datos actuales en el volumen de origen original. Este proceso sustituye los datos del volumen de origen original.

### Otras maneras de hacerlo en ONTAP

| Para ejecutar estas tareas con...                                        | Ver este contenido...                                                                   |
|--------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| System Manager Classic (disponible con ONTAP 9.7 y versiones anteriores) | <a href="#">"Información general sobre la recuperación ante desastres de volúmenes"</a> |
| La interfaz de línea de comandos de ONTAP                                | <a href="#">"Activar el volumen de destino"</a>                                         |

## Configurar la recuperación ante desastres de los equipos virtuales de almacenamiento

Mediante System Manager, es posible crear una relación de recuperación ante desastres (DR de VM de almacenamiento) para replicar una configuración de VM de almacenamiento a otra. En caso de desastre en el sitio principal, puede activar rápidamente la máquina virtual de almacenamiento de destino.

Complete este procedimiento desde el destino. Si necesita crear una nueva política de protección, por ejemplo, cuando su máquina virtual de almacenamiento de origen tiene SMB configurado, debe usar System Manager para crear la política y seleccionar la opción **Identity preserve** en la ventana **Add Protection Policy**.

Para obtener más información, consulte ["Cree políticas de protección de datos personalizadas"](#).


### Pasos

1. En el clúster de destino, haga clic en **Protección > Relaciones**.
2. En **Relaciones**, haga clic en proteger y elija **Storage VMs (DR)**.
3. Seleccione una política de protección. Si creó una política de protección personalizada, selecciónela, elija el clúster de origen y la máquina virtual de almacenamiento que desea replicar. También puede crear una máquina virtual de almacenamiento de destino introduciendo un nuevo nombre de máquina virtual de almacenamiento.
4. Haga clic en **Guardar**.

## Proporcione datos desde un destino de recuperación ante desastres de SVM

A partir de ONTAP 9.8, es posible utilizar System Manager para activar una máquina virtual de almacenamiento de destino después de un desastre. Si activa la máquina virtual de almacenamiento de destino, es posible escribir en los volúmenes de destino de SVM y proporcionar datos a los clientes.

### Pasos

1. Si se puede acceder al clúster de origen, compruebe que la SVM está detenida: Vaya a **almacenamiento > Storage VMs** y compruebe la columna **Estado** de la SVM.
2. Si el estado de la SVM de origen es "en ejecución", deténgase: Seleccione  Y seleccione **Detener**.
3. En el clúster de destino, localice la relación de protección deseada: Vaya a **Protección > Relaciones**.

4. Haga clic en  Y seleccione **Activar destino almacenamiento VM**.

## Reactivar una máquina virtual de almacenamiento de origen


A partir de ONTAP 9.8, podrá utilizar System Manager para reactivar un equipo virtual de almacenamiento de origen después de un desastre. Volver a activar la máquina virtual de almacenamiento de origen detiene la máquina virtual de almacenamiento de destino y vuelve a habilitar la replicación desde el origen al destino.

### Acerca de esta tarea

Cuando se reactiva la máquina virtual de almacenamiento de origen, System Manager realiza las siguientes operaciones en segundo plano:

- Crea una relación de recuperación ante desastres de SVM inversa del destino original al origen con una resincronización de SnapMirror
- Detiene la SVM de destino
- Actualiza la relación de SnapMirror
- Rompe la relación de SnapMirror
- Reinicia la SVM original
- El problema realiza una resincronización de SnapMirror del origen original del destino original
- Borra las relaciones de SnapMirror

### Pasos

1. Seleccione la relación de protección deseada: Haga clic en **Protección > Relaciones**.
2. Haga clic en  Y haga clic en **reactivar almacenamiento de origen VM**.
3. En **Relaciones**, supervise el progreso de reactivación de la fuente visualizando **Estado de transferencia** para obtener información sobre la relación de protección.


## Resincronizar una máquina virtual de almacenamiento de destino

A partir de ONTAP 9.8, es posible usar System Manager para volver a sincronizar los datos y los detalles de configuración de la máquina virtual de almacenamiento de origen con la máquina virtual de almacenamiento de destino en una relación de protección romada y restablecer la relación.

ONTAP 9.11.1 introduce una opción para omitir una reconstrucción completa del almacén de datos al realizar un ensayo de recuperación ante desastres, lo que permite volver a la producción más rápido.

La operación de resincronización solo se realiza desde el destino de la relación original. La resincronización elimina los datos del equipo virtual de almacenamiento de destino que son más nuevos que los de la máquina virtual de almacenamiento de origen.

### Pasos

1. Seleccione la relación de protección deseada: Haga clic en **Protección > Relaciones**.
2. Opcionalmente, seleccione **realizar una resincronización rápida** para omitir una reconstrucción completa del almacén de datos durante un ensayo de recuperación ante desastres.
3. Haga clic en  Y haga clic en **Resync**.

4. En **Relaciones**, supervise el progreso de la resincronización visualizando **Estado de transferencia** para la relación.

## Realice backups de datos en el cloud con SnapMirror

A partir de ONTAP 9.9.1, puede realizar backups de sus datos en el cloud y restaurar sus datos desde el almacenamiento en cloud a un volumen diferente mediante System Manager. Es posible usar StorageGRID o ONTAP S3 como almacén de objetos en el cloud.

Antes de usar la función SnapMirror Cloud, debe solicitar una clave de licencia de API de SnapMirror Cloud al sitio de soporte de NetApp: "[Solicite la clave de licencia de SnapMirror Cloud API](#)".

Siguiendo las instrucciones, debe proporcionar una descripción simple de su oportunidad de negocio y solicitar la clave API mediante el envío de un correo electrónico a la dirección de correo electrónico proporcionada. Debe recibir una respuesta por correo electrónico en un plazo de 24 horas con instrucciones adicionales sobre cómo adquirir la clave API.

### Añadir un almacén de objetos en la nube

Antes de configurar backups en el cloud de SnapMirror, tiene que añadir un almacén de objetos en el cloud StorageGRID o ONTAP S3.

#### Pasos

1. Haga clic en **Protección > Descripción general > Tiendas de objetos en la nube**.
2. Haga clic en **+ Add**.

### Realice un backup con la política predeterminada

Puede configurar rápidamente un backup de SnapMirror Cloud para un volumen existente usando la política de protección de cloud predeterminada, DailyBackup.

#### Pasos

1. Haga clic en **Protección > Descripción general** y seleccione **copia de seguridad de volúmenes en la nube**.
2. Si es la primera vez que realiza un backup en el cloud, introduzca su clave de licencia de API de SnapMirror Cloud en el campo de licencia, como se indica.
3. Haga clic en **autenticar y continuar**.
4. Seleccione un volumen de origen.
5. Seleccione un almacén de objetos en la nube.
6. Haga clic en **Guardar**.

### Cree una política de backup en el cloud personalizada

Si no quiere usar la política de cloud DailyBackup predeterminada para sus backups de SnapMirror Cloud, puede crear su propia política.

#### Pasos

1. Haga clic en **Protección > Descripción general > Configuración de directivas locales** y seleccione **Directivas de protección**.



2. Haga clic en **Agregar** e introduzca los nuevos detalles de la directiva.
3. En la sección **Tipo de directiva**, seleccione **copia de seguridad en la nube** para indicar que está creando una política de nube.
4. Haga clic en **Guardar**.

### Cree una copia de seguridad desde la página Volumes

Puede usar la página System Manager **Volumes** a cuando desea seleccionar y crear backups en la nube para varios volúmenes a la vez, o bien cuando desea usar una política de protección personalizada.

#### Pasos

1. Haga clic en **almacenamiento > volúmenes**.
2. Seleccione los volúmenes de los que desea realizar una copia de seguridad en la nube y haga clic en **proteger**.
3. En la ventana **proteger volumen**, haga clic en **más opciones**.
4. Seleccione una política.


Puede seleccionar la política predeterminada, DailyBackup o una política de cloud personalizada que haya creado.

5. Seleccione un almacén de objetos en la nube.
6. Haga clic en **Guardar**.

### Restaure desde el cloud

Puede usar System Manager para restaurar datos con backups del almacenamiento de cloud a otro volumen en el clúster de origen.


#### Pasos

1. Haga clic en **almacenamiento > volúmenes**.
2. Seleccione la ficha **copia de seguridad en la nube**.
3. Haga clic en  Junto al volumen de origen que desea restaurar y seleccione **Restaurar**.
4. En **Source**, seleccione una VM de almacenamiento y, a continuación, escriba el nombre del volumen en el que desea restaurar los datos.
5. En **destino**, seleccione la copia Snapshot que desea restaurar.
6. Haga clic en **Guardar**.

### Eliminar una relación de SnapMirror Cloud

Puede usar System Manager para eliminar una relación de cloud.


#### Pasos

1. Haga clic en **almacenamiento > volúmenes** y seleccione el volumen que desea eliminar.
2. Haga clic en  Junto al volumen de origen y seleccione **Eliminar**.
3. Seleccione **Eliminar el extremo del almacén de objetos en la nube (opcional)** si desea eliminar el extremo del almacén de objetos en la nube.
4. Haga clic en **Eliminar**.

## Quitar un almacén de objetos en la nube

Puede usar System Manager para quitar un almacén de objetos en cloud si no forma parte de una relación de backup en el cloud. Cuando un almacén de objetos en cloud forma parte de una relación de backup en el cloud, no se puede eliminar.

### Pasos

1. Haga clic en **Protección > Descripción general > Tiendas de objetos en la nube**.
2. Seleccione el almacén de objetos que desea eliminar; haga clic en  Y seleccione **Eliminar**.

## Realice backups de datos con Cloud Backup

A partir de ONTAP 9.9.1, se puede usar System Manager para realizar backups de datos en el cloud con Cloud Backup.



Cloud Backup admite volúmenes de lectura y escritura de FlexVol y volúmenes de protección de datos (DP). No se admiten los volúmenes de FlexGroup y SnapLock.

### Antes de empezar

Debe realizar los siguientes procedimientos para establecer una cuenta en BlueXP. Para la cuenta de servicio, debe crear la función como "Administrador de cuentas". (Otros roles de cuenta de servicio no tienen los privilegios necesarios para establecer una conexión desde System Manager).

1. ["Cree una cuenta en BlueXP"](#).
2. ["Cree un conector en BlueXP"](#) con uno de los siguientes proveedores de cloud:
  - Microsoft Azure
  - Amazon Web Services (AWS)
  - Google Cloud Platform (GCP)
  - StorageGRID (ONTAP 9.10.1)



A partir de ONTAP 9.10.1, puede seleccionar StorageGRID como proveedor de backup en cloud, pero solo si BlueXP está implementado en las instalaciones. El conector BlueXP debe instalarse en las instalaciones y estar disponible a través de la aplicación de software como servicio (SaaS) BlueXP.

3. ["Suscríbase a Cloud Backup Service en BlueXP"](#) (requiere la licencia adecuada).
4. ["Genere una clave de acceso y una clave secreta con BlueXP"](#).

## Registre el clúster con BlueXP

Puede registrar el clúster en BlueXP usando BlueXP o System Manager.

### Pasos

1. En System Manager, vaya a **Descripción general de la protección**.
2. En **Cloud Backup Service**, proporcione los siguientes detalles:
  - ID del cliente
  - Clave secreta de cliente

3. Seleccione **Registrar y continuar**.

## Habilite Cloud Backup

Después de registrar el clúster en BlueXP, necesitará habilitar Cloud Backup e iniciar el primer backup en el cloud.

### Pasos

1. En el Administrador del sistema, haga clic en **Protección > Descripción general** y, a continuación, desplácese a la sección **Cloud Backup Service**.
2. Introduzca **ID de cliente** y **Secreto de cliente**.



A partir de ONTAP 9.10.1, puede obtener más información sobre el coste de utilizar la nube haciendo clic en **más información sobre el costo de usar la nube**.

3. Haga clic en **conectar y activar Cloud Backup Service**.
4. En la página **Activar Cloud Backup Service**, proporcione los siguientes detalles, en función del proveedor que haya seleccionado.

| Para este proveedor de cloud...                                                                           | Introduzca los siguientes datos...                                                                                                                                                      |
|-----------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Azure                                                                                                     | <ul style="list-style-type: none"><li>• ID de suscripción de Azure</li><li>• Región</li><li>• Nombre del grupo de recursos (existente o nuevo)</li></ul>                                |
| AWS                                                                                                       | <ul style="list-style-type: none"><li>• ID de cuenta de AWS</li><li>• Clave de acceso</li><li>• Clave secreta</li><li>• Región</li></ul>                                                |
| Google Cloud Project (GCP)                                                                                | <ul style="list-style-type: none"><li>• Nombre del proyecto de Google Cloud</li><li>• Clave de acceso a Google Cloud</li><li>• Clave secreta de Google Cloud</li><li>• Región</li></ul> |
| StorageGRID<br>(ONTAP 9.10.1 y versiones posteriores y solo para la implementación on-premises de BlueXP) | <ul style="list-style-type: none"><li>• Servidor</li><li>• Clave de acceso de SG</li><li>• Clave secreta de SG</li></ul>                                                                |

5. Seleccione una **Política de protección**:
  - **Política existente**: Elija una política existente.
  - **Nueva directiva**: Especifique un nombre y configure un programa de transferencia.



A partir de ONTAP 9.10.1, es posible especificar si desea habilitar el archivado con Azure o AWS.



Si habilita el archivado para un volumen con Azure o AWS, no podrá deshabilitar el archivado.

Si habilita el archivado para Azure o AWS, especifique lo siguiente:

- El número de días después de los cuales se archiva el volumen.
- La cantidad de backups que se retendrán en el archivo. Especifique “0” (cero) para archivar hasta la última copia de seguridad.
- Para AWS, seleccione la clase de almacenamiento de archivado.


6. Seleccione los volúmenes de los que desea realizar el backup.

7. Seleccione **Guardar**.

## Edite la política de protección usada para Cloud Backup

Puede cambiar la política de protección que se usa con Cloud Backup.

### Pasos

1. En el Administrador del sistema, haga clic en **Protección > Descripción general** y, a continuación, desplácese a la sección **Cloud Backup Service**.
2. Haga clic en , Luego **Editar**.
3. Seleccione una **Política de protección**:
  - **Política existente**: Elija una política existente.
  - **Nueva directiva**: Especifique un nombre y configure un programa de transferencia.



A partir de ONTAP 9.10.1, es posible especificar si desea habilitar el archivado con Azure o AWS.



Si habilita el archivado para un volumen con Azure o AWS, no podrá deshabilitar el archivado.

Si habilita el archivado para Azure o AWS, especifique lo siguiente:

- El número de días después de los cuales se archiva el volumen.
- La cantidad de backups que se retendrán en el archivo. Especifique “0” (cero) para archivar hasta la última copia de seguridad.
- Para AWS, seleccione la clase de almacenamiento de archivado.

4. Seleccione **Guardar**.

## Proteja nuevos volúmenes o LUN en el cloud

Cuando se crea un volumen o LUN nuevo, puede establecer una relación de protección de SnapMirror que permita realizar backups en el cloud del volumen o LUN.

### Antes de empezar

- Debe tener una licencia de SnapMirror.
- Deben configurarse las LIF de interconexión de clústeres.
- NTP debe configurarse.
- El clúster debe ejecutar ONTAP 9.9.1.

### Acerca de esta tarea

No puede proteger volúmenes o LUN nuevos en el cloud para las siguientes configuraciones de clúster:

- El clúster no puede estar en un entorno de MetroCluster.
- No se admite SVM-DR.
- No se pueden realizar backups de FlexGroups con Cloud Backup.

### Pasos

1. Al aprovisionar un volumen o LUN, en la página **Protección** del Administrador del sistema, seleccione la casilla de verificación con la etiqueta **Activar SnapMirror (local o remoto)**.
2. Seleccione el tipo de política Cloud Backup.
3. Si la copia de seguridad en la nube no está activada, seleccione **Activar Cloud Backup Service**.

### Proteja los volúmenes o LUN existentes en el cloud

Puede establecer una relación de protección de SnapMirror para volúmenes y LUN existentes.

### Pasos

1. Seleccione un volumen o LUN existente y haga clic en **proteger**.
2. En la página **Protect Volumes**, especifique **copia de seguridad utilizando Cloud Backup Service** para la directiva de protección.
3. Haga clic en **proteger**.
4. En la página **Protección**, seleccione la casilla de verificación **Activar SnapMirror (local o remoto)**.
5. Seleccione **Activar Cloud Backup Service**.

### Restaurar datos de archivos de copia de seguridad

Puede realizar operaciones de administración de copias de seguridad, como restaurar datos, actualizar relaciones y eliminar relaciones, sólo cuando utilice la interfaz BlueXP. Consulte ["Restaurar datos a partir de archivos de copia de seguridad"](#) si quiere más información.

## Relaciones entre iguales de clústeres y SVM con la CLI

### Información general sobre relaciones entre iguales de clústeres y SVM con la CLI

Puede crear una relación entre iguales de clústeres de origen y de destino, y entre máquinas virtuales de almacenamiento (SVM) de origen y de destino. Debe crear relaciones entre iguales entre estas entidades antes de poder replicar copias de Snapshot con SnapMirror.

ONTAP 9.3 ofrece mejoras que simplifican la forma de configurar relaciones entre iguales entre clústeres y SVM. Los procedimientos de paridad de clústeres y SVM están disponibles para todas las versiones de

ONTAP 9. Debe utilizar el procedimiento adecuado para su versión de ONTAP.

Los procedimientos se realizan mediante la interfaz de línea de comandos (CLI), no con System Manager ni con una herramienta de secuencias de comandos automatizadas.

## Prepare la relación entre iguales de clústeres y SVM

### Conceptos básicos de peering

Debe crear *peer Relationships* entre los clústeres de origen y de destino, y entre las SVM de origen y de destino antes de poder replicar copias de Snapshot con SnapMirror. Una relación de paridad define las conexiones de red que permiten que clústeres y SVM intercambien datos de forma segura.

Los clústeres y las SVM en relaciones entre iguales se comunican a través de la red de interconexión de clústeres mediante las interfaces lógicas de interconexión de clústeres (LIF).\_ una LIF de interconexión de clústeres es una LIF compatible con el servicio de interfaz de red «núcleo entre clústeres» y normalmente se crea mediante la política de servicio de interfaz de red de «interconexión de clústeres predeterminada». Debe crear LIF de interconexión de clústeres en cada nodo en los clústeres que se van a establecer una relación entre iguales.

Las LIF de interconexión de clústeres utilizan las rutas que pertenecen a la SVM del sistema a la que se han asignado. ONTAP crea automáticamente una SVM del sistema para las comunicaciones a nivel de clúster dentro de un espacio IP.

Se admiten topologías en cascada y distribución ramificada. En una topología en cascada, solo necesita crear redes de interconexión de clústeres entre los clústeres principal y secundario, y entre los clústeres secundario y terciario. No es necesario crear una red de interconexión de clústeres entre el clúster principal y el terciario.



Es posible (pero no aconsejable) que un administrador elimine el servicio interclúster-core de la directiva de servicio de interconexión de clústeres predeterminada. Si esto sucede, las LIF creadas con «interconexión de clústeres predeterminada» no serán realmente LIF de interconexión de clústeres. Para confirmar que la política de servicio de interconexión de clústeres predeterminada contiene el servicio principal entre clústeres, utilice el siguiente comando:

```
network interface service-policy show -policy default-intercluster
```

### Requisitos previos para la relación de clústeres entre iguales

Antes de configurar cluster peering, debe confirmar que la conectividad, el puerto, la dirección IP, subred, firewall, y se cumplen los requisitos de nomenclatura de los clústeres.



A partir de ONTAP 9,6, el cifrado de pares de clústeres proporciona compatibilidad de cifrado TLS 1,2 AES-256 GCM para la replicación de datos de forma predeterminada. Los cifrados de seguridad predeterminados («PSK-AES256-GCM-SHA384») son necesarios para que el emparejamiento de clústeres funcione incluso si el cifrado está desactivado.

A partir de ONTAP 9.11.1, los cifrados de seguridad DHE-PSK están disponibles por defecto.

## Requisitos de conectividad

Todas las LIF de interconexión de clústeres del clúster local deben poder comunicarse con todas las LIF de interconexión de clústeres del clúster remoto.

Aunque no es necesario, generalmente es más fácil configurar las direcciones IP que se usan para las LIF de interconexión de clústeres de la misma subred. Las direcciones IP pueden residir en la misma subred que las LIF de datos, o en una subred diferente. La subred que se utiliza en cada clúster debe cumplir los siguientes requisitos:

- La subred debe pertenecer al dominio de retransmisión que contenga los puertos que se utilizan para la comunicación entre clústeres.
- La subred debe tener suficientes direcciones IP disponibles para asignar a una LIF de interconexión de clústeres por nodo.

Por ejemplo, en un clúster de cuatro nodos, la subred que se usa para la comunicación entre clústeres debe tener cuatro direcciones IP disponibles.

Cada nodo debe tener una LIF de interconexión de clústeres con una dirección IP en la red de interconexión de clústeres.

Las LIF entre clústeres pueden tener una dirección IPv4 o IPv6.



ONTAP le permite migrar sus redes entre iguales de IPv4 a IPv6 si, de manera opcional, permite que ambos protocolos estén presentes simultáneamente en las LIF de interconexión de clústeres. En las versiones anteriores, todas las relaciones de interconexión de clústeres de todo un clúster eran IPv4 o IPv6. Esto significaba que el cambio de protocolos era un evento que podía provocar interrupciones.

## Requisitos de puertos

Se pueden usar puertos dedicados para la comunicación entre clústeres o para compartir puertos que usa la red de datos. Los puertos deben cumplir con los siguientes requisitos:

- Todos los puertos que se utilizan para comunicarse con un clúster remoto determinado deben estar en el mismo espacio IP.

Se pueden utilizar varios espacios IP para establecer la misma relación entre iguales con varios clústeres. La conectividad de malla completa en par sólo se requiere dentro de un espacio IP.

- El dominio de retransmisión que se usa para la comunicación entre clústeres debe incluir al menos dos puertos por nodo para que la comunicación entre clústeres pueda conmutar por error de un puerto a otro.

Los puertos que se añaden a un dominio de retransmisión pueden ser puertos de red físicos, VLAN o grupos de interfaces (ifgrps).

- Todos los puertos deben estar cableadas.
- Todos los puertos deben estar en buen estado.
- La configuración de MTU de los puertos debe ser coherente.

## Requisitos del firewall



A partir de ONTAP 9.10.1, las políticas de firewall están obsoletas y sustituidas por completo por políticas de servicios LIF. Para obtener más información, consulte ["Configurar políticas de firewall para LIF"](#).

Los firewalls y la política de firewall de interconexión de clústeres deben permitir los siguientes protocolos:

- Tráfico ICMP bidireccional
- Tráfico TCP iniciado bidireccional hacia las direcciones IP de todas las LIF de interconexión de clústeres a través de los puertos 11104 y 11105
- HTTPS bidireccional entre las LIF de interconexión de clústeres

Aunque HTTPS no es necesario cuando se configura una relación de clústeres entre iguales con la CLI, se requiere HTTPS más adelante si se utiliza System Manager para configurar la protección de datos.

El valor predeterminado `intercluster` La directiva de firewall permite el acceso a través del protocolo HTTPS y desde todas las direcciones IP (0.0.0.0/0). Puede modificar o reemplazar la política si es necesario.

#### Requisitos del clúster

Los clústeres deben cumplir los siguientes requisitos:

- No puede haber un clúster en una relación de paridad con más de 255 clústeres.

#### Utilice puertos compartidos o dedicados

Se pueden usar puertos dedicados para la comunicación entre clústeres o para compartir puertos que usa la red de datos. Para decidir si se comparten puertos, debe tener en cuenta el ancho de banda de la red, el intervalo de replicación y la disponibilidad del puerto.



Es posible compartir puertos en un clúster con una relación entre iguales mientras se usan puertos dedicados en el otro.

#### Ancho de banda de red

Si tiene una red de alta velocidad, como 10 GbE, es posible que tenga suficiente ancho de banda LAN local para realizar la replicación con los mismos puertos de 10 GbE que se utilizan para el acceso a datos.

Incluso entonces, debería comparar su ancho de banda WAN disponible con su ancho de banda LAN. Si el ancho de banda WAN disponible es significativamente inferior a 10 GbE, es posible que deba utilizar puertos dedicados.



La única excepción a esta regla podría ser cuando todos los nodos del clúster replican los datos, en cuyo caso la utilización de ancho de banda suele extenderse por todos los nodos.

Si no utiliza puertos dedicados, el tamaño máximo de unidad de transmisión (MTU) de la red de replicación debe ser, por lo general, el mismo tamaño de MTU de la red de datos.

#### El intervalo de replicación

Si la replicación se realiza en horas de menor actividad, debería poder utilizar puertos de datos para la



replicación incluso sin conexión LAN de 10 GbE.

Si la replicación se realiza durante el horario laboral normal, debe tener en cuenta la cantidad de datos que se replicarán y si se requiere tanto ancho de banda como para provocar la contención con protocolos de datos. Si el uso de la red por protocolos de datos (SMB, NFS e iSCSI) supera el 50%, debe usar puertos dedicados para la comunicación entre clústeres con el fin de no degradar el rendimiento en caso de producirse una conmutación por error de nodo.

#### Disponibilidad de puertos

Si determina que el tráfico de replicación interfiere con el tráfico de datos, puede migrar las LIF de interconexión de clústeres a cualquier otro puerto compartido compatible con la interconexión de clústeres en el mismo nodo.

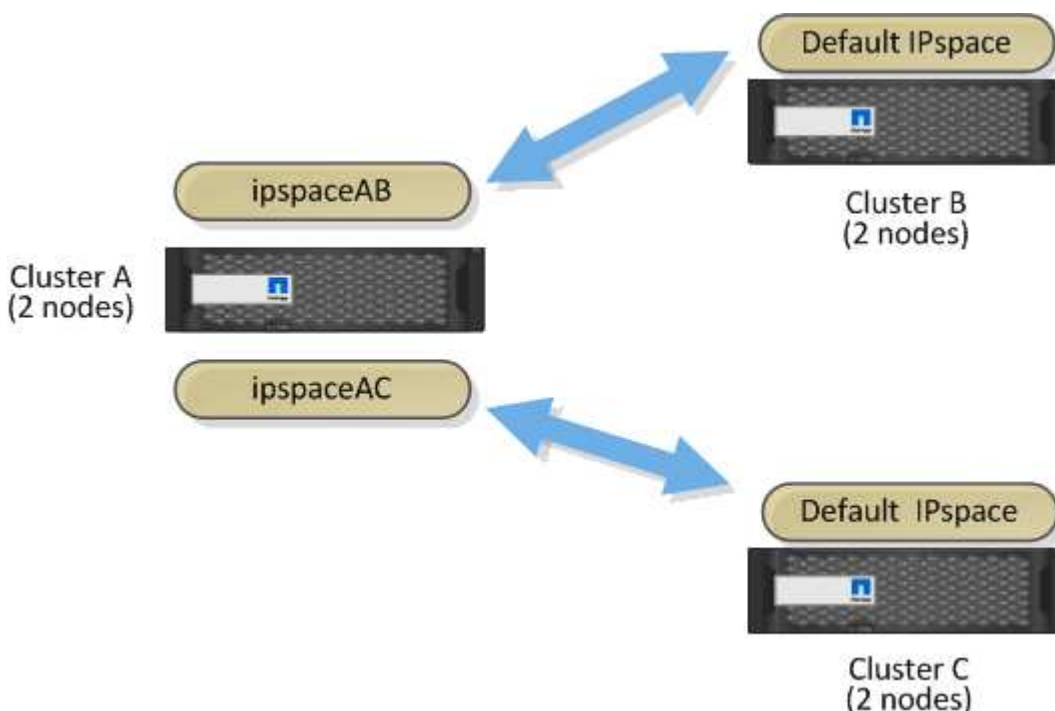
También puede dedicar puertos VLAN para la replicación. El ancho de banda del puerto se comparte entre todas las VLAN y el puerto base.

#### Utilice espacios IP personalizados para aislar el tráfico de replicación

Puede utilizar espacios IP personalizados para separar las interacciones que tiene un clúster con sus iguales. Esta configuración, denominada conectividad entre clústeres designada\_, permite a los proveedores de servicios aislar el tráfico de replicación en entornos multi-tenant.

Suponga, por ejemplo, que desea que el tráfico de replicación entre el clúster A y el clúster B esté separado del tráfico de replicación entre el clúster A y el clúster C. Para ello, puede crear dos espacios IP en el clúster A.

Un espacio IP contiene las LIF entre clústeres que utiliza para comunicarse con el clúster B. La otra contiene las LIF de interconexión de clústeres que utiliza para comunicarse con el clúster C, como se muestra en la siguiente ilustración.



Para obtener información sobre la configuración personalizada del espacio IP, consulte *Network Management*

## Configure las LIF de interconexión de clústeres

### Configure las LIF de interconexión de clústeres en puertos de datos compartidos

Las LIF de interconexión de clústeres se pueden configurar en los puertos compartidos con la red de datos. De este modo, se reduce el número de puertos necesarios para interconectar redes.

#### Pasos

1. Enumere los puertos del clúster:

```
network port show
```

Para obtener una sintaxis de comando completa, consulte la página man.

En el siguiente ejemplo se muestran los puertos de red en `cluster01`:

```
cluster01::> network port show
```

|              |       |         |           |        |       | Speed |            |
|--------------|-------|---------|-----------|--------|-------|-------|------------|
| (Mbps)       |       |         |           |        |       |       |            |
| Node         | Port  | IPspace | Broadcast | Domain | Link  | MTU   | Admin/Oper |
| -----        | ----- | -----   | -----     | -----  | ----- | ----- |            |
| cluster01-01 |       |         |           |        |       |       |            |
|              | e0a   | Cluster | Cluster   |        | up    | 1500  | auto/1000  |
|              | e0b   | Cluster | Cluster   |        | up    | 1500  | auto/1000  |
|              | e0c   | Default | Default   |        | up    | 1500  | auto/1000  |
|              | e0d   | Default | Default   |        | up    | 1500  | auto/1000  |
| cluster01-02 |       |         |           |        |       |       |            |
|              | e0a   | Cluster | Cluster   |        | up    | 1500  | auto/1000  |
|              | e0b   | Cluster | Cluster   |        | up    | 1500  | auto/1000  |
|              | e0c   | Default | Default   |        | up    | 1500  | auto/1000  |
|              | e0d   | Default | Default   |        | up    | 1500  | auto/1000  |

2. Cree LIF de interconexión de clústeres en una SVM de administrador (espacio IP predeterminado) o una SVM de sistema (espacio IP personalizado):

| Opción                    | Descripción                                                                                                                                                                    |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| En ONTAP 9.6 y posterior: | <pre>network interface create -vserver system_SVM -lif LIF_name -service -policy default-intercluster -home -node node -home-port port -address port_IP -netmask netmask</pre> |

| Opción                            | Descripción                                                                                                                                                                                            |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>En ONTAP 9.5 y anteriores:</b> | <code>network interface create -vserver <i>system_SVM</i> -lif <i>LIF_name</i> -role intercluster -home-node <i>node</i> -home-port <i>port</i> -address <i>port_IP</i> -netmask <i>netmask</i></code> |

Para obtener una sintaxis de comando completa, consulte la página [man](#).

En el siguiente ejemplo se crean LIF de interconexión de clústeres `cluster01_icl01` y `cluster01_icl02`:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

### 3. Compruebe que se han creado las LIF de interconexión de clústeres:

| Opción                            | Descripción                                                              |
|-----------------------------------|--------------------------------------------------------------------------|
| <b>En ONTAP 9.6 y posterior:</b>  | <code>network interface show -service-policy default-intercluster</code> |
| <b>En ONTAP 9.5 y anteriores:</b> | <code>network interface show -role intercluster</code>                   |

Para obtener una sintaxis de comando completa, consulte la página [man](#).

```

cluster01::> network interface show -service-policy default-intercluster
 Logical Status Network Current
Current Is
Vserver Interface Admin/Oper Address/Mask Node Port
Home

cluster01
 cluster01_icl01
 up/up 192.168.1.201/24 cluster01-01 e0c
true
 cluster01_icl02
 up/up 192.168.1.202/24 cluster01-02 e0c
true

```

#### 4. Compruebe que las LIF de interconexión de clústeres son redundantes:

| Opción                            | Descripción                                                                        |
|-----------------------------------|------------------------------------------------------------------------------------|
| <b>En ONTAP 9.6 y posterior:</b>  | <code>network interface show -service-policy default-intercluster -failover</code> |
| <b>En ONTAP 9.5 y anteriores:</b> | <code>network interface show -role intercluster -failover</code>                   |

Para obtener una sintaxis de comando completa, consulte la página [man](#).

El siguiente ejemplo muestra las LIF de interconexión de clústeres `cluster01_icl01` y `cluster01_icl02` en la `e0c` el puerto se conmuta al nodo de respaldo `e0d` puerto.

```

cluster01::> network interface show -service-policy default-intercluster
-failover
 Logical Home Failover Failover
Vserver Interface Node:Port Policy Group

cluster01
 cluster01_icl01 cluster01-01:e0c local-only
192.168.1.201/24
 Failover Targets: cluster01-01:e0c,
 cluster01-01:e0d
 cluster01_icl02 cluster01-02:e0c local-only
192.168.1.201/24
 Failover Targets: cluster01-02:e0c,
 cluster01-02:e0d

```

Configure las LIF de interconexión de clústeres en puertos dedicados

Puede configurar LIF de interconexión de clústeres en puertos dedicados. Al hacerlo, normalmente aumenta el ancho de banda disponible para el tráfico de replicación.

Pasos

- 1. Enumere los puertos del clúster:

```
network port show
```

Para obtener una sintaxis de comando completa, consulte la página man.

En el siguiente ejemplo se muestran los puertos de red en cluster01:

cluster01::> network port show

|              |      |         |           |        |      | Speed |            |
|--------------|------|---------|-----------|--------|------|-------|------------|
| (Mbps)       |      |         |           |        |      |       |            |
| Node         | Port | IPspace | Broadcast | Domain | Link | MTU   | Admin/Oper |
| -----        |      |         |           |        |      |       |            |
| -----        |      |         |           |        |      |       |            |
| cluster01-01 |      |         |           |        |      |       |            |
|              | e0a  | Cluster | Cluster   |        | up   | 1500  | auto/1000  |
|              | e0b  | Cluster | Cluster   |        | up   | 1500  | auto/1000  |
|              | e0c  | Default | Default   |        | up   | 1500  | auto/1000  |
|              | e0d  | Default | Default   |        | up   | 1500  | auto/1000  |
|              | e0e  | Default | Default   |        | up   | 1500  | auto/1000  |
|              | e0f  | Default | Default   |        | up   | 1500  | auto/1000  |
| cluster01-02 |      |         |           |        |      |       |            |
|              | e0a  | Cluster | Cluster   |        | up   | 1500  | auto/1000  |
|              | e0b  | Cluster | Cluster   |        | up   | 1500  | auto/1000  |
|              | e0c  | Default | Default   |        | up   | 1500  | auto/1000  |
|              | e0d  | Default | Default   |        | up   | 1500  | auto/1000  |
|              | e0e  | Default | Default   |        | up   | 1500  | auto/1000  |
|              | e0f  | Default | Default   |        | up   | 1500  | auto/1000  |

- 2. Determine qué puertos están disponibles para dedicar a la comunicación entre clústeres:

```
network interface show -fields home-port,curr-port
```

Para obtener una sintaxis de comando completa, consulte la página man.

En el siguiente ejemplo se muestran los puertos e0e y.. e0f No se han asignado LIF:

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif home-port curr-port

Cluster cluster01-01_clus1 e0a e0a
Cluster cluster01-01_clus2 e0b e0b
Cluster cluster01-02_clus1 e0a e0a
Cluster cluster01-02_clus2 e0b e0b
cluster01
 cluster_mgmt e0c e0c
cluster01
 cluster01-01_mgmt1 e0c e0c
cluster01
 cluster01-02_mgmt1 e0c e0c
```

### 3. Cree un grupo de recuperación tras fallos para los puertos dedicados:

```
network interface failover-groups create -vserver system_SVM -failover-group
failover_group -targets physical_or_logical_ports
```

En el siguiente ejemplo se asignan puertos e0e y.. e0f al grupo de recuperación tras fallos intercluster01 En la SVM del sistema cluster01:

```
cluster01::> network interface failover-groups create -vserver cluster01
-failover-group
intercluster01 -targets
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

### 4. Compruebe que el grupo de recuperación tras fallos se ha creado:

```
network interface failover-groups show
```

Para obtener una sintaxis de comando completa, consulte la página man.

```

cluster01::> network interface failover-groups show

Vserver Group Failover

Targets

Cluster
Cluster
cluster01 cluster01-01:e0a, cluster01-01:e0b,
 cluster01-02:e0a, cluster01-02:e0b
Default
cluster01 cluster01-01:e0c, cluster01-01:e0d,
 cluster01-02:e0c, cluster01-02:e0d,
 cluster01-01:e0e, cluster01-01:e0f
 cluster01-02:e0e, cluster01-02:e0f
intercluster01
cluster01-01:e0e, cluster01-01:e0f
cluster01-02:e0e, cluster01-02:e0f

```

5. Cree LIF de interconexión de clústeres en la SVM del sistema y asígnelas al grupo de recuperación tras fallos.

| Opción                            | Descripción                                                                                                                                                                                                       |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>En ONTAP 9.6 y posterior:</b>  | <pre> network interface create -vserver system_SVM -lif LIF_name -service -policy default-intercluster -home -node node -home- port port -address port_IP -netmask netmask -failover -group failover_group </pre> |
| <b>En ONTAP 9.5 y anteriores:</b> | <pre> network interface create -vserver system_SVM -lif LIF_name -role intercluster -home-node node -home -port port -address port_IP -netmask netmask -failover-group failover_group </pre>                      |

Para obtener una sintaxis de comando completa, consulte la página [man](#).

En el siguiente ejemplo se crean LIF de interconexión de clústeres `cluster01_icl01` y `cluster01_icl02` en el grupo de recuperación tras fallos `intercluster01`:

```

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0 -failover-group intercluster01

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01

```

6. Compruebe que se han creado las LIF de interconexión de clústeres:

| Opción                     | Descripción                                                 |
|----------------------------|-------------------------------------------------------------|
| En ONTAP 9.6 y posterior:  | network interface show -service-policy default-intercluster |
| En ONTAP 9.5 y anteriores: | network interface show -role intercluster                   |

Para obtener una sintaxis de comando completa, consulte la página man.

```

cluster01::> network interface show -service-policy default-intercluster

```

|            | Logical         | Status     | Network          | Current          |
|------------|-----------------|------------|------------------|------------------|
| Current Is |                 |            |                  |                  |
| Vserver    | Interface       | Admin/Oper | Address/Mask     | Node             |
| Home       |                 |            |                  | Port             |
| cluster01  | cluster01_icl01 | up/up      | 192.168.1.201/24 | cluster01-01 e0e |
| true       | cluster01_icl02 | up/up      | 192.168.1.202/24 | cluster01-02 e0f |
| true       |                 |            |                  |                  |

7. Compruebe que las LIF de interconexión de clústeres son redundantes:



| Opción                     | Descripción                                                           |
|----------------------------|-----------------------------------------------------------------------|
| En ONTAP 9.6 y posterior:  | network interface show -service-policy default-intercluster -failover |
| En ONTAP 9.5 y anteriores: | network interface show -role intercluster -failover                   |

Para obtener una sintaxis de comando completa, consulte la página man.

El siguiente ejemplo muestra las LIF de interconexión de clústeres `cluster01_icl01` y `cluster01_icl02`. En la SVM `e0e` el puerto se conmuta al nodo de respaldo `e0f` puerto.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
```

| Vserver        | Logical<br>Interface | Home<br>Node:Port | Failover<br>Policy                                      | Failover<br>Group |
|----------------|----------------------|-------------------|---------------------------------------------------------|-------------------|
| cluster01      | cluster01_icl01      | cluster01-01:e0e  | local-only                                              |                   |
| intercluster01 |                      |                   | Failover Targets: cluster01-01:e0e,<br>cluster01-01:e0f |                   |
| cluster01      | cluster01_icl02      | cluster01-02:e0e  | local-only                                              |                   |
| intercluster01 |                      |                   | Failover Targets: cluster01-02:e0e,<br>cluster01-02:e0f |                   |

## Configure las LIF de interconexión de clústeres en espacios IP personalizados

Puede configurar LIF de interconexión de clústeres en espacios IP personalizados. Al hacerlo, puede aislar el tráfico de replicación en entornos multi-tenant.

Cuando crea un espacio IP personalizado, el sistema crea una máquina virtual de almacenamiento (SVM) del sistema para que actúe como contenedor de los objetos del sistema en ese espacio IP. Puede usar la nueva SVM como contenedor de cualquier LIF entre clústeres del nuevo espacio IP. La nueva SVM tiene el mismo nombre que el espacio IP personalizado.

### Pasos

1. Enumere los puertos del clúster:

```
network port show
```

Para obtener una sintaxis de comando completa, consulte la página man.

En el siguiente ejemplo se muestran los puertos de red en `cluster01`:

```
cluster01::> network port show
```

| (Mbps)       |      | Speed   |                  |      |      |            |
|--------------|------|---------|------------------|------|------|------------|
| Node         | Port | IPspace | Broadcast Domain | Link | MTU  | Admin/Oper |
| -----        |      |         |                  |      |      |            |
| -----        |      |         |                  |      |      |            |
| cluster01-01 |      |         |                  |      |      |            |
|              | e0a  | Cluster | Cluster          | up   | 1500 | auto/1000  |
|              | e0b  | Cluster | Cluster          | up   | 1500 | auto/1000  |
|              | e0c  | Default | Default          | up   | 1500 | auto/1000  |
|              | e0d  | Default | Default          | up   | 1500 | auto/1000  |
|              | e0e  | Default | Default          | up   | 1500 | auto/1000  |
|              | e0f  | Default | Default          | up   | 1500 | auto/1000  |
| cluster01-02 |      |         |                  |      |      |            |
|              | e0a  | Cluster | Cluster          | up   | 1500 | auto/1000  |
|              | e0b  | Cluster | Cluster          | up   | 1500 | auto/1000  |
|              | e0c  | Default | Default          | up   | 1500 | auto/1000  |
|              | e0d  | Default | Default          | up   | 1500 | auto/1000  |
|              | e0e  | Default | Default          | up   | 1500 | auto/1000  |
|              | e0f  | Default | Default          | up   | 1500 | auto/1000  |

## 2. Cree espacios IP personalizados en el clúster:

```
network ipspace create -ipspace ipspace
```

En el siguiente ejemplo se crea el espacio IP personalizado `ipspace-IC1`:

```
cluster01::> network ipspace create -ipspace ipspace-IC1
```

## 3. Determine qué puertos están disponibles para dedicar a la comunicación entre clústeres:

```
network interface show -fields home-port,curr-port
```

Para obtener una sintaxis de comando completa, consulte la página `man`.

En el siguiente ejemplo se muestran los puertos `e0e` y `e0f`. No se han asignado LIF:

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif home-port curr-port

Cluster cluster01_clus1 e0a e0a
Cluster cluster01_clus2 e0b e0b
Cluster cluster02_clus1 e0a e0a
Cluster cluster02_clus2 e0b e0b
cluster01
 cluster_mgmt e0c e0c
cluster01
 cluster01-01_mgmt1 e0c e0c
cluster01
 cluster01-02_mgmt1 e0c e0c
```

4. Elimine los puertos disponibles del dominio de difusión predeterminado:

```
network port broadcast-domain remove-ports -broadcast-domain Default -ports
ports
```

Un puerto no puede estar en más de un dominio de retransmisión a la vez. Para obtener una sintaxis de comando completa, consulte la página man.

En el ejemplo siguiente se quitan puertos e0e y.. e0f desde el dominio de difusión predeterminado:

```
cluster01::> network port broadcast-domain remove-ports -broadcast
-domain Default -ports
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

5. Compruebe que los puertos se han eliminado del dominio de retransmisión predeterminado:

```
network port show
```

Para obtener una sintaxis de comando completa, consulte la página man.

En el siguiente ejemplo se muestran los puertos e0e y.. e0f se han eliminado del dominio de difusión predeterminado:

```
cluster01::> network port show
```

| Node         | Port | IPspace | Broadcast Domain | Link | MTU  | Speed (Mbps)<br>Admin/Oper |
|--------------|------|---------|------------------|------|------|----------------------------|
| -----        |      |         |                  |      |      |                            |
| cluster01-01 |      |         |                  |      |      |                            |
|              | e0a  | Cluster | Cluster          | up   | 9000 | auto/1000                  |
|              | e0b  | Cluster | Cluster          | up   | 9000 | auto/1000                  |
|              | e0c  | Default | Default          | up   | 1500 | auto/1000                  |
|              | e0d  | Default | Default          | up   | 1500 | auto/1000                  |
|              | e0e  | Default | -                | up   | 1500 | auto/1000                  |
|              | e0f  | Default | -                | up   | 1500 | auto/1000                  |
|              | e0g  | Default | Default          | up   | 1500 | auto/1000                  |
| cluster01-02 |      |         |                  |      |      |                            |
|              | e0a  | Cluster | Cluster          | up   | 9000 | auto/1000                  |
|              | e0b  | Cluster | Cluster          | up   | 9000 | auto/1000                  |
|              | e0c  | Default | Default          | up   | 1500 | auto/1000                  |
|              | e0d  | Default | Default          | up   | 1500 | auto/1000                  |
|              | e0e  | Default | -                | up   | 1500 | auto/1000                  |
|              | e0f  | Default | -                | up   | 1500 | auto/1000                  |
|              | e0g  | Default | Default          | up   | 1500 | auto/1000                  |

#### 6. Cree un dominio de retransmisión en el espacio IP personalizado:

```
network port broadcast-domain create -ipspace ipspace -broadcast-domain
broadcast_domain -mtu MTU -ports ports
```

En el siguiente ejemplo se crea el dominio de retransmisión `ipspace-IC1-bd` En el espacio IP `ipspace-IC1`:

```
cluster01::> network port broadcast-domain create -ipspace ipspace-IC1
-broadcast-domain
ipspace-IC1-bd -mtu 1500 -ports cluster01-01:e0e,cluster01-01:e0f,
cluster01-02:e0e,cluster01-02:e0f
```

#### 7. Compruebe que se ha creado el dominio de retransmisión:

```
network port broadcast-domain show
```

Para obtener una sintaxis de comando completa, consulte la página [man](#).

```
cluster01::> network port broadcast-domain show
```

| IPspace Broadcast |                |      | Update           |
|-------------------|----------------|------|------------------|
| Name              | Domain Name    | MTU  | Port List        |
|                   |                |      | Status Details   |
| Cluster           | Cluster        | 9000 |                  |
|                   |                |      | cluster01-01:e0a |
|                   |                |      | cluster01-01:e0b |
|                   |                |      | cluster01-02:e0a |
|                   |                |      | cluster01-02:e0b |
| Default           | Default        | 1500 |                  |
|                   |                |      | cluster01-01:e0c |
|                   |                |      | cluster01-01:e0d |
|                   |                |      | cluster01-01:e0f |
|                   |                |      | cluster01-01:e0g |
|                   |                |      | cluster01-02:e0c |
|                   |                |      | cluster01-02:e0d |
|                   |                |      | cluster01-02:e0f |
|                   |                |      | cluster01-02:e0g |
| ipspace-IC1       |                |      |                  |
|                   | ipspace-IC1-bd | 1500 |                  |
|                   |                |      | cluster01-01:e0e |
|                   |                |      | cluster01-01:e0f |
|                   |                |      | cluster01-02:e0e |
|                   |                |      | cluster01-02:e0f |

8. Cree LIF de interconexión de clústeres en la SVM del sistema y asígnelas al dominio de retransmisión:

| Opción                            | Descripción                                                                                                                                                                    |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>En ONTAP 9.6 y posterior:</b>  | <pre>network interface create -vserver system_SVM -lif LIF_name -service -policy default-intercluster -home -node node -home-port port -address port_IP -netmask netmask</pre> |
| <b>En ONTAP 9.5 y anteriores:</b> | <pre>network interface create -vserver system_SVM -lif LIF_name -role intercluster -home-node node -home -port port -address port_IP -netmask netmask</pre>                    |

La LIF se crea en el dominio de retransmisión al que está asignado el puerto inicial. El dominio de difusión tiene un grupo de conmutación por error predeterminado con el mismo nombre que el dominio de difusión. Para obtener una sintaxis de comando completa, consulte la página man.

En el siguiente ejemplo se crean LIF de interconexión de clústeres `cluster01_icl01` y `cluster01_icl02` en el dominio de retransmisión `ipspace-IC1`-bd:

```
cluster01::> network interface create -vserver ipspace-IC1 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver ipspace-IC1 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0
```

9. Compruebe que se han creado las LIF de interconexión de clústeres:

| Opción                     | Descripción                                                              |
|----------------------------|--------------------------------------------------------------------------|
| En ONTAP 9.6 y posterior:  | <code>network interface show -service-policy default-intercluster</code> |
| En ONTAP 9.5 y anteriores: | <code>network interface show -role intercluster</code>                   |

Para obtener una sintaxis de comando completa, consulte la página `man`.

```
cluster01::> network interface show -service-policy default-intercluster
Logical Status Network Current
Current Is
Vserver Interface Admin/Oper Address/Mask Node Port
Home

ipspace-IC1
 cluster01_icl01
 up/up 192.168.1.201/24 cluster01-01 e0e
true
 cluster01_icl02
 up/up 192.168.1.202/24 cluster01-02 e0f
true
```

10. Compruebe que las LIF de interconexión de clústeres son redundantes:

| Opción                     | Descripción                                                                        |
|----------------------------|------------------------------------------------------------------------------------|
| En ONTAP 9.6 y posterior:  | <code>network interface show -service-policy default-intercluster -failover</code> |
| En ONTAP 9.5 y anteriores: | <code>network interface show -role intercluster -failover</code>                   |

Para obtener una sintaxis de comando completa, consulte la página `man`.

El siguiente ejemplo muestra las LIF de interconexión de clústeres `cluster01_icl01` y `cluster01_icl02`. En la SVM `e0e` conmutación por error de puerto al puerto `e0f` por:

```
cluster01::> network interface show -service-policy default-intercluster
-failover
```

| Vserver        | Logical<br>Interface | Home<br>Node:Port | Failover<br>Policy                                      | Failover<br>Group |
|----------------|----------------------|-------------------|---------------------------------------------------------|-------------------|
| ipspace-IC1    | cluster01_icl01      | cluster01-01:e0e  | local-only                                              |                   |
| intercluster01 |                      |                   | Failover Targets: cluster01-01:e0e,<br>cluster01-01:e0f |                   |
|                | cluster01_icl02      | cluster01-02:e0e  | local-only                                              |                   |
| intercluster01 |                      |                   | Failover Targets: cluster01-02:e0e,<br>cluster01-02:e0f |                   |

## Configure las relaciones de paridad

### Cree una relación de paridad entre clústeres

Puede utilizar el `cluster peer create` comando para crear una relación entre iguales entre un clúster local y remoto. Una vez creada la relación de paridad, puede ejecutarse `cluster peer create` en el clúster remoto para autenticarse en el clúster local.

#### Antes de empezar

- Debe haber creado LIF de interconexión de clústeres en todos los nodos de los clústeres que se están interponiendo.
- Los clústeres deben ejecutar ONTAP 9.3 o una versión posterior. (Si los clústeres ejecutan ONTAP 9.2 o una versión anterior, consulte los procedimientos en ["este documento archivado"](#).)



#### Pasos

Lleve a cabo esta tarea mediante System Manager de ONTAP o la interfaz de línea de comandos de ONTAP.

## System Manager

1. En el clúster local, haga clic en **Clúster > Configuración**.
2. En la sección **Intercluster Settings**, haga clic en **Add Network Interfaces** y agregue interfaces de red de interconexión de clústeres para el clúster.

Repita este paso en el clúster remoto.

3. En el clúster remoto, haga clic en **Clúster > Configuración**.
4. Haga clic en  En la sección **Peones del clúster** y seleccione **Generar contraseña**.
5. Seleccione la versión del clúster de ONTAP remoto.
6. Copie la clave de acceso generada.
7. En el clúster local, en **Cluster peers**, haga clic en  Y seleccione **Peer cluster**.
8. En la ventana **Peer cluster**, pega la frase de acceso y haz clic en **Iniciar interconexión de clústeres**.

## CLI

1. En el clúster de destino, cree una relación entre iguales con el clúster de origen:

```
cluster peer create -generate-passphrase -offer-expiration
<MM/DD/YYYY HH:MM:SS>|1...7days|1...168hours -peer-addr
<peer_LIF_IPs > -initial-allowed-vserver-peers <svm_name>|* -ip
<ipspace>
```

Si especifica ambas `-generate-passphrase` y.. `-peer-addr`s, Sólo el clúster cuyas LIF de interconexión de clústeres se especifican en `-peer-addr`s puede utilizar la contraseña generada.

Puede ignorar la `-ipspace` Si no está utilizando un espacio IP personalizado. Para obtener una sintaxis de comando completa, consulte la página `man`.

Si va a crear la relación de paridad en ONTAP 9.6 o una versión posterior y no desea que se cifren las comunicaciones entre clústeres, debe utilizar el `-encryption-protocol-proposed none` opción para deshabilitar el cifrado.

En el siguiente ejemplo, se crea una relación de paridad entre clústeres con un clúster remoto no especificado y se preautORIZA relaciones entre iguales con SVM `vs1` y.. `vs2` en el clúster local:



```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers vs1,vs2

Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
Expiration Time: 6/7/2017 08:16:10 EST
Initial Allowed Vserver Peers: vs1,vs2
Intercluster LIF IP: 192.140.112.101
Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

En el siguiente ejemplo se crea una relación entre iguales de clústeres con el clúster remoto en las direcciones IP de LIF entre clústeres 192.140.112.103 y 192.140.112.104, y se autoriza previamente una relación entre iguales con cualquier SVM del clúster local:

```
cluster02::> cluster peer create -generate-passphrase -peer-addr
192.140.112.103,192.140.112.104 -offer-expiration 2days -initial
-allowed-vserver-peers *

Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
Expiration Time: 6/7/2017 08:16:10 EST
Initial Allowed Vserver Peers: vs1,vs2
Intercluster LIF IP: 192.140.112.101,192.140.112.102
Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

En el siguiente ejemplo, se crea una relación de paridad entre clústeres con un clúster remoto no especificado y se preautoriza relaciones entre iguales con SVM<sub>vs1</sub> y.. <sub>vs2</sub> en el clúster local:

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers vs1,vs2

Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
Expiration Time: 6/7/2017 08:16:10 EST
Initial Allowed Vserver Peers: vs1,vs2
Intercluster LIF IP: 192.140.112.101
Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

2. En el clúster de origen, autentique el clúster de origen al clúster de destino:

```
cluster peer create -peer-addr <peer_LIF_IPs> -ipspace <ipspace>
```

Para obtener una sintaxis de comando completa, consulte la página man.

En el siguiente ejemplo se autentica el clúster local en el clúster remoto en las direcciones IP de LIF entre clústeres 192.140.112.101 y 192.140.112.102:

```
cluster01::> cluster peer create -peer-addr
192.140.112.101,192.140.112.102
```

Notice: Use a generated passphrase or choose a passphrase of 8 or more characters.

To ensure the authenticity of the peering relationship, use a phrase or sequence of characters that would be hard to guess.

Enter the passphrase:

Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.

Introduzca la frase de acceso para la relación entre iguales cuando se le solicite.

3. Compruebe que se ha creado la relación de paridad entre clústeres:

```
cluster peer show -instance
```

```
cluster01::> cluster peer show -instance
```

```
Peer Cluster Name: cluster02
Remote Intercluster Addresses: 192.140.112.101,
192.140.112.102
Availability of the Remote Cluster: Available
Remote Cluster Name: cluster2
Active IP Addresses: 192.140.112.101,
192.140.112.102
Cluster Serial Number: 1-80-123456
Address Family of Relationship: ipv4
Authentication Status Administrative: no-authentication
Authentication Status Operational: absent
Last Update Time: 02/05 21:05:41
IPspace for the Relationship: Default
```

4. Compruebe la conectividad y el estado de los nodos en la relación de paridad:

```
cluster peer health show
```

```
cluster01::> cluster peer health show
Node cluster-Name Node-Name
 Ping-Status RDB-Health Cluster-Health
Avail...

cluster01-01
 cluster02 cluster02-01
 Data: interface_reachable
 ICMP: interface_reachable true true
true
 cluster02-02
 Data: interface_reachable
 ICMP: interface_reachable true true
true
cluster01-02
 cluster02 cluster02-01
 Data: interface_reachable
 ICMP: interface_reachable true true
true
 cluster02-02
 Data: interface_reachable
 ICMP: interface_reachable true true
true
```

Otras maneras de hacerlo en ONTAP

| Para ejecutar estas tareas con...                                            | Ver este contenido...                                                                                 |
|------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| System Manager rediseñado (disponible con ONTAP 9.7 y versiones posteriores) | <a href="#">"Prepare el mirroring y el almacenamiento"</a>                                            |
| System Manager Classic (disponible con ONTAP 9.7 y versiones anteriores)     | <a href="#">"Información general de preparación para la recuperación ante desastres de volúmenes"</a> |

Cree una relación entre iguales de SVM entre clústeres

Puede utilizar el `vserver peer create` Comando para crear una relación entre iguales entre SVM en clústeres locales y remotos.

Antes de empezar

- Los clústeres de origen y destino deben tener una relación entre iguales.
- Los clústeres deben ejecutar ONTAP 9.3. (Si los clústeres ejecutan ONTAP 9.2 o una versión anterior, consulte los procedimientos en ["este documento archivado"](#).)
- Debe tener relaciones entre iguales "preautorizadas" para las SVM en el clúster remoto.

Para obtener más información, consulte ["Creación de una relación de paridad entre clústeres"](#).

### Acerca de esta tarea

En ONTAP 9.2 y versiones anteriores, solo se puede autorizar una relación entre iguales para una SVM a la vez. Esto significa que debe ejecutar el `vserver peer accept` Comando cada vez que se autoriza una relación entre iguales de SVM pendiente.

A partir de ONTAP 9.3, puede "preautorizar" relaciones entre iguales para varias SMV mediante la lista de las SMV en el `-initial-allowed-vserver` opción cuando se crea una relación de paridad entre clústeres. Para obtener más información, consulte ["Creación de una relación de paridad entre clústeres"](#).

### Pasos

1. En el clúster de destino de protección de datos, muestre las SVM que están autorizadas previamente para la paridad:

```
vserver peer permission show
```

```
cluster02::> vserver peer permission show
Peer Cluster Vserver Applications

cluster02 vs1,vs2 snapmirror
```

2. En el clúster de origen de protección de datos, cree una relación entre iguales con una SVM preautorizada en el clúster de destino de protección de datos:

```
vserver peer create -vserver local_SVM -peer-vserver remote_SVM
```

Para obtener una sintaxis de comando completa, consulte la página man.

En el siguiente ejemplo se crea una relación entre iguales entre la SVM local `pvs1` Y la SVM remota preautorizada `vs1`:

```
cluster01::> vserver peer create -vserver pvs1 -peer-vserver vs1
```

3. Compruebe las relaciones entre iguales de SVM:

```
vserver peer show
```

```
cluster01::> vserver peer show
```

|         | Peer    | Peer    |           | Peering      |
|---------|---------|---------|-----------|--------------|
| Remote  | Vserver | Vserver | State     | Peer Cluster |
| Vserver |         |         |           | Applications |
| -----   | -----   | -----   | -----     | -----        |
| -----   |         |         |           |              |
| pvs1    | vs1     | peered  | cluster02 | snapmirror   |
| vs1     |         |         |           |              |

## Añada una relación entre iguales de SVM de interconexión de clústeres

Si crea una SVM después de configurar una relación de paridad de clústeres, deberá añadir una relación de paridad para la SVM manualmente. Puede utilizar el `vserver peer create` Comando para crear una relación entre iguales entre SVM. Una vez creada la relación de paridad, puede ejecutarse `vserver peer accept` en el clúster remoto para autorizar la relación de paridad.

### Antes de empezar

Los clústeres de origen y destino deben tener una relación entre iguales.

### Acerca de esta tarea

Puede crear relaciones entre iguales entre SVM en el mismo clúster para el backup de datos local. Para obtener más información, consulte `vserver peer create` página de manual.

Los administradores utilizan ocasionalmente el `vserver peer reject` Comando para rechazar una relación de paridad de SVM propuesta. Si la relación entre las SVM está en la `rejected` estado, debe eliminar la relación antes de poder crear una nueva. Para obtener más información, consulte `vserver peer delete` página de manual.

### Pasos

1. En el clúster de origen de protección de datos, cree una relación entre iguales con una SVM en el clúster de destino de protección de datos:

```
vserver peer create -vserver local_SVM -peer-vserver remote_SVM -applications snapmirror|file-copy|lun-copy -peer-cluster remote_cluster
```

En el siguiente ejemplo se crea una relación entre iguales entre la SVM local `pvs1` Y la SVM remota `vs1`

```
cluster01::> vserver peer create -vserver pvs1 -peer-vserver vs1
-applications snapmirror -peer-cluster cluster02
```

Si las SVM locales y remotas tienen los mismos nombres, debe usar un *local name* para crear la relación entre iguales de SVM:

```
cluster01::> vserver peer create -vserver vs1 -peer-vserver
vs1 -applications snapmirror -peer-cluster cluster01
-local-name cluster1vs1LocallyUniqueName
```

2. En el clúster de origen de protección de datos, compruebe que se ha iniciado la relación de paridad:

```
vserver peer show-all
```

Para obtener una sintaxis de comando completa, consulte la página man.

En el siguiente ejemplo, se muestra la relación entre iguales entre SVM<sub>pvs1</sub> Y SVM<sub>vs1</sub> se ha iniciado:

```
cluster01::> vserver peer show-all
```

| Vserver | Peer<br>Vserver | Peer<br>State | Peer Cluster | Peering<br>Applications |
|---------|-----------------|---------------|--------------|-------------------------|
| -----   | -----           | -----         | -----        | -----                   |
| pvs1    | vs1             | initiated     | Cluster02    | snapmirror              |

3. En el clúster de destino de la protección de datos, muestre la relación entre iguales de SVM pendiente:

```
vserver peer show
```

Para obtener una sintaxis de comando completa, consulte la página man.

En el siguiente ejemplo, se enumeran las relaciones entre iguales pendientes para cluster02:

```
cluster02::> vserver peer show
```

| Vserver | Peer<br>Vserver | Peer<br>State |
|---------|-----------------|---------------|
| -----   | -----           | -----         |
| vs1     | pvs1            | pending       |

4. En el clúster de destino de la protección de datos, autorice la relación entre iguales pendiente:

```
vserver peer accept -vserver local_SVM -peer-vserver remote_SVM
```

Para obtener una sintaxis de comando completa, consulte la página man.

En el siguiente ejemplo, se autoriza la relación entre iguales entre la SVM local vs1 Y la SVM remota pvs1:

```
cluster02::> vserver peer accept -vserver vs1 -peer-vserver pvs1
```

5. Compruebe las relaciones entre iguales de SVM:

```
vserver peer show
```

```
cluster01::> vserver peer show
```

| Remote  | Peer    | Peer   | Peer      | Peering      |
|---------|---------|--------|-----------|--------------|
| Vserver | Vserver | State  | Cluster   | Applications |
| Vserver |         |        |           |              |
| -----   | -----   | -----  | -----     | -----        |
| -----   |         |        |           |              |
| pvs1    | vs1     | peered | cluster02 | snapmirror   |
| vs1     |         |        |           |              |

## Habilite el cifrado de paridad de clústeres en una relación de paridad existente

A partir de ONTAP 9.6, el cifrado de paridad de clústeres está habilitado de forma predeterminada en todas las relaciones de paridad de clústeres que haya creado recientemente. El cifrado de interconexión de clústeres utiliza una clave precompartida (PSK) y la capa de seguridad de transporte (TLS) para proteger las comunicaciones de interconexión entre clústeres. Esto añade una capa adicional de seguridad entre los clústeres con una relación entre iguales.

### Acerca de esta tarea

Si va a actualizar clústeres con una relación entre iguales a ONTAP 9.6 o posterior y la relación de paridad se creó en ONTAP 9.5 o versiones anteriores, el cifrado de paridad de clústeres se debe habilitar manualmente después de la actualización. Ambos clústeres de la relación de paridad deben ejecutar ONTAP 9.6 o una versión posterior para habilitar el cifrado de paridad de clústeres.

### Pasos

1. En el clúster de destino, habilite el cifrado para las comunicaciones con el clúster de origen:

```
cluster peer modify source_cluster -auth-status-admin use-authentication
-encryption-protocol-proposed tls-psk
```

2. Cuando se le solicite, introduzca una frase de contraseña.
3. En el clúster de origen de la protección de datos, habilite el cifrado para la comunicación con el clúster de destino de la protección de datos:

```
cluster peer modify data_protection_destination_cluster -auth-status-admin
use-authentication -encryption-protocol-proposed tls-psk
```

4. Cuando se le solicite, escriba la misma clave de acceso introducida en el clúster de destino.

## Quite el cifrado de paridad de clústeres de una relación de paridad existente

De forma predeterminada, el cifrado de paridad de clústeres está habilitado en todas las relaciones entre iguales creadas en ONTAP 9.6 o posterior. Si no desea utilizar el cifrado para las comunicaciones entre clústeres entre iguales, puede deshabilitarlo.

## Pasos

1. En el clúster de destino, modifique las comunicaciones con el clúster de origen para interrumpir el uso del cifrado de interconexión de clústeres :

- Para eliminar el cifrado, pero mantener la autenticación, introduzca:

```
cluster peer modify _source_cluster_ -auth-status-admin use-
authentication -encryption-protocol-proposed none
```

- Para eliminar el cifrado y la autenticación, introduzca:

```
cluster peer modify _source_cluster_ -auth-status no-authentication
```

2. Cuando se le solicite, introduzca una frase de contraseña.
3. En el clúster de origen, deshabilite el cifrado para la comunicación con el clúster de destino:

- Para eliminar el cifrado, pero mantener la autenticación, introduzca:

```
cluster peer modify _destination_cluster_ -auth-status-admin use-
authentication -encryption-protocol-proposed none
```

- Para eliminar el cifrado y la autenticación, introduzca:

```
cluster peer modify _destination_cluster_ -auth-status no-
authentication
```

4. Cuando se le solicite, escriba la misma clave de acceso introducida en el clúster de destino.

## Gestione copias Snapshot locales

### Información general sobre la gestión de copias Snapshot locales

Una *Snapshot copy* es una imagen puntual de solo lectura de un volumen. La imagen consume un espacio de almacenamiento mínimo y tiene una sobrecarga del rendimiento mínima, ya que solo registra los cambios realizados en los archivos desde la última copia Snapshot.

Puede usar una copia Snapshot para restaurar el contenido completo de un volumen o para recuperar archivos o LUN individuales. Las copias Snapshot se almacenan en el directorio `.snapshot` en el volumen.

En ONTAP 9.3 y versiones anteriores, un volumen puede contener hasta 255 copias snapshot. A partir de la versión 9.4 de ONTAP, un volumen de FlexVol puede contener hasta 1023 copias snapshot.





A partir de ONTAP 9.8, los volúmenes FlexGroup pueden contener 1023 copias snapshot. Para obtener más información, consulte ["Protección de volúmenes de FlexGroup mediante copias de Snapshot"](#).

## Configuración de políticas de Snapshot personalizadas

### Información general de configuración de políticas de Snapshot personalizadas

Una *política de Snapshot* define el modo en que el sistema crea copias Snapshot. La política especifica cuándo crear copias Snapshot, cuántas copias se retendrán y cómo nombrarlas. Por ejemplo, un sistema puede crear una copia Snapshot todos los días a las 12:10, conservar las dos copias más recientes y nombrar las copias "día a día.*timestamp*".

La política predeterminada de un volumen crea automáticamente copias de Snapshot en la siguiente programación, con las copias de Snapshot más antiguas eliminadas para hacer espacio para las copias más nuevas:

- Un máximo de seis copias Snapshot cada hora tardan cinco minutos.
- Un máximo de dos copias Snapshot diarias que se tomaban de lunes a sábado a las 10 minutos después de la medianoche.
- Un máximo de dos copias snapshot semanales cada domingo a las 15 minutos después de la medianoche.

A menos que especifique una política de Snapshot cuando crea un volumen, el volumen hereda la política de Snapshot asociada con su máquina virtual de almacenamiento (SVM).

### Cuándo configurar una política de Snapshot personalizada

Si la política de Snapshot predeterminada no es adecuada para un volumen, puede configurar una política personalizada que modifique la frecuencia, la retención y el nombre de las copias de Snapshot. La programación estará dictada principalmente por la tasa de cambio del sistema de archivos activo.

Puede ser recomendable realizar el backup de un sistema de archivos muy utilizado, como una base de datos, cada hora, mientras que el backup de archivos de uso poco frecuente una vez al día. Incluso en el caso de una base de datos, suele ejecutar un backup completo una o dos veces al día, mientras realiza el backup de los registros de transacciones cada hora.

Otros factores son la importancia de los archivos para la organización, el SLA, el RPO y el RTO. En general, sólo debe conservar tantas copias snapshot como sea necesario.

### Crear una programación de trabajo de Snapshot

Una política de Snapshot requiere al menos una programación de trabajo de copia de Snapshot. Puede utilizar el `job schedule cron create` para crear una programación de trabajo.

#### Acerca de esta tarea

De forma predeterminada, ONTAP forma los nombres de las copias Snapshot anexando una Marca de tiempo

al nombre de la programación del trabajo.

Si especifica valores para el día del mes y el día de la semana, los valores se consideran independientes. Por ejemplo, una programación cron con la especificación del día `Friday` y el día de la especificación del mes `13` Funciona todos los viernes y el día 13 de cada mes, no sólo cada viernes 13.

## Paso

### 1. Crear un programa de trabajo:

```
job schedule cron create -name job_name -month month -dayofweek day_of_week
-day day_of_month -hour hour -minute minute
```

Para `-month`, `-dayofweek`, y `-hour`, puede especificar `all` para ejecutar el trabajo cada mes, día de la semana y hora, respectivamente.

A partir de ONTAP 9.10.1, puede incluir Vserver para su programación de trabajo:

```
job schedule cron create -name job_name -vserver Vserver_name -month month
-dayofweek day_of_week -day day_of_month -hour hour -minute minute
```

En el ejemplo siguiente se crea una programación de trabajo denominada `myweekly` Es decir, los sábados a las 3:00 horas:

```
cluster1::> job schedule cron create -name myweekly -dayofweek
"Saturday" -hour 3 -minute 0
```

En el siguiente ejemplo se crea una programación llamada `myweeklymulti` esto especifica varios días, horas y minutos:

```
job schedule cron create -name myweeklymulti -dayofweek
"Monday,Wednesday,Sunday" -hour 3,9,12 -minute 0,20,50
```

## Cree una política de Snapshot

Una política de Snapshot especifica cuándo crear copias de Snapshot, cuántas copias se retendrán y cómo nombrarlas. Por ejemplo, un sistema puede crear una copia Snapshot todos los días a las 12:10, conservar las dos copias más recientes y nombrarlas "día tras día.*timestamp*." Una política de Snapshot puede contener hasta cinco programaciones de trabajo.

### Acerca de esta tarea

De forma predeterminada, ONTAP forma los nombres de las copias Snapshot anexando una Marca de tiempo al nombre de programación de trabajo:

|                         |                         |
|-------------------------|-------------------------|
| daily.2017-05-14_0013/  | hourly.2017-05-15_1106/ |
| daily.2017-05-15_0012/  | hourly.2017-05-15_1206/ |
| hourly.2017-05-15_1006/ | hourly.2017-05-15_1306/ |

Si lo prefiere, puede sustituir un prefijo por el nombre del programa de trabajo.

La `snapmirror-label` Esta opción es para la replicación de SnapMirror. Para obtener más información, consulte ["Definición de una regla para una política"](#).

## Paso

1. Cree una política de Snapshot:

```
volume snapshot policy create -vserver SVM -policy policy_name -enabled
true|false -schedule1 schedule1_name -count1 copies_to_retain -prefix1
snapshot_prefix -snapmirror-label1 snapshot_label ... -schedule5 schedule5_name
-count5 copies_to_retain-prefix5 snapshot_prefix -snapmirror-label5
snapshot_label
```

En el ejemplo siguiente se crea una política de Snapshot llamada `snap_policy_daily` eso se ejecuta en un `daily` programación. La política tiene un máximo de cinco copias Snapshot, cada una con el nombre `daily.timestamp` Y la etiqueta de SnapMirror `daily`:

```
cluster1::> volume snapshot policy create -vserver vs0 -policy
snap_policy_daily -schedule1 daily -count1 5 -snapmirror-label1 daily
```

## Gestionar copias Snapshot manualmente

### Crear y eliminar copias Snapshot manualmente

Puede crear copias Snapshot manualmente cuando no se puede esperar a que se cree una copia Snapshot programada para eliminar copias Snapshot cuando ya no son necesarias.

#### Crear una copia Snapshot manualmente

Puede crear manualmente una copia Snapshot mediante System Manager o la interfaz de línea de comandos de ONTAP.

## System Manager

### Pasos

1. Vaya a **Almacenamiento > Volúmenes** y seleccione la pestaña **Copias de instantánea**.
2. Haga clic en **+ Add**.
3. En la ventana **Agregar una copia snapshot**, acepte el nombre predeterminado de la copia snapshot o edítelo si lo desea.
4. **Opcional:** Añade una etiqueta de SnapMirror.
5. Haga clic en **Agregar**.

### CLI

1. Cree una copia Snapshot:

```
volume snapshot create -vserver <SVM> -volume <volume> -snapshot
<snapshot_name>
```

## Eliminar una copia Snapshot de forma manual

Puede eliminar manualmente una copia Snapshot mediante System Manager o la interfaz de línea de comandos de ONTAP.

## System Manager

### Pasos

1. Vaya a **Almacenamiento > Volúmenes** y seleccione la pestaña **Copias de instantánea**.
2. Busque la copia Snapshot que desee eliminar y haga clic en **:**, Y seleccione **Eliminar**.
3. En la ventana **Eliminar copia de instantánea**, seleccione **Eliminar copia de instantánea**.
4. Haga clic en **Eliminar**.

### CLI

1. Eliminar una copia Snapshot:

```
volume snapshot delete -vserver <SVM> -volume <volume> -snapshot
<snapshot_name>
```

## Gestione la reserva de copias Snapshot

### Gestione la descripción general de la reserva de copias Snapshot

El *Snapshot copy reserve* deja un porcentaje del espacio en disco para las copias Snapshot, del cinco por ciento de forma predeterminada. Debido a que las copias Snapshot utilizan espacio en el sistema de archivos activo cuando se agota la reserva de

copia Snapshot, puede aumentar la reserva de copia Snapshot según sea necesario. También puede realizar copias Snapshot de forma automática cuando la reserva esté llena.

### **Cuándo aumentar la reserva para copias Snapshot**

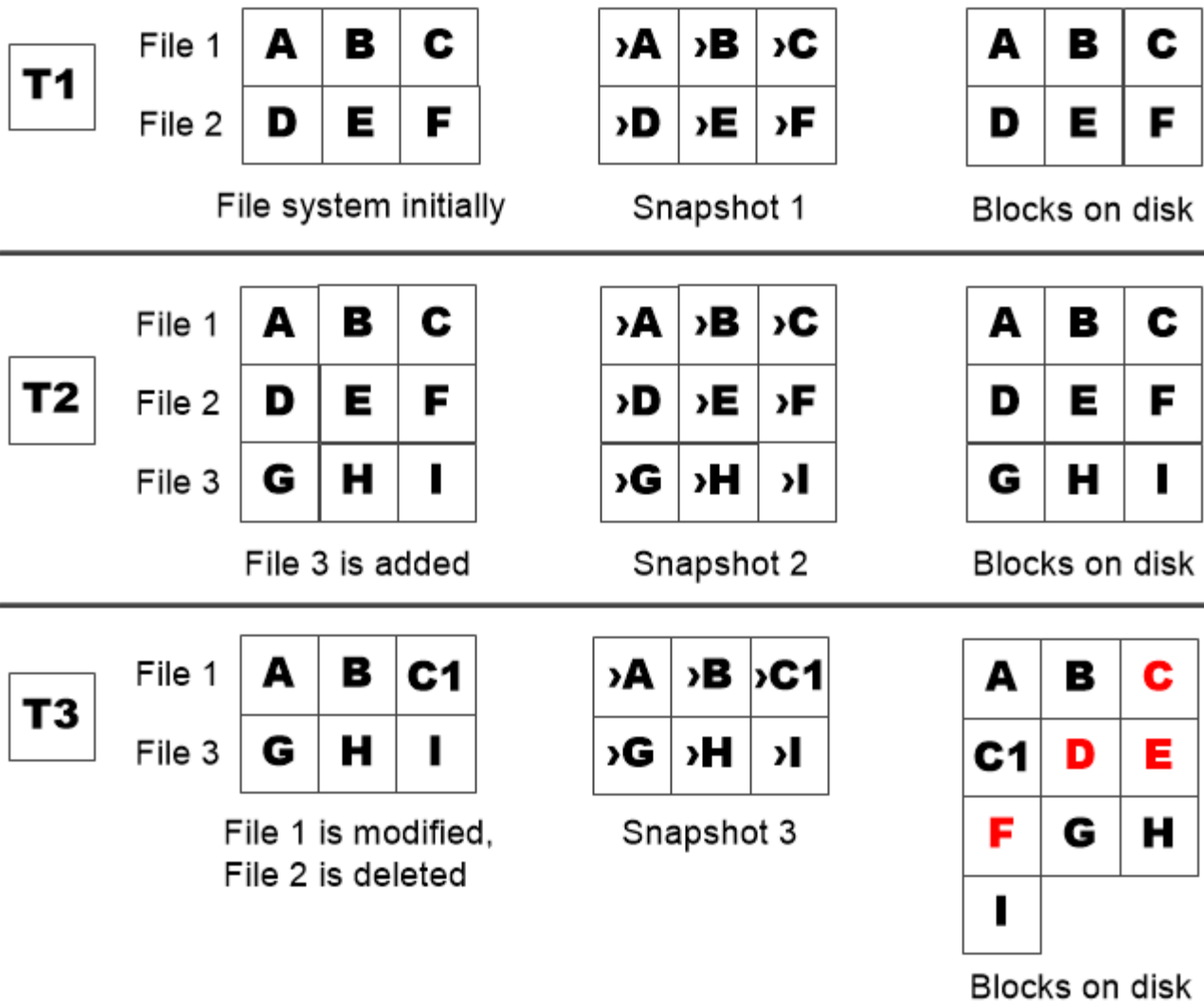
Para decidir si se debe aumentar la reserva Snapshot, es importante recordar que una copia Snapshot solo registra los cambios en los archivos desde que se realizó la última copia Snapshot. Consume espacio en disco solo si se modifican o eliminan bloques del sistema de archivos activo.

Esto significa que la tasa de cambio del sistema de archivos es el factor clave para determinar la cantidad de espacio en disco que utilizan las copias snapshot. No importa cuántas copias snapshot cree, no consumirán espacio en disco si el sistema de archivos activo no ha cambiado.

Por ejemplo, un volumen FlexVol que contenga registros de transacciones de base de datos puede tener una reserva de copia Snapshot de hasta el 20 % para justificar su mayor tasa de cambio. No solo querrá crear más copias Snapshot para capturar las actualizaciones más frecuentes de la base de datos, sino que también querrá tener una reserva de copia Snapshot mayor para gestionar el espacio en disco adicional que consumen las copias Snapshot.



Una copia Snapshot consta de punteros a bloques en lugar de copias de bloques. Puede pensar en un puntero como «reclamación» en un bloque: «Mantiene» ONTAP el bloque hasta que se elimine la copia snapshot.



*A Snapshot copy consumes disk space only when blocks in the active file system are modified or deleted.*

**La eliminación de archivos protegidos puede reducir el espacio de archivos de lo esperado**

Una copia snapshot señala a un bloque incluso después de eliminar el archivo que utilizó el bloque. Esto explica por qué una reserva de copia snapshot agotada puede dar lugar al resultado contrario-intuitivo en el que la eliminación de todo un sistema de archivos da como resultado menos espacio disponible que el sistema de archivos ocupado.

Observe el siguiente ejemplo. Antes de eliminar cualquier archivo, el `df` el resultado del comando es el siguiente:

```
Filesystem kbytes used avail capacity
/vol/vol0/ 3000000 3000000 0 100%
/vol/vol0/.snapshot 1000000 500000 500000 50%
```

Tras eliminar todo el sistema de archivos y realizar una copia snapshot del volumen, la `df` el comando genera

la siguiente salida:

```
Filesystem kbytes used avail capacity
/vol/vol0/ 3000000 2500000 500000 83%
/vol/vol0/.snapshot 1000000 3500000 0 350%
```

Tal y como se muestra en el resultado, ahora los 3 GB completos que utilizaba el sistema de archivos activo son utilizados por las copias snapshot, además de los 0.5 GB utilizados antes de la eliminación.

Como el espacio en disco utilizado por las copias snapshot supera ahora la reserva de copia snapshot, el desbordamiento de 2.5 GB de «píldoras» en el espacio reservado para los archivos activos, dejándole con 0.5 GB de espacio libre para los archivos en los que razonablemente se podrían haber esperado 3 GB.

### Supervisar el consumo de discos de la copia snapshot

Puede supervisar el consumo de discos de copias Snapshot mediante la `df` comando. El comando muestra la cantidad de espacio libre en el sistema de archivos activo y la reserva de copias de Snapshot.

#### Paso

1. Mostrar consumo de disco de copia Snapshot: `df`

El siguiente ejemplo muestra el consumo de discos de copia Snapshot:

```
cluster1::> df
Filesystem kbytes used avail capacity
/vol/vol0/ 3000000 3000000 0 100%
/vol/vol0/.snapshot 1000000 500000 500000 50%
```

### Compruebe la reserva de copias Snapshot disponibles en un volumen

Puede comprobar la cantidad de reserva de copias Snapshot disponible en un volumen mediante el `snapshot-reserve-available` con el `volume show` comando.

#### Paso

1. Compruebe la reserva de copia Snapshot disponible en un volumen:

```
vol show -vserver SVM -volume volume -fields snapshot-reserve-available
```

Para obtener una sintaxis de comando completa, consulte la página `man`.

En el ejemplo siguiente se muestra la reserva disponible de copias Snapshot para `vol1`:

```
cluster1::> vol show -vserver vs0 -volume vol1 -fields snapshot-reserve-
available

vserver volume snapshot-reserve-available

vs0 vol1 4.84GB
```

## Modificar la reserva de copias Snapshot

Se recomienda configurar una reserva de copia de Snapshot más grande para evitar que las copias de Snapshot utilicen el espacio reservado para el sistema de archivos activo. Puede reducir la reserva de copias Snapshot cuando ya no necesite tanto espacio para las copias Snapshot.

### Paso

1. Modifique la reserva de copias Snapshot:

```
volume modify -vserver SVM -volume volume -percent-snapshot-space snap_reserve
```

Para obtener una sintaxis de comando completa, consulte la página man.

En el ejemplo siguiente se establece la reserva de copias Snapshot para `vol1` al 10 por ciento:

```
cluster1::> volume modify -vserver vs0 -volume vol1 -percent-snapshot
-space 10
```

## Eliminación automática de copias snapshot

Puede utilizar el `volume snapshot autodelete modify` Comando para activar la eliminación automática de copias Snapshot cuando se supera la reserva Snapshot. De manera predeterminada, las copias de Snapshot más antiguas se eliminan primero.

### Acerca de esta tarea

Los clones de LUN y archivos se eliminan cuando no hay más copias snapshot que se pueden eliminar.

### Paso

1. Eliminación automática de copias Snapshot:

```
volume snapshot autodelete modify -vserver SVM -volume volume -enabled
true|false -trigger volume|snap_reserve
```

Para obtener una sintaxis de comando completa, consulte la página man.

En el ejemplo siguiente se eliminan automáticamente las copias Snapshot para `vol1` Cuando la reserva de la copia Snapshot se haya agotado:



```
cluster1::> volume snapshot autodelete modify -vserver vs0 -volume vol1
-enabled true -trigger snap_reserve
```

## Restaurar archivos desde copias snapshot

### Restaurar un archivo de una copia Snapshot en un cliente NFS o SMB

Un usuario en un cliente NFS o SMB puede restaurar un archivo directamente desde una copia Snapshot sin la intervención de un administrador del sistema de almacenamiento.

Cada directorio del sistema de archivos contiene un subdirectorio llamado `.snapshot` Accesible para los usuarios de NFS y SMB. La `.snapshot` Este subdirectorio contiene subdirectorios que corresponden a las copias snapshot del volumen:

```
$ ls .snapshot
daily.2017-05-14_0013/ hourly.2017-05-15_1106/
daily.2017-05-15_0012/ hourly.2017-05-15_1206/
hourly.2017-05-15_1006/ hourly.2017-05-15_1306/
```

Cada subdirectorio contiene los archivos a los que hace referencia la copia snapshot. Si los usuarios eliminan o sobrescriben accidentalmente un archivo, pueden restaurarlo al directorio primario de lectura y escritura copiando el archivo desde el subdirectorio Snapshot al directorio de lectura y escritura:

```
$ ls my.txt
ls: my.txt: No such file or directory
$ ls .snapshot
daily.2017-05-14_0013/ hourly.2017-05-15_1106/
daily.2017-05-15_0012/ hourly.2017-05-15_1206/
hourly.2017-05-15_1006/ hourly.2017-05-15_1306/
$ ls .snapshot/hourly.2017-05-15_1306/my.txt
my.txt
$ cp .snapshot/hourly.2017-05-15_1306/my.txt .
$ ls my.txt
my.txt
```

### Habilitar y deshabilitar el acceso de clientes NFS y SMB al directorio de copia Snapshot

Para determinar si el directorio de copia Snapshot es visible para los clientes NFS y SMB para restaurar un archivo o LUN de una copia Snapshot, puede habilitar y deshabilitar el acceso al directorio de la copia Snapshot con el `-snapdir-access` opción de `volume modify` comando.

### Pasos

## 1. Compruebe el estado de acceso al directorio de Snapshot:

```
volume show -vserver SVM_name -volume vol_name -fields snapdir-access
```

Ejemplo:

```
clus1::> volume show -vserver vs0 -volume vol1 -fields snapdir-access
vserver volume snapdir-access

vs0 vol1 false
```

## 2. Habilite o deshabilite el acceso al directorio de copia Snapshot:

```
volume modify -vserver SVM_name -volume vol_name -snapdir-access true|false
```

En el ejemplo siguiente se habilita el acceso al directorio de copia Snapshot en vol1:

```
clus1::> volume modify -vserver vs0 -volume vol1 -snapdir-access true
Volume modify successful on volume vol1 of Vserver vs0.
```

## Restaurar un solo archivo de una copia Snapshot

Puede utilizar el `volume snapshot restore-file` Comando para restaurar un solo archivo o LUN desde una copia Snapshot. Es posible restaurar el archivo a otra ubicación en el volumen primario de lectura y escritura si no desea reemplazar un archivo existente.

### Acerca de esta tarea

Si va a restaurar una LUN existente, se crea un clon de LUN y se realiza un backup en forma de copia Snapshot. Durante la operación de restauración, puede leer la LUN y escribir en ella.

Los archivos con flujos se restauran de forma predeterminada.

### Pasos

#### 1. Enumere las copias Snapshot en un volumen:

```
volume snapshot show -vserver SVM -volume volume
```

Para obtener una sintaxis de comando completa, consulte la página `man`.

El ejemplo siguiente muestra las copias Snapshot en `vol1`:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1
```

| Vserver | Volume | Snapshot               | State | Size  | Total% | Used% |
|---------|--------|------------------------|-------|-------|--------|-------|
| vs1     | vol1   | hourly.2013-01-25_0005 | valid | 224KB | 0%     | 0%    |
|         |        | daily.2013-01-25_0010  | valid | 92KB  | 0%     | 0%    |
|         |        | hourly.2013-01-25_0105 | valid | 228KB | 0%     | 0%    |
|         |        | hourly.2013-01-25_0205 | valid | 236KB | 0%     | 0%    |
|         |        | hourly.2013-01-25_0305 | valid | 244KB | 0%     | 0%    |
|         |        | hourly.2013-01-25_0405 | valid | 244KB | 0%     | 0%    |
|         |        | hourly.2013-01-25_0505 | valid | 244KB | 0%     | 0%    |

7 entries were displayed.

## 2. Restaurar un archivo desde una copia Snapshot:

```
volume snapshot restore-file -vserver SVM -volume volume -snapshot snapshot
-path file_path -restore-path destination_path
```

Para obtener una sintaxis de comando completa, consulte la página man.

En el siguiente ejemplo se restaura el archivo `myfile.txt`:

```
cluster1::> volume snapshot restore-file -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010 -path /myfile.txt
```

### Restaurar parte de un archivo desde una copia snapshot

Puede utilizar el `volume snapshot partial-restore-file` Comando para restaurar un rango de datos desde una copia Snapshot a una LUN o un archivo de contenedor NFS o SMB, suponiendo que se conozca el desplazamiento de bytes de inicio de los datos y el número de bytes. Este comando puede usarse para restaurar una de las bases de datos en un host que almacena varias bases de datos en el mismo LUN.

A partir de ONTAP 9.12.1, hay una restauración parcial disponible para los volúmenes en una relación de SM-BC.

### Pasos

1. Enumere las copias Snapshot en un volumen:

```
volume snapshot show -vserver SVM -volume volume
```

Para obtener una sintaxis de comando completa, consulte la página man.

El ejemplo siguiente muestra las copias Snapshot en `vol1`:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1
```

| Vserver | Volume | Snapshot               | State | Size  | Total% | Used% |
|---------|--------|------------------------|-------|-------|--------|-------|
| vs1     | vol1   | hourly.2013-01-25_0005 | valid | 224KB | 0%     | 0%    |
|         |        | daily.2013-01-25_0010  | valid | 92KB  | 0%     | 0%    |
|         |        | hourly.2013-01-25_0105 | valid | 228KB | 0%     | 0%    |
|         |        | hourly.2013-01-25_0205 | valid | 236KB | 0%     | 0%    |
|         |        | hourly.2013-01-25_0305 | valid | 244KB | 0%     | 0%    |
|         |        | hourly.2013-01-25_0405 | valid | 244KB | 0%     | 0%    |
|         |        | hourly.2013-01-25_0505 | valid | 244KB | 0%     | 0%    |

7 entries were displayed.

## 2. Restaurar parte de un archivo desde una copia Snapshot:

```
volume snapshot partial-restore-file -vserver SVM -volume volume -snapshot
snapshot -path file_path -start-byte starting_byte -byte-count byte_count
```

El desplazamiento de bytes de inicio y el número de bytes deben ser múltiplos de 4,096.

En el ejemplo siguiente se restauran los primeros 4,096 bytes del archivo `myfile.txt`:

```
cluster1::> volume snapshot partial-restore-file -vserver vs0 -volume
vol1 -snapshot daily.2013-01-25_0010 -path /myfile.txt -start-byte 0
-byte-count 4096
```

## Restaure el contenido de un volumen de una copia Snapshot

Puede utilizar el `volume snapshot restore` Comando para restaurar el contenido de un volumen desde una copia Snapshot.

### Acerca de esta tarea

Si el volumen tiene relaciones de SnapMirror, replique manualmente todas las copias de reflejo del volumen inmediatamente después de restaurar desde una copia de Snapshot. Si no lo hace, puede provocar copias reflejadas inutilizables que se deban eliminar y volver a crear.

## 1. Enumere las copias Snapshot en un volumen:

```
volume snapshot show -vserver SVM -volume volume
```

El ejemplo siguiente muestra las copias Snapshot en `vol1`:

```
clus1::> volume snapshot show -vserver vs1 -volume voll
```

| Vserver | Volume | Snapshot               | State | Size  | Total% | Used% |
|---------|--------|------------------------|-------|-------|--------|-------|
| vs1     | voll   | hourly.2013-01-25_0005 | valid | 224KB | 0%     | 0%    |
|         |        | daily.2013-01-25_0010  | valid | 92KB  | 0%     | 0%    |
|         |        | hourly.2013-01-25_0105 | valid | 228KB | 0%     | 0%    |
|         |        | hourly.2013-01-25_0205 | valid | 236KB | 0%     | 0%    |
|         |        | hourly.2013-01-25_0305 | valid | 244KB | 0%     | 0%    |
|         |        | hourly.2013-01-25_0405 | valid | 244KB | 0%     | 0%    |
|         |        | hourly.2013-01-25_0505 | valid | 244KB | 0%     | 0%    |

7 entries were displayed.

## 2. Restaure el contenido de un volumen de una copia Snapshot:

```
volume snapshot restore -vserver SVM -volume volume -snapshot snapshot
```

En el ejemplo siguiente se restaura el contenido de voll:

```
cluster1::> volume snapshot restore -vserver vs0 -volume voll -snapshot
daily.2013-01-25_0010
```

# Replicación de volúmenes de SnapMirror

## Conceptos básicos de la recuperación ante desastres de SnapMirror asíncrono

*SnapMirror* es la tecnología de recuperación ante desastres diseñada para la conmutación al nodo de respaldo del almacenamiento principal al secundario en un sitio geográficamente remoto. Como su nombre indica, SnapMirror crea una réplica, o *mirror*, de sus datos de trabajo en el almacenamiento secundario desde el cual puede continuar proporcionando datos en caso de catástrofe en el sitio principal.

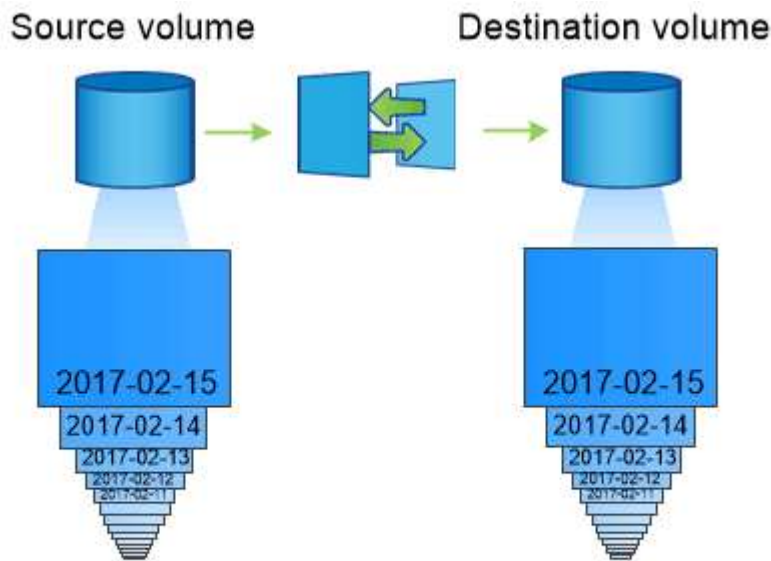
Si el sitio primario sigue disponible para servir datos, sólo tiene que transferir cualquier dato que necesite y no facilitar el servicio a los clientes del espejo. Como se indica en el caso de uso de conmutación por error, las controladoras del sistema secundario deben ser equivalentes o casi equivalentes a las controladoras del sistema primario para servir datos de forma eficiente desde el almacenamiento reflejado.

## Relaciones de protección de datos

Los datos se reflejan en el nivel de volumen. La relación entre el volumen de origen del almacenamiento primario y el volumen de destino del almacenamiento secundario se denomina «relación de protección de datos». Los clústeres en los que residen los volúmenes y las SVM que sirven datos de los volúmenes deben tener una relación entre iguales. Una relación entre iguales permite que los clústeres y las SVM se intercambien datos con seguridad.

## "Relaciones entre iguales de clústeres y SVM"

La siguiente figura muestra las relaciones de protección de datos de SnapMirror.



*A SnapMirror data protection relationship typically mirrors the Snapshot copies available on the source volume.*

### Ámbito de las relaciones de protección de datos

Puede crear una relación de protección de datos directamente entre los volúmenes o entre las SVM que poseen los volúmenes. En una relación de protección de datos \_SVM, se replica toda la configuración de SVM o parte de ella, desde las exportaciones NFS y los recursos compartidos de SMB a RBAC, así como los datos de los volúmenes que posee la SVM.

También puede utilizar SnapMirror para aplicaciones especiales de protección de datos:

- Una copia *mirror* de uso compartido de la carga del volumen raíz de la SVM garantiza que los datos permanecen accesibles en caso de interrupción del servicio o conmutación por error de un nodo.
- Una relación de protección de datos entre *SnapLock Volumes* permite replicar los archivos WORM en el almacenamiento secundario.

### "Archivado y cumplimiento de normativas con tecnología SnapLock"

- A partir de ONTAP 9.13.1, se puede utilizar SnapMirror asíncrono para proteger [grupos de consistencia](#). A partir de ONTAP 9.14.1, se puede utilizar SnapMirror asíncrono para replicar copias Snapshot granulares de volúmenes en el clúster de destino mediante la relación del grupo de coherencia. Para obtener más información, consulte [Configurar la protección asíncrona de SnapMirror](#).

### Cómo se inicializan las relaciones de protección de datos de SnapMirror

La primera vez que se invoca SnapMirror, se realiza una transferencia *baseline* del volumen de origen al volumen de destino. La directiva *SnapMirror* de la relación define el contenido de la línea base y las actualizaciones.

Transferencia completa con la política de SnapMirror predeterminada `MirrorAllSnapshots` implica los siguientes pasos:

- Haga una copia Snapshot del volumen de origen.
- Transfiera la copia Snapshot y todos los bloques de datos que hace referencia al volumen de destino.
- Transferir las copias snapshot restantes y menos recientes del volumen de origen al volumen de destino para su uso en caso de que el espejo «activo» esté dañado.

### Cómo se actualizan las relaciones de protección de datos de SnapMirror

Las actualizaciones son asíncronas, según la programación configurada. La retención refleja la política de Snapshot en el origen.

En cada actualización bajo MirrorAllSnapshots Política, SnapMirror crea una copia Snapshot del volumen de origen y transfiere esa copia Snapshot y todas las copias Snapshot que se hayan realizado desde la última actualización. En el siguiente resultado de la `snapmirror policy show` comando para MirrorAllSnapshots política, tenga en cuenta lo siguiente:

- Create Snapshot es «verdadero», lo que lo indica MirrorAllSnapshots Crea una copia Snapshot cuando SnapMirror actualiza la relación.
- MirrorAllSnapshots Dispone de las reglas «m\_creado» y «all\_source\_snapshots», lo cual indica que tanto la copia snapshot creada por SnapMirror como cualquier copia snapshot realizada desde la última actualización se transfieren cuando SnapMirror actualiza la relación.

```
cluster_dst:> snapmirror policy show -policy MirrorAllSnapshots -instance

Vserver: vs0
SnapMirror Policy Name: MirrorAllSnapshots
SnapMirror Policy Type: async-mirror
Policy Owner: cluster-admin
Tries Limit: 8
Transfer Priority: normal
Ignore accesstime Enabled: false
Transfer Restartability: always
Network Compression Enabled: false
Create Snapshot: true
Comment: Asynchronous SnapMirror policy for mirroring
all snapshots
and the latest active file system.
Total Number of Rules: 2
Total Keep: 2
Rules: SnapMirror Label Keep Preserve Warn
Schedule Prefix

sm_created 1 false 0 -
all_source_snapshots 1 false 0 -
```

Política de MirrorLatest

Preconfigurados MirrorLatest la política funciona exactamente de la misma manera que MirrorAllSnapshots, Excepto que sólo la copia snapshot creada por SnapMirror se transfiere al inicializar y actualizar.

|          |        | Rules: SnapMirror Label | Keep | Preserve | Warn |
|----------|--------|-------------------------|------|----------|------|
| Schedule | Prefix |                         |      |          |      |
| -----    | -----  | -----                   | ---- | -----    | ---- |
| -        |        | sm_created              | 1    | false    | 0 -  |

Conceptos básicos de la recuperación ante desastres de SnapMirror Synchronous

A partir de ONTAP 9.5, la tecnología SnapMirror síncrono (SM-S) es compatible con todas las plataformas FAS y AFF que tengan al menos 16 GB de memoria y en todas las plataformas ONTAP Select. La tecnología SnapMirror Synchronous es una función con licencia por nodo que proporciona replicación de datos síncrona a nivel de volumen.

Esta funcionalidad aborda las normativas regulatorias y nacionales para la replicación síncrona en sectores financieros, sanitarios y otros regulados, en los que no es necesaria una pérdida de datos nula.

Operaciones síncronas de SnapMirror permitidas

El límite del número de operaciones de replicación síncrona de SnapMirror por par de alta disponibilidad depende del modelo de controladora.

En la siguiente tabla, se enumera el número de operaciones de SnapMirror Synchronous que se permiten por par de alta disponibilidad en función del tipo de plataforma y la versión ONTAP.

| Plataforma   | Versiones anteriores a ONTAP 9.9.1 | ONTAP 9.9.1 | ONTAP 9.10.1 | ONTAP 9.11.1 a ONTAP 9.14.1 |
|--------------|------------------------------------|-------------|--------------|-----------------------------|
| AFF          | 80                                 | 160         | 200          | 400                         |
| ASA          | 80                                 | 160         | 200          | 400                         |
| FAS          | 40                                 | 80          | 80           | 80                          |
| ONTAP Select | 20                                 | 40          | 40           | 40                          |

Funciones admitidas

La siguiente tabla indica las funciones compatibles con SnapMirror Synchronous y las versiones de ONTAP que admiten.



| Función                                                                                                                                                                  | Se admite la primera versión | Información adicional                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Antivirus en el volumen primario de la relación de SnapMirror síncrono                                                                                                   | ONTAP 9,6                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Replicación de copia Snapshot creada por la aplicación                                                                                                                   | ONTAP 9,7                    | Si una copia Snapshot se etiqueta con la etiqueta correspondiente en el momento de la <code>snapshot create</code> Funcionamiento, mediante la interfaz de línea de comandos o la API de ONTAP, SnapMirror Synchronous replica las copias Snapshot, tanto las creadas por el usuario como las creadas con scripts externos, tras desactivar las aplicaciones. Las copias Snapshot programadas creadas con una política de Snapshot no se replican. Para obtener más información sobre la replicación de copias Snapshot creadas por la aplicación, consulte el artículo de la base de conocimientos: <a href="#">"Cómo replicar las copias Snapshot de aplicación creadas con SnapMirror Synchronous"</a> . |
| Clonar eliminación automática                                                                                                                                            | ONTAP 9,6                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Los agregados de FabricPool con política de organización en niveles de Ninguna, Snapshot o Automática son compatibles con el origen y el destino de SnapMirror síncrono. | ONTAP 9,5                    | El volumen de destino de un agregado de FabricPool no se puede establecer en la política de organización en niveles All.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| FC                                                                                                                                                                       | ONTAP 9,5                    | En todas las redes para las que la latencia no supere los 10ms ms                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| FC-NVMe                                                                                                                                                                  | ONTAP 9,7                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Clones de archivo                                                                                                                                                        | ONTAP 9,7                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| FPolicy en el volumen primario de la relación de SnapMirror síncrono                                                                                                     | ONTAP 9,6                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Cuotas duras y flexibles en el volumen principal de la relación síncrona de SnapMirror                                                                                   | ONTAP 9,6                    | Las reglas de cuota no se replican en el destino; por lo tanto, la base de datos de cuotas no se replica en el destino.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Relaciones síncronas dentro del clúster                                                                                                                                  | ONTAP 9.14.1                 | La alta disponibilidad se proporciona cuando los volúmenes de origen y de destino se encuentran en diferentes pares de alta disponibilidad. Si se desactiva todo el clúster, no será posible el acceso a los volúmenes hasta que se recupere el clúster. Las relaciones síncronas de SnapMirror dentro del clúster contribuirán al límite general de datos simultáneos <a href="#">Relaciones por pareja de alta disponibilidad</a> .                                                                                                                                                                                                                                                                       |
| ISCSI                                                                                                                                                                    | ONTAP 9,5                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Clones LUN y clones de espacio de nombres NVMe                                                                                                                           | ONTAP 9,7                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

|                                                                                            |              |                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------------------------------------------------------------|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Clones LUN respaldados por copias Snapshot creadas por la aplicación                       | ONTAP 9,7    |                                                                                                                                                                                                                                                                                                                                                                           |
| Acceso de protocolo mixto (NFS v3 y SMB)                                                   | ONTAP 9,6    |                                                                                                                                                                                                                                                                                                                                                                           |
| Restauración de NDMP/NDMP                                                                  | ONTAP 9.13.1 | El clúster de origen y de destino deben ejecutar ONTAP 9.13.1 o versiones posteriores para usar NDMP con SnapMirror síncrono. Para obtener más información, consulte <a href="#">Transferencia de datos mediante la copia ndmp</a> .                                                                                                                                      |
| Operaciones síncronas de SnapMirror (NDO) sin interrupciones en plataformas AFF/ASA, solo. | ONTAP 9.12.1 | La compatibilidad con operaciones no disruptivas le permite realizar muchas tareas de mantenimiento comunes sin necesidad de programar un tiempo de inactividad. Las operaciones admitidas incluyen la toma de control y el retorno al nodo primario, y el movimiento de volúmenes, siempre y cuando haya un solo nodo superviviente entre cada uno de los dos clústeres. |
| NFS v4,2                                                                                   | ONTAP 9.10.1 |                                                                                                                                                                                                                                                                                                                                                                           |
| NFS v4,3                                                                                   | ONTAP 9,5    |                                                                                                                                                                                                                                                                                                                                                                           |
| NFS v4,0                                                                                   | ONTAP 9,6    |                                                                                                                                                                                                                                                                                                                                                                           |
| NFS v4,1                                                                                   | ONTAP 9,6    |                                                                                                                                                                                                                                                                                                                                                                           |
| NVMe/TCP                                                                                   | 9.10.1       |                                                                                                                                                                                                                                                                                                                                                                           |
| Eliminación de una limitación elevada de la frecuencia de funcionamiento de metadatos      | ONTAP 9,6    |                                                                                                                                                                                                                                                                                                                                                                           |
| Seguridad para datos confidenciales en tránsito con cifrado TLS 1.2                        | ONTAP 9,6    |                                                                                                                                                                                                                                                                                                                                                                           |
| Restauración parcial de archivos y archivos individuales                                   | ONTAP 9.13.1 |                                                                                                                                                                                                                                                                                                                                                                           |
| SMB 2,0 o posterior                                                                        | ONTAP 9,6    |                                                                                                                                                                                                                                                                                                                                                                           |
| Cascada de reflejo-reflejo síncrono de SnapMirror                                          | ONTAP 9,6    | La relación del volumen de destino de la relación de SnapMirror síncrono debe ser una relación de SnapMirror asíncrono.                                                                                                                                                                                                                                                   |

|                                                                           |              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------------------------------------------------|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Recuperación ante desastres de SVM                                        | ONTAP 9,6    | <p>* Un origen de SnapMirror Synchronous también puede ser un origen de recuperación ante desastres de SVM, por ejemplo, una configuración ramificada con SnapMirror Synchronous como un tramo y recuperación ante desastres de SVM como el otro.</p> <p>* Un origen de SnapMirror Synchronous no puede ser un destino de recuperación ante desastres de SVM porque SnapMirror Synchronous no admite la configuración en cascada de un origen de protección de datos.<br/>Debe liberar la relación síncrona antes de ejecutar un cambio de sincronización de recuperación ante desastres de SVM en el clúster de destino.</p> <p>* Un destino de SnapMirror síncrono no puede ser un origen de recuperación ante desastres de SVM porque la recuperación ante desastres de SVM no admite la replicación de volúmenes de DP.<br/>Una resincronización flip del origen síncrono provocaría la recuperación ante desastres de SVM excepto el volumen DP en el clúster de destino.</p> |
| Restauración basada en cinta al volumen de origen                         | ONTAP 9.13.1 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Paridad de marca de hora entre los volúmenes de origen y destino para NAS | ONTAP 9,6    | Si se actualizó de ONTAP 9,5 a ONTAP 9,6, la marca de tiempo se replica solo para todos los archivos nuevos y modificados en el volumen de origen. La Marca de hora de los archivos existentes en el volumen de origen no está sincronizada.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## Funciones no admitidas

Las siguientes funciones no se admiten con las relaciones de SnapMirror síncrono:

- Grupos de consistencia
- Sistemas DPO optimizados para DP
- Volúmenes de FlexGroup
- Volúmenes de FlexCache
- Limitación global
- En una configuración de dispersión, solo una relación puede ser una relación de SnapMirror síncrono; todas las demás relaciones del volumen de origen deben ser relaciones de SnapMirror asíncronas.
- Movimiento de LUN
- Configuraciones de MetroCluster
- Acceso SAN y NVMe mixto  
El mismo volumen o SVM no admiten espacios de nombres LUN y NVMe.
- SnapCenter
- Volúmenes de SnapLock

- Copias Snapshot a prueba de manipulaciones
- Backup a cinta o restauración con volcado y SMTape en el volumen de destino
- Piso de rendimiento (QoS mín.) para volúmenes de origen
- SnapRestore de volumen
- VVol

## Modos de funcionamiento

SnapMirror Synchronous tiene dos modos de funcionamiento basados en el tipo de política de SnapMirror utilizada:

### • Modo de sincronización

En el modo de sincronización, las operaciones de I/O de la aplicación se envían en paralelo al primario y el secundario

sistemas de almacenamiento. Si la escritura en el almacenamiento secundario no se realiza por ningún motivo, se permite que la aplicación continúe escribiendo en el almacenamiento principal. Una vez corregida la condición de error, la tecnología SnapMirror Synchronous vuelve a sincronizar automáticamente con el almacenamiento secundario y reanuda la replicación del almacenamiento principal al almacenamiento secundario en modo síncrono.

En el modo síncrono, RPO=0 y RTO son muy bajos hasta que se produce un fallo de replicación secundaria en el momento en el que el objetivo de punto de recuperación y el objetivo de tiempo de recuperación se vuelven indeterminados, pero igual que el tiempo para reparar el problema que provocó un error en la replicación secundaria y para finalizar la resincronización.

### • Modo StrictSync

SnapMirror Synchronous puede funcionar opcionalmente en el modo StrictSync. Si la escritura en el almacenamiento secundario no se completa por ningún motivo, las operaciones de I/O de la aplicación fallan y, por lo tanto, se garantiza que el almacenamiento primario y secundario sean idénticos. Las operaciones de I/O de la aplicación en el principal se reanudan solo una vez que la relación de SnapMirror se devuelve a la InSync estado. Si falla el almacenamiento primario, se pueden reanudar las operaciones de I/O de la aplicación en el almacenamiento secundario después de la conmutación por error, sin pérdida de datos.

En el modo StrictSync, el objetivo de punto de recuperación es siempre cero y el objetivo de tiempo de recuperación es muy bajo.

## Estado de la relación

El estado de una relación de SnapMirror Synchronous siempre está en la InSync estado durante el funcionamiento normal. Si por algún motivo la transferencia de SnapMirror falla, el destino no está sincronizado con el origen y puede ir a la OutofSync estado.

Para las relaciones de SnapMirror Synchronous, el sistema comprueba automáticamente el estado de la relación (InSync o OutofSync) a un intervalo fijo. Si el estado de la relación es OutofSync, ONTAP activa automáticamente el proceso de resincronización automática para devolver la relación al InSync estado. La resincronización automática se activa solo si la transferencia falla debido a alguna operación, como la conmutación por error no planificada del almacenamiento en el origen o en el destino, o una interrupción del servicio de red. Operaciones iniciadas por el usuario como, por ejemplo `snapmirror quiesce y.. snapmirror break` no active la resincronización automática.

Si el estado de la relación es OutofSync Para una relación de SnapMirror Synchronous en el modo StrictSync, se detienen todas las operaciones de I/O del volumen primario. La OutofSync el estado de la relación SnapMirror Synchronous en el modo Sync no genera interrupciones en el volumen primario, y se

permiten las operaciones de I/O en el volumen primario.

#### Información relacionada

["Informe técnico de NetApp 4733: Prácticas recomendadas y configuración de SnapMirror síncrono"](#)

## Acerca de las cargas de trabajo compatibles con las políticas de StrictSync y Sync

Las políticas de StrictSync y Sync admiten todas las aplicaciones basadas en LUN con los protocolos FC, iSCSI y FC-NVMe, así como los protocolos NFSv3 y NFSv4 para aplicaciones empresariales como bases de datos, VMware, Quota, SMB, etc. A partir de ONTAP 9.6, SnapMirror Synchronous se puede utilizar para servicios de archivos empresariales como los de automatización de diseño electrónico (EDA), directorios iniciales y cargas de trabajo de creación de software.

En ONTAP 9.5, para una política de sincronización, debe tener en cuenta algunos aspectos importantes a la vez que selecciona las cargas de trabajo NFSv3 o NFSv4. No se tiene en cuenta la cantidad de datos que realizan las operaciones de lectura o escritura por parte de las cargas de trabajo, ya que la política de sincronización puede gestionar cargas de trabajo de lectura o escritura elevadas. En ONTAP 9.5, las cargas de trabajo que tienen una creación de archivos, una creación de directorios, cambios de permisos de archivos o cambios de permisos de directorio pueden no ser adecuadas (estas se denominan cargas de trabajo con metadatos elevados). Un ejemplo típico de una carga de trabajo con metadatos altos es una carga de trabajo de DevOps en la que se crean varios archivos de prueba, se ejecuta la automatización y se eliminan los archivos. Otro ejemplo es la carga de trabajo de compilación paralela que genera varios archivos temporales durante la compilación. El impacto de una tasa alta de la actividad de metadatos de escritura es que puede provocar que la sincronización entre los reflejos se rompa temporalmente, lo que bloquea la I/O de lectura y escritura del cliente.

A partir de ONTAP 9.6, se eliminan estas limitaciones y se puede utilizar SnapMirror Synchronous para las cargas de trabajo de servicios de archivos empresariales que incluyen entornos de varios usuarios, como directorios iniciales y cargas de trabajo de compilación de software.

#### Información relacionada

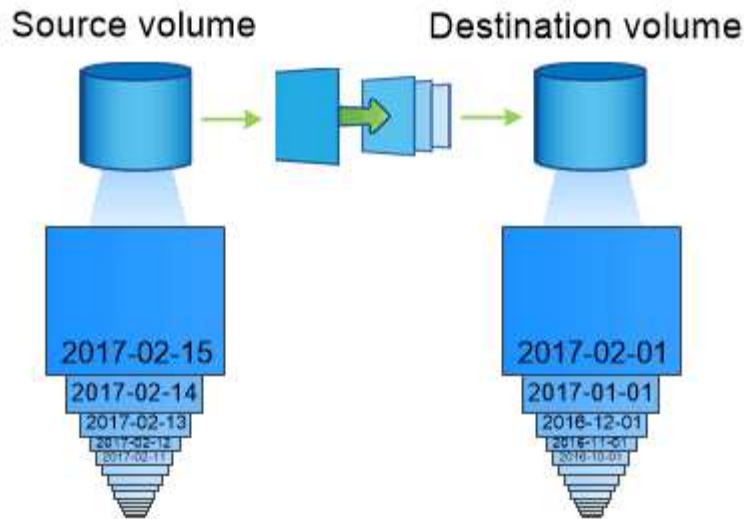
["Configuración síncrona de SnapMirror y prácticas recomendadas"](#)

## Archivado de vault con tecnología SnapMirror

Las políticas de almacén de SnapMirror sustituyen a la tecnología SnapVault en ONTAP 9.3 y versiones posteriores. Se utiliza una política de almacén de SnapMirror para la replicación de copias Snapshot de disco a disco para el cumplimiento de normativas y otros fines relacionados con la gobernanza. A diferencia de la relación de SnapMirror, en la que el destino normalmente solo contiene las copias Snapshot que actualmente se encuentran en el volumen de origen, un destino de almacén normalmente conserva las copias Snapshot puntuales creadas durante un período mucho más largo.

Es posible que desee conservar copias Snapshot mensuales de sus datos en un plazo de 20 años, por ejemplo, para cumplir con las normativas de contabilidad gubernamental de su empresa. Como no hay necesidad de servir datos desde un almacenamiento de almacén, puede utilizar discos más lentos y menos costosos en el sistema de destino.

La siguiente figura muestra las relaciones de protección de datos de SnapMirror Vault.



*A SnapVault data protection relationship typically retains point-in-time Snapshot copies created over a longer period than the Snapshot copies on the source volume.*

### Cómo se inicializan las relaciones de protección de datos del almacén

La política de SnapMirror para la relación define el contenido de la línea de base y cualquier actualización.

Una transferencia de línea de base en la política de almacén predeterminada `XDPDefault` Realiza una copia Snapshot del volumen de origen, luego transfiere esa copia y los bloques de datos que hace referencia al volumen de destino. A diferencia de las relaciones de SnapMirror, un backup de almacén no incluye copias Snapshot anteriores en la base.

### Cómo se actualizan las relaciones de protección de datos de almacén

Las actualizaciones son asíncronas, según la programación configurada. Las reglas que defina en la política para la relación identifican qué nuevas copias Snapshot deben incluir en las actualizaciones y cuántas copias deben retener. Las etiquetas definidas en la política ("mensual", por ejemplo) deben coincidir con una o más etiquetas definidas en la política de Snapshot en la fuente. De lo contrario, la replicación falla.

En cada actualización bajo `XDPDefault` Política, SnapMirror transfiere copias Snapshot que se han realizado desde la última actualización, siempre que tengan las etiquetas que coincidan con las etiquetas definidas en las reglas de la política. En el siguiente resultado de la `snapmirror policy show` comando para `XDPDefault` política, tenga en cuenta lo siguiente:

- `Create Snapshot` es «falso», lo que lo indica `XDPDefault` No crea una copia Snapshot cuando SnapMirror actualiza la relación.
- `XDPDefault` Dispone de reglas «diaria» y «semanal», que indican que todas las copias Snapshot con etiquetas coincidentes del origen se transfieren cuando SnapMirror actualiza la relación.

```
cluster_dst:> snapmirror policy show -policy XDPDefault -instance

 Vserver: vs0
SnapMirror Policy Name: XDPDefault
SnapMirror Policy Type: vault
 Policy Owner: cluster-admin
 Tries Limit: 8
 Transfer Priority: normal
Ignore accesstime Enabled: false
 Transfer Restartability: always
Network Compression Enabled: false
 Create Snapshot: false
 Comment: Default policy for XDP relationships with
daily and weekly
 rules.
 Total Number of Rules: 2
 Total Keep: 59
 Rules: SnapMirror Label Keep Preserve Warn
Schedule Prefix

 daily 7 false 0 -
-
 weekly 52 false 0 -
-
```

## Conceptos básicos de la replicación unificada de SnapMirror

SnapMirror *Unified replication* permite configurar la recuperación ante desastres y el archivado en el mismo volumen de destino. Cuando la replicación unificada es apropiada, ofrece ventajas en la reducción de la cantidad de almacenamiento secundario que se necesita, lo que limita el número de transferencias básicas y reduce el tráfico de red.

### Cómo se inicializan las relaciones de protección de datos unificadas

Al igual que sucede con SnapMirror, la protección de datos unificada realiza una transferencia de referencia la primera vez que se invoca. La política de SnapMirror para la relación define el contenido de la línea de base y cualquier actualización.

Una transferencia completa con la política de protección de datos unificada predeterminada MirrorAndVault Realiza una copia Snapshot del volumen de origen, luego transfiere esa copia y los bloques de datos que hace referencia al volumen de destino. Al igual que el archivado de almacenes, la protección de datos unificada no incluye copias Snapshot anteriores en la referencia.

Cómo se actualizan las relaciones de protección de datos unificadas

En cada actualización bajo MirrorAndVault Política, SnapMirror crea una copia Snapshot del volumen de origen y transfiere esa copia Snapshot y todas las copias Snapshot que se hayan realizado desde la última actualización, siempre que tengan las etiquetas que coincidan con los definidos en las reglas de la política de Snapshot. En el siguiente resultado de la snapmirror policy show comando para MirrorAndVault política, tenga en cuenta lo siguiente:

- Create Snapshot es «verdadero», lo que lo indica MirrorAndVault Crea una copia Snapshot cuando SnapMirror actualiza la relación.
- MirrorAndVault Dispone de las reglas «m\_creado», «diario» y «semanal», que indican que tanto la copia snapshot creada por SnapMirror como las copias Snapshot con etiquetas coincidentes en el origen se transfieren cuando SnapMirror actualiza la relación.

```
cluster_dst::> snapmirror policy show -policy MirrorAndVault -instance

 Vserver: vs0
 SnapMirror Policy Name: MirrorAndVault
 SnapMirror Policy Type: mirror-vault
 Policy Owner: cluster-admin
 Tries Limit: 8
 Transfer Priority: normal
Ignore accesstime Enabled: false
 Transfer Restartability: always
Network Compression Enabled: false
 Create Snapshot: true
 Comment: A unified Synchronous SnapMirror and
SnapVault policy for
 mirroring the latest file system and daily
and weekly snapshots.
 Total Number of Rules: 3
 Total Keep: 59
 Rules: SnapMirror Label Keep Preserve Warn
Schedule Prefix

- sm_created 1 false 0 -
- daily 7 false 0 -
- weekly 52 false 0 -
-
```

Política Unified7year

Preconfigurados Unified7year la política funciona exactamente de la misma manera que MirrorAndVault, Excepto que una cuarta regla transfiere copias snapshot mensuales y las conserva



durante siete años.

| Schedule Prefix | Rules: SnapMirror Label | Keep | Preserve | Warn |
|-----------------|-------------------------|------|----------|------|
| -----           | -----                   | ---- | -----    | ---- |
| -               | sm_created              | 1    | false    | 0 -  |
| -               | daily                   | 7    | false    | 0 -  |
| -               | weekly                  | 52   | false    | 0 -  |
| -               | monthly                 | 84   | false    | 0 -  |
| -               |                         |      |          |      |

### Proporcionar protección frente a una posible corrupción de datos

La replicación unificada limita el contenido de la transferencia básica a la copia de Snapshot creada por SnapMirror en el momento de la inicialización. En cada actualización, SnapMirror crea otra copia Snapshot del origen y transfiere esa copia Snapshot y todas las copias Snapshot nuevas que tengan las etiquetas que coincidan con los definidos en las reglas de la política de Snapshot.

Puede protegerse contra la posibilidad de que una copia Snapshot actualizada esté dañada al crear una copia de la última copia Snapshot transferida en el destino. Esta «copia local» se conserva independientemente de las reglas de retención del origen, de modo que, aunque la copia Snapshot transferida mediante SnapMirror ya no esté disponible en el origen, dicha copia estará disponible en el destino.

### Cuándo utilizar la replicación de datos unificada

Debe sopesar las ventajas que supone mantener una copia completa frente a las ventajas que ofrece la replicación unificada para reducir la cantidad de almacenamiento secundario, limitar el número de transferencias básicas y reducir el tráfico de red.

El factor clave para determinar la idoneidad de la replicación unificada es la tasa de cambio del sistema de archivos activo. Un reflejo tradicional puede ser más adecuado para un volumen que contiene copias Snapshot cada hora de los registros de transacciones de las bases de datos, por ejemplo.

### XDP sustituye a DP como la opción predeterminada de SnapMirror

A partir de ONTAP 9.3, el modo de protección de datos ampliada (XDP) de SnapMirror sustituye al modo de protección de datos (DP) de SnapMirror como valor predeterminado.

Antes de actualizar a ONTAP 9.12.1, debe convertir las relaciones de tipo DP existentes a XDP antes de poder actualizar a ONTAP 9.12.1 y versiones posteriores. Para obtener más información, consulte ["Convierta una relación de tipo DP existente a XDP"](#).

Hasta ONTAP 9.3, SnapMirror invocado en modo DP y SnapMirror invocado en modo XDP utilizaba distintos motores de replicación, con distintos enfoques respecto a la dependencia de versión:

- SnapMirror que se invoca en el modo DP utilizaba un motor de replicación *version-dependent* en el que la versión de ONTAP debía ser la misma en el almacenamiento primario y secundario:

```
cluster_dst::> snapmirror create -type DP -source-path ... -destination
-path ...
```

- SnapMirror, al que se invocó en el modo XDP, utilizó un motor de replicación de *version-flexible* que admitía diferentes versiones de ONTAP en el almacenamiento primario y secundario:

```
cluster_dst::> snapmirror create -type XDP -source-path ...
-destination-path ...
```

Las importantes ventajas de SnapMirror, que ofrece una versión flexible, superan la ligera ventaja del rendimiento de la replicación obtenido con el modo basado en la versión. Por este motivo, a partir de ONTAP 9.3, se ha creado el modo XDP como nuevo valor predeterminado, y cualquier invocación del modo DP en la línea de comandos o en scripts nuevos o existentes se convierte automáticamente al modo XDP.

Las relaciones existentes no se ven afectadas. Si una relación ya es del tipo DP, seguirá siendo del tipo DP. A partir de ONTAP 9.5, MirrorAndVault es la nueva política predeterminada cuando no se especifica ningún modo de protección de datos o cuando se especifica el modo XDP como tipo de relación. La siguiente tabla muestra el comportamiento que puede esperar.

| Si especifica...    | El tipo es... | La política predeterminada (si no se especifica una política) es... |
|---------------------|---------------|---------------------------------------------------------------------|
| PROTECCIÓN DE DATOS | XDP           | MirrorAllSnapshots (recuperación ante desastres de SnapMirror)      |
| Nada                | XDP           | MirrorAndVault (replicación unificada)                              |
| XDP                 | XDP           | MirrorAndVault (replicación unificada)                              |

Como se muestra en la tabla, las directivas predeterminadas asignadas a XDP en circunstancias diferentes garantizan que la conversión mantenga la equivalencia funcional de los tipos antiguos. Por supuesto, puede utilizar diferentes políticas según sea necesario, incluidas las políticas para la replicación unificada:

| Si especifica...      | Y la política es... | El resultado es...                        |
|-----------------------|---------------------|-------------------------------------------|
| PROTECCIÓN DE DATOS   | MirrorAllSnapshots  | Recuperación ante desastres de SnapMirror |
| XDPDefault            | SnapVault           | Reflejo de AndVault                       |
| Replicación unificada | XDP                 | MirrorAllSnapshots                        |

|                                           |            |           |
|-------------------------------------------|------------|-----------|
| Recuperación ante desastres de SnapMirror | XDPDefault | SnapVault |
|-------------------------------------------|------------|-----------|

Las únicas excepciones a la conversión son las siguientes:

- Las relaciones de protección de datos de SVM siguen siendo las predeterminadas para el modo DP en ONTAP 9.3 y versiones anteriores.

A partir de ONTAP 9.4, las relaciones de protección de datos de la SVM se establecen en el modo XDP de manera predeterminada.

- Las relaciones de protección de datos con uso compartido de carga de volumen raíz continúan hasta los valores predeterminados en el modo DP.
- Las relaciones de protección de datos de SnapLock continúan en el modo DP de ONTAP 9.4 y versiones anteriores.

A partir de ONTAP 9.5, las relaciones de protección de datos de SnapLock se establecen en el modo XDP de manera predeterminada.

- Las invocaciones explícitas de DP siguen en el modo DP de forma predeterminada si establece la siguiente opción para todo el clúster:

```
options replication.create_data_protection_rels.enable on
```

Esta opción se ignora si no invoca explícitamente DP.

## Cuando un volumen de destino aumenta automáticamente

Durante una transferencia de mirroring para la protección de datos, el volumen de destino aumenta automáticamente su tamaño si se ha incrementado el volumen de origen, siempre y cuando haya espacio disponible en el agregado que contiene el volumen.

Este comportamiento se produce independientemente de cualquier configuración de crecimiento automático en el destino. No es posible limitar el crecimiento del volumen ni evitar que ONTAP lo haga.

De manera predeterminada, los volúmenes de protección de datos se establecen en `grow_shrink` el modo `autosize`, que permite que el volumen crezca o se reduzca en respuesta a la cantidad de espacio usado. El tamaño máximo automático de los volúmenes de protección de datos es igual al tamaño máximo de FlexVol y depende de la plataforma. Por ejemplo:

- FAS6220, volumen DP predeterminado máx.-autosize = 70 TB
- FAS8200, volumen DP predeterminado máx.-autosize = 100 TB

Para obtener más información, consulte ["Hardware Universe de NetApp"](#).

## Puestas en marcha de protección de datos en cascada y distribución ramificada

Puede utilizar una implementación de *fan-out* para ampliar la protección de datos a

varios sistemas secundarios. Puede utilizar una implementación *Cascade* para ampliar la protección de datos a sistemas terciarios.

Tanto las puestas en marcha en cascada como de distribución ramificada admiten cualquier combinación de recuperación ante desastres de SnapMirror, SnapVault o replicación unificada. Sin embargo, las relaciones de SnapMirror síncrono (compatibles a partir de ONTAP 9.5) solo admiten puestas en marcha en cascada con una o más relaciones de SnapMirror asíncronas y no admiten puestas en marcha en cascada. Solo una relación en la configuración de dispersión puede ser una relación de SnapMirror síncrono, todas las demás relaciones del volumen de origen deben ser relaciones de SnapMirror asíncronas. [Continuidad del negocio de SnapMirror](#) (Se admite a partir de ONTAP 9.8) también admite configuraciones de dispersión.



Puede utilizar una implementación *fan-in* para crear relaciones de protección de datos entre varios sistemas principales y un único sistema secundario. Cada relación debe usar un volumen diferente en el sistema secundario.

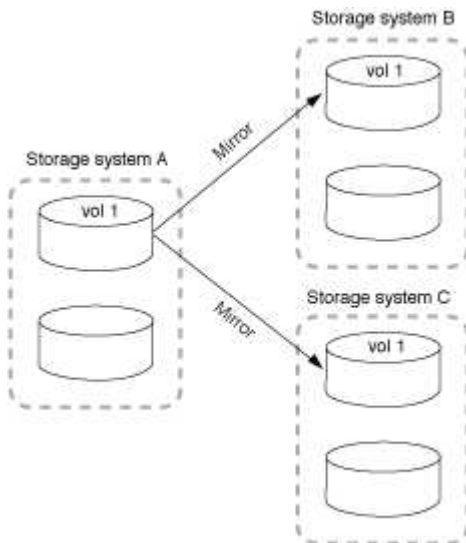


Debe saber que los volúmenes que forman parte de una configuración ramificada o en cascada pueden tardar más en resincronizar. No es poco frecuente ver los informes de relaciones de SnapMirror el estado de preparación para un período de tiempo extendido.

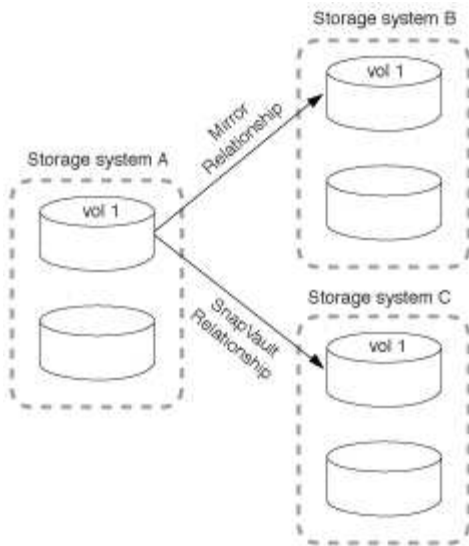
### Cómo funcionan las implementaciones de dispersión

SnapMirror admite la puesta en marcha de «varios duplicados\_ y de «mirror-vault» con «fan-out».

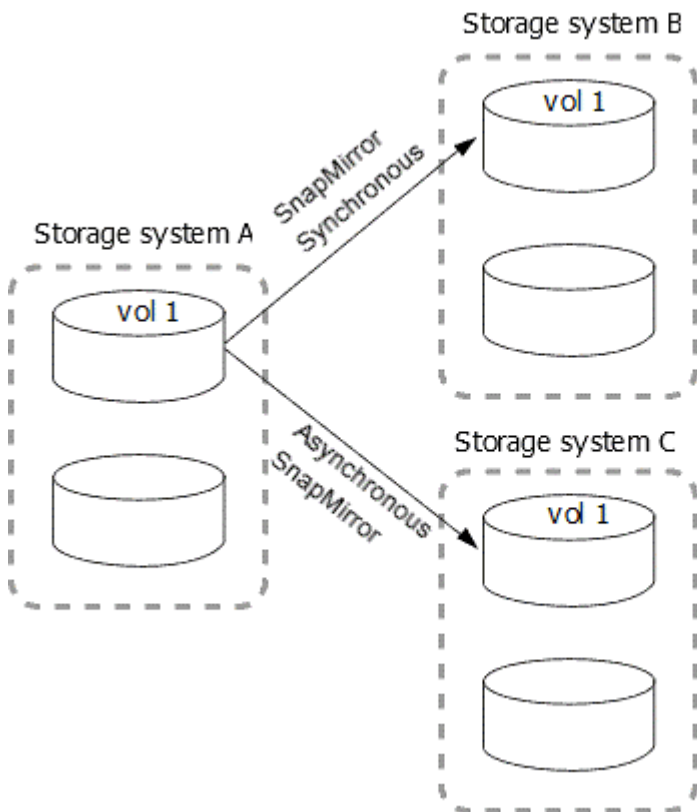
Una puesta en marcha de «fan-out» de varios reflejos consiste en un volumen de origen que tiene una relación de reflejo con varios volúmenes secundarios.



Una implementación de «fan-out» de reflejo-almacén consta de un volumen de origen que tiene una relación de mirroring con un volumen secundario y una relación de SnapVault con otro volumen secundario.



A partir de ONTAP 9.5, puede tener implementaciones de dispersión con relaciones de SnapMirror síncrono; sin embargo, solo una relación de la configuración de dispersión puede ser una relación de SnapMirror síncrono, todas las demás relaciones del volumen de origen deben ser relaciones de SnapMirror asíncronas.

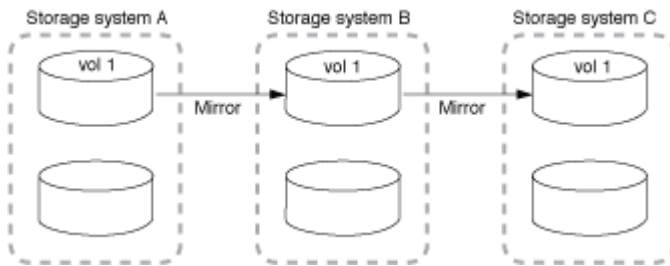


### Cómo funcionan las implementaciones en cascada

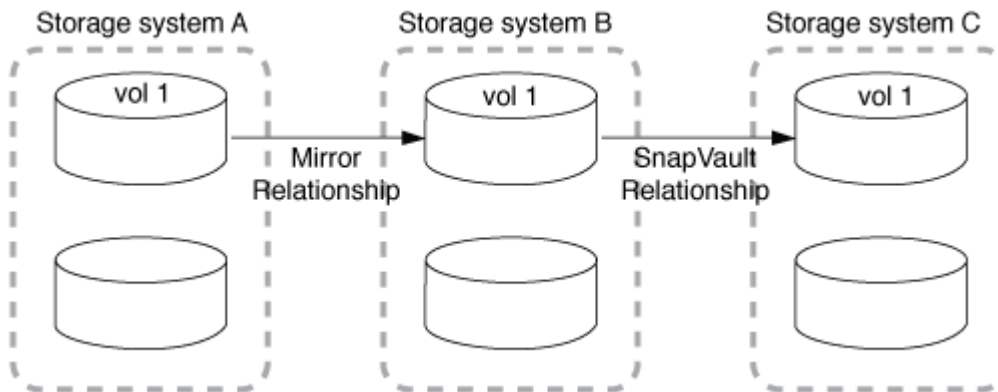
SnapMirror admite puestas en marcha en cascada de *mirror-mirror*, *mirror-vault*, *vault-mirror* y *vault-vault*.

Una puesta en marcha en cascada de reflejos consiste en una cadena de relaciones en las que un volumen de origen se refleja en un volumen secundario, mientras que el volumen secundario se duplica en un volumen terciario. Si el volumen secundario deja de estar disponible, puede sincronizar la relación entre los volúmenes primario y terciario sin necesidad de realizar una nueva transferencia de base de referencia.

A partir de ONTAP 9.6, se admiten las relaciones SnapMirror síncrono en una puesta en marcha en cascada de reflejos. Solo los volúmenes primario y secundario pueden estar en una relación de SnapMirror Synchronous. La relación entre los volúmenes secundarios y los volúmenes terciarios debe ser asíncrona.



Una puesta en marcha en cascada de copias-vault consta de una cadena de relaciones en las que un volumen de origen se refleja en un volumen secundario y el volumen secundario se realiza en un volumen terciario.



También se admiten operaciones de mirroring de vault y, a partir de ONTAP 9.2, puestas en marcha en cascada de vault-vault:

- Una puesta en marcha en cascada de reflejos de almacén consta de una cadena de relaciones en las que se realiza un volumen de origen en un volumen secundario, mientras que el volumen secundario se duplica en un volumen terciario.
- (A partir de ONTAP 9.2) una puesta en marcha en cascada de vault consta de una cadena de relaciones en las que se realiza una copia vault de un volumen de origen a un volumen secundario y a la que se realiza la copia del volumen secundario en un volumen terciario.

#### Lecturas adicionales

- [Reanude la protección en una configuración de salida de ventilador con SM-BC](#)

## Licencias de SnapMirror

### Información general sobre la licencia de SnapMirror

A partir de ONTAP 9.3, se ha simplificado la licencia para la replicación entre instancias de ONTAP. En las versiones ONTAP 9, la licencia de SnapMirror admite tanto relaciones de almacén como de mirroring. Puede usar una licencia de SnapMirror para admitir la replicación de ONTAP tanto en casos prácticos de backup como de recuperación ante desastres.

Antes de la versión 9,3 de ONTAP, era necesaria una licencia independiente de SnapVault para configurar las

relaciones *vault* entre las instancias de ONTAP, donde la instancia de DP podía retener una mayor cantidad de copias de Snapshot para admitir casos de uso de backup con tiempos de retención más largos, y se necesitaba una licencia de SnapMirror para configurar las relaciones *mirror* entre las instancias de ONTAP, en las que cada instancia de ONTAP mantendría el mismo número de copias de Snapshot (es decir, una imagen *mirror*) para admitir casos de uso de recuperación ante desastres para hacer posible la recuperación tras fallos de clústeres. Las licencias de SnapMirror y SnapVault siguen usándose y son compatibles con las versiones de ONTAP 8.x y 9.x.

Aunque las licencias de SnapVault siguen funcionando y son compatibles con las versiones ONTAP 8.x y 9.x, la licencia de SnapMirror puede usarse en lugar de una licencia de SnapVault y puede usarse para configuraciones de mirroring y almacén.

Para la replicación asíncrona de ONTAP, a partir de ONTAP 9.3, se usa un único motor de replicación unificado para configurar las políticas de modo de protección de datos ampliado (XDP), donde la licencia de SnapMirror se puede configurar para una política de mirroring, una normativa de almacén o una política de mirroring-almacén. Se requiere una licencia de SnapMirror en los clústeres de origen y destino. Una licencia de SnapVault no es necesaria si ya se ha instalado una licencia de SnapMirror. La licencia perpetua asíncrona de SnapMirror se incluye en la suite de software ONTAP One que está instalada en los nuevos sistemas AFF y FAS.

Los límites de configuración de protección de datos se determinan por varios factores, como la versión de ONTAP, la plataforma de hardware y las licencias instaladas. Para obtener más información, consulte ["Hardware Universe"](#).

#### **Licencia de SnapMirror Synchronous**

A partir de ONTAP 9.5, se admiten las relaciones de SnapMirror síncrono. Requiere las siguientes licencias para crear una relación de SnapMirror síncrono:

- Se requiere la licencia de SnapMirror Synchronous en el clúster de origen y en el de destino.

La licencia de SnapMirror Synchronous forma parte de la ["Suite de licencia ONTAP ONE"](#).

Si su sistema fue adquirido antes del 2019 de junio con un paquete Premium o Flash, puede descargar una clave maestra de NetApp para obtener la licencia de SnapMirror Synchronous necesaria en el sitio de soporte de NetApp: ["Claves de licencia principal"](#).

- Se requiere la licencia de SnapMirror en los clústeres de origen y destino.

#### **Licencia de SnapMirror Cloud**

A partir de ONTAP 9.8, la licencia Cloud de SnapMirror proporciona la replicación asíncrona de copias Snapshot de instancias de ONTAP a extremos de almacenamiento de objetos. Los destinos de replicación se pueden configurar usando almacenes de objetos locales, así como servicios de almacenamiento de objetos en cloud público compatibles con S3 y S3. Los sistemas ONTAP admiten relaciones de cloud de SnapMirror para destinos de almacenamiento de objetos preconfigurados.

SnapMirror Cloud no está disponible como licencia independiente. Solo se necesita una licencia por clúster ONTAP. Además de una licencia de SnapMirror Cloud, también se necesita la licencia asíncrona de SnapMirror.

Requiere las siguientes licencias para crear una relación de cloud de SnapMirror:

- Tanto una licencia de SnapMirror como una licencia de SnapMirror Cloud para replicar directamente en el extremo del almacén de objetos.

- Cuando se configura un flujo de trabajo de replicación de varias políticas (por ejemplo, disco a disco y al cloud), se requiere una licencia de SnapMirror en todas las instancias de ONTAP, mientras que la licencia de SnapMirror Cloud solo se requiere para el clúster de origen que se replica directamente en el extremo de almacenamiento de objetos.

A partir de ONTAP 9.9.1, puede hacerlo ["Utilice System Manager para la replicación de SnapMirror Cloud"](#).

En la página web de NetApp se publica una lista de aplicaciones de terceros autorizadas de SnapMirror Cloud.

### **Licencia optimizada de Data Protection**

Las licencias de protección de datos optimizada (DPO) ya no se venden y DPO no es compatible con las plataformas actuales; sin embargo, si tiene una licencia DPO instalada en una plataforma compatible, NetApp sigue ofreciendo soporte hasta el fin de la disponibilidad de dicha plataforma.

DPO no se incluye con el paquete de licencia ONTAP One y no se puede actualizar al paquete de licencia ONTAP One si la licencia DPO está instalada en un sistema.

Para obtener más información sobre las plataformas compatibles, consulte ["Hardware Universe"](#).

### **Instalar las licencias de SnapMirror Cloud**

Las relaciones de SnapMirror Cloud se pueden orquestar con aplicaciones de backup de terceros cualificadas previamente. A partir de ONTAP 9.9.1, también puede usar System Manager para orquestar la replicación de SnapMirror Cloud. Tanto las licencias de capacidad de SnapMirror como de SnapMirror Cloud son necesarias al utilizar System Manager para orquestar backups de almacenamiento de objetos de ONTAP en las instalaciones. También deberá solicitar e instalar la licencia de SnapMirror Cloud API.

### **Acerca de esta tarea**

Las licencias de SnapMirror Cloud y SnapMirror S3 son licencias de clúster, no licencias de nodos, por lo que se suministran *no* con el paquete de licencia ONTAP One. Estas licencias están incluidas en el paquete de compatibilidad ONTAP One aparte. Si desea habilitar SnapMirror Cloud, debe solicitar este paquete.

Además, la orquestación de System Manager de backups de SnapMirror Cloud en el almacenamiento de objetos requiere una clave de la API de SnapMirror Cloud. Esta licencia de API es una licencia para todo el clúster de instancia única, lo que significa que no es necesario instalarla en todos los nodos del clúster.

### **Pasos**

Necesita solicitar y descargar el paquete de compatibilidad de ONTAP One y la licencia de API de SnapMirror Cloud y, posteriormente, instalarlos mediante System Manager.

1. Localice y registre el UUID de clúster del clúster para el que desea obtener licencia.

El UUID de clúster se requiere cuando envía la solicitud para solicitar el bundle de compatibilidad ONTAP One para el clúster.

2. Póngase en contacto con su equipo de ventas de NetApp y solicite el paquete de compatibilidad de ONTAP One.
3. Solicite la licencia de la API de SnapMirror Cloud siguiendo las instrucciones que se proporcionan en el sitio de soporte de NetApp.



## "Solicite la clave de licencia de SnapMirror Cloud API"

4. Cuando haya recibido y descargado los archivos de licencia, use System Manager para cargar al clúster la NLF de compatibilidad con cloud de ONTAP y la NLF de la API de cloud de SnapMirror:
  - a. Haga clic en **clúster > Configuración**.
  - b. En la ventana **Configuración**, haz clic en **Licencias**.
  - c. En la ventana **Licencias**, haga clic en **+ Add**.
  - d. En el cuadro de diálogo **Agregar licencia**, haga clic en **examinar** para seleccionar el NLF que descargó y, a continuación, haga clic en **Agregar** para cargar el archivo en el clúster.

### Información relacionada

["Realice backups de datos en el cloud con SnapMirror"](#)

["Búsqueda de licencias de software de NetApp"](#)

## Los sistemas DPO ofrecen mejoras

A partir de ONTAP 9.6, el número máximo de volúmenes FlexVol admitidos aumenta cuando se instala la licencia DP\_Optimized (DPO). A partir de la versión 9,4 de ONTAP, los sistemas con licencia DPO admiten el respaldo de SnapMirror, la deduplicación en segundo plano entre volúmenes, el uso de bloques Snapshot como donantes y la compactación.

A partir de ONTAP 9.6, se ha incrementado el número máximo admitido de volúmenes FlexVol en sistemas secundarios o de protección de datos, lo que permite escalar hasta 2,500 volúmenes FlexVol por nodo o hasta 5,000 en modo de conmutación por error. El aumento de los volúmenes de FlexVol se habilita con el ["Licencia DP\\_Optimized \(DPO\)"](#). A. ["Licencia de SnapMirror"](#) también se requiere en los nodos de origen y destino.

A partir de ONTAP 9.4, se realizan las siguientes mejoras en las funciones de los sistemas DPO:

- Backoff de SnapMirror: En sistemas DPO, el tráfico de replicación tiene la misma prioridad que se da a las cargas de trabajo del cliente.

La funcionalidad de backup de SnapMirror está deshabilitada de forma predeterminada en los sistemas DPO.

- Deduplicación en segundo plano de volumen y deduplicación en segundo plano entre volúmenes: Se habilitan la deduplicación en segundo plano de volúmenes y la deduplicación en segundo plano entre volúmenes en sistemas DPO.

Puede ejecutar el `storage aggregate efficiency cross-volume-dedupe start -aggregate aggregate_name -scan-old-data true` comando para deduplicar los datos existentes. La práctica recomendada es ejecutar el comando durante las horas de menor actividad para reducir el impacto en el rendimiento.

- Mayor ahorro usando los bloques Snapshot como donantes: Los bloques de datos que no están disponibles en el sistema de archivos activo, pero están atrapados en las copias Snapshot se utilizan como donantes para la deduplicación de volúmenes.

Los datos nuevos pueden deduplicarse con los datos que estaban atrapados en las copias Snapshot, compartiendo de forma efectiva también los bloques Snapshot. El aumento del espacio de los donantes permite obtener más ahorro, especialmente cuando el volumen tiene un gran número de copias snapshot.

- Compactación: La compactación de datos está habilitada de forma predeterminada en los volúmenes DPO.

## Gestione la replicación de volúmenes de SnapMirror

### Flujo de trabajo de replicación de SnapMirror

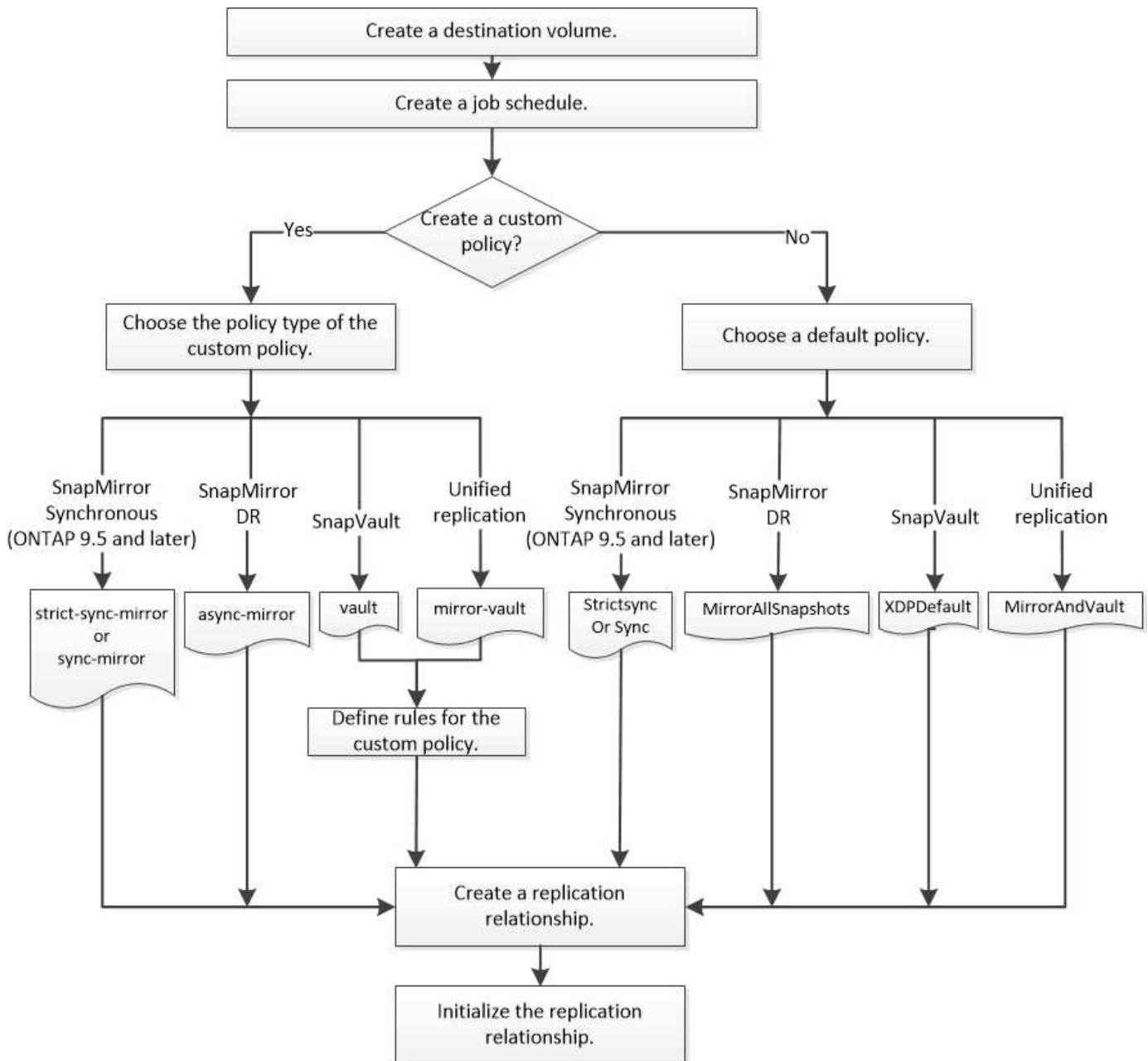
SnapMirror ofrece tres tipos de relación de protección de datos: Recuperación ante desastres de SnapMirror, archivado (anteriormente conocido como SnapVault) y replicación unificada. Puede seguir el mismo flujo de trabajo básico para configurar cada tipo de relación.

A partir de la disponibilidad general de ONTAP 9.9.1, SnapMirror Business Continuity (SM-BC) proporciona un objetivo de tiempo de recuperación cero (RTO cero) o recuperación tras fallos de aplicaciones transparente (TAF) para permitir la conmutación automática al nodo de respaldo de aplicaciones vitales para el negocio en entornos SAN. SM-BC se admite en una configuración de dos clústeres AFF o dos clústeres de Cabina SAN all-flash (ASA).

["Documentación de NetApp: Continuidad empresarial de SnapMirror"](#)

Para cada tipo de relación de protección de datos de SnapMirror, el flujo de trabajo es el mismo: Crear un volumen de destino, crear una programación de trabajos, especificar una política, crear e inicializar la relación.

A partir de ONTAP 9.3, puede utilizar la `snapmirror protect` comando para configurar una relación de protección de datos en un solo paso. Incluso si usted utiliza `snapmirror protect`, debe comprender cada paso del flujo de trabajo.



## Configurar una relación de replicación en un paso

A partir de ONTAP 9.3, puede utilizar la `snapmirror protect` comando para configurar una relación de protección de datos en un solo paso. Especifique una lista de volúmenes que se van a replicar, una SVM en el clúster de destino, una programación de trabajos y una política de SnapMirror. `snapmirror protect` hace el resto.

### Lo que necesitará

- Las SVM y los clústeres de origen y destino deben tener una relación entre iguales.

["Relaciones entre iguales de clústeres y SVM"](#)

- El idioma del volumen de destino debe ser el mismo que el del volumen de origen.

### Acerca de esta tarea

La `snapmirror protect` El comando elige un agregado asociado con la SVM especificada. Si no hay ningún agregado asociado con la SVM, elige de todos los agregados del clúster. La elección del agregado se basa en la cantidad de espacio libre y el número de volúmenes del agregado.

La `snapmirror protect` a continuación, el comando realiza los siguientes pasos:

- Crea un volumen de destino con un tipo adecuado y la cantidad de espacio reservado para cada volumen de la lista de volúmenes que se van a replicar.
- Configura una relación de replicación adecuada para la directiva que usted especifique.
- Inicializa la relación.

El nombre del volumen de destino tiene el formato `source_volume_name_dst`. En caso de un conflicto con un nombre existente, el comando añade un número al nombre del volumen. Puede especificar un prefijo o sufijo en las opciones del comando. El sufijo sustituye al suministrado por el sistema `dst` sufijo.

En ONTAP 9.3 y versiones anteriores, los volúmenes de destino pueden contener hasta 251 copias Snapshot. A partir de la versión 9.4 de ONTAP, un volumen de destino puede contener hasta 1019 copias snapshot.



La inicialización puede requerir mucho tiempo. `snapmirror protect` no espera a que se complete la inicialización antes de que termine el trabajo. Por esta razón, debe utilizar la `snapmirror show` en lugar de la `job show` comando para determinar cuándo se ha completado la inicialización.

A partir de ONTAP 9.5, las relaciones de SnapMirror síncrono se pueden crear mediante el `snapmirror protect` comando.

## Paso

1. Cree e inicialice una relación de replicación en un paso:

Antes de ejecutar este comando, debe sustituir las variables entre paréntesis angulares por los valores requeridos.

```
snapmirror protect -path-list <SVM:volume> -destination-vserver
<destination_SVM> -policy <policy> -schedule <schedule> -auto-initialize
<true|false> -destination-volume-prefix <prefix> -destination-volume
-suffix <suffix>
```



Se debe ejecutar este comando desde la SVM de destino o el clúster de destino. La `-auto-initialize` la opción predeterminada es «true».

En el siguiente ejemplo se crea e inicializa una relación de recuperación ante desastres de SnapMirror con los valores predeterminados `MirrorAllSnapshots` política:

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy MirrorAllSnapshots -schedule
replication_daily
```



Puede utilizar una directiva personalizada si lo prefiere. Para obtener más información, consulte ["Creación de una política de replicación personalizada"](#).

En el siguiente ejemplo se crea e inicializa una relación SnapVault con el valor predeterminado XDPDefault política:

```
cluster_dst:> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy XDPDefault -schedule
replication_daily
```

En el ejemplo siguiente se crea e inicializa una relación de replicación unificada con el valor predeterminado MirrorAndVault política:

```
cluster_dst:> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy MirrorAndVault
```

En el siguiente ejemplo se crea e inicializa una relación de SnapMirror síncrono con el valor predeterminado Sync política:

```
cluster_dst:> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_sync -policy Sync
```



Para las políticas de SnapVault y de replicación unificada, puede que sea útil definir una programación para crear una copia de la última copia de Snapshot transferida en el destino. Para obtener más información, consulte ["Definir una programación para crear una copia local en el destino"](#).

## Después de terminar

Utilice la `snapmirror show` Comando para verificar que la relación de SnapMirror se ha creado. Para obtener una sintaxis de comando completa, consulte la página man.

## Configure una relación de replicación paso a paso

### Crear un volumen de destino

Puede utilizar el `volume create` comando en el destino para crear un volumen de destino. El volumen de destino debe tener el mismo tamaño o más que el volumen de origen.

### Paso

1. Cree un volumen de destino:

```
volume create -vserver SVM -volume volume -aggregate aggregate -type DP -size
size
```

Para obtener una sintaxis de comando completa, consulte la página man.

En el ejemplo siguiente se crea un volumen de destino de 2 GB denominado `volA_dst`:

```
cluster_dst::> volume create -vserver SVM_backup -volume volA_dst
-aggregate node01_aggr -type DP -size 2GB
```

## Cree una programación de trabajo de replicación

Puede utilizar el `job schedule cron create` comando para crear una programación de trabajo de replicación. La programación de tareas determina el momento en que SnapMirror actualiza automáticamente la relación de protección de datos a la que se asigna la programación.

### Acerca de esta tarea

Debe asignar una programación de tareas cuando crea una relación de protección de datos. Si no asigna una programación de trabajo, debe actualizar la relación manualmente.

### Paso

1. Crear un programa de trabajo:

```
job schedule cron create -name job_name -month month -dayofweek day_of_week
-day day_of_month -hour hour -minute minute
```

Para `-month`, `-dayofweek`, y `-hour`, puede especificar `all` para ejecutar el trabajo cada mes, día de la semana y hora, respectivamente.

A partir de ONTAP 9.10.1, puede incluir Vserver para su programación de trabajo:

```
job schedule cron create -name job_name -vserver Vserver_name -month month
-dayofweek day_of_week -day day_of_month -hour hour -minute minute
```



La programación mínima admitida (RPO) para volúmenes FlexVol en una relación de SnapMirror para volúmenes es de 5 minutos. La programación mínima admitida (RPO) para volúmenes FlexGroup en una relación de SnapMirror para volúmenes es de 30 minutos.

En el ejemplo siguiente se crea una programación de trabajo denominada `my_weekly`. Es decir, los sábados a las 3:00 horas:

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

## Personalizar una política de replicación

### Cree una política de replicación personalizada

Puede crear una directiva de replicación personalizada si la directiva predeterminada

para una relación no es adecuada. Puede que desee comprimir datos en una transferencia de red, por ejemplo, o modificar el número de intentos que realiza SnapMirror para transferir copias Snapshot.

Puede usar una directiva predeterminada o personalizada al crear una relación de replicación. Para un archivo personalizado (anteriormente SnapVault) o una política de replicación unificada, debe definir una o más *rules* que determinen qué copias Snapshot se transfieren durante la inicialización y la actualización. También es posible que desee definir una programación para crear copias Snapshot locales en el destino.

El *policy type* de la directiva de replicación determina el tipo de relación que admite. En la siguiente tabla se muestran los tipos de directivas disponibles.

| Tipo de política         | Tipo de relación                                                                  |
|--------------------------|-----------------------------------------------------------------------------------|
| reflejo asíncrono        | Recuperación ante desastres de SnapMirror                                         |
| almacén                  | SnapVault                                                                         |
| mirror-vault             | Replicación unificada                                                             |
| estricto-síncrono-mirror | SnapMirror Synchronous en el modo StrictSync (compatible empezando con ONTAP 9.5) |
| reflejo síncrono         | SnapMirror Synchronous en el modo Sync (admitido empezando por ONTAP 9.5)         |



Al crear una directiva de replicación personalizada, es una buena idea modelar la directiva después de una directiva predeterminada.

## Paso

1. Cree una política de replicación personalizada:

```
snapmirror policy create -vserver SVM -policy policy -type async-
mirror|vault|mirror-vault|strict-sync-mirror|sync-mirror -comment comment
-tries transfer_tries -transfer-priority low|normal -is-network-compression
-enabled true|false
```

Para obtener una sintaxis de comando completa, consulte la página man.

A partir de ONTAP 9.5, puede especificar la programación para crear una programación de copia Snapshot común para relaciones de SnapMirror síncrono mediante la `-common-snapshot-schedule` parámetro. De forma predeterminada, la programación común de copias de Snapshot para relaciones de SnapMirror síncrono es una hora. Puede especificar un valor de 30 minutos a dos horas para la programación de la copia de Snapshot para las relaciones de SnapMirror Synchronous.

En el ejemplo siguiente se crea una política de replicación personalizada para la recuperación ante desastres de SnapMirror que permite la compresión de red para las transferencias de datos:

```
cluster_dst:> snapmirror policy create -vserver svml -policy
DR_compressed -type async-mirror -comment "DR with network compression
enabled" -is-network-compression-enabled true
```

En el ejemplo siguiente se crea una política de replicación personalizada para SnapVault:

```
cluster_dst:> snapmirror policy create -vserver svml -policy
my_snapvault -type vault
```

En el ejemplo siguiente se crea una política de replicación personalizada para la replicación unificada:

```
cluster_dst:> snapmirror policy create -vserver svml -policy my_unified
-type mirror-vault
```

En el ejemplo siguiente se crea una política de replicación personalizada para la relación de SnapMirror Synchronous en el modo StrictSync:

```
cluster_dst:> snapmirror policy create -vserver svml -policy
my_strictsync -type strict-sync-mirror -common-snapshot-schedule
my_sync_schedule
```

## Después de terminar

En el caso de los tipos de políticas «'vault» y «'mercado», deberá definir las reglas que determinen las copias snapshot que se transfieren durante la inicialización y actualización.

Utilice la `snapmirror policy show` Comando para comprobar que la política de SnapMirror se ha creado. Para obtener una sintaxis de comando completa, consulte la página man.

## Defina una regla para una política

En el caso de las directivas personalizadas con el tipo de política «'vault» o «'márror-vault», debe definir al menos una regla que determine qué copias snapshot se transfieren durante la inicialización y la actualización. También puede definir reglas para las políticas predeterminadas con el tipo de política «'vault» o «'mirror-vault».

## Acerca de esta tarea

Todas las normas que tengan el tipo de política «'vault» o «'márror-vault» deberán tener una regla que especifique qué copias snapshot replicar. La regla «'bimensual'», por ejemplo, indica que sólo deben replicarse las copias snapshot asignadas a la etiqueta «'bimensual'» de SnapMirror. Debe especificar la etiqueta de SnapMirror al configurar la política de Snapshot en el origen.

Cada tipo de política está asociado a una o más reglas definidas por el sistema. Estas reglas se asignan automáticamente a una directiva cuando se especifica su tipo de directiva. La siguiente tabla muestra las reglas definidas por el sistema.



| Regla definida por el sistema | Se utiliza en tipos de políticas                               | Resultado                                                                                                                                                       |
|-------------------------------|----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| sm_creado                     | Reflejo asíncrono, reflejo-almacén, sincronización, StrictSync | Una copia Snapshot creada por SnapMirror se transfiere tras la inicialización y la actualización.                                                               |
| all_source_snapshots          | reflejo asíncrono                                              | Las nuevas copias snapshot del origen se transfieren tras la inicialización y actualización.                                                                    |
| todos los días                | almacén, reflejo-almacén                                       | Las nuevas copias snapshot del origen con la etiqueta de SnapMirror «día» se transfieren durante la inicialización y actualización.                             |
| semanal                       | almacén, reflejo-almacén                                       | Al inicializar y actualizar, se transfieren las nuevas copias snapshot del origen con la etiqueta de SnapMirror «'Weekly'».                                     |
| mensual                       | mirror-vault                                                   | Las nuevas copias snapshot en el origen con la etiqueta de SnapMirror «mensual» se transfieren durante la inicialización y actualización.                       |
| coherente con la aplicación   | Sync, StrictSync                                               | Las copias Snapshot con la etiqueta de SnapMirror «'app_coherente'» en el origen se replican de forma síncrona en el destino. Compatible a partir de ONTAP 9.7. |

Excepto para el tipo de política «'duplicación asíncrona'», puede especificar reglas adicionales según sea necesario, para directivas predeterminadas o personalizadas. Por ejemplo:

- Para el valor predeterminado `MirrorAndVault` Política puede crear una regla llamada «bimensual» para hacer coincidir las copias Snapshot de la fuente con la etiqueta «bimensual» de SnapMirror.
- En el caso de una política personalizada con el tipo de política «mercado de productos vault», puede crear una regla llamada «bisemanal» para hacer coincidir las copias Snapshot del origen con la etiqueta de SnapMirror «bisemanales».

## Paso

1. Definir una regla para una directiva:

```
snapmirror policy add-rule -vserver SVM -policy policy_for_rule -snapmirror
-label snapmirror-label -keep retention_count
```

Para obtener una sintaxis de comando completa, consulte la página man.

En el siguiente ejemplo, se añade una regla con la etiqueta de SnapMirror `bi-monthly` al valor predeterminado `MirrorAndVault` política:

```
cluster_dst:> snapmirror policy add-rule -vserver svm1 -policy
MirrorAndVault -snapmirror-label bi-monthly -keep 6
```

En el siguiente ejemplo, se añade una regla con la etiqueta de SnapMirror `bi-weekly` al personalizado `my_snapvault` política:

```
cluster_dst:> snapmirror policy add-rule -vserver svm1 -policy
my_snapvault -snapmirror-label bi-weekly -keep 26
```

En el siguiente ejemplo, se añade una regla con la etiqueta de SnapMirror `app_consistent` al personalizado `Sync` política:

```
cluster_dst:> snapmirror policy add-rule -vserver svm1 -policy Sync
-snapmirror-label app_consistent -keep 1
```

Luego, puede replicar las copias Snapshot del clúster de origen que coincidan con esta etiqueta de SnapMirror:

```
cluster_src:> snapshot create -vserver vs1 -volume vol1 -snapshot
snapshot1 -snapmirror-label app_consistent
```

#### Defina una programación para crear una copia local en el destino

Para las relaciones de SnapVault y de replicación unificada, puede protegerse contra la posibilidad de que una copia Snapshot actualizada se dañe al crear una copia de la última copia Snapshot transferida en el destino. Esta «copia local» se conserva independientemente de las reglas de retención del origen, de modo que, aunque la copia Snapshot transferida mediante SnapMirror ya no esté disponible en el origen, dicha copia estará disponible en el destino.

#### Acerca de esta tarea

Se especifica la programación para crear una copia local en el `-schedule` opción de `snapmirror policy add-rule` comando.

#### Paso

1. Definir una programación para crear una copia local en el destino:

```
snapmirror policy add-rule -vserver SVM -policy policy_for_rule -snapmirror
-label snapmirror-label -schedule schedule
```

Para obtener una sintaxis de comando completa, consulte la página man. Para ver un ejemplo de cómo

crear una programación de trabajos, consulte ["Crear una programación de trabajo de replicación"](#).

En el ejemplo siguiente se añade una programación para crear una copia local en los valores predeterminados `MirrorAndVault` política:

```
cluster_dst:> snapmirror policy add-rule -vserver svml -policy
MirrorAndVault -snapmirror-label my_monthly -schedule my_monthly
```

En el siguiente ejemplo, se agrega una programación para crear una copia local en el personalizado `my_unified` política:

```
cluster_dst:> snapmirror policy add-rule -vserver svml -policy
my_unified -snapmirror-label my_monthly -schedule my_monthly
```

## Cree una relación de replicación

La relación entre el volumen de origen del almacenamiento principal y el volumen de destino del almacenamiento secundario se denomina *relación de protección de datos*. puede usar la `snapmirror create` Comando para crear relaciones de protección de datos de recuperación ante desastres, SnapVault o replicación unificada de SnapMirror.

### Lo que necesitará

- Las SVM y los clústeres de origen y destino deben tener una relación entre iguales.

#### ["Relaciones entre iguales de clústeres y SVM"](#)

- El idioma del volumen de destino debe ser el mismo que el del volumen de origen.

### Acerca de esta tarea

Hasta ONTAP 9.3, SnapMirror invocado en modo DP y SnapMirror invocado en modo XDP utilizaba distintos motores de replicación, con distintos enfoques respecto a la dependencia de versión:

- SnapMirror que se invoca en el modo DP utilizaba un motor de replicación *version-dependent* en el que la versión de ONTAP debía ser la misma en el almacenamiento primario y secundario:

```
cluster_dst:> snapmirror create -type DP -source-path ... -destination
-path ...
```

- SnapMirror, al que se invocó en el modo XDP, utilizó un motor de replicación de *version-flexible* que admitía diferentes versiones de ONTAP en el almacenamiento primario y secundario:

```
cluster_dst:> snapmirror create -type XDP -source-path ...
-destination-path ...
```

Las importantes ventajas de SnapMirror, que ofrece una versión flexible, superan la ligera ventaja del

rendimiento de la replicación obtenido con el modo basado en la versión. Por este motivo, a partir de ONTAP 9.3, se ha creado el modo XDP como nuevo valor predeterminado, y cualquier invocación del modo DP en la línea de comandos o en scripts nuevos o existentes se convierte automáticamente al modo XDP.

Las relaciones existentes no se ven afectadas. Si una relación ya es del tipo DP, seguirá siendo del tipo DP. La siguiente tabla muestra el comportamiento que puede esperar.

| Si especifica...    | El tipo es... | La política predeterminada (si no se especifica una política) es... |
|---------------------|---------------|---------------------------------------------------------------------|
| PROTECCIÓN DE DATOS | XDP           | MirrorAllSnapshots (recuperación ante desastres de SnapMirror)      |
| Nada                | XDP           | MirrorAllSnapshots (recuperación ante desastres de SnapMirror)      |
| XDP                 | XDP           | XDPDefault (SnapVault)                                              |

Consulte también los ejemplos del procedimiento siguiente.

Las únicas excepciones a la conversión son las siguientes:

- Las relaciones de protección de datos de SVM siguen siendo las predeterminadas en el modo DP.

Especifique XDP explícitamente para obtener el modo XDP con el valor predeterminado `MirrorAllSnapshots` política.

- Las relaciones de protección de datos con uso compartido de carga siguen siendo las predeterminadas en el modo DP.
- Las relaciones de protección de datos de SnapLock siguen siendo las predeterminadas en el modo DP.
- Las invocaciones explícitas de DP siguen en el modo DP de forma predeterminada si establece la siguiente opción para todo el clúster:

```
options replication.create_data_protection_rels.enable on
```

Esta opción se ignora si no invoca explícitamente DP.

En ONTAP 9.3 y versiones anteriores, los volúmenes de destino pueden contener hasta 251 copias Snapshot. A partir de la versión 9.4 de ONTAP, un volumen de destino puede contener hasta 1019 copias snapshot.

A partir de ONTAP 9.5, se admiten las relaciones de SnapMirror síncrono.

**Paso**

1. En el clúster de destino, cree una relación de replicación:

Antes de ejecutar este comando, debe sustituir las variables entre paréntesis angulares por los valores requeridos.

```
snapmirror create -source-path <SVM:volume> -destination-path
<SVM:volume> -type <DP|XDP> -schedule <schedule> -policy <policy>
```

Para obtener una sintaxis de comando completa, consulte la página [man](#).



La `schedule` No aplica el parámetro cuando se crean relaciones de SnapMirror síncrono.

En el siguiente ejemplo se crea una relación de recuperación ante desastres de SnapMirror con los valores predeterminados `MirrorLatest` política:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily -policy
MirrorLatest
```

En el siguiente ejemplo se crea una relación de SnapVault con los valores predeterminados `XDPDefault` política:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily -policy
XDPDefault
```

En el ejemplo siguiente se crea una relación de replicación unificada con la opción predeterminada `MirrorAndVault` política:

```
cluster_dst:> snapmirror create -source-path svm1:volA -destination-path
svm_backup:volA_dst -type XDP -schedule my_daily -policy MirrorAndVault
```

En el siguiente ejemplo se crea una relación de replicación unificada mediante el método personalizado `my_unified` política:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily -policy
my_unified
```

En el siguiente ejemplo se crea una relación de SnapMirror Synchronous con el valor predeterminado `Sync` política:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy Sync
```

En el siguiente ejemplo se crea una relación de SnapMirror Synchronous con el valor predeterminado

StrictSync política:

```
cluster_dst:> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy StrictSync
```

En el siguiente ejemplo se crea una relación de recuperación ante desastres de SnapMirror. Con el tipo de DP convertido automáticamente a XDP y sin ninguna directiva especificada, la política predeterminada es la MirrorAllSnapshots política:

```
cluster_dst:> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type DP -schedule my_daily
```

En el siguiente ejemplo se crea una relación de recuperación ante desastres de SnapMirror. Si no se especifica ningún tipo o política, la directiva se establece de forma predeterminada en MirrorAllSnapshots política:

```
cluster_dst:> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -schedule my_daily
```

En el siguiente ejemplo se crea una relación de recuperación ante desastres de SnapMirror. Sin ninguna directiva especificada, la directiva se establece de forma predeterminada en XDPDefault política:

```
cluster_dst:> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily
```

En el siguiente ejemplo se crea una relación de SnapMirror Synchronous con la política predefinida SnapCenterSync:

```
cluster_dst:> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy SnapCenterSync
```



La política predefinida SnapCenterSync es de tipo Sync. Esta normativa replica cualquier copia snapshot que se cree con el snapmirror-label de "coherente con la aplicación".

## Después de terminar

Utilice la `snapmirror show` Comando para verificar que la relación de SnapMirror se ha creado. Para obtener una sintaxis de comando completa, consulte la página man.

## Información relacionada

- ["Crear y eliminar volúmenes de prueba de conmutación al nodo de respaldo de SnapMirror"](#).

| Para ejecutar estas tareas con...                                            | Ver este contenido...                                                              |
|------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| System Manager rediseñado (disponible con ONTAP 9.7 y versiones posteriores) | <a href="#">"Configure los reflejos y almacenes"</a>                               |
| System Manager Classic (disponible con ONTAP 9.7 y versiones anteriores)     | <a href="#">"Información general sobre backup de volúmenes mediante SnapVault"</a> |

## Inicializar una relación de replicación

Para todos los tipos de relaciones, la inicialización realiza una *transferencia\_de base*: Realiza una copia Snapshot del volumen de origen y, a continuación, transfiere esa copia y todos los bloques de datos a los que hace referencia al volumen de destino. De lo contrario, el contenido de la transferencia depende de la política.

### Lo que necesitará

Las SVM y los clústeres de origen y destino deben tener una relación entre iguales.

["Relaciones entre iguales de clústeres y SVM"](#)

### Acerca de esta tarea

La inicialización puede requerir mucho tiempo. Puede ser conveniente ejecutar la transferencia básica en horas de menor actividad.

A partir de ONTAP 9.5, se admiten las relaciones de SnapMirror síncrono.

### Paso

1. Inicializar una relación de replicación:

```
snapmirror initialize -source-path SVM:volume|cluster://SVM/volume, ...
-destination-path SVM:volume|cluster://SVM/volume, ...
```

Para obtener una sintaxis de comando completa, consulte la página man.



Se debe ejecutar este comando desde la SVM de destino o el clúster de destino.

En el siguiente ejemplo, se inicializa la relación entre el volumen de origen volA encendido svm1 y el volumen de destino volA\_dst encendido svm\_backup:

```
cluster_dst::> snapmirror initialize -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

## Ejemplo: Configure una cascada de vault-vault

Un ejemplo mostrará en términos concretos cómo puede configurar las relaciones de replicación paso a paso. Puede utilizar la puesta en marcha en cascada de vault configurada en el ejemplo para conservar más de 251 copias snapshot con el nombre

«my semanal».

### Lo que necesitará

- Las SVM y los clústeres de origen y destino deben tener una relación entre iguales.
- Debe ejecutar ONTAP 9,2 o una versión posterior. Las cascadas de vault-vault no son compatibles con versiones anteriores de ONTAP.

### Acerca de esta tarea

En el ejemplo se dan por hechos los siguientes elementos:

- Se han configurado copias Snapshot en el clúster de origen con las etiquetas de SnapMirror «mi día a día», «mi semana a semana» y «mi mes».
- Ha configurado volúmenes de destino denominados «'Vola'» en los clústeres de destino secundario y terciario.
- Ha configurado programas de trabajos de replicación denominados «my\_snapvault» en los clústeres de destino secundario y terciario.

El ejemplo muestra cómo crear relaciones de replicación basadas en dos políticas personalizadas:

- La política de «snapvault\_secondary» conserva 7 copias snapshot diarias, 52 semanales y 180 mensuales en el clúster de destino secundario.
- La «política de almacén\_terciario» conserva 250 copias Snapshot semanales en el clúster de destino terciario.

### Pasos

1. En el clúster secundario de destino, cree la política «napvault\_secondary»:

```
cluster_secondary::> snapmirror policy create -policy snapvault_secondary
-type vault -comment "Policy on secondary for vault to vault cascade" -vserver
svm_secondary
```

2. En el grupo secundario de destino, definir la regla «mi día a día» de la política:

```
cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary
-snapmirror-label my-daily -keep 7 -vserver svm_secondary
```

3. En el grupo secundario de destino, definir la regla «mi semana» para la política:

```
cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary
-snapmirror-label my-weekly -keep 52 -vserver svm_secondary
```

4. En el grupo secundario de destino, definir la regla «mi mes» de la política:

```
cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary
-snapmirror-label my-monthly -keep 180 -vserver svm_secondary
```

5. En el clúster de destino secundario, compruebe la política:

```
cluster_secondary::> snapmirror policy show snapvault_secondary -instance
```



```

Vserver: svm_secondary
SnapMirror Policy Name: snapvault_secondary
SnapMirror Policy Type: vault
Policy Owner: cluster-admin
Tries Limit: 8
Transfer Priority: normal
Ignore accesstime Enabled: false
Transfer Restartability: always
Network Compression Enabled: false
Create Snapshot: false
Comment: Policy on secondary for vault to vault
cascade
Total Number of Rules: 3
Total Keep: 239
Rules: SnapMirror Label Keep Preserve Warn
Schedule Prefix

my-daily 7 false 0 -
-
my-weekly 52 false 0 -
-
my-monthly 180 false 0 -
-

```

6. En el clúster de destino secundario, cree la relación con el clúster de origen:

```
cluster_secondary::> snapmirror create -source-path svm_primary:volA
-destination-path svm_secondary:volA -type XDP -schedule my_snapvault -policy
snapvault_secondary
```

7. En el clúster de destino secundario, inicialice la relación con el clúster de origen:

```
cluster_secondary::> snapmirror initialize -source-path svm_primary:volA
-destination-path svm_secondary:volA
```

8. En el clúster de destino terciario, cree la política «napvault\_terciario»:

```
cluster_tertiary::> snapmirror policy create -policy snapvault_tertiary -type
vault -comment "Policy on tertiary for vault to vault cascade" -vserver
svm_tertiary
```

9. En el grupo de destino terciario, defina la regla «mi semana» para la política:

```
cluster_tertiary::> snapmirror policy add-rule -policy snapvault_tertiary
-snapmirror-label my-weekly -keep 250 -vserver svm_tertiary
```

10. En el clúster de destino terciario, compruebe la política:

```
cluster_tertiary::> snapmirror policy show snapvault_tertiary -instance
```

```

 Vserver: svm_tertiary
SnapMirror Policy Name: snapvault_tertiary
SnapMirror Policy Type: vault
 Policy Owner: cluster-admin
 Tries Limit: 8
 Transfer Priority: normal
Ignore accesstime Enabled: false
 Transfer Restartability: always
Network Compression Enabled: false
 Create Snapshot: false
 Comment: Policy on tertiary for vault to vault
cascade
 Total Number of Rules: 1
 Total Keep: 250
 Rules: SnapMirror Label Keep Preserve Warn
Schedule Prefix

 my-weekly 250 false 0 -
-

```

11. En el clúster de destino terciario, cree la relación con el clúster secundario:

```
cluster_tertiary::> snapmirror create -source-path svm_secondary:volA
-destination-path svm_tertiary:volA -type XDP -schedule my_snapvault -policy
snapvault_tertiary
```

12. En el clúster de destino terciario, inicialice la relación con el clúster secundario:

```
cluster_tertiary::> snapmirror initialize -source-path svm_secondary:volA
-destination-path svm_tertiary:volA
```

## Convierta una relación de tipo DP existente a XDP

Si actualiza a ONTAP 9.12.1 o una versión posterior, debe convertir las relaciones de tipo DP a XDP antes de realizar la actualización. ONTAP 9.12.1 y las versiones posteriores no admiten relaciones de tipo DP. Puede convertir fácilmente una relación de tipo de DP existente a XDP para poder aprovechar las ventajas de la flexibilidad de versión de SnapMirror.

### Acerca de esta tarea

- SnapMirror no convierte automáticamente las relaciones de tipo DP existentes a XDP. Para convertir la relación, debe romper y eliminar la relación existente, crear una nueva relación XDP y volver a sincronizar la relación. Para obtener información previa, consulte ["XDP sustituye a DP como la opción predeterminada de SnapMirror"](#).

- Al planificar la conversión, tenga en cuenta que la preparación en segundo plano y la fase de almacenamiento de datos de una relación de SnapMirror para XDP pueden llevar mucho tiempo. No es poco frecuente ver la relación de SnapMirror que informa sobre el estado "preparación" para un periodo de tiempo prolongado.



Después de convertir un tipo de relación de SnapMirror de DP a XDP, las configuraciones relacionadas con el espacio, como la configuración automática de tamaño y la garantía de espacio, ya no se replican en el destino.

## Pasos

1. En el clúster de destino, compruebe que la relación SnapMirror sea del tipo DP, que el estado de mirroring sea en SnapMirror, que el estado de la relación sea inactivo y que la relación esté en buen estado:

```
snapmirror show -destination-path <SVM:volume>
```

En el siguiente ejemplo, se muestra el resultado de `snapmirror show` comando:

```
cluster_dst::>snapmirror show -destination-path svm_backup:volA_dst

Source Path: svm1:volA
Destination Path: svm_backup:volA_dst
Relationship Type: DP
SnapMirror Schedule: -
Tries Limit: -
Throttle (KB/sec): unlimited
Mirror State: Snapmirrored
Relationship Status: Idle
Transfer Snapshot: -
Snapshot Progress: -
Total Progress: -
Snapshot Checkpoint: -
Newest Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Newest Snapshot Timestamp: 06/27 10:00:55
Exported Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Exported Snapshot Timestamp: 06/27 10:00:55
Healthy: true
```



Puede que le resulte útil conservar una copia del `snapmirror show` salida de comando para realizar un seguimiento de la configuración de relaciones existente.

2. En los volúmenes de origen y destino, asegúrese de que ambos volúmenes tengan una copia Snapshot común:

```
volume snapshot show -vserver <SVM> -volume <volume>
```

En el siguiente ejemplo se muestra el `volume snapshot show` salida de los volúmenes de origen y destino:

```
cluster_src:> volume snapshot show -vserver vsml -volume volA
---Blocks---
Vserver Volume Snapshot State Size Total% Used%

svm1 volA
weekly.2014-06-09_0736 valid 76KB 0% 28%
weekly.2014-06-16_1305 valid 80KB 0% 29%
daily.2014-06-26_0842 valid 76KB 0% 28%
hourly.2014-06-26_1205 valid 72KB 0% 27%
hourly.2014-06-26_1305 valid 72KB 0% 27%
hourly.2014-06-26_1405 valid 76KB 0% 28%
hourly.2014-06-26_1505 valid 72KB 0% 27%
hourly.2014-06-26_1605 valid 72KB 0% 27%
daily.2014-06-27_0921 valid 60KB 0% 24%
hourly.2014-06-27_0921 valid 76KB 0% 28%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
valid 44KB 0% 19%
11 entries were displayed.
```

```
cluster_dest:> volume snapshot show -vserver svm_backup -volume volA_dst
---Blocks---
Vserver Volume Snapshot State Size Total% Used%

svm_backup volA_dst
weekly.2014-06-09_0736 valid 76KB 0% 30%
weekly.2014-06-16_1305 valid 80KB 0% 31%
daily.2014-06-26_0842 valid 76KB 0% 30%
hourly.2014-06-26_1205 valid 72KB 0% 29%
hourly.2014-06-26_1305 valid 72KB 0% 29%
hourly.2014-06-26_1405 valid 76KB 0% 30%
hourly.2014-06-26_1505 valid 72KB 0% 29%
hourly.2014-06-26_1605 valid 72KB 0% 29%
daily.2014-06-27_0921 valid 60KB 0% 25%
hourly.2014-06-27_0921 valid 76KB 0% 30%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
```

3. Para garantizar que las actualizaciones programadas no se ejecuten durante la conversión, desactive la relación de tipo DP existente:

```
snapmirror quiesce -source-path <SVM:volume> -destination-path
<SVM:volume>
```

Para obtener una sintaxis completa del comando, consulte ["página de manual"](#).



Se debe ejecutar este comando desde la SVM de destino o el clúster de destino.

En el siguiente ejemplo, se pausa la relación entre el volumen de origen volA encendido svm1 y el volumen de destino volA\_dst encendido svm\_backup:

```
cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
```

#### 4. Rompa la relación de tipo de DP existente:

```
snapmirror break -destination-path <SVM:volume>
```

Para obtener una sintaxis completa del comando, consulte ["página de manual"](#).



Se debe ejecutar este comando desde la SVM de destino o el clúster de destino.

En el siguiente ejemplo, se rompe la relación entre el volumen de origen volA encendido svm1 y el volumen de destino volA\_dst encendido svm\_backup:

```
cluster_dst::> snapmirror break -destination-path svm_backup:volA_dst
```

#### 5. Si la eliminación automática de las copias Snapshot está habilitada en el volumen de destino, desactívelo:

```
volume snapshot autodelete modify -vserver _SVM_ -volume _volume_
-enabled false
```

En el ejemplo siguiente se deshabilita la eliminación automática de copias Snapshot en el volumen de destino volA\_dst:

```
cluster_dst::> volume snapshot autodelete modify -vserver svm_backup
-volume volA_dst -enabled false
```

#### 6. Elimine la relación de tipo de DP existente:

```
snapmirror delete -destination-path <SVM:volume>
```

Para obtener una sintaxis completa del comando, consulte ["página de manual"](#).



Se debe ejecutar este comando desde la SVM de destino o el clúster de destino.

En el siguiente ejemplo, se elimina la relación entre el volumen de origen volA encendido svm1 y el volumen de destino volA\_dst encendido svm\_backup:

```
cluster_dst::> snapmirror delete -destination-path svm_backup:volA_dst
```

7. Libere la relación de recuperación ante desastres de la SVM de origen en el origen:

```
snapmirror release -destination-path <SVM:volume> -relationship-info
-only true
```

En el ejemplo siguiente se libera la relación de recuperación de desastres de SVM:

```
cluster_src::> snapmirror release -destination-path svm_backup:volA_dst
-relationship-info-only true
```

8. Puede utilizar la salida que ha retenido de `snapmirror show` Comando para crear la nueva relación de tipo XDP:

```
snapmirror create -source-path <SVM:volume> -destination-path
<SVM:volume> -type XDP -schedule <schedule> -policy <policy>
```

La nueva relación debe usar el mismo volumen de origen y destino. Para obtener una sintaxis de comando completa, consulte la página man.



Se debe ejecutar este comando desde la SVM de destino o el clúster de destino.

En el siguiente ejemplo se crea una relación de recuperación de desastres de SnapMirror entre el volumen de origen volA encendido svm1 y el volumen de destino volA\_dst encendido svm\_backup con el valor predeterminado MirrorAllSnapshots política:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst
-type XDP -schedule my_daily -policy MirrorAllSnapshots
```

9. Resincronización de los volúmenes de origen y destino:

```
snapmirror resync -source-path <SVM:volume> -destination-path
<SVM:volume>
```

Para mejorar el tiempo de resincronización, puede utilizar el `-quick-resync` opcional, pero debe tener en cuenta que se pueden perder ahorros en eficiencia del almacenamiento. Para obtener una sintaxis completa del comando, consulte la página man: "[Comando SnapMirror resync](#)".



Se debe ejecutar este comando desde la SVM de destino o el clúster de destino. Aunque la resincronización no requiere una transferencia básica, puede requerir mucho tiempo. Puede que desee ejecutar la resincronización en horas de menor actividad.

En el siguiente ejemplo, vuelva a establecer la relación entre el volumen de origen `volA` encendido `svm1` y el volumen de destino `volA_dst` encendido `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

10. Si ha deshabilitado la eliminación automática de copias Snapshot, vuelva a habilitarla:

```
volume snapshot autodelete modify -vserver <SVM> -volume <volume>
-enabled true
```

### Después de terminar

1. Utilice la `snapmirror show` Comando para verificar que la relación de SnapMirror se ha creado.
2. Una vez que el volumen de destino de SnapMirror XDP comienza a actualizar las copias snapshot tal como se define en la política de SnapMirror, utilice el resultado de `snapmirror list-destinations` Comando del clúster de origen para mostrar la nueva relación de XDP de SnapMirror.

## Convierta el tipo de una relación de SnapMirror

A partir de ONTAP 9.5, SnapMirror Synchronous es compatible. Puede convertir una relación de SnapMirror asíncrona en una relación de SnapMirror síncrono o viceversa sin realizar una transferencia de referencia.

### Acerca de esta tarea

No se puede convertir una relación de SnapMirror asíncrona en una relación de SnapMirror síncrono o viceversa cambiando la política de SnapMirror

### Pasos

- **Convertir una relación asíncrona de SnapMirror en una relación de SnapMirror síncrono**

- a. En el clúster de destino, elimine la relación asíncrona de SnapMirror:

```
snapmirror delete -destination-path SVM:volume
```

```
cluster2::>snapmirror delete -destination-path vs1_dr:vol1
```

- b. A partir del clúster de origen, libere la relación SnapMirror sin eliminar las copias Snapshot comunes:



```
snapmirror release -relationship-info-only true -destination-path
dest_SVM:dest_volume
```

```
cluster1::>snapmirror release -relationship-info-only true
-destination-path vs1_dr:vol1
```

- c. En el clúster de destino, cree una relación de SnapMirror Synchronous:

```
snapmirror create -source-path src_SVM:src_volume -destination-path
dest_SVM:dest_volume -policy sync-mirror
```

```
cluster2::>snapmirror create -source-path vs1:vol1 -destination-path
vs1_dr:vol1 -policy sync
```

- d. Resincronice la relación de SnapMirror síncrono:

```
snapmirror resync -destination-path dest_SVM:dest_volume
```

```
cluster2::>snapmirror resync -destination-path vs1_dr:vol1
```

• **Convertir una relación de SnapMirror Synchronous en una relación asíncrona de SnapMirror**

- a. En el clúster de destino, desactive la relación de SnapMirror síncrono existente:

```
snapmirror quiesce -destination-path dest_SVM:dest_volume
```

```
cluster2::> snapmirror quiesce -destination-path vs1_dr:vol1
```

- b. En el clúster de destino, elimine la relación asíncrona de SnapMirror:

```
snapmirror delete -destination-path SVM:volume
```

```
cluster2::>snapmirror delete -destination-path vs1_dr:vol1
```

- c. A partir del clúster de origen, libere la relación SnapMirror sin eliminar las copias Snapshot comunes:

```
snapmirror release -relationship-info-only true -destination-path
dest_SVM:dest_volume
```

```
cluster1::>snapmirror release -relationship-info-only true
-destination-path vs1_dr:vol1
```

d. A partir del clúster de destino, cree una relación de SnapMirror asíncrona:

```
snapmirror create -source-path src_SVM:src_volume -destination-path
dest_SVM:dest_volume -policy MirrorAllSnapshots
```

```
cluster2::>snapmirror create -source-path vs1:vol1 -destination-path
vs1_dr:vol1 -policy sync
```

e. Resincronice la relación de SnapMirror síncrono:

```
snapmirror resync -destination-path dest_SVM:dest_volume
```

```
cluster2::>snapmirror resync -destination-path vs1_dr:vol1
```

## Convertir el modo de una relación de SnapMirror Synchronous

A partir de ONTAP 9.5, se admiten las relaciones de SnapMirror síncrono. Puede convertir el modo de una relación de SnapMirror Synchronous de StrictSync a Sync o viceversa.

### Acerca de esta tarea

No se puede modificar la política de una relación de SnapMirror Synchronous para convertir su modo.

### Pasos

1. En el clúster de destino, desactive la relación de SnapMirror síncrono existente:

```
snapmirror quiesce -destination-path dest_SVM:dest_volume
```

```
cluster2::> snapmirror quiesce -destination-path vs1_dr:vol1
```

2. En el clúster de destino, elimine la relación de SnapMirror Synchronous existente:

```
snapmirror delete -destination-path dest_SVM:dest_volume
```

```
cluster2::> snapmirror delete -destination-path vs1_dr:vol1
```

3. A partir del clúster de origen, libere la relación SnapMirror sin eliminar las copias Snapshot comunes:

```
snapmirror release -relationship-info-only true -destination-path
dest_SVM:dest_volume
```

```
cluster1::> snapmirror release -relationship-info-only true -destination
-path vs1_dr:vol1
```

4. Desde el clúster de destino, cree una relación SnapMirror Synchronous especificando el modo en que desea convertir la relación SnapMirror Synchronous:

```
snapmirror create -source-path vs1:vol1 -destination-path dest_SVM:dest_volume
-policy Sync|StrictSync
```

```
cluster2::> snapmirror create -source-path vs1:vol1 -destination-path
vs1_dr:vol1 -policy Sync
```

5. En el clúster de destino, resincronice la relación SnapMirror:

```
snapmirror resync -destination-path dest_SVM:dest_volume
```

```
cluster2::> snapmirror resync -destination-path vs1_dr:vol1
```

## Crear y eliminar volúmenes de prueba de conmutación al nodo de respaldo de SnapMirror

A partir de ONTAP 9.14.1, puede usar System Manager para crear un clon de volumen a fin de probar la conmutación por error y la recuperación ante desastres de SnapMirror sin interrumpir la relación de SnapMirror activa. Cuando termine la prueba, puede limpiar los datos asociados y eliminar el volumen de prueba.

### Crear un volumen de prueba de conmutación por error de SnapMirror


#### Acerca de esta tarea


- Puede llevar a cabo pruebas de conmutación al nodo de respaldo en relaciones de SnapMirror síncronas y asíncronas.
- Se crea un clon de volumen para realizar la prueba de recuperación ante desastres.
- El volumen clonado se crea en la misma máquina virtual de almacenamiento que el destino de SnapMirror.
- Se pueden usar las relaciones de SnapMirror de FlexVol y FlexGroup.
- Si ya existe un clon de prueba para la relación seleccionada, no puede crear otro clon para esa relación.
- No se admiten las relaciones de almacén de SnapLock.

#### Antes de empezar

- Debe ser un administrador de clústeres.
- La licencia de SnapMirror debe instalarse en los clústeres de origen y de destino.

#### Pasos


1. En el clúster de destino, seleccione **Protección > Relaciones**.
2. Seleccione  Junto al origen de la relación y elija **Test Failover**.
3. En la ventana **Test Failover**, selecciona **Test Failover**.
4. Seleccione **Almacenamiento > Volúmenes** y compruebe que el volumen de conmutación por error de prueba aparece en la lista.

5. Seleccione **Almacenamiento > Compartir**.
6. Haga clic en  Y elige **Share**.
7. En la ventana **Agregar recurso compartido**, escriba un nombre para el recurso compartido en el campo **Compartir nombre**.
8. En el campo **Carpeta**, seleccione **Examinar**, seleccione el volumen de clonación de prueba y **Guardar**.
9. En la parte inferior de la ventana **Agregar Compartir**, seleccione **Guardar**.
10. Abra el recurso compartido en el cliente y verifique que el volumen de prueba tenga capacidades de lectura y escritura.

## Limpe los datos de conmutación por error y elimine el volumen de prueba

Después de completar las pruebas de conmutación al nodo de respaldo, puede borrar todos los datos asociados al volumen de prueba y eliminarlos.

### Pasos

1. En el clúster de destino, seleccione **Protección > Relaciones**.
2. Seleccione  Junto a la fuente de la relación y elija **Limpiar prueba de failover**.
3. En la ventana **Limpiar prueba de failover**, seleccione **Limpiar**.
4. Seleccione **Almacenamiento > Volúmenes** y compruebe que se ha eliminado el volumen de prueba.

## Proporcione datos desde un volumen de destino de recuperación ante desastres de SnapMirror

### Haga que el volumen de destino sea modificable

Debe hacer que el volumen de destino sea editable, para poder proporcionar datos del volumen a los clientes. Puede utilizar el `snapmirror quiesce` comando para detener las transferencias programadas al destino, el `snapmirror abort` comando para detener las transferencias continuas y el `snapmirror break` comando para hacer que el destino sea editable.

### Acerca de esta tarea

Debe realizar esta tarea desde la SVM de destino o el clúster de destino.

### Pasos

1. Detenga las transferencias programadas al destino:

```
snapmirror quiesce -source-path SVM:volume|cluster://SVM/volume, ...
-destination-path SVM:volume|cluster://SVM/volume, ...
```

Para obtener una sintaxis de comando completa, consulte la página man.

El siguiente ejemplo detiene las transferencias programadas entre el volumen de origen `volA` encendido `svm1` y el volumen de destino `volA_dst` encendido `svm_backup`:

```
cluster_dst:> snapmirror quiesce -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

## 2. Detenga las transferencias continuas al destino:

```
snapmirror abort -source-path SVM:volume|cluster://SVM/volume, ... -destination
-path SVM:volume|cluster://SVM/volume, ...
```

Para obtener una sintaxis de comando completa, consulte la página man.



Este paso no es necesario para relaciones de SnapMirror síncrono (se admite a partir de ONTAP 9.5).

El siguiente ejemplo detiene las transferencias continuas entre el volumen de origen volA encendido svm1 y el volumen de destino volA\_dst encendido svm\_backup:

```
cluster_dst:> snapmirror abort -source-path svm1:volA -destination-path
svm_backup:volA_dst
```

## 3. Rompa la relación de recuperación ante desastres de SnapMirror:

```
snapmirror break -source-path SVM:volume|cluster://SVM/volume, ... -destination
-path SVM:volume|cluster://SVM/volume, ...
```

Para obtener una sintaxis de comando completa, consulte la página man.

En el siguiente ejemplo, se rompe la relación entre el volumen de origen volA encendido svm1 y el volumen de destino volA\_dst encendido svm\_backup:

```
cluster_dst:> snapmirror break -source-path svm1:volA -destination-path
svm_backup:volA_dst
```

### Otras maneras de hacerlo en ONTAP

| Para ejecutar estas tareas con...                                            | Ver este contenido...                                                                   |
|------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| System Manager rediseñado (disponible con ONTAP 9.7 y versiones posteriores) | <a href="#">"Sirva datos desde un destino de SnapMirror"</a>                            |
| System Manager Classic (disponible con ONTAP 9.7 y versiones anteriores)     | <a href="#">"Información general sobre la recuperación ante desastres de volúmenes"</a> |

## Configure el volumen de destino para acceder a los datos

Tras hacer que el volumen de destino sea editable, debe configurar el volumen para el acceso a los datos. Los clientes NAS, el subsistema NVMe y hosts SAN pueden acceder a los datos desde el volumen de destino hasta que se reactive el volumen de origen.

## Entorno NAS:

1. Monte el volumen NAS en el espacio de nombres mediante la misma ruta de unión en la que se montó el volumen de origen en la SVM de origen.
2. Aplique las ACL adecuadas para los recursos compartidos de SMB en el volumen de destino.
3. Asigne las políticas de exportación de NFS al volumen de destino.
4. Aplique las reglas de cuota al volumen de destino.
5. Redirija a los clientes al volumen de destino.
6. Vuelva a montar los recursos compartidos de NFS y SMB en los clientes.

## ENTORNO SAN:

1. Asigne las LUN del volumen al iGroup correspondiente.
2. Para iSCSI, cree sesiones iSCSI desde los iniciadores de host SAN hasta las LIF DE SAN.
3. En el cliente SAN, realice una nueva exploración del almacenamiento para detectar las LUN conectadas.

Para obtener más información sobre el entorno NVMe, consulte ["Administración de SAN"](#).

## Vuelva a activar el volumen de origen original

Puede restablecer la relación de protección de datos original entre los volúmenes de origen y destino cuando ya no necesite servir datos desde el destino.

### Acerca de esta tarea

- En el siguiente procedimiento se asume que la línea base del volumen de origen original está intacta. Si la base de referencia no está intacta, debe crear e inicializar la relación entre el volumen desde el que se sirven datos y el volumen de origen original antes de realizar el procedimiento.
- La preparación en segundo plano y la fase de almacenamiento de datos de una relación de SnapMirror para XDP pueden llevar mucho tiempo. No es poco frecuente ver la relación de SnapMirror que informa sobre el estado "preparación" para un periodo de tiempo prolongado.

### Pasos

1. Invierta la relación de protección de datos original:

```
snapmirror resync -source-path SVM:volume -destination-path SVM:volume
```

Para obtener una sintaxis de comando completa, consulte la página man.



Se debe ejecutar este comando desde la SVM de origen original o desde el clúster de origen original. Aunque la resincronización no requiere una transferencia básica, puede requerir mucho tiempo. Puede que desee ejecutar la resincronización en horas de menor actividad. El comando genera errores si no existe una copia Snapshot común en el origen y el destino. Uso `snapmirror initialize` para volver a inicializar la relación.

En el siguiente ejemplo, se revierte la relación entre el volumen de origen original, `volA` encendido `svm1`, y el volumen desde el que se proporcionan datos, `volA_dst` encendido `svm_backup`:

```
cluster_src::> snapmirror resync -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

2. Una vez que esté listo para restablecer el acceso a los datos en el origen original, detenga el acceso al volumen de destino original. Una manera de hacerlo es detener la SVM de destino original:

```
vserver stop -vserver SVM
```

Para obtener una sintaxis de comando completa, consulte la página man.



Debe ejecutar este comando desde la SVM de destino original o desde el clúster de destino original. Este comando detiene el acceso del usuario a la SVM original completa de destino. Puede que desee detener el acceso al volumen de destino original mediante otros métodos.

En el ejemplo siguiente se detiene la SVM de destino original:

```
cluster_dst::> vserver stop svm_backup
```

3. Actualice la relación de inversión:

```
snapmirror update -source-path SVM:volume -destination-path SVM:volume
```

Para obtener una sintaxis de comando completa, consulte la página man.



Se debe ejecutar este comando desde la SVM de origen original o desde el clúster de origen original.

En el siguiente ejemplo, se actualiza la relación entre el volumen desde el que se proporcionan datos, volA\_dst encendido svm\_backup, y el volumen de origen original, volA encendido svm1:

```
cluster_src::> snapmirror update -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

4. Desde la SVM de origen original o el clúster de origen original, detenga las transferencias programadas para la relación inversa:

```
snapmirror quiesce -source-path SVM:volume -destination-path SVM:volume
```

Para obtener una sintaxis de comando completa, consulte la página man.



Se debe ejecutar este comando desde la SVM de origen original o desde el clúster de origen original.

En el ejemplo siguiente se detienen las transferencias programadas entre el volumen de destino original, volA\_dst encendido svm\_backup, y el volumen de origen original, volA encendido svm1:

```
cluster_src::> snapmirror quiesce -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

5. Cuando la actualización final se completa y la relación indica "Quiesced" para el estado de la relación, ejecute el siguiente comando desde la SVM de origen original o el clúster de origen original para romper la relación inversa:

```
snapmirror break -source-path SVM:volume -destination-path SVM:volume
```

Para obtener una sintaxis de comando completa, consulte la página man.



Se debe ejecutar este comando desde la SVM de origen original o desde el clúster de origen.

En el siguiente ejemplo, se rompe la relación entre el volumen de destino original, volA\_dst encendido svm\_backup, y el volumen de origen original, volA encendido svm1:

```
cluster_src::> snapmirror break -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

6. En la SVM de origen original o en el clúster de origen original, elimine la relación de protección de datos inversa:

```
snapmirror delete -source-path SVM:volume -destination-path SVM:volume
```

Para obtener una sintaxis de comando completa, consulte la página man.



Se debe ejecutar este comando desde la SVM de origen original o desde el clúster de origen original.

En el siguiente ejemplo, se elimina la relación inversa entre el volumen de origen original, volA encendido svm1, y el volumen desde el que se proporcionan datos, volA\_dst encendido svm\_backup:

```
cluster_src::> snapmirror delete -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

7. Libere la relación inversa de la SVM de destino original o el clúster de destino original.

```
snapmirror release -source-path SVM:volume -destination-path SVM:volume
```



Debe ejecutar este comando desde la SVM de destino original o desde el clúster de destino original.

En el ejemplo siguiente se libera la relación inversa entre el volumen de destino original, volA\_dst encendido svm\_backup, y el volumen de origen original, volA encendido svm1:



```
cluster_dst:> snapmirror release -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

8. Restablezca la relación de protección de datos original desde el destino original:

```
snapmirror resync -source-path SVM:volume -destination-path SVM:volume
```

Para obtener una sintaxis de comando completa, consulte la página man.

En el siguiente ejemplo, se restablece la relación entre el volumen de origen original, volA encendido svm1, y el volumen de destino original, volA\_dst encendido svm\_backup:

```
cluster_dst:> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

9. Si es necesario, inicie la SVM de destino original:

```
vserver start -vserver SVM
```

Para obtener una sintaxis de comando completa, consulte la página man.

En el ejemplo siguiente se inicia la SVM de destino original:

```
cluster_dst:> vserver start svm_backup
```

### Después de terminar

Utilice la `snapmirror show` Comando para verificar que la relación de SnapMirror se ha creado. Para obtener una sintaxis de comando completa, consulte la página man.

## Restaurar los archivos de un volumen de destino de SnapMirror

### Restaure un solo espacio de nombres de archivos, LUN o NVMe desde un destino de SnapMirror

Puede restaurar un solo archivo, LUN, un conjunto de archivos o LUN a partir de una copia Snapshot o un espacio de nombres NVMe desde un volumen de destino de SnapMirror. A partir de ONTAP 9.7, también es posible restaurar espacios de nombres NVMe desde un destino de SnapMirror síncrono. Es posible restaurar archivos en el volumen de origen original o en otro volumen.

### Lo que necesitará

Para restaurar un archivo o una LUN a partir de un destino de SnapMirror síncrono (compatible a partir de ONTAP 9.5), primero debe eliminar y liberar la relación.

### Acerca de esta tarea

El volumen al que va a restaurar archivos o LUN (el volumen de destino) debe ser un volumen de lectura y escritura:

- SnapMirror realiza una *restauración incremental* si los volúmenes de origen y destino tienen una copia Snapshot común (como suele ocurrir cuando se restaura al volumen de origen original).
- De lo contrario, SnapMirror realiza una *restauración\_base*, en la que la copia Snapshot especificada y todos los bloques de datos a los que hace referencia se transfieren al volumen de destino.

## Pasos

1. Enumere las copias Snapshot en el volumen de destino:

```
volume snapshot show -vserver SVM -volume volume
```

Para obtener una sintaxis de comando completa, consulte la página [man](#).

En el ejemplo siguiente se muestran las copias Snapshot en el `vserverB:secondary1` destino:

```
cluster_dst::> volume snapshot show -vserver vserverB -volume secondary1
```

| Vserver<br>Used% | Volume     | Snapshot               | State | Size  | Total% |
|------------------|------------|------------------------|-------|-------|--------|
| -----            | -----      | -----                  | ----- | ----- | -----  |
| vserverB<br>0%   | secondary1 | hourly.2013-01-25_0005 | valid | 224KB | 0%     |
| 0%               |            | daily.2013-01-25_0010  | valid | 92KB  | 0%     |
| 0%               |            | hourly.2013-01-25_0105 | valid | 228KB | 0%     |
| 0%               |            | hourly.2013-01-25_0205 | valid | 236KB | 0%     |
| 0%               |            | hourly.2013-01-25_0305 | valid | 244KB | 0%     |
| 0%               |            | hourly.2013-01-25_0405 | valid | 244KB | 0%     |
| 0%               |            | hourly.2013-01-25_0505 | valid | 244KB | 0%     |

7 entries were displayed.

2. Restaure un solo archivo o LUN, o un conjunto de archivos o LUN a partir de una copia Snapshot en un volumen de destino de SnapMirror:

```
snapmirror restore -source-path SVM:volume|cluster://SVM/volume, ...
-destination-path SVM:volume|cluster://SVM/volume, ... -source-snapshot snapshot
-file-list source_file_path,@destination_file_path
```

Para obtener una sintaxis de comando completa, consulte la página [man](#).



Se debe ejecutar este comando desde la SVM de destino o el clúster de destino.

El siguiente comando restaura los archivos file1 y.. file2 Desde la copia Snapshot daily.2013-01-25\_0010 en el volumen de destino original secondary1, en la misma ubicación del sistema de archivos activo del volumen de origen original primary1:

```
cluster_dst:> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list /dir1/file1,/dir2/file2
```

```
[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

El siguiente comando restaura los archivos file1 y.. file2 Desde la copia Snapshot daily.2013-01-25\_0010 en el volumen de destino original secondary1, a una ubicación diferente en el sistema de archivos activo del volumen de origen original primary1.

La ruta del archivo de destino comienza con el símbolo @ seguido por la ruta del archivo desde la raíz del volumen de origen original. En este ejemplo: file1 se restaura a. /dir1/file1.new y file2 se restaura a. /dir2.new/file2 encendido primary1:

```
cluster_dst:> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list
/dir/file1,@/dir1/file1.new,/dir2/file2,@/dir2.new/file2
```

```
[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

El siguiente comando restaura los archivos file1 y.. file3 Desde la copia Snapshot daily.2013-01-25\_0010 en el volumen de destino original secondary1, a distintas ubicaciones del sistema de archivos activo del volumen de origen original primary1, y restauraciones file2 de snap1 a la misma ubicación en el sistema de archivos activo de primary1.

En este ejemplo, el archivo file1 se restaura a. /dir1/file1.new y.. file3 se restaura a. /dir3.new/file3:

```
cluster_dst:> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list
/dir/file1,@/dir1/file1.new,/dir2/file2,/dir3/file3,@/dir3.new/file3
```

```
[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

## Restaurar el contenido de un volumen a partir de un destino de SnapMirror

Puede restaurar el contenido de un volumen completo desde una copia Snapshot en un volumen de destino de SnapMirror. Es posible restaurar el contenido del volumen en el volumen de origen original o en otro volumen.

### Acerca de esta tarea

El volumen de destino de la operación de restauración debe ser uno de los siguientes:

- Un volumen de lectura y escritura, en cuyo caso SnapMirror realiza una *incremental restore*, siempre y cuando los volúmenes de origen y destino tengan una copia Snapshot común (como suele ser el caso en el momento de restaurar el volumen de origen original).



Error del comando si no hay una copia Snapshot común. No es posible restaurar el contenido de un volumen en un volumen vacío de lectura/escritura.

- Un volumen de protección de datos vacío, en cuyo caso SnapMirror ejecuta una *restauración básica*, en la que la copia Snapshot especificada y todos los bloques de datos a los que hace referencia se transfieren al volumen de origen.

La restauración del contenido de un volumen es una operación disruptiva. No debe ejecutarse el tráfico de SMB en el volumen primario de SnapVault cuando se ejecuta una operación de restauración.

Si el volumen de destino de la operación de restauración tiene la compresión habilitada y el volumen de origen no tiene la compresión habilitada, se debe deshabilitar la compresión en el volumen de destino. Es necesario volver a habilitar la compresión una vez que se completa la operación de restauración.

Las reglas de cuota definidas para el volumen de destino se desactivan antes de ejecutar la restauración. Puede utilizar el `volume quota modify` comando para reactivar las reglas de cuota una vez completada la operación de restauración.

### Pasos

1. Enumere las copias Snapshot en el volumen de destino:

```
volume snapshot show -vserver <SVM> -volume <volume>
```

Para obtener una sintaxis de comando completa, consulte la página man.

En el ejemplo siguiente se muestran las copias Snapshot en el `vserverB:secondary1` destino:

```
cluster_dst::> volume snapshot show -vserver vserverB -volume secondary1
```

| Vserver  | Volume     | Snapshot               | State | Size  | Total%<br>Used% |
|----------|------------|------------------------|-------|-------|-----------------|
| -----    | -----      | -----                  | ----- | ----- | -----           |
| vserverB | secondary1 | hourly.2013-01-25_0005 | valid | 224KB | 0%              |
|          |            | daily.2013-01-25_0010  | valid | 92KB  | 0%              |
|          |            | hourly.2013-01-25_0105 | valid | 228KB | 0%              |
|          |            | hourly.2013-01-25_0205 | valid | 236KB | 0%              |
|          |            | hourly.2013-01-25_0305 | valid | 244KB | 0%              |
|          |            | hourly.2013-01-25_0405 | valid | 244KB | 0%              |
|          |            | hourly.2013-01-25_0505 | valid | 244KB | 0%              |

7 entries were displayed.

## 2. Restaure el contenido de un volumen de una copia Snapshot en un volumen de destino de SnapMirror:

```
snapmirror restore -source-path <SVM:volume>|<cluster://SVM/volume>
-destination-path <SVM:volume>|<cluster://SVM/volume> -source-snapshot
<snapshot>
```

Para obtener una sintaxis de comando completa, consulte la página man.



Se debe ejecutar este comando desde la SVM de origen original o desde el clúster de origen original.

El siguiente comando restaura el contenido del volumen de origen original primary1 Desde la copia Snapshot daily.2013-01-25\_0010 en el volumen de destino original secondary1:

```
cluster_src::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010
```

Warning: All data newer than Snapshot copy daily.2013-01-25\_0010 on volume vserverA:primary1 will be deleted.

Do you want to continue? {y|n}: y

[Job 34] Job is queued: snapmirror restore from source vserverB:secondary1 for the snapshot daily.2013-01-25\_0010.

3. Vuelva a montar el volumen restaurado y reinicie todas las aplicaciones que utilizan el volumen.

#### Otras maneras de hacerlo en ONTAP

| Para ejecutar estas tareas con...                                            | Ver este contenido...                                                                       |
|------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| System Manager rediseñado (disponible con ONTAP 9.7 y versiones posteriores) | <a href="#">"Restaurar un volumen de una copia de Snapshot anterior"</a>                    |
| System Manager Classic (disponible con ONTAP 9.7 y versiones anteriores)     | <a href="#">"Información general sobre la restauración de volúmenes mediante SnapVault"</a> |

## Actualice manualmente una relación de replicación

Es posible que deba actualizar una relación de replicación manualmente si falla una actualización debido a que se trasladó el volumen de origen.

#### Acerca de esta tarea

SnapMirror cancela todas las transferencias desde un volumen de origen movido hasta que se actualice la relación de replicación de forma manual.

A partir de ONTAP 9.5, se admiten las relaciones de SnapMirror síncrono. Si bien los volúmenes de origen y destino están sincronizados en todo momento en estas relaciones, la vista del clúster secundario se sincroniza con el primario solo por hora. Si desea ver los datos de un momento específico en el destino, debe realizar una actualización manual ejecutando el `snapmirror update` comando.

#### Paso

1. Actualice manualmente una relación de replicación:

```
snapmirror update -source-path SVM:volume|cluster://SVM/volume, ... -destination
-path SVM:volume|cluster://SVM/volume, ...
```

Para obtener una sintaxis de comando completa, consulte la página man.



Se debe ejecutar este comando desde la SVM de destino o el clúster de destino. El comando genera errores si no existe una copia Snapshot común en el origen y el destino. Use `snapmirror initialize` para volver a inicializar la relación.

En el ejemplo siguiente se actualiza la relación entre el volumen de origen `volA` encendido `svm1` y el volumen de destino `volA_dst` encendido `svm_backup`:

```
cluster_src::> snapmirror update -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

## Resincronice una relación de replicación

Es necesario volver a sincronizar una relación de replicación después de hacer que un volumen de destino sea modificable, después de un error en la actualización porque no existe una copia Snapshot común en los volúmenes de origen y destino o si desea cambiar la política de replicación de la relación.

### Acerca de esta tarea

- Aunque la resincronización no requiere una transferencia básica, puede requerir mucho tiempo. Puede que desee ejecutar la resincronización en horas de menor actividad.
- Los volúmenes que forman parte de una configuración en cascada o de dispersión pueden tardar más en resincronizar. No es poco frecuente ver la relación de SnapMirror que informa sobre el estado "preparación" para un periodo de tiempo prolongado.

### Paso

1. Resincronización de los volúmenes de origen y destino:

```
snapmirror resync -source-path SVM:volume|cluster://SVM/volume, ... -destination
-path SVM:volume|cluster://SVM/volume, ... -type DP|XDP -policy policy
```

Para obtener una sintaxis de comando completa, consulte la página `man`.



Se debe ejecutar este comando desde la SVM de destino o el clúster de destino.

En el siguiente ejemplo, vuelva a establecer la relación entre el volumen de origen `volA` encendido `svm1` y el volumen de destino `volA_dst` encendido `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

## Elimine una relación de replicación de volúmenes

Puede utilizar el `snapmirror delete` y `snapmirror release` comandos para eliminar una relación de replicación de volumen. A continuación, puede eliminar manualmente los volúmenes de destino innecesarios.

### Acerca de esta tarea

La `snapmirror release` Comando elimina todas las copias Snapshot creadas con SnapMirror del origen. Puede utilizar el `-relationship-info-only` Opción a conservar las copias Snapshot.

## Pasos

1. Desactive la relación de replicación:

```
snapmirror quiesce -destination-path SVM:volume|cluster://SVM/volume
```

```
cluster_dst:> snapmirror quiesce -destination-path svm_backup:volA_dst
```

2. (Opcional) rompa la relación de replicación si requiere que el volumen de destino sea un volumen de lectura/escritura. Puede omitir este paso si planea eliminar el volumen de destino o si no necesita que el volumen sea de lectura/escritura:

```
snapmirror break -source-path SVM:volume|cluster://SVM/volume, ... -destination-path SVM:volume|cluster://SVM/volume, ...
```

```
cluster_dst:> snapmirror break -source-path svm1:volA -destination-path svm_backup:volA_dst
```

3. Elimine la relación de replicación:

```
snapmirror delete -source-path SVM:volume|cluster://SVM/volume, ... -destination-path SVM:volume|cluster://SVM/volume, ...
```

Para obtener una sintaxis de comando completa, consulte la página man.



Debe ejecutar este comando desde el clúster de destino o la SVM de destino.

En el siguiente ejemplo, se elimina la relación entre el volumen de origen `volA` encendido `svm1` y el volumen de destino `volA_dst` encendido `svm_backup`:

```
cluster_dst:> snapmirror delete -source-path svm1:volA -destination-path svm_backup:volA_dst
```

4. Libere la información de relaciones de replicación desde la SVM de origen:

```
snapmirror release -source-path SVM:volume|cluster://SVM/volume, ... -destination-path SVM:volume|cluster://SVM/volume, ...
```

Para obtener una sintaxis de comando completa, consulte la página man.



Se debe ejecutar este comando desde el clúster de origen o la SVM de origen.

En el siguiente ejemplo, se libera información para la relación de replicación especificada desde la SVM de origen `svm1`:



```
cluster_src::> snapmirror release -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

## Gestión de la eficiencia del almacenamiento

SnapMirror mantiene la eficiencia del almacenamiento en los volúmenes de origen y destino, con una excepción, cuando se habilita la compresión de datos de postprocesamiento en el destino. En este caso, se pierde toda la eficiencia del almacenamiento en el destino. Para corregir este problema, hay que deshabilitar la compresión de postprocesamiento en el destino, actualizar la relación manualmente y volver a habilitar la eficiencia del almacenamiento.

### Lo que necesitará

- Las SVM y los clústeres de origen y destino deben tener una relación entre iguales.

#### "Relaciones entre iguales de clústeres y SVM"

- Debe deshabilitar la compresión de postprocesamiento en el destino.

### Acerca de esta tarea

Puede utilizar el `volume efficiency show` comando para determinar si la eficiencia está habilitada en un volumen. Para obtener más información, consulte las páginas de manual.

Puede comprobar si SnapMirror mantiene la eficiencia del almacenamiento consultando los registros de auditoría de SnapMirror y buscando la descripción de la transferencia. Si aparece la descripción de la transferencia `transfer_desc=Logical Transfer`, SnapMirror no mantiene la eficiencia del almacenamiento. Si aparece la descripción de la transferencia `transfer_desc=Logical Transfer with Storage Efficiency`, SnapMirror mantiene la eficiencia del almacenamiento. Por ejemplo:

```
Fri May 22 02:13:02 CDT 2020 ScheduledUpdate[May 22 02:12:00]:cc0fbc29-
b665-11e5-a626-00a09860c273 Operation-Uid=39fbcf48-550a-4282-a906-
df35632c73a1 Group=none Operation-Cookie=0 action=End source=<sourcepath>
destination=<destpath> status=Success bytes_transferred=117080571
network_compression_ratio=1.0:1 transfer_desc=Logical Transfer - Optimized
Directory Mode
```

### Transferencia lógica con almacenamiento

A partir de ONTAP 9.3, ya no se requiere la actualización manual para volver a habilitar la eficiencia del almacenamiento. Si SnapMirror detecta que la compresión de postprocesamiento se ha deshabilitado, vuelve a habilitar automáticamente la eficiencia del almacenamiento en la siguiente actualización programada. Tanto el origen como el destino deben ejecutar ONTAP 9.3.

A partir de ONTAP 9.3, los sistemas AFF gestionan las configuraciones de eficiencia del almacenamiento de forma diferente a las de los sistemas FAS después de crear su escritura en un volumen de destino:

- Después de hacer que un volumen de destino pueda ser modificable mediante el `snapmirror break` la

política de almacenamiento en caché del volumen se establece automáticamente en "auto" (valor predeterminado).



Este comportamiento se aplica solo a volúmenes FlexVol, y no se aplica a volúmenes FlexGroup.

- En la resincronización, la política de almacenamiento en caché se establece automáticamente en «'none'» y la deduplicación y la compresión en línea se deshabilitan automáticamente, independientemente de la configuración original. Debe modificar los ajustes manualmente según sea necesario.



Las actualizaciones manuales con eficiencia del almacenamiento, que pueden ser laboriosas. Se recomienda ejecutar la operación en horas de menor actividad.

## Paso

1. Actualice una relación de replicación y vuelva a habilitar la eficiencia del almacenamiento:

```
snapmirror update -source-path SVM:volume|cluster://SVM/volume, ... -destination
-path SVM:volume|cluster://SVM/volume, ... -enable-storage-efficiency true
```

Para obtener una sintaxis de comando completa, consulte la página man.



Se debe ejecutar este comando desde la SVM de destino o el clúster de destino. El comando genera errores si no existe una copia Snapshot común en el origen y el destino. Uso `snapmirror initialize` para volver a inicializar la relación.

En el ejemplo siguiente se actualiza la relación entre el volumen de origen `volA` encendido `svm1` y el volumen de destino `volA_dst` encendido `svm_backup` y reactivación de la eficacia de almacenamiento:

```
cluster_dst::> snapmirror update -source-path svm1:volA -destination
-path svm_backup:volA_dst -enable-storage-efficiency true
```

## Use la limitación global de SnapMirror

La limitación de red global está disponible para todas las transferencias de SnapMirror y SnapVault a nivel de nodo.

### Acerca de esta tarea

La limitación global de SnapMirror restringe el ancho de banda utilizado por transferencias entrantes o salientes de SnapMirror y SnapVault. La restricción se aplica en todo el clúster en todos los nodos del clúster.

Por ejemplo, si el acelerador saliente está establecido en 100 Mbps, cada nodo del clúster tendrá el ancho de banda saliente establecido en 100 Mbps. Si la regulación global está deshabilitada, se desactiva en todos los nodos.

Aunque las velocidades de transferencia de datos a menudo se expresan en bits por segundo (bps), los valores del acelerador deben introducirse en kilobytes por segundo (kbps).



En las versiones ONTAP 9.9.1 y anteriores, el acelerador no tiene ningún efecto activado `volume move` transferencias o transferencias de reflejos con uso compartido de la carga. A partir de ONTAP 9.10.0, es posible especificar una opción para acelerar las operaciones de movimiento de volúmenes. Para obtener más información, consulte ["Cómo acelerar el movimiento del volumen en ONTAP 9.10 y versiones posteriores."](#)

La limitación global funciona con la función acelerador por relación para transferencias de SnapMirror y SnapVault. El acelerador por relación se aplica hasta que el ancho de banda combinado de las transferencias por relación supere el valor de la aceleración global, después de lo cual se aplica la aceleración global. Un valor de acelerador 0 implica que la limitación global está desactivada.



La regulación global de SnapMirror no tiene ningún efecto en las relaciones de SnapMirror síncrono cuando están en sincronización. Sin embargo, el acelerador hace efecto en las relaciones de SnapMirror síncrono cuando realizan una fase de transferencia asíncrona, como una operación de inicialización o después de un evento de no sincronización. Por este motivo, no se recomienda habilitar la regulación global con relaciones de SnapMirror síncrono.

## Pasos

1. Habilitar la limitación global:

```
options -option-name replication.throttle.enable on|off
```

El siguiente ejemplo muestra cómo habilitar la regulación global de SnapMirror `cluster_dst`:

```
cluster_dst::> options -option-name replication.throttle.enable on
```

2. Especifique el ancho de banda total máximo utilizado por las transferencias entrantes en el clúster de destino:

```
options -option-name replication.throttle.incoming.max_kbs KBps
```

El ancho de banda mínimo recomendado del acelerador es de 4 kbps y el máximo es de 2 TB/s. El valor predeterminado de esta opción es `unlimited`, lo que significa que no hay límite en el ancho de banda total utilizado.

El siguiente ejemplo muestra cómo establecer el ancho de banda total máximo utilizado por las transferencias entrantes en 100 Mbps:

```
cluster_dst::> options -option-name
replication.throttle.incoming.max_kbs 12500
```



100 Mbps = 12500 kbps

3. Especifique el ancho de banda total máximo que utilizan las transferencias salientes en el clúster de origen:

```
options -option-name replication.throttle.outgoing.max_kbs KBps
```

El ancho de banda mínimo recomendado del acelerador es de 4 kbps y el máximo es de 2 TB/s. El valor

predeterminado de esta opción es `unlimited`, lo que significa que no hay límite en el ancho de banda total utilizado. Los valores de los parámetros están en kbps.

En el siguiente ejemplo se muestra cómo establecer el ancho de banda total máximo utilizado por las transferencias salientes en 100 Mbps:

```
cluster_src::> options -option-name
replication.throttle.outgoing.max_kbs 12500
```

## Gestione la replicación de SVM de SnapMirror

### Acerca de la replicación de SVM de SnapMirror

Puede usar SnapMirror para crear una relación de protección de datos entre SVM. En este tipo de relación de protección de datos, se replica toda o parte de la configuración de la SVM, desde las exportaciones NFS y los recursos compartidos de SMB hasta el RBAC, así como los datos en los volúmenes que posee la SVM.

#### Tipos de relaciones admitidos

Solo los SVM que proporcionan servicios de datos pueden replicarse. Se admiten los siguientes tipos de relaciones de protección de datos:

- *SnapMirror DR*, en el que el destino normalmente solo contiene las copias Snapshot que están actualmente en el origen.

A partir de ONTAP 9.9.1, este comportamiento cambia cuando se utiliza la directiva `mirror-vault`. A partir de ONTAP 9.9.1, puede crear diferentes políticas de Snapshot en el origen y el destino; las copias Snapshot en el destino no se sobrescriben con las copias Snapshot en el origen:

- No se sobrescriben del origen al destino durante las operaciones programadas normales, las actualizaciones y la resincronización
- No se eliminan durante las operaciones de interrupción.
- No se eliminan durante las operaciones de resincronización.  
Cuando configura una relación de desastre de SVM con la política de reflejo-almacén con ONTAP 9.9.1 y versiones posteriores, la política se comporta de la siguiente manera:
- Las políticas de copia de Snapshot definidas por el usuario en el origen no se copian en el destino.
- Las políticas de copia de Snapshot definidas por el sistema no se copian en el destino.
- La asociación de volumen con políticas de Snapshot definidas por el usuario y el sistema no se copia en el destino.

SVM.

- A partir de ONTAP 9.2, se *replicación unificada de SnapMirror*, en el que el destino está configurado para recuperación ante desastres y retención a largo plazo.

Aquí puede encontrar información detallada sobre estos tipos de relaciones: ["Replicación de volúmenes de SnapMirror"](#).

El *policy type* de la directiva de replicación determina el tipo de relación que admite. La siguiente tabla muestra los tipos de políticas disponibles.

| Tipo de política  | Tipo de relación                          |
|-------------------|-------------------------------------------|
| reflejo asíncrono | Recuperación ante desastres de SnapMirror |
| mirror-vault      | Replicación unificada                     |

### XDP sustituye a DP como la replicación SVM predeterminada en ONTAP 9.4

A partir de ONTAP 9.4, las relaciones de protección de datos de la SVM se establecen en el modo XDP de manera predeterminada. Las relaciones de protección de datos de SVM siguen siendo las predeterminadas para el modo DP en ONTAP 9.3 y versiones anteriores.

Las relaciones existentes no se ven afectadas por el nuevo valor predeterminado. Si una relación ya es del tipo DP, seguirá siendo del tipo DP. La siguiente tabla muestra el comportamiento que puede esperar.

| Si especifica...    | El tipo es... | La política predeterminada (si no se especifica una política) es... |
|---------------------|---------------|---------------------------------------------------------------------|
| PROTECCIÓN DE DATOS | XDP           | MirrorAllSnapshots (recuperación ante desastres de SnapMirror)      |
| Nada                | XDP           | MirrorAllSnapshots (recuperación ante desastres de SnapMirror)      |
| XDP                 | XDP           | MirrorAndVault (replicación unificada)                              |

Puede encontrar más información sobre los cambios en el valor predeterminado aquí: ["XDP sustituye a DP como la opción predeterminada de SnapMirror"](#).



La independencia de la versión no se admite para la replicación de SVM. En una configuración de recuperación ante desastres de SVM, la máquina virtual de almacenamiento de destino debe estar en un clúster que ejecute la misma versión de ONTAP que el clúster de SVM de origen para admitir operaciones de conmutación al nodo de respaldo y conmutación de conmutación por error.

### "Versiones de ONTAP compatibles para relaciones de SnapMirror"

### Cómo se replican las configuraciones de SVM

El contenido de una relación de replicación de SVM se determina por la interacción de los siguientes campos:

- La `-identity-preserve true` opción de `snapmirror create` El comando replica toda la configuración de SVM.

La `-identity-preserve false` La opción replica solamente los volúmenes y las configuraciones de autenticación y autorización de la SVM, así como los ajustes del protocolo y del servicio de nombres indicados en ["Configuraciones replicadas en las relaciones de recuperación ante desastres de máquina"](#)

virtual de almacenamiento".

- La `-discard-configs network` opción de `snapmirror policy create` El comando excluye las LIF y la configuración de red relacionada desde la replicación de SVM, para su uso en casos en los que las SVM de origen y destino se encuentran en subredes distintas.
- La `-vserver-dr-protection unprotected` opción de `volume modify` El comando excluye el volumen especificado de la replicación de SVM.

De lo contrario, la replicación de SVM es casi idéntica a la replicación de volúmenes. Puede utilizar prácticamente el mismo flujo de trabajo para la replicación de SVM que el que utiliza para la replicación de volúmenes.

## Detalles de soporte

La siguiente tabla muestra detalles de soporte para la replicación de SVM de SnapMirror.

| Recurso o característica                         | Detalles de soporte                                                                                                                                                                                                                                                                    |
|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Tipos de implementación                          | <ul style="list-style-type: none"><li>• Origen único en destino único</li><li>• A partir de ONTAP 9.4, punto de salida. Solo puede fan-out a dos destinos.</li></ul> <p>De forma predeterminada, solo se permite una relación de conservación de identidad real por SVM de origen.</p> |
| Tipos de relación                                | <ul style="list-style-type: none"><li>• Recuperación ante desastres con SnapMirror</li><li>• A partir de ONTAP 9.2, la replicación unificada de SnapMirror</li></ul>                                                                                                                   |
| Alcance de replicación                           | Solo interconexión de clústeres. No puede replicar SVM en el mismo clúster.                                                                                                                                                                                                            |
| Protección autónoma de ransomware                | <ul style="list-style-type: none"><li>• Compatible a partir de ONTAP 9.12.1. Para obtener más información, consulte <a href="#">"Protección autónoma de ransomware"</a></li></ul>                                                                                                      |
| Compatibilidad asíncrona de grupos de coherencia | A partir de ONTAP 9.14.1, se admiten un máximo de 32 relaciones de recuperación ante desastres de SVM cuando hay grupos de coherencia. Consulte <a href="#">"Proteja un grupo de consistencia"</a> y.. <a href="#">"Límites del grupo de consistencia"</a> si quiere más información.  |
| FabricPool                                       | A partir de ONTAP 9.6, la replicación de SVM de SnapMirror es compatible con FabricPool.                                                                                                                                                                                               |

|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>MetroCluster</p> | <p>A partir de ONTAP 9.11.1, ambos lados de una relación de recuperación ante desastres de SVM dentro de una configuración de MetroCluster pueden actuar como origen para configuraciones de recuperación ante desastres adicionales de SVM.</p> <p>A partir de ONTAP 9.5, la replicación de SVM de SnapMirror es compatible con las configuraciones de MetroCluster.</p> <ul style="list-style-type: none"> <li>• En versiones anteriores a ONTAP 9,10.X, una configuración de MetroCluster no puede ser el destino de una relación de recuperación ante desastres de SVM.</li> <li>• En ONTAP 9.10.1 y versiones posteriores, una configuración de MetroCluster puede ser el destino de una relación de recuperación de desastres de SVM únicamente con fines de migración y debe cumplir con todos los requisitos necesarios descritos en <a href="#">"TR-4966: Migración de una SVM a una solución de MetroCluster"</a>.</li> <li>• Solo una SVM activa en una configuración de MetroCluster puede ser el origen de una relación de recuperación ante desastres de SVM.</li> </ul> <p>Un origen puede ser una SVM sincronizada en origen antes de realizar una conmutación de sitios o una SVM sincronizada en destino después de efectuar una conmutación de sitios.</p> <ul style="list-style-type: none"> <li>• Cuando una configuración de MetroCluster presenta un estado estable, la SVM sincronizada en destino de MetroCluster no puede ser el origen de una relación de recuperación ante desastres de SVM, ya que los volúmenes no están en línea.</li> <li>• Cuando la SVM sincronizada en origen es el origen de una relación de recuperación ante desastres de SVM, la información sobre la relación de recuperación ante desastres de SVM de origen se replica en el partner de MetroCluster.</li> <li>• Durante los procesos de conmutación de sitios y conmutación de estado, se podría producir un error en la replicación al destino de recuperación ante desastres de SVM.</li> </ul> <p>Sin embargo, una vez que finalice el proceso de conmutación de sitios o conmutación de estado, se realizarán las siguientes actualizaciones programadas para la recuperación ante desastres de la máquina virtual de almacenamiento.</p> |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Grupo de consistencia      | Compatible a partir de ONTAP 9.14.1. Para obtener más información, consulte <a href="#">Proteja un grupo de consistencia</a> .                                                                                                                                                                                                                                                                                                                                 |
| ONTAP S3                   | No compatible con la recuperación ante desastres de SVM.                                                                                                                                                                                                                                                                                                                                                                                                       |
| SnapMirror síncrono        | No compatible con la recuperación ante desastres de SVM.                                                                                                                                                                                                                                                                                                                                                                                                       |
| Independencia de versiones | No admitido.                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Cifrado de volúmenes       | <ul style="list-style-type: none"> <li>• Los volúmenes cifrados en el origen se cifran en el destino.</li> <li>• Los servidores incorporados de Key Manager o KMIP deben configurarse en el destino.</li> <li>• En el destino se generan nuevas claves de cifrado.</li> <li>• Si el destino no contiene un nodo compatible con el cifrado de volúmenes ., la replicación se realiza correctamente, pero los volúmenes de destino no están cifrados.</li> </ul> |

### Configuraciones replicadas en las relaciones de recuperación ante desastres de máquina virtual de almacenamiento

La siguiente tabla muestra la interacción del `snapmirror create -identity-preserve` y la `snapmirror policy create -discard-configs network` opción:

| Configuración replicada            |         | <b>-identity-preserve true</b>                                |                                                               | <b>-identity-preserve false</b> |
|------------------------------------|---------|---------------------------------------------------------------|---------------------------------------------------------------|---------------------------------|
|                                    |         | <b>Política sin<br/>-discard<br/>-configs<br/>network set</b> | <b>Política con<br/>-discard<br/>-configs<br/>network set</b> |                                 |
| Red                                | LIF NAS | Sí                                                            | No                                                            | No                              |
| Configuración de Kerberos para LIF | Sí      | No                                                            | No                                                            | LIF SAN                         |
| No                                 | No      | No                                                            | Directivas de firewall                                        | Sí                              |
| Sí                                 | No      | Normativas de servicio                                        | Sí                                                            | Sí                              |
| No                                 | Rutas   | Sí                                                            | No                                                            | No                              |



|                          |                                      |                                |                                              |                                                                |
|--------------------------|--------------------------------------|--------------------------------|----------------------------------------------|----------------------------------------------------------------|
| Dominio de retransmisión | No                                   | No                             | No                                           | Subred                                                         |
| No                       | No                                   | No                             | Espacio IP                                   | No                                                             |
| No                       | No                                   | SMB                            | Servidor SMB                                 | Sí                                                             |
| Sí                       | No                                   | Grupos locales y usuario local | Sí                                           | Sí                                                             |
| Sí                       | Privilegio                           | Sí                             | Sí                                           | Sí                                                             |
| Copia oculta             | Sí                                   | Sí                             | Sí                                           | BranchCache                                                    |
| Sí                       | Sí                                   | Sí                             | Opciones del servidor                        | Sí                                                             |
| Sí                       | Sí                                   | Seguridad del servidor         | Sí                                           | Sí                                                             |
| No                       | Directorio inicial, compartir        | Sí                             | Sí                                           | Sí                                                             |
| Enlace simbólico         | Sí                                   | Sí                             | Sí                                           | Política de Fpolicy, política de FSecurity y NTFS de FSecurity |
| Sí                       | Sí                                   | Sí                             | Asignación de nombres y asignación de grupos | Sí                                                             |
| Sí                       | Sí                                   | Información de auditoría       | Sí                                           | Sí                                                             |
| Sí                       | NFS                                  | Políticas de exportación       | Sí                                           | Sí                                                             |
| No                       | Reglas de la política de exportación | Sí                             | Sí                                           | No                                                             |
| Servidor NFS             | Sí                                   | Sí                             | No                                           | RBAC                                                           |

|                           |                                                                              |                           |                      |                                                                                  |
|---------------------------|------------------------------------------------------------------------------|---------------------------|----------------------|----------------------------------------------------------------------------------|
| Certificados de seguridad | Sí                                                                           | Sí                        | No                   | Inicio de sesión de usuario, clave pública, función y configuración de funciones |
| Sí                        | Sí                                                                           | Sí                        | SSL                  | Sí                                                                               |
| Sí                        | No                                                                           | Servicios de nombres      | Hosts DNS y DNS      | Sí                                                                               |
| Sí                        | No                                                                           | Usuario UNIX y grupo UNIX | Sí                   | Sí                                                                               |
| Sí                        | Kerberos Reino y bloques de claves Kerberos                                  | Sí                        | Sí                   | No                                                                               |
| Cliente LDAP y LDAP       | Sí                                                                           | Sí                        | No                   | Grupo de red                                                                     |
| Sí                        | Sí                                                                           | No                        | NIS                  | Sí                                                                               |
| Sí                        | No                                                                           | Acceso Web y Web          | Sí                   | Sí                                                                               |
| No                        | Volumen                                                                      | Objeto                    | Sí                   | Sí                                                                               |
| Sí                        | Copias Snapshot, políticas de Snapshot y políticas de eliminación automática | Sí                        | Sí                   | Sí                                                                               |
| Política de eficiencia    | Sí                                                                           | Sí                        | Sí                   | Regla de política de cuotas y de política de cuotas                              |
| Sí                        | Sí                                                                           | Sí                        | Cola de recuperación | Sí                                                                               |
| Sí                        | Sí                                                                           | Volumen raíz              | Espacio de nombres   | Sí                                                                               |
| Sí                        | Sí                                                                           | Datos de usuarios         | No                   | No                                                                               |
| No                        | Qtrees                                                                       | No                        | No                   | No                                                                               |

|                       |        |                                        |                                                                                                               |                                                 |
|-----------------------|--------|----------------------------------------|---------------------------------------------------------------------------------------------------------------|-------------------------------------------------|
| Cuotas                | No     | No                                     | No                                                                                                            | Calidad de servicio en el nivel de los archivos |
| No                    | No     | No                                     | Atributos: estado del volumen raíz, garantía de espacio, tamaño, tamaño automático y número total de archivos | No                                              |
| No                    | No     | Calidad de servicio del almacenamiento | Grupo de políticas de calidad de servicio                                                                     | Sí                                              |
| Sí                    | Sí     | Fibre Channel (FC)                     | No                                                                                                            | No                                              |
| No                    | ISCSI  | No                                     | No                                                                                                            | No                                              |
| LUN                   | Objeto | Sí                                     | Sí                                                                                                            | Sí                                              |
| grupos de iniciadores | No     | No                                     | No                                                                                                            | conjuntos de puertos                            |
| No                    | No     | No                                     | Números de serie                                                                                              | No                                              |
| No                    | No     | SNMP                                   | usuarios v3                                                                                                   | Sí                                              |

### Límites de almacenamiento para recuperación ante desastres de SVM

En la siguiente tabla se muestra el número máximo recomendado de volúmenes y relaciones de recuperación ante desastres de SVM admitidas por objeto de almacenamiento. Debe ser consciente de que los límites dependen a menudo de la plataforma. Consulte la ["Hardware Universe"](#) para conocer los límites de su configuración específica.

| Objeto de almacenamiento | Límite                            |
|--------------------------|-----------------------------------|
| SVM                      | 300 volúmenes flexibles           |
| Pareja de HA             | 1,000 volúmenes flexibles         |
| Clúster                  | 128 Relaciones de desastre de SVM |

### Replicar las configuraciones de SVM

## Flujo de trabajo de replicación SVM de SnapMirror

La replicación SVM de SnapMirror implica la creación de la SVM de destino, la creación de una programación de trabajos de replicación y la creación e inicialización de una relación de SnapMirror.

Debe determinar qué flujo de trabajo de replicación se adapta mejor a sus necesidades:

- ["Replique toda una configuración de SVM"](#)
- ["Excluya las LIF y la configuración de red relacionada desde la replicación de SVM"](#)
- ["Exlude red, servicio de nombres y otros ajustes de la configuración de la máquina virtual de almacenamiento"](#)

## Criterios para colocar volúmenes en las SVM de destino

Al replicar volúmenes de la SVM de origen a la SVM de destino, es importante conocer los criterios para la selección de agregados.

Los agregados se seleccionan según los siguientes criterios:

- Los volúmenes siempre se colocan en agregados que no son raíz.
- Los agregados no raíz se seleccionan en función del espacio libre disponible y de la cantidad de volúmenes que ya se encuentran alojados en el agregado.

Los agregados con más espacio libre y menos volúmenes tienen prioridad. Se selecciona el agregado con la prioridad más alta.

- Los volúmenes de origen en agregados de FabricPool se colocan en agregados de FabricPool en el destino con la misma política de organización en niveles.
- Si un volumen de la SVM de origen se encuentra en un agregado de Flash Pool, el volumen se coloca en un agregado de Flash Pool en la SVM de destino, si existe un agregado de este tipo y tiene suficiente espacio libre.
- Si la `-space-guarantee` la opción del volumen que se replica se establece en `volume`, sólo se tienen en cuenta los agregados con un espacio libre superior al tamaño del volumen.
- El tamaño del volumen crece automáticamente en la SVM de destino durante la replicación, según el tamaño del volumen de origen.

Si desea reservar de antemano el tamaño en la SVM de destino, debe cambiar el tamaño del volumen. El tamaño del volumen no se reduce automáticamente en la SVM de destino según la SVM de origen.

Si desea mover un volumen de un agregado a otro, puede usar el `volume move` En la SVM de destino.

## Replique toda una configuración de SVM

Puede utilizar el `-identity-preserve true` opción de `snapmirror create` Para replicar una configuración de SVM completa.

### Antes de empezar

Las SVM y los clústeres de origen y destino deben tener una relación entre iguales.

Para obtener más información, consulte ["Cree una relación de paridad entre clústeres"](#) y.. ["Cree una relación](#)

de interconexión de clústeres entre iguales de SVM".

Para obtener una sintaxis de comando completa, consulte la página man.

### Acerca de esta tarea

Este flujo de trabajo supone que ya está usando una directiva predeterminada o una directiva de replicación personalizada.

A partir de ONTAP 9.9.1, cuando se utiliza la política de mirroring-almacén, puede crear diferentes políticas de Snapshot en la SVM de origen y de destino; las copias de Snapshot en el destino no se sobrescriben con las copias Snapshot en el origen. Para obtener más información, consulte ["Replicación de SVM de SnapMirror"](#).

### Pasos

1. Cree una SVM de destino:

```
vserver create -vserver SVM_name -subtype dp-destination
```

El nombre de SVM debe ser único en los clústeres de origen y destino.

En el ejemplo siguiente se crea una SVM de destino llamada `svm_backup`:

```
cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
```

2. En el clúster de destino, cree una relación entre iguales de SVM mediante el `vserver peer create` comando.

Para obtener más información, consulte ["Cree una relación de interconexión de clústeres entre iguales de SVM"](#).

3. Crear una programación de trabajo de replicación:

```
job schedule cron create -name job_name -month month -dayofweek day_of_week
-day day_of_month -hour hour -minute minute
```

Para `-month`, `-dayofweek`, y `-hour`, puede especificar `all` para ejecutar el trabajo cada mes, día de la semana y hora, respectivamente.



La programación mínima admitida (RPO) para volúmenes FlexVol en una relación de SnapMirror de SVM es de 15 minutos. La programación mínima admitida (RPO) para volúmenes FlexGroup en una relación de SnapMirror de SVM es de 30 minutos.

En el ejemplo siguiente se crea una programación de trabajo denominada `my_weekly`. Es decir, los sábados a las 3:00 horas:

```
cluster_dst:> job schedule cron create -name my_weekly -dayofweek
saturday -hour 3 -minute 0
```

4. A partir de la SVM de destino o el clúster de destino, cree una relación de replicación:

```
snapmirror create -source-path SVM_name: -destination-path SVM_name: -type
```

```
DP|XDP -schedule schedule -policy policy -identity-preserve true
```



Después del nombre de la SVM en el, se deben introducir dos puntos (:) -source-path y.. -destination-path opciones.

En el siguiente ejemplo se crea una relación de recuperación ante desastres de SnapMirror con los valores predeterminados `MirrorAllSnapshots` política:

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy MirrorAllSnapshots
-identity-preserve true
```

En el ejemplo siguiente se crea una relación de replicación unificada con la opción predeterminada `MirrorAndVault` política:

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy MirrorAndVault
-identity-preserve true
```

Suponiendo que ha creado una directiva personalizada con el tipo de directiva `async-mirror`, En el siguiente ejemplo se crea una relación de recuperación ante desastres de SnapMirror:

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_mirrored -identity
-preserve true
```

Suponiendo que ha creado una directiva personalizada con el tipo de directiva `mirror-vault`, en el ejemplo siguiente se crea una relación de replicación unificada:

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_unified -identity
-preserve true
```

##### 5. Detenga la SVM de destino:

```
vserver stop
```

*SVM name*

En el ejemplo siguiente se detiene una SVM de destino denominada `dvs1`:

```
cluster_dst:> vserver stop -vserver dvs1
```

6. En la SVM de destino o en el clúster de destino, inicialice la relación de replicación de SVM: +

```
snapmirror initialize -source-path SVM_name: -destination-path SVM_name:
```

En el siguiente ejemplo se inicializa la relación entre la SVM de origen, `svm1` y la SVM de destino, `svm_backup`:

```
cluster_dst:> snapmirror initialize -source-path svm1: -destination
-path svm_backup:
```

### Excluya las LIF y la configuración de red relacionada desde la replicación de SVM

Si las SVM de origen y destino están en subredes diferentes, puede utilizar `-discard -configs network` opción de `snapmirror policy create` Comando para excluir LIF y configuración de red relacionada desde la replicación de SVM.

#### Lo que necesitará

Las SVM y los clústeres de origen y destino deben tener una relación entre iguales.

Para obtener más información, consulte ["Cree una relación de paridad entre clústeres"](#) y.. ["Cree una relación de interconexión de clústeres entre iguales de SVM"](#).

#### Acerca de esta tarea

La `-identity-preserve` opción de `snapmirror create` el comando debe estar establecido en `true` Al crear la relación de replicación de SVM.

Para obtener una sintaxis de comando completa, consulte la página `man`.

#### Pasos

1. Cree una SVM de destino:

```
vserver create -vserver SVM -subtype dp-destination
```

El nombre de SVM debe ser único en los clústeres de origen y destino.

En el ejemplo siguiente se crea una SVM de destino llamada `svm_backup`:

```
cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
```

2. En el clúster de destino, cree una relación entre iguales de SVM mediante el `vserver peer create` comando.

Para obtener más información, consulte ["Cree una relación de interconexión de clústeres entre iguales de SVM"](#).

3. Crear un programa de trabajo:

```
job schedule cron create -name job_name -month month -dayofweek day_of_week
```

`-day day_of_month -hour hour -minute minute`

Para `-month`, `-dayofweek`, y `-hour`, puede especificar `all` para ejecutar el trabajo cada mes, día de la semana y hora, respectivamente.



La programación mínima admitida (RPO) para volúmenes FlexVol en una relación de SnapMirror de SVM es de 15 minutos. La programación mínima admitida (RPO) para volúmenes FlexGroup en una relación de SnapMirror de SVM es de 30 minutos.

En el ejemplo siguiente se crea una programación de trabajo denominada `my_weekly`. Es decir, los sábados a las 3:00 horas:

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

#### 4. Cree una política de replicación personalizada:

```
snapmirror policy create -vserver SVM -policy policy -type async-
mirror|vault|mirror-vault -comment comment -tries transfer_tries -transfer
-priority low|normal -is-network-compression-enabled true|false -discard
-configs network
```

Para obtener una sintaxis de comando completa, consulte la página `man`.

En el ejemplo siguiente se crea una normativa de replicación personalizada para recuperación ante desastres de SnapMirror que excluye las LIF:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
DR_exclude_LIFs -type async-mirror -discard-configs network
```

En el ejemplo siguiente se crea una directiva de replicación personalizada para la replicación unificada que excluye las LIF:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
unified_exclude_LIFs -type mirror-vault -discard-configs network
```

#### 5. A partir de la SVM de destino o el clúster de destino, ejecute el siguiente comando para crear una relación de replicación:

```
snapmirror create -source-path SVM: -destination-path SVM: -type DP|XDP
-schedule schedule -policy policy -identity-preserve true|false
```



Después del nombre de la SVM en el, se deben introducir dos puntos (:) `-source-path` y `-destination-path` opciones. Vea los ejemplos a continuación.

En el ejemplo siguiente se crea una relación de recuperación ante desastres de SnapMirror que excluye las LIF:



```
cluster_dst:> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy DR_exclude_LIFs
-identity-preserve true
```

En el ejemplo siguiente se crea una relación de replicación unificada de SnapMirror que excluye las LIF:

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy unified_exclude_LIFs
-identity-preserve true
```

#### 6. Detenga la SVM de destino:

```
vserver stop
```

*SVM name*

En el ejemplo siguiente se detiene una SVM de destino denominada dvs1:

```
cluster_dst:> vserver stop -vserver dvs1
```

#### 7. En la SVM de destino o el clúster de destino, inicialice una relación de replicación:

```
snapmirror initialize -source-path SVM: -destination-path SVM:
```

Para obtener una sintaxis de comando completa, consulte la página [man](#).

En el siguiente ejemplo se inicializa la relación entre el origen, `svm1` y el destino, `svm_backup`:

```
cluster_dst:> snapmirror initialize -source-path svm1: -destination
-path svm_backup:
```

#### Después de terminar

Es necesario configurar la red y los protocolos en la SVM de destino para acceder a los datos en caso de que se produzca un desastre.

#### Excluya la red, el servicio de nombres y otras configuraciones de la replicación de SVM

Puede utilizar el `-identity-preserve false` opción de `snapmirror create` Comando para replicar solo los volúmenes y las configuraciones de seguridad de una SVM. También se conservan algunos ajustes de protocolo y servicio de nombres.

#### Acerca de esta tarea

Para obtener una lista de los ajustes de protocolo y servicio de nombres conservados, consulte ["Configuraciones replicadas en relaciones de recuperación ante desastres de SVM"](#).

Para obtener una sintaxis de comando completa, consulte la página man.

## Antes de empezar

Las SVM y los clústeres de origen y destino deben tener una relación entre iguales.

Para obtener más información, consulte ["Cree una relación de paridad entre clústeres"](#) y.. ["Cree una relación de interconexión de clústeres entre iguales de SVM"](#).

## Pasos

1. Cree una SVM de destino:

```
vserver create -vserver SVM -subtype dp-destination
```

El nombre de SVM debe ser único en los clústeres de origen y destino.

En el ejemplo siguiente se crea una SVM de destino llamada `svm_backup`:

```
cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
```

2. En el clúster de destino, cree una relación entre iguales de SVM mediante el `vserver peer create` comando.

Para obtener más información, consulte ["Cree una relación de interconexión de clústeres entre iguales de SVM"](#).

3. Crear una programación de trabajo de replicación:

```
job schedule cron create -name job_name -month month -dayofweek day_of_week
-day day_of_month -hour hour -minute minute
```

Para `-month`, `-dayofweek`, y. `-hour`, puede especificar `all` para ejecutar el trabajo cada mes, día de la semana y hora, respectivamente.



La programación mínima admitida (RPO) para volúmenes FlexVol en una relación de SnapMirror de SVM es de 15 minutos. La programación mínima admitida (RPO) para volúmenes FlexGroup en una relación de SnapMirror de SVM es de 30 minutos.

En el ejemplo siguiente se crea una programación de trabajo denominada `my_weekly`. Es decir, los sábados a las 3:00 horas:

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

4. Cree una relación de replicación que excluya la red, el servicio de nombres y otras opciones de configuración:

```
snapmirror create -source-path SVM: -destination-path SVM: -type DP|XDP
-schedule schedule -policy policy -identity-preserve false
```



Después del nombre de la SVM en el, se deben introducir dos puntos (:) -source-path y.. -destination-path opciones. Vea los ejemplos a continuación. Se debe ejecutar este comando desde la SVM de destino o el clúster de destino.

En el siguiente ejemplo se crea una relación de recuperación ante desastres de SnapMirror con los valores predeterminados `MirrorAllSnapshots` política. La relación excluye la red, el servicio de nombres y otras opciones de configuración de la replicación de SVM:

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy MirrorAllSnapshots
-identity-preserve false
```

En el ejemplo siguiente se crea una relación de replicación unificada con la opción predeterminada `MirrorAndVault` política. La relación excluye la red, el servicio de nombres y otras opciones de configuración:

```
cluster_dst:> snapmirror create svm1: -destination-path svm_backup:
-type XDP -schedule my_daily -policy MirrorAndVault -identity-preserve
false
```

Suponiendo que ha creado una directiva personalizada con el tipo de directiva `async-mirror`, En el siguiente ejemplo se crea una relación de recuperación ante desastres de SnapMirror. La relación excluye la red, el servicio de nombres y otras opciones de configuración de la replicación de SVM:

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_mirrored -identity
-preserve false
```

Suponiendo que ha creado una directiva personalizada con el tipo de directiva `mirror-vault`, en el ejemplo siguiente se crea una relación de replicación unificada. La relación excluye la red, el servicio de nombres y otras opciones de configuración de la replicación de SVM:

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_unified -identity
-preserve false
```

## 5. Detenga la SVM de destino:

```
vserver stop
```

*SVM name*

En el ejemplo siguiente se detiene una SVM de destino denominada `dvs1`:

```
destination_cluster::> vserver stop -vserver dvs1
```

6. Si utiliza SMB, también debe configurar un servidor SMB.

Consulte ["Solo SMB: Crear un servidor SMB"](#).

7. En la SVM de destino o el clúster de destino, inicialice la relación de replicación de SVM:

```
snapmirror initialize -source-path SVM_name: -destination-path SVM_name:
```

### Después de terminar

Es necesario configurar la red y los protocolos en la SVM de destino para acceder a los datos en caso de que se produzca un desastre.

### Especifique los agregados que se utilizarán para las relaciones de recuperación ante desastres de SVM

Después de crear una SVM de recuperación ante desastres, puede usar la `aggr-list` opción con `vserver modify` Comando para limitar qué agregados se usan para alojar los volúmenes de destino de recuperación ante desastres de SVM.

### Paso

1. Cree una SVM de destino:

```
vserver create -vserver SVM -subtype dp-destination
```

2. Modifique la lista de agregados de la SVM para recuperación ante desastres a fin de limitar los agregados que se usan para alojar el volumen de la SVM para recuperación ante desastres:

```
cluster_dest::> vserver modify -vserver SVM -aggr-list <comma-separated-list>
```

### SMB Only: Cree un servidor SMB

Si la SVM de origen tiene una configuración de SMB y se optó por establecer `identity-preserve` para `false`, Debe crear un servidor SMB para la SVM de destino. En algunas configuraciones SMB, como los recursos compartidos durante la inicialización de la relación de SnapMirror, es necesario el servidor SMB.

### Pasos

1. Inicie la SVM de destino con el `vserver start` comando.

```
destination_cluster::> vserver start -vserver dvs1
[Job 30] Job succeeded: DONE
```

2. Compruebe que la SVM de destino está en la `running` el estado y el subtipo es `dp-destination` mediante el uso de `vserver show` comando.

```
destination_cluster::> vserver show
```

| Vserver   | Type | Subtype        | Admin State | Operational State | Root Volume |
|-----------|------|----------------|-------------|-------------------|-------------|
| Aggregate |      |                |             |                   |             |
| -----     |      |                |             |                   |             |
| dvs1      | data | dp-destination | running     | running           | -           |

3. Cree una LIF mediante el `network interface create` comando.

```
destination_cluster::>network interface create -vserver dvs1 -lif NAS1
-role data -data-protocol cifs -home-node destination_cluster-01 -home
-port a0a-101 -address 192.0.2.128 -netmask 255.255.255.128
```

4. Cree una ruta mediante `network route create` comando.

```
destination_cluster::>network route create -vserver dvs1 -destination
0.0.0.0/0
-gateway 192.0.2.1
```

### "Gestión de redes"

5. Configure DNS mediante la `vserver services dns create` comando.

```
destination_cluster::>vserver services dns create -domains
mydomain.example.com -vserver
dvs1 -name-servers 192.0.2.128 -state enabled
```

6. Agregue el controlador de dominio preferido mediante `vserver cifs domain preferred-dc add` comando.

```
destination_cluster::>vserver cifs domain preferred-dc add -vserver dvs1
-preferred-dc
192.0.2.128 -domain mydomain.example.com
```

7. Cree el servidor SMB mediante el `vserver cifs create` comando.

```
destination_cluster::>vserver cifs create -vserver dvs1 -domain
mydomain.example.com
-cifs-server CIFS1
```

8. Detenga la SVM de destino con el `vserver stop` comando.

```
destination_cluster::> vserver stop -vserver dvs1
[Job 46] Job succeeded: DONE
```

## Excluya volúmenes de la replicación de SVM

De forma predeterminada, se replican todos los volúmenes de datos RW de la SVM de origen. Si no desea proteger todos los volúmenes de la SVM de origen, puede usar la `-vserver-dr-protection unprotected` opción de `volume modify` Comando para excluir volúmenes de la replicación de SVM.

### Pasos

1. Excluya un volumen de la replicación SVM:

```
volume modify -vserver SVM -volume volume -vserver-dr-protection unprotected
```

Para obtener una sintaxis de comando completa, consulte la página `man`.

En el siguiente ejemplo, se excluye el volumen `volA_src` A partir de la replicación de SVM:

```
cluster_src::> volume modify -vserver SVM1 -volume volA_src -vserver-dr
-protection unprotected
```

Si más adelante desea incluir un volumen en la replicación de SVM que originalmente excluyó, ejecute el siguiente comando:

```
volume modify -vserver SVM -volume volume -vserver-dr-protection protected
```

En el siguiente ejemplo, se incluye el volumen `volA_src` En la replicación de SVM:

```
cluster_src::> volume modify -vserver SVM1 -volume volA_src -vserver-dr
-protection protected
```

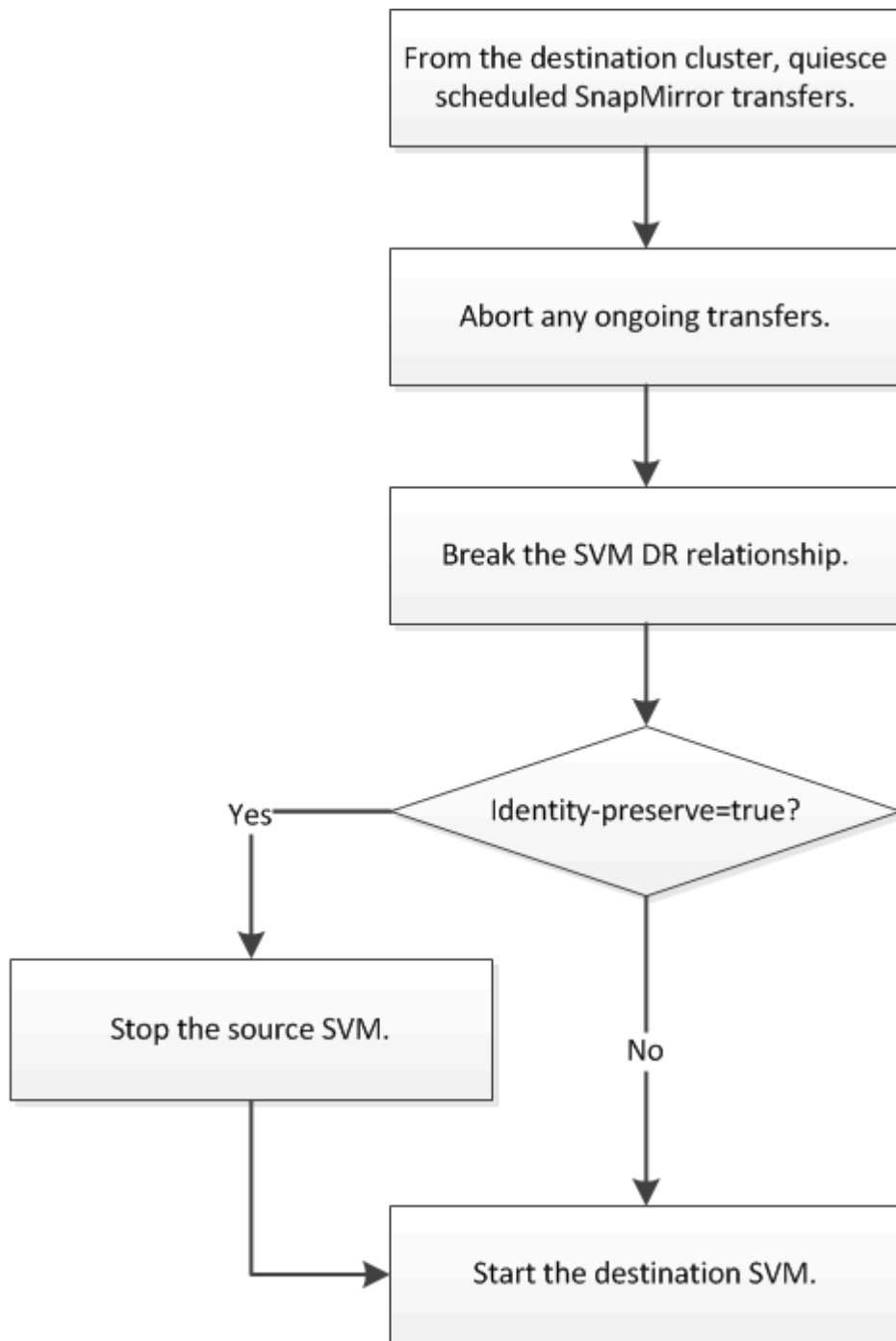
2. Cree e inicialice la relación de replicación de SVM como se describe en ["Replicar una configuración de SVM completa"](#).

## Proporcione datos desde un destino de recuperación ante desastres de SVM

### Flujo de trabajo de recuperación ante desastres de SVM

Para la recuperación ante desastres y proporcionar datos desde la SVM de destino, debe activar la SVM de destino. La activación de la SVM de destino implica la detención de transferencias programadas de SnapMirror, la anulación de las transferencias continuas de SnapMirror, la ruptura de la relación de replicación, la detención de la SVM de origen

y la inicio de la SVM de destino.



#### Haga que se puedan escribir los volúmenes de destino de SVM

Debe hacer que los volúmenes de destino de SVM sean editables antes de proporcionar datos a los clientes. El procedimiento es en gran medida idéntico al procedimiento de replicación de volúmenes, con una excepción. Si ha configurado `-identity-preserve true` Cuando se creó la relación de replicación de SVM, debe detener la SVM de origen antes de activar la SVM de destino.

#### Acerca de esta tarea

Para obtener una sintaxis de comando completa, consulte la página man.



En una situación de recuperación ante desastres, no puede realizar una actualización de SnapMirror del SVM de origen a la SVM de destino de recuperación ante desastres porque no podrá acceder a la SVM de origen y a sus datos, así como porque las actualizaciones desde la última resincronización pueden estar dañadas o estar dañadas.

## Pasos

1. Desde la SVM de destino o el clúster de destino, detenga las transferencias programadas hacia el destino:

```
snapmirror quiesce -source-path SVM: -destination-path SVM:
```



Después del nombre de la SVM en el, se deben introducir dos puntos (:) -source-path y.. -destination-path opciones. Vea el ejemplo siguiente.

En el siguiente ejemplo, se detienen las transferencias programadas entre la SVM de origen `svm1` Y la SVM de destino `svm_backup`:

```
cluster_dst::> snapmirror quiesce -source-path svm1: -destination-path
svm_backup:
```

2. Desde la SVM de destino o el clúster de destino, detenga las transferencias continuas al destino:

```
snapmirror abort -source-path SVM: -destination-path SVM:
```



Después del nombre de la SVM en el, se deben introducir dos puntos (:) -source-path y.. -destination-path opciones. Vea el ejemplo siguiente.

En el siguiente ejemplo, se detienen las transferencias continuas entre la SVM de origen `svm1` Y la SVM de destino `svm_backup`:

```
cluster_dst::> snapmirror abort -source-path svm1: -destination-path
svm_backup:
```

3. Desde la SVM de destino o el clúster de destino, rompa la relación de replicación:

```
snapmirror break -source-path SVM: -destination-path SVM:
```



Después del nombre de la SVM en el, se deben introducir dos puntos (:) -source-path y.. -destination-path opciones. Vea el ejemplo siguiente.

En el siguiente ejemplo, se rompe la relación entre la SVM de origen `svm1` Y la SVM de destino `svm_backup`:

```
cluster_dst::> snapmirror break -source-path svm1: -destination-path
svm_backup:
```



4. Si ha configurado `-identity-preserve true` Cuando creó la relación de replicación de SVM, detenga la SVM de origen:

```
vserver stop -vserver SVM
```

En el ejemplo siguiente se detiene la SVM de origen `svm1`:

```
cluster_src::> vserver stop svm1
```

5. Inicie la SVM de destino:

```
vserver start -vserver SVM
```

En el ejemplo siguiente se inicia la SVM de destino `svm_backup`:

```
cluster_dst::> vserver start svm_backup
```

### Después de terminar

Configure los volúmenes de destino de SVM para acceder a los datos, como se describe en ["Configurar el volumen de destino para acceder a los datos"](#).

## Reactivar la SVM de origen

### Flujo de trabajo de reactivación de SVM de origen

Si la SVM de origen existe después de un desastre, puede reactivarlo y protegerlo; para ello, vuelva a crear la relación de recuperación ante desastres de SVM.



### Reactivar la SVM de origen original

Puede restablecer la relación original de protección de datos entre la SVM de origen y la de destino cuando ya no necesite servir datos desde el destino. El procedimiento es en gran medida idéntico al procedimiento de replicación de volúmenes, con una excepción. Debe detener la SVM de destino antes de volver a activar la SVM de origen.

#### Antes de empezar

Si ha aumentado el tamaño del volumen de destino mientras se sirven los datos, antes de reactivar el volumen de origen, debería aumentar manualmente el tamaño máximo automático en el volumen de origen original para garantizar que pueda crecer lo suficiente.

"Cuando un volumen de destino aumenta automáticamente"

#### Acerca de esta tarea

A partir de ONTAP 9.11.1, puede reducir el tiempo de resincronización durante un ensayo de recuperación ante desastres mediante el `-quick-resync true` opción de `snapmirror resync` Comando mientras se realiza una resincronización inversa de una relación de recuperación ante desastres de SVM. Una resincronización rápida puede reducir el tiempo que lleva volver a la producción evitando las operaciones de reconstrucción y restauración del almacén de datos.



Una resincronización rápida no conserva la eficiencia del almacenamiento de los volúmenes de destino. Al habilitar una resincronización rápida, puede aumentar el espacio de volumen utilizado por los volúmenes de destino.

En este procedimiento se asume que la línea base del volumen de origen original está intacta. Si la base de referencia no está intacta, debe crear e inicializar la relación entre el volumen desde el que se sirven datos y el volumen de origen original antes de realizar el procedimiento.

Para obtener una sintaxis completa del comando en los comandos, consulte la página man.

## Pasos

1. A partir de la SVM de origen original o del clúster de origen original, cree una relación de recuperación ante desastres de SVM inversa con la misma configuración, política y conservación de identidad que la relación de recuperación ante desastres de SVM original:

```
snapmirror create -source-path SVM: -destination-path SVM:
```



Después del nombre de la SVM en el, se deben introducir dos puntos (:) -source-path y.. -destination-path opciones. Vea el ejemplo siguiente.

En el siguiente ejemplo se crea una relación entre la SVM desde la cual se proporcionan datos, svm\_backup`Y la SVM de origen original, `svm1:

```
cluster_src::> snapmirror create -source-path svm_backup: -destination
-path svm1:
```

2. Desde la SVM de origen original o el clúster de origen original, ejecute el siguiente comando para invertir la relación de protección de datos:

```
snapmirror resync -source-path SVM: -destination-path SVM:
```



Después del nombre de la SVM en el, se deben introducir dos puntos (:) -source-path y.. -destination-path opciones. Vea el ejemplo siguiente.

Aunque la resincronización no requiere una transferencia básica, puede requerir mucho tiempo. Puede que desee ejecutar la resincronización en horas de menor actividad.



El comando genera errores si no existe una copia Snapshot común en el origen y el destino. Uso `snapmirror initialize` para reiniciar la relación.

En el siguiente ejemplo se revierte la relación entre la SVM de origen original, svm1, Y la SVM desde la que se proporcionan datos, svm\_backup:

```
cluster_src::> snapmirror resync -source-path svm_backup: -destination
-path svm1:
```

Ejemplo con la opción -Quick-resync:

```
cluster_src::> snapmirror resync -source-path svm_backup: -destination
-path svm1: -quick-resync true
```

3. Cuando esté listo para restablecer el acceso a los datos a la SVM de origen original, detenga la SVM de destino original para desconectar los clientes que actualmente estén conectados a la SVM de destino original.

```
vserver stop -vserver SVM
```

En el ejemplo siguiente se detiene la SVM de destino original, que actualmente proporciona datos:

```
cluster_dst::> vserver stop svm_backup
```

4. Compruebe que la SVM de destino original esté en estado detenido con el `vserver show` comando.

```
cluster_dst::> vserver show
```

| Vserver    | Type  | Subtype | Admin State | Operational State | Root Volume |
|------------|-------|---------|-------------|-------------------|-------------|
| Aggregate  |       |         |             |                   |             |
| -----      | ----- | -----   | -----       | -----             | -----       |
| -----      |       |         |             |                   |             |
| svm_backup | data  | default | stopped     | stopped           | rv          |
| aggr1      |       |         |             |                   |             |

5. A partir de la SVM de origen original o del clúster de origen original, ejecute el siguiente comando para realizar la actualización final de la relación inversa para transferir todos los cambios de la SVM de destino original a la SVM de origen original:

```
snapmirror update -source-path SVM: -destination-path SVM:
```



Después del nombre de la SVM en el, se deben introducir dos puntos (:) -source-path y.. -destination-path opciones. Vea el ejemplo siguiente.

En el ejemplo siguiente se actualiza la relación entre la SVM de destino original a partir de la cual se proporcionan datos, `svm_backup`Y` la SVM de origen original, ``svml:`

```
cluster_src::> snapmirror update -source-path svm_backup: -destination-path svml:
```

6. Desde la SVM de origen original o el clúster de origen original, ejecute el siguiente comando para detener las transferencias programadas para la relación inversa:

```
snapmirror quiesce -source-path SVM: -destination-path SVM:
```



Después del nombre de la SVM en el, se deben introducir dos puntos (:) -source-path y.. -destination-path opciones. Vea el ejemplo siguiente.

En el ejemplo siguiente se detienen las transferencias programadas entre la SVM desde la que se proporcionan datos: `svm_backup`Y` la SVM original, ``svml:`

```
cluster_src::> snapmirror quiesce -source-path svm_backup: -destination
-path svm1:
```

7. Cuando la actualización final se completa y la relación indica "Quiesced" para el estado de la relación, ejecute el siguiente comando desde la SVM de origen original o el clúster de origen original para romper la relación inversa:

```
snapmirror break -source-path SVM: -destination-path SVM:
```



Después del nombre de la SVM en el, se deben introducir dos puntos (:) -source-path y.. -destination-path opciones. Vea el ejemplo siguiente.

En el siguiente ejemplo, se rompe la relación entre la SVM de destino original, en la que se estaban sirviendo datos, `svm_backup`Y` la SVM de origen original, ``svm1`:

```
cluster_src::> snapmirror break -source-path svm_backup: -destination
-path svm1:
```

8. Si la SVM de origen se había detenido anteriormente, desde el clúster de origen original, inicie la SVM de origen original:

```
vserver start -vserver SVM
```

En el ejemplo siguiente se inicia la SVM de origen original:

```
cluster_src::> vserver start svm1
```

9. A partir de la SVM de destino original o del clúster de destino original, restablezca la relación de protección de datos original:

```
snapmirror resync -source-path SVM: -destination-path SVM:
```



Después del nombre de la SVM en el, se deben introducir dos puntos (:) -source-path y.. -destination-path opciones. Vea el ejemplo siguiente.

En el siguiente ejemplo, se vuelve a establecer la relación entre la SVM de origen original, `svm1`Y` la SVM de destino original, ``svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1: -destination-path
svm_backup:
```

10. Desde la SVM de origen original o el clúster de origen original, ejecute el siguiente comando para eliminar la relación de protección de datos inversa:

```
snapmirror delete -source-path SVM: -destination-path SVM:
```



Después del nombre de la SVM en el, se deben introducir dos puntos (:) -source-path y.. -destination-path opciones. Vea el ejemplo siguiente.

En el siguiente ejemplo, se elimina la relación inversa entre la SVM de destino original, svm\_backup`Y la SVM de origen original, `svm1:

```
cluster_src::> snapmirror delete -source-path svm_backup: -destination
-path svm1:
```

11. Desde la SVM de destino original o el clúster de destino original, libere la relación de protección de datos inversa:

```
snapmirror release -source-path SVM: -destination-path SVM:
```



Después del nombre de la SVM en el, se deben introducir dos puntos (:) -source-path y.. -destination-path opciones. Vea el ejemplo siguiente.

En el siguiente ejemplo, se libera la relación inversa entre la SVM de destino original, svm\_backup y la SVM de origen original, svm1

```
cluster_dst::> snapmirror release -source-path svm_backup: -destination
-path svm1:
```

## Después de terminar

Utilice la `snapmirror show` Comando para verificar que la relación de SnapMirror se ha creado. Para obtener una sintaxis de comando completa, consulte la página man.

## Reactivar la SVM de origen original (solo volúmenes de FlexGroup)

Puede restablecer la relación original de protección de datos entre la SVM de origen y la de destino cuando ya no necesite servir datos desde el destino. Para reactivar la SVM de origen original cuando usa volúmenes de FlexGroup, debe realizar algunos pasos adicionales, como la eliminación de la relación de recuperación ante desastres de SVM original y la liberación de la relación original antes de revertir la relación. También debe liberar la relación inversa y volver a crear la relación original antes de detener las transferencias programadas.

## Pasos

1. De la SVM de destino original o del clúster de destino original, elimine la relación de recuperación ante desastres de SVM original:

```
snapmirror delete -source-path SVM: -destination-path SVM:
```



Después del nombre de la SVM en el, se deben introducir dos puntos (:) -source-path y.. -destination-path opciones. Vea el ejemplo siguiente.

En el siguiente ejemplo, se elimina la relación original entre la SVM de origen, svm1 y la SVM de destino original, svm\_backup:

```
cluster_dst::> snapmirror delete -source-path svm1: -destination-path
svm_backup:
```

2. A partir de la SVM de origen original o del clúster de origen original, libere la relación original mientras mantiene las copias Snapshot intactas:

```
snapmirror release -source-path SVM: -destination-path SVM: -relationship-info
-only true
```



Después del nombre de la SVM en el, se deben introducir dos puntos (:) -source-path y.. -destination-path opciones. Vea el ejemplo siguiente.

En el siguiente ejemplo, se libera la relación original entre la SVM de origen, svm1 y la SVM de destino original, svm\_backup.

```
cluster_src::> snapmirror release -source-path svm1: -destination-path
svm_backup: -relationship-info-only true
```

3. A partir de la SVM de origen original o del clúster de origen original, cree una relación de recuperación ante desastres de SVM inversa con la misma configuración, política y conservación de identidad que la relación de recuperación ante desastres de SVM original:

```
snapmirror create -source-path SVM: -destination-path SVM:
```



Después del nombre de la SVM en el, se deben introducir dos puntos (:) -source-path y.. -destination-path opciones. Vea el ejemplo siguiente.

En el siguiente ejemplo se crea una relación entre la SVM desde la cual se proporcionan datos, svm\_backup`Y la SVM de origen original, `svm1:

```
cluster_src::> snapmirror create -source-path svm_backup: -destination
-path svm1:
```

4. Desde la SVM de origen original o el clúster de origen original, ejecute el siguiente comando para invertir la relación de protección de datos:

```
snapmirror resync -source-path SVM: -destination-path SVM:
```



Después del nombre de la SVM en el, se deben introducir dos puntos (:) -source-path y.. -destination-path opciones. Vea el ejemplo siguiente.

Aunque la resincronización no requiere una transferencia básica, puede requerir mucho tiempo. Puede que desee ejecutar la resincronización en horas de menor actividad.



El comando genera errores si no existe una copia Snapshot común en el origen y el destino. Uso `snapmirror initialize` para reiniciar la relación.

En el siguiente ejemplo se revierte la relación entre la SVM de origen original, `svm1`, Y la SVM desde la que se proporcionan datos, `svm_backup`:

```
cluster_src::> snapmirror resync -source-path svm_backup: -destination
-path svm1:
```

5. Cuando esté listo para restablecer el acceso a los datos a la SVM de origen original, detenga la SVM de destino original para desconectar los clientes que actualmente estén conectados a la SVM de destino original.

```
vserver stop -vserver SVM
```

En el ejemplo siguiente se detiene la SVM de destino original, que actualmente proporciona datos:

```
cluster_dst::> vserver stop svm_backup
```

6. Compruebe que la SVM de destino original esté en estado detenido con el `vserver show` comando.

```
cluster_dst::> vserver show
```

| Vserver    | Type  | Subtype | Admin State | Operational State | Root Volume |
|------------|-------|---------|-------------|-------------------|-------------|
| Aggregate  |       |         |             |                   |             |
| -----      | ----- | -----   | -----       | -----             | -----       |
| svm_backup | data  | default | stopped     | stopped           | rv          |
| aggr1      |       |         |             |                   |             |

7. A partir de la SVM de origen original o del clúster de origen original, ejecute el siguiente comando para realizar la actualización final de la relación inversa para transferir todos los cambios de la SVM de destino original a la SVM de origen original:

```
snapmirror update -source-path SVM: -destination-path SVM:
```



Después del nombre de la SVM en el, se deben introducir dos puntos (:) `-source-path` y.. `-destination-path` opciones. Vea el ejemplo siguiente.

En el ejemplo siguiente se actualiza la relación entre la SVM de destino original a partir de la cual se proporcionan datos, `svm_backup` Y la SVM de origen original, `svm1`:

```
cluster_src::> snapmirror update -source-path svm_backup: -destination
-path svm1:
```



8. Desde la SVM de origen original o el clúster de origen original, ejecute el siguiente comando para detener las transferencias programadas para la relación inversa:

```
snapmirror quiesce -source-path SVM: -destination-path SVM:
```



Después del nombre de la SVM en el, se deben introducir dos puntos (:) -source-path y.. -destination-path opciones. Vea el ejemplo siguiente.

En el ejemplo siguiente se detienen las transferencias programadas entre la SVM desde la que se proporcionan datos: svm\_backup`Y la SVM original, `svm1:

```
cluster_src::> snapmirror quiesce -source-path svm_backup: -destination
-path svm1:
```

9. Cuando la actualización final se completa y la relación indica "Quiesced" para el estado de la relación, ejecute el siguiente comando desde la SVM de origen original o el clúster de origen original para romper la relación inversa:

```
snapmirror break -source-path SVM: -destination-path SVM:
```



Después del nombre de la SVM en el, se deben introducir dos puntos (:) -source-path y.. -destination-path opciones. Vea el ejemplo siguiente.

En el siguiente ejemplo, se rompe la relación entre la SVM de destino original, en la que se estaban sirviendo datos. svm\_backup`Y la SVM de origen original, `svm1:

```
cluster_src::> snapmirror break -source-path svm_backup: -destination
-path svm1:
```

10. Si la SVM de origen se había detenido anteriormente, desde el clúster de origen original, inicie la SVM de origen original:

```
vserver start -vserver SVM
```

En el ejemplo siguiente se inicia la SVM de origen original:

```
cluster_src::> vserver start svm1
```

11. En la SVM de origen original o en el clúster de origen, elimine la relación de recuperación ante desastres de SVM inversa:

```
snapmirror delete -source-path SVM: -destination-path SVM:
```



Después del nombre de la SVM en el, se deben introducir dos puntos (:) -source-path y.. -destination-path opciones. Vea el ejemplo siguiente.

En el siguiente ejemplo, se elimina la relación inversa entre la SVM de destino original, svm\_backup y la SVM de origen original, svm1:

```
cluster_src::> snapmirror delete -source-path svm_backup: -destination
-path svm1:
```

12. Desde la SVM de destino original o el clúster de destino original, libere la relación inversa mientras mantiene las copias Snapshot intactas:

```
snapmirror release -source-path SVM: -destination-path SVM: -relationship-info
-only true
```



Después del nombre de la SVM en el, se deben introducir dos puntos (:) -source-path y.. -destination-path opciones. Vea el ejemplo siguiente.

En el siguiente ejemplo, se libera la relación inversa entre la SVM de destino original, svm\_backup y la SVM de origen original, svm1:

```
cluster_dst::> snapmirror release -source-path svm_backup: -destination
-path svm1: -relationship-info-only true
```

13. Desde la SVM de destino original o el clúster de destino original, vuelva a crear la relación original. Utilice la misma configuración, política y conservación de identidad que la relación de recuperación ante desastres original de la SVM:

```
snapmirror create -source-path SVM: -destination-path SVM:
```



Después del nombre de la SVM en el, se deben introducir dos puntos (:) -source-path y.. -destination-path opciones. Vea el ejemplo siguiente.

En el siguiente ejemplo, se crea una relación entre la SVM de origen original, svm1 y la SVM de destino original, svm\_backup:

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup:
```

14. A partir de la SVM de destino original o del clúster de destino original, restablezca la relación de protección de datos original:

```
snapmirror resync -source-path SVM: -destination-path SVM:
```



Después del nombre de la SVM en el, se deben introducir dos puntos (:) -source-path y.. -destination-path opciones. Vea el ejemplo siguiente.

En el siguiente ejemplo, se vuelve a establecer la relación entre la SVM de origen original, svm1 y la SVM de destino original, svm\_backup:

```
cluster_dst:> snapmirror resync -source-path svm1: -destination-path
svm_backup:
```

## Convertir relaciones de replicación de volúmenes en una relación de replicación de SVM

Puede convertir relaciones de replicación entre volúmenes en una relación de replicación entre las máquinas virtuales de almacenamiento (SVM) a las que pertenecen los volúmenes, siempre que se replique cada volumen del origen (excepto el volumen raíz), y cada volumen del origen (incluido el volumen raíz) tiene el mismo nombre que el volumen en el destino.

### Acerca de esta tarea

Utilice la `volume rename` Comando cuando la relación de SnapMirror está inactiva para cambiar el nombre de los volúmenes de destino si es necesario.

### Pasos

1. Desde la SVM de destino o el clúster de destino, ejecute el siguiente comando para volver a sincronizar los volúmenes de origen y destino:

```
snapmirror resync -source-path SVM:volume -destination-path SVM:volume -type
DP|XDP -policy policy
```

Para obtener una sintaxis de comando completa, consulte la página man.



Aunque la resincronización no requiere una transferencia básica, puede requerir mucho tiempo. Puede que desee ejecutar la resincronización en horas de menor actividad.

En el siguiente ejemplo, vuelva a establecer la relación entre el volumen de origen `volA` encendido `svm1` y el volumen de destino `volA` encendido `svm_backup`:

```
cluster_dst:> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA
```

2. Cree una relación de replicación de SVM entre las SVM de origen y de destino, como se describe en ["Replicando configuraciones de SVM"](#).

Debe utilizar el `-identity-preserve true` opción de `snapmirror create` comando al crear la relación de replicación.

3. Detenga la SVM de destino:

```
vserver stop -vserver SVM
```

Para obtener una sintaxis de comando completa, consulte la página man.

En el ejemplo siguiente se detiene la SVM de destino `svm_backup`:

```
cluster_dst:> vserver stop svm_backup
```

4. Desde la SVM de destino o el clúster de destino, ejecute el siguiente comando para volver a sincronizar las SVM de origen y destino:

```
snapmirror resync -source-path SVM: -destination-path SVM: -type DP|XDP
-policy policy
```

Para obtener una sintaxis de comando completa, consulte la página man.



Después del nombre de la SVM en el, se deben introducir dos puntos (:) -source-path y.. -destination-path opciones. Vea el ejemplo siguiente.

Aunque la resincronización no requiere una transferencia básica, puede requerir mucho tiempo. Puede que desee ejecutar la resincronización en horas de menor actividad.

En el siguiente ejemplo, vuelva a establecer la relación entre la SVM de origen `svm1` Y la SVM de destino `svm_backup`:

```
cluster_dst:> snapmirror resync -source-path svm1: -destination-path
svm_backup:
```

## Eliminar una relación de replicación de SVM

Puede utilizar el `snapmirror delete` y.. `snapmirror release` Comandos para eliminar una relación de replicación de SVM. A continuación, puede eliminar manualmente los volúmenes de destino innecesarios.

### Acerca de esta tarea

La `snapmirror release` Comando elimina todas las copias Snapshot creadas con SnapMirror del origen. Puede utilizar el `-relationship-info-only` Opción a conservar las copias Snapshot.

Para obtener una sintaxis completa del comando en los comandos, consulte la página man.

### Pasos

1. Ejecute el siguiente comando desde la SVM de destino o el clúster de destino para romper la relación de replicación:

```
snapmirror break -source-path SVM: -destination-path SVM:
```



Después del nombre de la SVM en el, se deben introducir dos puntos (:) -source-path y.. -destination-path opciones. Vea el ejemplo siguiente.

En el siguiente ejemplo, se rompe la relación entre la SVM de origen `svm1` Y la SVM de destino `svm_backup`:

```
cluster_dst::> snapmirror break -source-path svm1: -destination-path
svm_backup:
```

2. Ejecute el siguiente comando desde la SVM de destino o el clúster de destino para eliminar la relación de replicación:

```
snapmirror delete -source-path SVM: -destination-path SVM:
```



Después del nombre de la SVM en el, se deben introducir dos puntos (:) -source-path y.. -destination-path opciones. Vea el ejemplo siguiente.

En el siguiente ejemplo, se elimina la relación entre la SVM de origen `svm1` Y la SVM de destino `svm_backup`:

```
cluster_dst::> snapmirror delete -source-path svm1: -destination-path
svm_backup:
```

3. Ejecute el siguiente comando desde la SVM de origen o el clúster de origen para liberar la información de relaciones de replicación desde la SVM de origen:

```
snapmirror release -source-path SVM: -destination-path SVM:
```



Después del nombre de la SVM en el, se deben introducir dos puntos (:) -source-path y.. -destination-path opciones. Vea el ejemplo siguiente.

En el siguiente ejemplo, se libera información para la relación de replicación especificada desde la SVM de origen `svm1`:

```
cluster_src::> snapmirror release -source-path svm1: -destination-path
svm_backup:
```

## Gestionar la replicación de volúmenes raíz de SnapMirror

### Información general sobre la replicación de volúmenes raíz de Manage SnapMirror

Cada SVM de un entorno NAS cuenta con un espacio de nombres único. El volumen SVM *root*, que contiene sistema operativo e información relacionada, es el punto de entrada de la jerarquía del espacio de nombres. Para garantizar que los clientes puedan acceder a los datos en caso de interrupción del servicio o conmutación al nodo de respaldo, debería crear una copia de mirroring con uso compartido de la carga del volumen raíz de la SVM.

El principal objetivo de los reflejos de uso compartido de carga para los volúmenes raíz de SVM ya no es para el uso compartido de carga; en su lugar, su finalidad es la recuperación ante desastres.

- Si el volumen raíz no está disponible temporalmente, el reflejo de uso compartido de carga proporciona acceso de solo lectura a los datos del volumen raíz.
- Si el volumen raíz no está disponible permanentemente, se puede promocionar uno de los volúmenes compartidos de carga para proporcionar acceso de escritura a los datos del volumen raíz.

## Crear e inicializar relaciones de mirroring de uso compartido de carga

Debe crear un reflejo de uso compartido de carga (LSM) para cada volumen raíz de SVM que sirva datos NAS en el clúster. En el caso de los clústeres formados por dos o más pares de alta disponibilidad, debe considerar los reflejos de uso compartido de carga de los volúmenes raíz de SVM para garantizar que los clientes sigan accesible el espacio de nombres en caso de que esto siga siendo

Los dos nodos de una pareja de alta disponibilidad fallan. Los reflejos de uso compartido de carga no son adecuados para clústeres que constan de una única pareja de alta disponibilidad.

### Acerca de esta tarea

Si crea un LSM en el mismo nodo y el nodo no está disponible, tendrá un único punto de error y no tendrá una segunda copia para garantizar que los datos sigan siendo accesibles para los clientes. Pero cuando crea el LSM en un nodo distinto al que contiene el volumen raíz o en un par de alta disponibilidad diferente, todavía se puede acceder a los datos en caso de una interrupción del servicio.

Por ejemplo, en un clúster de cuatro nodos con volumen raíz en tres nodos:

- Para el volumen raíz en el nodo 1 de alta disponibilidad, cree el LSM en el nodo 1 de alta disponibilidad 2 o el nodo 2 de alta disponibilidad.
- Para el volumen raíz en el nodo de alta disponibilidad 1 2, cree el LSM en el nodo de alta disponibilidad 2 1 o el nodo de alta disponibilidad 2.
- Para el volumen raíz en el nodo 1 de alta disponibilidad 2, cree el LSM en el nodo 1 de alta disponibilidad o el nodo 2 de alta disponibilidad 1.

### Pasos

1. Crear un volumen de destino para el LSM:

Antes de ejecutar este comando, debe sustituir las variables entre paréntesis angulares por los valores requeridos.

```
volume create -vserver <SVM> -volume <volume> -aggregate <aggregate>
-type DP -size <size>
```

El tamaño del volumen de destino debe ser igual o mayor que el del volumen raíz.

Se recomienda nombrar el volumen raíz y el volumen de destino con sufijos, como `_root` y `_m1`.

Para obtener una sintaxis de comando completa, consulte la página man.

En el siguiente ejemplo, se crea un volumen de reflejos de uso compartido de carga para el volumen raíz `svm1_root` `pulg cluster_src`:

```
cluster_src:> volume create -vserver svm1 -volume svm1_m1 -aggregate
aggr_1 -size 1gb -state online -type DP
```

2. "Cree un programa de trabajo de replicaciones".

3. Crear una relación de mirroring de uso compartido de carga entre el volumen raíz de SVM y el volumen de destino para LSM:

Antes de ejecutar este comando, debe sustituir las variables entre paréntesis angulares por los valores requeridos.

```
snapmirror create -source-path <SVM:volume> -destination-path
<SVM:volume> -type LS -schedule <schedule>
```

Para obtener una sintaxis de comando completa, consulte la página man.

En el siguiente ejemplo, se crea una relación de reflejo de uso compartido de la carga entre el volumen raíz svm1\_root y el volumen reflejado de uso compartido de la carga svm1\_m1:

```
cluster_src::> snapmirror create -source-path svm1:svm1_root
-destination-path svm1:svm1_m1 -type LS -schedule hourly
```

El atributo type del reflejo de carga compartida cambia de DP para LS.

4. Inicialice el reflejo de uso compartido de carga:

Antes de ejecutar este comando, debe sustituir las variables entre paréntesis angulares por los valores requeridos.

```
snapmirror initialize-ls-set -source-path <SVM:volume>
```

La inicialización puede requerir mucho tiempo. Puede ser conveniente ejecutar la transferencia básica en horas de menor actividad.

Para obtener una sintaxis de comando completa, consulte la página man.

En el ejemplo siguiente se inicializa el reflejo de uso compartido de carga para el volumen raíz svm1\_root:

```
cluster_src:> snapmirror initialize-ls-set -source-path svm1:svm1_root
```

## Actualizar una relación de reflejo de carga compartida

Las relaciones de mirroring (LSM) de uso compartido de carga se actualizan

automáticamente para los volúmenes raíz de SVM después de montar o desmontar un volumen en la SVM, y durante esta `volume create` operaciones que incluyen la "opción de la ruta de unión". Puede actualizar manualmente una relación LSM si desea actualizarla antes de la siguiente actualización programada.

Las relaciones de reflejos de uso compartido de carga se actualizan automáticamente en las siguientes circunstancias:

- Ha llegado el momento de realizar una actualización programada
- Se realiza una operación de montaje o desmontaje en un volumen del volumen raíz de la SVM
- A. `volume create` se emite el comando que incluye la `junction-path` opción

### Paso

1. Actualice manualmente una relación de reflejo de carga compartida:

Antes de ejecutar este comando, debe sustituir las variables entre paréntesis angulares por los valores requeridos.

```
snapmirror update-ls-set -source-path <SVM:volume>
```

En el siguiente ejemplo se actualiza la relación de reflejo de uso compartido de carga para el volumen raíz `svm1_root`:

```
cluster_src::> snapmirror update-ls-set -source-path svm1:svm1_root
```

## Promover un espejo de uso compartido de la carga

Si un volumen raíz no está disponible de forma permanente, se puede promocionar el volumen de reflejos de uso compartido de carga (LSM) para proporcionar acceso de escritura a los datos del volumen raíz.

### Lo que necesitará

Para esta tarea, debe utilizar comandos de nivel de privilegio avanzado.

### Pasos

1. Cambie al nivel de privilegio avanzado:

```
set -privilege advanced
```

2. Ascender un volumen LSM:

Antes de ejecutar este comando, debe sustituir las variables entre paréntesis angulares por los valores requeridos.



```
snapmirror promote -destination-path <SVM:volume>
```

Para obtener una sintaxis de comando completa, consulte la página [man](#).

En el siguiente ejemplo, se promociona el volumen `svm1_m2` Como nuevo volumen raíz de la SVM:

```
cluster_src::*> snapmirror promote -destination-path svm1:svm1_m2

Warning: Promote will delete the offline read-write volume
cluster_src://svm1/svm1_root and replace it with
cluster_src://svm1/svm1_m2. Because the volume is offline,
it is not possible to determine whether this promote will
affect other relationships associated with this source.
Do you want to continue? {y|n}: y
```

Introduzca `y`. ONTAP convierte al volumen LSM en un volumen de lectura/escritura y elimina el volumen raíz original, si es accesible.



Es posible que el volumen raíz promocionado no tenga todos los datos que estaban en el volumen raíz original, si no se realizó la última actualización recientemente.

### 3. Volver al nivel de privilegio de administrador:

```
set -privilege admin
```

### 4. Cambie el nombre del volumen promocionado según la convención de nomenclatura que utilizó para el volumen raíz:

Antes de ejecutar este comando, debe sustituir las variables entre paréntesis angulares por los valores requeridos.

```
volume rename -vserver <SVM> -volume <volume> -newname <new_name>
```

En el ejemplo siguiente se cambia el nombre del volumen promocionado `svm1_m2` con el nombre `svm1_root`:

```
cluster_src::> volume rename -vserver svm11 -volume svm1_m2 -newname
svm1_root
```

### 5. Proteja el volumen raíz cambiado de nombre, tal como se describe en el paso 3 hasta el paso 4 en ["Creación e inicialización de relaciones de mirroring de uso compartido de carga"](#).

# Detalles técnicos de SnapMirror

## Utilizar coincidencia de patrón de nombre de ruta de acceso

Puede utilizar la coincidencia de patrones para especificar las rutas de origen y destino en `snapmirror` comandos.

``snapmirror`` los comandos utilizan nombres de ruta completos con el siguiente formato: ``vserver:volume``. No se puede introducir el nombre de la SVM para abreviar el nombre de la ruta de acceso. Si lo hace, el ``snapmirror`` El comando asume el contexto de SVM local del usuario.

Suponiendo que la SVM se denomine «vserver1» y que el volumen se llama «vol1», el nombre de ruta completo es `vserver1:vol1`.

Puede utilizar el asterisco (\*) en las rutas de acceso como comodín para seleccionar nombres de ruta de acceso coincidentes y completos. En la siguiente tabla, se proporcionan ejemplos del uso del comodín para seleccionar un rango de volúmenes.

|       |                                                                                                   |
|-------|---------------------------------------------------------------------------------------------------|
| *     | Coincide con todas las rutas.                                                                     |
| vs*   | Coincide con todas las SVM y los volúmenes con nombres de SVM que comienzan con <code>vs</code> . |
| :*src | Coincide con todas las SVM con los nombres de los volúmenes que contienen <code>src</code> texto. |
| :vol  | Coincide con todas las SVM con nombres de volúmenes que comienzan con <code>vol</code> .          |

```
vs1::> snapmirror show -destination-path *:*dest*

Progress
Source Destination Mirror Relationship Total
Last
Path Type Path State Status Progress
Healthy Updated

vs1:sm_src2 DP vs2:sm_dest1
 Snapmirrored Idle -
true -
```

## Use consultas ampliadas para actuar en muchas relaciones de SnapMirror

Puede utilizar *extended queries* para realizar operaciones de SnapMirror en varias relaciones de SnapMirror a la vez. Por ejemplo, es posible que tenga varias relaciones SnapMirror no inicializarse que desea inicializar con un comando.

### Acerca de esta tarea

Puede aplicar consultas ampliadas a las siguientes operaciones de SnapMirror:

- Inicializando relaciones no iniciadas
- Reanude relaciones en modo inactivo
- Resincronizando relaciones rotas
- Actualizando relaciones de inactividad
- Anulación de transferencias de datos de relaciones

### Paso

1. Realice una operación de SnapMirror en varias relaciones:

```
snapmirror command {-state state } *
```

El siguiente comando inicializa las relaciones de SnapMirror que se encuentran en un Uninitialized provincia:

```
vs1::> snapmirror initialize {-state Uninitialized} *
```

## Garantice una copia Snapshot común en una instalación de mirror-vault

Puede utilizar el `snapmirror snapshot-owner create` Comando para conservar una copia Snapshot etiquetada en el secundario en una implementación de reflejo-almacén. Al hacerlo se garantiza que exista una copia snapshot común para la actualización de la relación de almacén.

### Acerca de esta tarea

Si utiliza una combinación de ventilador-almacén de reflejos o puesta en marcha en cascada, debe tener en cuenta que fallarán las actualizaciones si no existe una copia snapshot común en los volúmenes de origen y destino.

Esto no supone ningún problema en la relación de mirroring en una puesta en marcha en cascada o en distribución ramificada-vault, ya que SnapMirror siempre crea una copia snapshot del volumen de origen antes de realizar la actualización.

Puede ser un problema en la relación de almacén, sin embargo, ya que SnapMirror no crea una copia Snapshot del volumen de origen al actualizar una relación de almacén. Debe utilizar el `snapmirror snapshot-owner create` Para garantizar que hay al menos una copia Snapshot común en el origen y el destino de la relación del almacén.

### Pasos

1. En el volumen de origen, asigne un propietario a la copia Snapshot etiquetada que desea conservar:

```
snapmirror snapshot-owner create -vserver SVM -volume volume -snapshot
snapshot -owner owner
```

El ejemplo siguiente asigna ApplicationA como propietario del snap1 Copia Snapshot:

```
clust1::> snapmirror snapshot-owner create -vserver vs1 -volume vol1
-snapshot snap1 -owner ApplicationA
```

2. Actualice la relación de reflejo, como se describe en ["Actualizar manualmente una relación de replicación"](#).

También puede esperar a la actualización programada de la relación de reflejo.

3. Transfiera la copia Snapshot etiquetada como al destino de almacén:

```
snapmirror update -source-path SVM:volume|cluster://SVM/volume, ... -destination
-path SVM:volume|cluster://SVM/volume, ... -source-snapshot snapshot
```

Para obtener una sintaxis de comando completa, consulte la página man.

**En el siguiente ejemplo se transfiere el snap1 Copia Snapshot**

```
clust1::> snapmirror update -vserver vs1 -volume vol1
-source-snapshot snap1
```

La copia snapshot etiquetada se conservará cuando se actualice la relación de almacén.

4. En el volumen de origen, quite el propietario de la copia Snapshot etiquetada:

```
snapmirror snapshot-owner delete -vserver SVM -volume volume -snapshot
snapshot -owner owner
```

Los ejemplos siguientes eliminan ApplicationA como propietario del snap1 Copia Snapshot:

```
clust1::> snapmirror snapshot-owner delete -vserver vs1 -volume vol1
-snapshot snap1 -owner ApplicationA
```

## Versiones de ONTAP compatibles para relaciones de SnapMirror

Los volúmenes de origen y destino deben ejecutar versiones de ONTAP compatibles antes de crear una relación de protección de datos de SnapMirror. Antes de actualizar ONTAP, debe comprobar que la versión actual de ONTAP sea compatible con la versión de ONTAP de destino para las relaciones de SnapMirror.

## Relaciones de replicación unificadas

En lo que respecta a las relaciones de SnapMirror del tipo «'XDP», utilizando las versiones locales o de Cloud Volumes ONTAP:



A partir de ONTAP 9,9.0:

- Las versiones ONTAP 9.x,0 son versiones de solo cloud y son compatibles con los sistemas Cloud Volumes ONTAP. El asterisco (\*) después de la versión indica una versión de sólo nube.
- Las versiones ONTAP 9.x,1 son versiones generales y son compatibles tanto con los sistemas locales como con los sistemas Cloud Volumes ONTAP.



La interoperabilidad es bidireccional.

## Interoperabilidad para ONTAP versión 9,3 y posterior

| Versión ONTAP ... | Interactúa con estas versiones anteriores de ONTAP... |         |        |         |        |         |        |         |        |         |       |        |     |     |     |     |     |     |
|-------------------|-------------------------------------------------------|---------|--------|---------|--------|---------|--------|---------|--------|---------|-------|--------|-----|-----|-----|-----|-----|-----|
|                   | 9.14.1                                                | 9.14.0* | 9.13.1 | 9.13.0* | 9.12.1 | 9.12.0* | 9.11.1 | 9.11.0* | 9.10.1 | 9.10.0* | 9.9.1 | 9.9.0* | 9,8 | 9,7 | 9,6 | 9,5 | 9,4 | 9,3 |
| 9.14.1            | Sí                                                    | Sí      | Sí     | Sí      | Sí     | Sí      | Sí     | Sí      | Sí     | Sí      | Sí    | Sí     | No  | No  | No  | No  | No  | No  |
| 9.14.0*           | Sí                                                    | Sí      | Sí     | No      | Sí     | No      | Sí     | No      | Sí     | No      | Sí    | No     | Sí  | No  | No  | No  | No  | No  |
| 9.13.1            | Sí                                                    | Sí      | Sí     | Sí      | Sí     | Sí      | Sí     | Sí      | Sí     | Sí      | Sí    | Sí     | Sí  | No  | No  | No  | No  | No  |
| 9.13.0*           | Sí                                                    | No      | Sí     | Sí      | Sí     | No      | Sí     | No      | Sí     | No      | Sí    | No     | Sí  | No  | No  | No  | No  | No  |
| 9.12.1            | Sí                                                    | Sí      | Sí     | Sí      | Sí     | Sí      | Sí     | Sí      | Sí     | Sí      | Sí    | Sí     | Sí  | Sí  | No  | No  | No  | No  |
| 9.12.0*           | Sí                                                    | No      | Sí     | No      | Sí     | Sí      | Sí     | No      | Sí     | No      | Sí    | No     | Sí  | Sí  | No  | No  | No  | No  |
| 9.11.1            | Sí                                                    | Sí      | Sí     | Sí      | Sí     | Sí      | Sí     | Sí      | Sí     | Sí      | Sí    | Sí     | Sí  | Sí  | Sí  | No  | No  | No  |
| 9.11.0*           | Sí                                                    | No      | Sí     | No      | Sí     | No      | Sí     | Sí      | Sí     | No      | Sí    | No     | Sí  | Sí  | Sí  | No  | No  | No  |
| 9.10.1            | Sí                                                    | Sí      | Sí     | Sí      | Sí     | Sí      | Sí     | Sí      | Sí     | Sí      | Sí    | Sí     | Sí  | Sí  | Sí  | Sí  | No  | No  |
| 9.10.0*           | Sí                                                    | No      | Sí     | No      | Sí     | No      | Sí     | No      | Sí     | Sí      | Sí    | No     | Sí  | Sí  | Sí  | Sí  | No  | No  |
| 9.9.1             | Sí                                                    | Sí      | Sí     | Sí      | Sí     | Sí      | Sí     | Sí      | Sí     | Sí      | Sí    | Sí     | Sí  | Sí  | Sí  | Sí  | No  | No  |

|        |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|--------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 9.9.0* | Sí | No | Sí | No | Sí | No | Sí | No | Sí | No | Sí | Sí | Sí | Sí | Sí | Sí | No | No |
| 9,8    | No | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | No | Sí |
| 9,7    | No | No | No | No | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | No | Sí |
| 9,6    | No | No | No | No | No | No | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | No | Sí |
| 9,5    | No | No | No | No | No | No | No | No | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí | Sí |
| 9,4    | No | No | No | No | No | No | No | No | No | No | No | No | No | No | No | Sí | Sí | Sí |
| 9,3    | No | No | No | No | No | No | No | No | No | No | No | No | Sí | Sí | Sí | Sí | Sí | Sí |

## Relaciones de SnapMirror Synchronous



SnapMirror Synchronous no es compatible con las instancias de cloud de ONTAP.

| Versión ONTAP ... | Interactúa con estas versiones anteriores de ONTAP... |        |        |        |        |       |     |     |     |     |
|-------------------|-------------------------------------------------------|--------|--------|--------|--------|-------|-----|-----|-----|-----|
|                   | 9.14.1                                                | 9.13.1 | 9.12.1 | 9.11.1 | 9.10.1 | 9.9.1 | 9,8 | 9,7 | 9,6 | 9,5 |
| 9.14.1            | Sí                                                    | Sí     | Sí     | Sí     | Sí     | Sí    | Sí  | No  | No  | No  |
| 9.13.1            | Sí                                                    | Sí     | Sí     | Sí     | Sí     | Sí    | Sí  | Sí  | No  | No  |
| 9.12.1            | Sí                                                    | Sí     | Sí     | Sí     | Sí     | Sí    | Sí  | Sí  | No  | No  |
| 9.11.1            | Sí                                                    | Sí     | Sí     | Sí     | Sí     | Sí    | No  | No  | No  | No  |
| 9.10.1            | Sí                                                    | Sí     | Sí     | Sí     | Sí     | Sí    | Sí  | No  | No  | No  |
| 9.9.1             | Sí                                                    | Sí     | Sí     | Sí     | Sí     | Sí    | Sí  | Sí  | No  | No  |
| 9,8               | Sí                                                    | Sí     | Sí     | No     | Sí     | Sí    | Sí  | Sí  | Sí  | No  |
| 9,7               | No                                                    | Sí     | Sí     | No     | No     | Sí    | Sí  | Sí  | Sí  | Sí  |
| 9,6               | No                                                    | No     | No     | No     | No     | No    | Sí  | Sí  | Sí  | Sí  |
| 9,5               | No                                                    | No     | No     | No     | No     | No    | No  | Sí  | Sí  | Sí  |

## Relaciones de recuperación ante desastres de SVM de SnapMirror

- Para los datos de recuperación ante desastres de SVM y la protección de SVM:

La recuperación ante desastres de SVM solo se admite entre clústeres que ejecutan la misma versión de ONTAP. **La independencia de versiones no es compatible con la replicación de SVM.**

- Para la recuperación ante desastres de SVM para la migración de SVM:
  - La replicación es compatible en una sola dirección de una versión anterior de ONTAP en origen para que la misma versión de ONTAP o una posterior en el destino.
- La versión de ONTAP en el clúster de destino no debe tener más de dos versiones locales principales más nuevas o dos versiones de cloud principales más recientes, como se muestra en la tabla a continuación.
  - La replicación no es compatible con los casos de uso de protección de datos a largo plazo.

El asterisco (\*) después de la versión indica una versión de sólo nube.

Para determinar la compatibilidad, busque la versión de origen en la columna de la tabla izquierda y, a continuación, busque la versión de destino en la fila superior (DR/Migración para versiones similares y Migración sólo para versiones más recientes).

| Orig en | Destino                                  |                                          |                                          |           |           |           |           |       |         |        |         |        |         |        |         |        |         |        |
|---------|------------------------------------------|------------------------------------------|------------------------------------------|-----------|-----------|-----------|-----------|-------|---------|--------|---------|--------|---------|--------|---------|--------|---------|--------|
|         | 9,3                                      | 9,4                                      | 9,5                                      | 9,6       | 9,7       | 9,8       | 9.9.0*    | 9.9.1 | 9.10.0* | 9.10.1 | 9.11.0* | 9.11.1 | 9.12.0* | 9.12.1 | 9.13.0* | 9.13.1 | 9.14.0* | 9.14.1 |
| 9,3     | Recuperación antes de astr es/ Migración | Migración                                | Migración                                | Migración | Migración |           |           |       |         |        |         |        |         |        |         |        |         |        |
| 9,4     |                                          | Recuperación antes de astr es/ Migración | Migración                                | Migración | Migración | Migración |           |       |         |        |         |        |         |        |         |        |         |        |
| 9,5     |                                          |                                          | Recuperación antes de astr es/ Migración | Migración | Migración | Migración | Migración |       |         |        |         |        |         |        |         |        |         |        |

|        |  |  |  |                                                 |                                                 |                                                 |                                                 |           |           |           |           |  |  |  |  |  |  |
|--------|--|--|--|-------------------------------------------------|-------------------------------------------------|-------------------------------------------------|-------------------------------------------------|-----------|-----------|-----------|-----------|--|--|--|--|--|--|
| 9,6    |  |  |  | Recuperación antes de las pruebas/<br>Migración | Migración                                       | Migración                                       | Migración                                       | Migración |           |           |           |  |  |  |  |  |  |
| 9,7    |  |  |  |                                                 | Recuperación antes de las pruebas/<br>Migración | Migración                                       | Migración                                       | Migración | Migración |           |           |  |  |  |  |  |  |
| 9,8    |  |  |  |                                                 |                                                 | Recuperación antes de las pruebas/<br>Migración | Migración                                       | Migración | Migración | Migración |           |  |  |  |  |  |  |
| 9.9.0* |  |  |  |                                                 |                                                 |                                                 | Recuperación antes de las pruebas/<br>Migración | Migración | Migración | Migración | Migración |  |  |  |  |  |  |



|             |  |  |  |  |  |  |  |                                                 |                                                 |                                                 |           |           |           |           |  |  |  |  |
|-------------|--|--|--|--|--|--|--|-------------------------------------------------|-------------------------------------------------|-------------------------------------------------|-----------|-----------|-----------|-----------|--|--|--|--|
| 9.9.<br>1   |  |  |  |  |  |  |  | Recuperación antes de las pruebas/<br>Migración | Migración                                       | Migración                                       | Migración | Migración |           |           |  |  |  |  |
| 9.10<br>.0* |  |  |  |  |  |  |  | Recuperación antes de las pruebas/<br>Migración | Migración                                       | Migración                                       | Migración | Migración |           |           |  |  |  |  |
| 9.10<br>.1  |  |  |  |  |  |  |  |                                                 | Recuperación antes de las pruebas/<br>Migración | Migración                                       | Migración | Migración | Migración |           |  |  |  |  |
| 9.11<br>.0* |  |  |  |  |  |  |  |                                                 |                                                 | Recuperación antes de las pruebas/<br>Migración | Migración | Migración | Migración | Migración |  |  |  |  |

|             |  |  |  |  |  |  |  |  |  |  |                                                 |                                                 |                                                 |           |           |           |  |
|-------------|--|--|--|--|--|--|--|--|--|--|-------------------------------------------------|-------------------------------------------------|-------------------------------------------------|-----------|-----------|-----------|--|
| 9.11<br>.1  |  |  |  |  |  |  |  |  |  |  | Recuperación antes de las pruebas/<br>Migración | Migración                                       | Migración                                       | Migración | Migración |           |  |
| 9.12<br>.0* |  |  |  |  |  |  |  |  |  |  | Recuperación antes de las pruebas/<br>Migración | Migración                                       | Migración                                       | Migración | Migración |           |  |
| 9.12<br>.1  |  |  |  |  |  |  |  |  |  |  |                                                 | Recuperación antes de las pruebas/<br>Migración | Migración                                       | Migración | Migración | Migración |  |
| 9.13<br>.0* |  |  |  |  |  |  |  |  |  |  |                                                 |                                                 | Recuperación antes de las pruebas/<br>Migración | Migración | Migración | Migración |  |

|             |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |                                                  |                                                  |                                                  |
|-------------|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--------------------------------------------------|--------------------------------------------------|--------------------------------------------------|
| 9.13<br>.1  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | Recuperación antes de<br>desastres/<br>Migración | Migración                                        | Migración                                        |
| 9.14<br>.0* |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |                                                  | Recuperación antes de<br>desastres/<br>Migración | Migración                                        |
| 9.14<br>.1  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |                                                  |                                                  | Recuperación antes de<br>desastres/<br>Migración |

Relaciones de recuperación ante desastres de SnapMirror

Para relaciones de SnapMirror del tipo «DP» y del tipo de política «duplicación asíncrona»:



Los reflejos de tipo DP no se pueden inicializar comenzando con ONTAP 9.11.1 y están completamente obsoletos en ONTAP 9.12.1. Para obtener más información, consulte ["Amortización de las relaciones de SnapMirror para la protección de datos"](#).



En la siguiente tabla, la columna de la izquierda indica la versión de ONTAP en el volumen de origen y la fila superior indica las versiones de ONTAP que se pueden tener en el volumen de destino.

| Origen | Destino |        |       |     |     |     |     |     |     |     |     |    |
|--------|---------|--------|-------|-----|-----|-----|-----|-----|-----|-----|-----|----|
|        | 9.11.1  | 9.10.1 | 9.9.1 | 9,8 | 9,7 | 9,6 | 9,5 | 9,4 | 9,3 | 9,2 | 9,1 | 9  |
| 9.11.1 | Sí      | No     | No    | No  | No  | No  | No  | No  | No  | No  | No  | No |

|        |    |    |    |    |    |    |    |    |    |    |    |    |
|--------|----|----|----|----|----|----|----|----|----|----|----|----|
| 9.10.1 | Sí | Sí | No | No | No | No | No | No | No | No | No | No |
| 9.9.1  | Sí | Sí | Sí | No | No | No | No | No | No | No | No | No |
| 9,8    | No | Sí | Sí | Sí | No | No | No | No | No | No | No | No |
| 9,7    | No | No | Sí | Sí | Sí | No | No | No | No | No | No | No |
| 9,6    | No | No | No | Sí | Sí | Sí | No | No | No | No | No | No |
| 9,5    | No | No | No | No | Sí | Sí | Sí | No | No | No | No | No |
| 9,4    | No | No | No | No | No | Sí | Sí | Sí | No | No | No | No |
| 9,3    | No | No | No | No | No | No | Sí | Sí | Sí | No | No | No |
| 9,2    | No | No | No | No | No | No | No | Sí | Sí | Sí | No | No |
| 9,1    | No | No | No | No | No | No | No | No | Sí | Sí | Sí | No |
| 9      | No | No | No | No | No | No | No | No | No | Sí | Sí | Sí |



La interoperabilidad no es bidireccional.

## Limitaciones de SnapMirror

Debe conocer las limitaciones básicas de SnapMirror antes de crear una relación de protección de datos.

- Un volumen de destino solo puede tener un volumen de origen.



Un volumen de origen puede tener varios volúmenes de destino. El volumen de destino puede ser el volumen de origen de cualquier tipo de relación de replicación de SnapMirror.

- Según el modelo de cabinas, se pueden distribuir de forma ramificada un máximo de ocho o dieciséis volúmenes de destino de un único volumen de origen. Consulte "[Hardware Universe](#)" para obtener detalles sobre su configuración específica.
- No puede restaurar archivos en el destino de una relación de recuperación ante desastres de SnapMirror.
- Los volúmenes de SnapVault de origen o destino no pueden tener 32 bits.
- El volumen de origen de una relación de SnapVault no debe ser un volumen FlexClone.



La relación funcionará, pero no se conservará la eficiencia que ofrecen los volúmenes FlexClone.

## Archivado y cumplimiento de normativas con tecnología SnapLock

### Qué es SnapLock

SnapLock es una solución de cumplimiento de normativas de alto rendimiento para organizaciones que utilizan almacenamiento WORM para conservar archivos de forma no modificada a efectos de regulación y gobernanza.

SnapLock ayuda a evitar la eliminación, el cambio de nombre o el cambio de nombre de los datos para cumplir normativas como SEC 17a-4, HIPAA, FINRA, CFTC y RGPD. Gracias a SnapLock, puede crear volúmenes con fines especiales en los que los archivos se pueden almacenar y comprometidos a mantener su estado no borrable y no modificable durante un período de retención determinado o de forma indefinida. SnapLock permite llevar a cabo esta retención en el nivel de archivo mediante protocolos de archivos abiertos estándar como CIFS y NFS. Los protocolos de archivos abiertos compatibles con SnapLock son NFS (versiones 2, 3 y 4) y CIFS (SMB 1.0, 2.0 y 3.0).

Con SnapLock, se conservan archivos y copias Snapshot en almacenamiento WORM y se establecen períodos de retención para datos protegidos WORM. El almacenamiento WORM de SnapLock utiliza la tecnología Snapshot de NetApp y puede aprovechar la replicación de SnapMirror y los backups de SnapVault como tecnología base para ofrecer protección de recuperación de datos mediante backup. Más información sobre el almacenamiento WORM: ["Almacenamiento WORM conforme a la normativa con SnapLock de NetApp: TR-4526"](#).

Puede usar una aplicación para comprometer archivos a WORM mediante NFS o CIFS, o utilizar la función de compromiso automático de SnapLock para comprometer archivos automáticamente a WORM. Puede utilizar un *WORM appable file* para conservar datos que se escriben de forma incremental, como la información de registro. Para obtener más información, consulte ["Use el modo de adición de volúmenes para crear archivos WORM flexibles"](#).

SnapLock admite métodos de protección de datos que deberían satisfacer la mayoría de los requisitos de cumplimiento de normativas:

- Puede usar SnapLock para SnapVault para proteger CON WORM las copias Snapshot en el almacenamiento secundario. Consulte ["Copias Snapshot a WORM"](#).
- Puede usar SnapMirror para replicar archivos WORM a otra ubicación geográfica a fin de realizar la recuperación ante desastres. Consulte ["Refleje los archivos WORM"](#).

SnapLock es una función basada en licencia de NetApp ONTAP. Una única licencia le da derecho a usar SnapLock en modo de cumplimiento estricto para satisfacer mandatos externos como la normativa SEC 17a-4 y un modo empresarial más flexible, con el fin de cumplir las normativas internas aplicables a la protección de activos digitales. Las licencias de SnapLock forman parte de la ["ONTAP One"](#) suite de software.

SnapLock es compatible con todos los sistemas AFF y FAS, así como con ONTAP Select. SnapLock no es una solución exclusivamente de software, es una solución integrada de hardware y software. Esta distinción es importante para las estrictas regulaciones DE WORM, como SEC 17a-4, que requieren una solución de hardware y software integrada. Para obtener más información, consulte ["SEC interpretation: Almacenamiento electrónico de registros de intermediarios y concesionarios"](#).

## **Puede hacer con SnapLock**

Después de configurar SnapLock, es posible completar las siguientes tareas:

- ["Los archivos cumplen CON WORM"](#)
- ["Conservar copias Snapshot a WORM para su almacenamiento secundario"](#)
- ["Refleje los archivos WORM para la recuperación ante desastres"](#)
- ["Conserve los archivos WORM durante su litigio gracias a su conservación legal"](#)
- ["Elimine los archivos WORM utilizando la función de eliminación privilegiada"](#)
- ["Defina el período de retención de archivos"](#)
- ["Mover un volumen de SnapLock"](#)

- "Bloquee una copia Snapshot para obtener protección contra ataques de ransomware"
- "Revise el uso de SnapLock con el registro de auditoría"
- "Utilice las API de SnapLock"

## Modos SnapLock Compliance y Enterprise

Los modos SnapLock Compliance y Enterprise difieren principalmente en el nivel en el que cada modo protege los archivos WORM:

| Modo SnapLock        | Nivel de protección  | Archivo WORM eliminado durante la retención                                                                      |
|----------------------|----------------------|------------------------------------------------------------------------------------------------------------------|
| Modo de cumplimiento | A nivel de archivo   | No se puede eliminar                                                                                             |
| Modo empresarial     | En el nivel de disco | El administrador de cumplimiento puede eliminar mediante un procedimiento auditado de "eliminación privilegiada" |

Una vez transcurrido el período de retención, es responsable de eliminar los archivos que ya no se necesiten. Una vez que un archivo se ha comprometido con WORM, ya sea en modo Compliance o Enterprise, no se podrá modificar, ni siquiera después de que haya caducado el período de retención.

No se puede mover un archivo WORM durante el período de retención o después del mismo. Puede copiar un archivo WORM, pero la copia no conservará sus características WORM.

En la siguiente tabla se muestran las diferencias en las capacidades que admiten los modos SnapLock Compliance y Enterprise:

| Capacidad                                                                        | Cumplimiento de normativas SnapLock | Empresa SnapLock                                                      |
|----------------------------------------------------------------------------------|-------------------------------------|-----------------------------------------------------------------------|
| Activar y eliminar archivos mediante la eliminación con privilegios              | No                                  | Sí                                                                    |
| Reinicie los discos                                                              | No                                  | Sí                                                                    |
| Destrucción de agregados y volúmenes de SnapLock durante el período de retención | No                                  | Sí, con la excepción del volumen de registro de auditoría de SnapLock |
| Cambie el nombre de los agregados o volúmenes                                    | No                                  | Sí                                                                    |
| Utilice discos que no sean de NetApp                                             | No                                  | Sí (con "Virtualización FlexArray")                                   |

|                                                       |    |                           |
|-------------------------------------------------------|----|---------------------------|
| Use el volumen SnapLock para el registro de auditoría | Sí | Sí, a partir de ONTAP 9,5 |
|-------------------------------------------------------|----|---------------------------|

### Funciones compatibles y no compatibles con SnapLock

En la siguiente tabla se muestran las funciones compatibles con el modo de cumplimiento de normativas SnapLock, el modo SnapLock Enterprise o ambos:

| Función                             | Compatible con SnapLock Compliance                                                                     | Compatible con SnapLock Enterprise                                                                                    |
|-------------------------------------|--------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Grupos de consistencia              | No                                                                                                     | No                                                                                                                    |
| Volúmenes cifrados                  | Sí, a partir de ONTAP 9,2. Más información acerca de <a href="#">Cifrado y SnapLock</a> .              | Sí, a partir de ONTAP 9,2. Más información acerca de <a href="#">Cifrado y SnapLock</a> .                             |
| FabricPool en agregados de SnapLock | No                                                                                                     | Sí, a partir de ONTAP 9.8. Más información acerca de <a href="#">FabricPool en agregados de SnapLock Enterprise</a> . |
| Agregados de Flash Pool             | Sí, a partir de ONTAP 9,1.                                                                             | Sí, a partir de ONTAP 9,1.                                                                                            |
| FlexClone                           | Es posible clonar volúmenes de SnapLock, pero no es posible clonar archivos en un volumen de SnapLock. | Es posible clonar volúmenes de SnapLock, pero no es posible clonar archivos en un volumen de SnapLock.                |
| Volúmenes de FlexGroup              | Sí, a partir de ONTAP 9.11.1. Más información acerca de <a href="#">[flexgroup]</a> .                  | Sí, a partir de ONTAP 9.11.1. Más información acerca de <a href="#">[flexgroup]</a> .                                 |
| LUN                                 | No Más información acerca de <a href="#">Compatibilidad con LUN Con SnapLock</a> .                     | No Más información acerca de <a href="#">Compatibilidad con LUN Con SnapLock</a> .                                    |
| Configuraciones de MetroCluster     | Sí, a partir de ONTAP 9,3. Más información acerca de <a href="#">Soporte de MetroCluster</a> .         | Sí, a partir de ONTAP 9,3. Más información acerca de <a href="#">Soporte de MetroCluster</a> .                        |
| Verificación multi-admin (MAV)      | Sí, a partir de ONTAP 9.13.1. Más información acerca de <a href="#">Compatibilidad con MAV</a> .       | Sí, a partir de ONTAP 9.13.1. Más información acerca de <a href="#">Compatibilidad con MAV</a> .                      |
| SAN                                 | No                                                                                                     | No                                                                                                                    |
| SnapRestore de archivo único        | No                                                                                                     | Sí                                                                                                                    |

|                                                  |                                                                                                                   |                                                                                                                   |
|--------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| Continuidad del negocio de SnapMirror            | No                                                                                                                | No                                                                                                                |
| SnapRestore                                      | No                                                                                                                | Sí                                                                                                                |
| SMTape                                           | No                                                                                                                | No                                                                                                                |
| SnapMirror síncrono                              | No                                                                                                                | No                                                                                                                |
| SSD                                              | Sí, a partir de ONTAP 9,1.                                                                                        | Sí, a partir de ONTAP 9,1.                                                                                        |
| Funcionalidades de eficiencia del almacenamiento | Sí, a partir de ONTAP 9,9.1. Más información acerca de <a href="#">soporte de eficiencia del almacenamiento</a> . | Sí, a partir de ONTAP 9,9.1. Más información acerca de <a href="#">soporte de eficiencia del almacenamiento</a> . |

## FabricPool en agregados de SnapLock Enterprise

Las instancias de FabricPool son compatibles con los agregados empresariales de SnapLock, a partir de ONTAP 9.8. Sin embargo, su equipo de cuenta tiene que abrir una solicitud de variación de productos que documente que SnapLock ya no protege los datos de FabricPool organizados en niveles en un cloud público o privado porque un administrador de cloud puede eliminar dichos datos.



Cualquier dato que FabricPool proporcione en niveles en un cloud público o privado ya no está protegido por SnapLock, ya que un administrador de cloud puede eliminar estos datos.

## Volúmenes de FlexGroup

SnapLock admite volúmenes FlexGroup que comiencen con ONTAP 9.11.1; sin embargo, no se admiten las siguientes funciones:

- Conservación legal
- Retención basada en eventos
- SnapLock para SnapVault (compatible a partir de ONTAP 9.12.1)

También debe ser consciente de los siguientes comportamientos:

- El reloj de cumplimiento de volumen (VCC) de un volumen FlexGroup está determinado por el VCC del componente raíz. Todos los componentes que no son de raíz tendrán su VCC estrechamente sincronizado con la VCC raíz.
- Las propiedades de configuración de SnapLock se establecen únicamente en la FlexGroup en su conjunto. Los componentes individuales no pueden tener diferentes propiedades de configuración, como el tiempo de retención predeterminado y el período de compromiso automático.

## Compatibilidad con LUN

Los LUN se admiten en volúmenes de SnapLock solo en casos en los que las copias de Snapshot creadas en un volumen distinto de SnapLock se transfieren a un volumen de SnapLock para la protección como parte de la relación de almacén de SnapLock. Los LUN no son compatibles con los volúmenes de SnapLock de lectura/escritura. Las copias Snapshot a prueba de manipulaciones son compatibles tanto con los volúmenes



de origen como con los volúmenes de destino de SnapMirror que contienen LUN.

## **Soporte de MetroCluster**

La compatibilidad con SnapLock en configuraciones MetroCluster es diferente del modo de cumplimiento de normativas SnapLock al modo empresarial de SnapLock.

### **Cumplimiento de normativas SnapLock**

- A partir de ONTAP 9.3, SnapLock Compliance se admite en los agregados de MetroCluster no reflejados.
- A partir de ONTAP 9.3, SnapLock Compliance se admite en agregados reflejados, pero solo si el agregado se utiliza para alojar los volúmenes de registros de auditoría de SnapLock.
- Las configuraciones de SnapLock específicas para SVM se pueden replicar en sitios principales y secundarios mediante MetroCluster.

### **Empresa SnapLock**

- A partir de la versión 9 de ONTAP, se admiten los agregados de SnapLock Enterprise.
- A partir de ONTAP 9.3, se admiten los agregados de SnapLock Enterprise con eliminación privilegiada.
- Las configuraciones de SnapLock específicas para SVM se pueden replicar en ambos sitios mediante MetroCluster.

### **Configuraciones de MetroCluster y relojes de cumplimiento**

Las configuraciones de MetroCluster utilizan dos mecanismos de reloj de conformidad, el reloj de cumplimiento de volumen (VCC) y el reloj de cumplimiento del sistema (SCC). El VCC y el SCC están disponibles para todas las configuraciones SnapLock. Cuando se crea un nuevo volumen en un nodo, su VCC se inicializa con el valor actual del SCC en ese nodo. Una vez creado el volumen, el VCC siempre se realiza un seguimiento del volumen y del tiempo de retención de archivos.

Cuando un volumen se replica en otro sitio, su VCC también se replica. Cuando se produce una conmutación de volumen, del sitio A al sitio B, por ejemplo, el VCC continúa siendo actualizado en el sitio B mientras que el SCC en el sitio A se detiene cuando el sitio A se desconecta.

Cuando el sitio A se vuelve a poner en línea y se realiza la vuelta de volumen, el reloj SCC del sitio se reinicia mientras el VCC del volumen continúa siendo actualizado. Como el VCC se actualiza continuamente, independientemente de las operaciones de conmutación de sitios y conmutación de estado, los tiempos de retención de archivos no dependen de los relojes SCC y no se amplían.

### **Compatibilidad con verificación multiadministrador (MAV)**

A partir de la versión ONTAP 9.13.1, un administrador de clúster puede habilitar de forma explícita la verificación multiadministrador en un clúster para requerir la aprobación de quórum antes de ejecutar algunas operaciones de SnapLock. Cuando MAV está activado, las propiedades del volumen SnapLock como default-retention-time, minimum-retention-time, maximum-retention-time, volume-append-mode, autocommit-period y privileged-delete requerirán aprobación del quórum. Más información acerca de ["MAV"](#).

### **Eficiencia del almacenamiento**

A partir de ONTAP 9.9.1, SnapLock admite funciones de eficiencia del almacenamiento, como la compactación de datos, la deduplicación entre volúmenes y la compresión adaptativa para volúmenes y agregados de SnapLock. Para obtener más información sobre la eficiencia del almacenamiento, consulte ["Información general sobre la gestión de almacenamiento lógico con la CLI"](#).

## Cifrado

ONTAP ofrece tecnologías de cifrado basadas en software y hardware para garantizar que los datos en reposo no se puedan leer en caso de reasignación, devolución, pérdida o robo del medio de almacenamiento.

**Exención de responsabilidad:** NetApp no puede garantizar que los archivos WORM protegidos SnapLock en unidades o volúmenes de autocifrado se puedan recuperar si se pierde la clave de autenticación o si el número de intentos de autenticación con errores supera el límite especificado y hace que la unidad se bloquee de forma permanente. Usted es responsable de garantizar el cumplimiento de los fallos de autenticación.



A partir de ONTAP 9.2, los volúmenes cifrados se admiten en agregados de SnapLock.

## Transición de 7-Mode

Puede migrar volúmenes SnapLock de 7-Mode a ONTAP usando la función de transición basada en copias (CBT) de la herramienta de transición de 7-Mode. El modo SnapLock del volumen de destino, Compliance o Enterprise, debe coincidir con el modo SnapLock del volumen de origen. No se puede usar la transición sin copia (CFT) para migrar volúmenes de SnapLock.

## Configure SnapLock

### Configure SnapLock

Antes de utilizar SnapLock, tiene que configurar SnapLock realizando varias tareas, como ["Instale la licencia de SnapLock"](#) Para cada nodo que aloja un agregado con un volumen SnapLock, inicialice el ["Reloj de cumplimiento"](#), Crear un agregado de SnapLock para clusters que ejecuten versiones de ONTAP anteriores a ONTAP 9.10.1, ["Cree y monte un volumen de SnapLock"](#), y más.

### Inicialice el reloj de cumplimiento

SnapLock utiliza *volume Compliance Clock* para garantizar la manipulación que puede alterar el período de retención de los archivos WORM. Primero, debe inicializar *system ComplianceClock* en cada nodo que aloje un agregado de SnapLock.

A partir de ONTAP 9.14.1, puede inicializar o reinicializar el reloj de cumplimiento de normativas del sistema cuando no hay volúmenes de SnapLock o ningún volumen con el bloqueo de copia de Snapshot habilitado. La capacidad de reinicializar permite a los administradores del sistema restablecer el reloj de cumplimiento del sistema en casos en los que podría haberse inicializado incorrectamente o corregir la desviación del reloj del sistema. En ONTAP 9.13.1 y versiones anteriores, una vez que se inicializa el reloj de cumplimiento de normativas en un nodo, no puede volver a inicializarlo.

### Antes de empezar

Para reinicializar el reloj de conformidad:

- Todos los nodos del clúster deben tener el estado correcto.
- Todos los volúmenes deben estar en línea.
- No puede haber volúmenes presentes en la cola de recuperación.
- No hay volúmenes SnapLock presentes.
- No se puede presentar ningún volumen con bloqueo de copia de SnapVault habilitado.

Requisitos generales para inicializar el reloj de conformidad:

- Para realizar esta tarea, debe ser un administrador de clústeres.
- "La licencia de SnapLock debe instalarse en el nodo".

### Acerca de esta tarea

La hora en el reloj de cumplimiento del sistema se hereda por el *volume Compliance Clock*, este último de los cuales controla el período de retención de los archivos WORM en el volumen. El reloj de cumplimiento de normativas del volumen se inicializa automáticamente cuando se crea un volumen de SnapLock nuevo.



El ajuste inicial del reloj de cumplimiento del sistema se basa en el reloj del sistema de hardware actual. Por este motivo, debe verificar que la hora y la zona horaria del sistema sean correctas antes de inicializar el reloj de cumplimiento de normativas del sistema en cada nodo. Una vez que se inicializa el reloj de cumplimiento de normativas del sistema en un nodo, no se puede volver a inicializar cuando hay volúmenes de SnapLock o volúmenes con el bloqueo habilitado.

### Pasos

Es posible usar la interfaz de línea de comandos de ONTAP para inicializar el reloj de cumplimiento de normativas o, a partir de ONTAP 9.12.1, puede utilizar System Manager para inicializar el reloj de cumplimiento de normativas.

## System Manager

1. Vaya a **Cluster > Overview**.
2. En la sección **Nodes**, haga clic en **inicializar reloj de cumplimiento de SnapLock**.
3. Para mostrar la columna **Reloj de cumplimiento** y verificar que el Reloj de cumplimiento está inicializado, en la sección **Clúster > Descripción general > Nodos**, haga clic en **Mostrar/ocultar** y seleccione **Reloj de cumplimiento de SnapLock**.

## CLI

1. Inicialice el reloj de cumplimiento del sistema:

```
snaplock compliance-clock initialize -node node_name
```

El siguiente comando inicializa el reloj de cumplimiento del sistema node1:

```
cluster1::> snaplock compliance-clock initialize -node node1
```

2. Cuando se le solicite, confirme que el reloj del sistema es correcto y que desea inicializar el reloj de conformidad:

```
Warning: You are about to initialize the secure ComplianceClock of
the node "node1" to the current value of the node's system clock.
This procedure can be performed only once on a given node, so you
should ensure that the system time is set correctly before
proceeding.
```

```
The current node's system clock is: Mon Apr 25 06:04:10 GMT 2016
```

```
Do you want to continue? (y|n): y
```

3. Repita este procedimiento para cada nodo que aloje un agregado de SnapLock.

## Habilite la resincronización del reloj de cumplimiento de normativas para un sistema configurado por NTP

Puede habilitar la función de sincronización de hora de reloj de cumplimiento de normativas SnapLock cuando se configura un servidor NTP.

### Lo que necesitará

- Esta función solo está disponible en el nivel de privilegios avanzado.
- Para realizar esta tarea, debe ser un administrador de clústeres.
- ["La licencia de SnapLock debe instalarse en el nodo"](#).
- Esta función sólo está disponible para plataformas Cloud Volumes ONTAP, ONTAP Select y VSIM.

### Acerca de esta tarea

Cuando el daemon de reloj seguro de SnapLock detecta una desviación más allá del umbral, ONTAP utiliza la

hora del sistema para restablecer los relojes de cumplimiento del sistema y del volumen. Se establece un período de 24 horas como umbral de desviación. Esto significa que el reloj de cumplimiento del sistema se sincroniza con el reloj del sistema solo si la inclinación tiene más de un día de antigüedad.

El daemon de reloj seguro de SnapLock detecta una inclinación y cambia el reloj de cumplimiento a la hora del sistema. Cualquier intento de modificar la hora del sistema para forzar que el reloj de cumplimiento se sincronice con la hora del sistema falla, ya que el reloj de cumplimiento se sincroniza con la hora del sistema solo si la hora del sistema está sincronizada con la hora NTP.

## Pasos

1. Habilite la función de sincronización de hora del reloj de cumplimiento de normativas de SnapLock cuando se configure un servidor NTP:

```
snaplock compliance-clock ntp
```

El siguiente comando habilita la función de sincronización de hora del reloj de cumplimiento de normativas del sistema:

```
cluster1::*> snaplock compliance-clock ntp modify -is-sync-enabled true
```

2. Cuando se le solicite, confirme que los servidores NTP configurados son de confianza y que el canal de comunicación es seguro para habilitar la función:
3. Compruebe que la función está activada:

```
snaplock compliance-clock ntp show
```

El siguiente comando comprueba que la función de sincronización de hora del reloj de cumplimiento de normativas del sistema esté habilitada:

```
cluster1::*> snaplock compliance-clock ntp show

Enable clock sync to NTP system time: true
```

## Cree un agregado de SnapLock

Se utiliza el volumen `-snaplock-type` Opción para especificar un tipo de volumen Compliance o Enterprise SnapLock. Para las versiones anteriores a ONTAP 9.10.1, se debe crear un agregado de SnapLock independiente. A partir de ONTAP 9.10.1, los volúmenes de SnapLock y otros de SnapLock pueden existir en el mismo agregado; por lo tanto, ya no es necesario crear un agregado de SnapLock separado si se utiliza ONTAP 9.10.1.

### Antes de empezar

- Para realizar esta tarea, debe ser un administrador de clústeres.
- El SnapLock ["se debe instalar la licencia"](#) en el nodo. Esta licencia se incluye en ["ONTAP One"](#).
- ["Se debe inicializar el reloj de cumplimiento de normativas del nodo"](#).

- Si ha particionado los discos como «'root'», «dn1» y «atado2», deberá asegurarse de que los discos de repuesto están disponibles.

### Consideraciones de renovación

Al actualizar a ONTAP 9.10.1, los agregados existentes de SnapLock y otros componentes de SnapLock se actualizan para admitir la existencia de volúmenes SnapLock y distintos de SnapLock; sin embargo, los atributos de volumen de SnapLock existentes no se actualizan automáticamente. Por ejemplo, los campos de compactación de datos, deduplicación entre volúmenes y deduplicación entre volúmenes en segundo plano siguen sin cambios. Los nuevos volúmenes SnapLock creados en agregados existentes tienen los mismos valores predeterminados que los volúmenes que no son de SnapLock, y los valores predeterminados de los nuevos volúmenes y agregados dependen de la plataforma.

### Consideraciones sobre la reversión

Si necesita volver a una versión de ONTAP anterior a la 9.10.1, debe mover todos los volúmenes de SnapLock Compliance, SnapLock Enterprise y SnapLock a sus propios agregados de SnapLock.

### Acerca de esta tarea

- No se pueden crear agregados de cumplimiento para las LUN de FlexArray, pero los agregados de SnapLock Compliance son compatibles con las LUN de FlexArray.
- No se pueden crear agregados de cumplimiento con la opción SyncMirror.
- Solo se pueden crear agregados de cumplimiento reflejado en una configuración de MetroCluster si el agregado se utiliza para alojar volúmenes de registro de auditoría de SnapLock.



En una configuración MetroCluster, es compatible con SnapLock Enterprise con los agregados reflejados y no reflejados. SnapLock Compliance solo se admite en agregados no reflejados.

### Pasos

1. Cree un agregado de SnapLock:

```
storage aggregate create -aggregate <aggregate_name> -node <node_name>
-diskcount <number_of_disks> -snaplock-type <compliance|enterprise>
```

La página man del comando contiene una lista completa de opciones.

El siguiente comando crea una SnapLock Compliance agregado con nombre aggr1 con tres discos activados node1:

```
cluster1::> storage aggregate create -aggregate aggr1 -node node1
-diskcount 3 -snaplock-type compliance
```

### Cree y monte volúmenes de SnapLock

Debe crear un volumen SnapLock para los archivos o las copias de Snapshot que desee confirmar al estado WORM. A partir de ONTAP 9.10.1, todos los volúmenes que cree, independientemente del tipo de agregado, se crearán de forma predeterminada como

volumen que no sea de SnapLock. Debe utilizar el `-snaplock-type` Opción para crear explícitamente un volumen de SnapLock especificando Compliance o Enterprise como el tipo de SnapLock. De forma predeterminada, el tipo de SnapLock se establece en `non-snaplock`.

#### Antes de empezar

- El agregado de SnapLock debe estar en línea.
- Usted debe ["Compruebe que hay instalada una licencia de SnapLock"](#). Si no hay una licencia de SnapLock instalada en el nodo, debe ["instale"](#) ti. Esta licencia se incluye con ["ONTAP One"](#). Antes de ONTAP One, la licencia de SnapLock se incluía en el paquete de seguridad y cumplimiento de normativas. El paquete de seguridad y cumplimiento ya no se ofrece, pero sigue siendo válido. Aunque actualmente no es obligatorio, los clientes existentes pueden optar por hacerlo ["Actualice a ONTAP One"](#).
- ["Se debe inicializar el reloj de cumplimiento de normativas del nodo"](#).

#### Acerca de esta tarea

Con los permisos de SnapLock adecuados, puede destruir un volumen empresarial o cambiar su nombre en cualquier momento. No se puede destruir un volumen de cumplimiento hasta que haya transcurrido el período de retención. Nunca se puede cambiar el nombre de un volumen de cumplimiento.

Es posible clonar volúmenes de SnapLock, pero no es posible clonar archivos en un volumen de SnapLock. El volumen clonado tendrá el mismo tipo de SnapLock que el volumen principal.



Los LUN no son compatibles con los volúmenes de SnapLock. Los LUN se admiten en volúmenes de SnapLock solo en casos en los que las copias de Snapshot creadas en un volumen distinto de SnapLock se transfieren a un volumen de SnapLock para la protección como parte de la relación de almacén de SnapLock. Los LUN no son compatibles con los volúmenes de SnapLock de lectura/escritura. Las copias Snapshot a prueba de manipulaciones son compatibles tanto con los volúmenes de origen como con los volúmenes de destino de SnapMirror que contienen LUN.

Lleve a cabo esta tarea mediante System Manager de ONTAP o la interfaz de línea de comandos de ONTAP.

## System Manager

A partir de ONTAP 9.12.1, se puede usar System Manager para crear un volumen de SnapLock.

### Pasos

1. Vaya a **almacenamiento > volúmenes** y haga clic en **Agregar**.
2. En la ventana **Agregar volumen**, haga clic en **más opciones**.
3. Introduzca la nueva información del volumen, incluidos el nombre y el tamaño del volumen.
4. Seleccione **Activar SnapLock** y elija el tipo de SnapLock, ya sea Compliance o Enterprise.
5. En la sección **Archivos de registro automático**, seleccione **modificado** e introduzca la cantidad de tiempo que un archivo debe permanecer sin cambios antes de que se confirme automáticamente. El valor mínimo es de 5 minutos y el valor máximo es de 10 años.
6. En la sección **retención de datos**, seleccione el período de retención mínimo y máximo.
7. Seleccione el período de retención predeterminado.
8. Haga clic en **Guardar**.
9. Seleccione el nuevo volumen en la página **Volumes** para verificar la configuración de SnapLock.

### CLI

1. Cree un volumen de SnapLock:

```
volume create -vserver <SVM_name> -volume <volume_name> -aggregate
<aggregate_name> -snaplock-type <compliance|enterprise>
```

Para obtener una lista completa de las opciones, consulte la página de manual del comando. Las siguientes opciones no están disponibles para SnapLock Volumes: `-nvfail`, `-atime-update`, `-is-autobalance-eligible`, `-space-mgmt-try-first`, y `vmalign`.

El siguiente comando crea una SnapLock Compliance volumen denominado `vol1` encendido `aggr1` encendido `vs1`:

```
cluster1::> volume create -vserver vs1 -volume vol1 -aggregate aggr1
-snaplock-type compliance
```

## Montar un volumen de SnapLock

Puede montar un volumen SnapLock en una ruta de unión en el espacio de nombres de la SVM para el acceso de clientes NAS.

### Lo que necesitará

El volumen SnapLock debe estar en línea.

### Acerca de esta tarea

- Los volúmenes de SnapLock solo se pueden montar en la raíz de la SVM.



- No se puede montar un volumen normal en un volumen de SnapLock.

## Pasos

1. Montar un volumen de SnapLock:

```
volume mount -vserver SVM_name -volume volume_name -junction-path path
```

Para obtener una lista completa de las opciones, consulte la página de manual del comando.

El siguiente comando monta un volumen SnapLock llamado `vol1` a la ruta de unión `/sales` en la `vs1` espacio de nombres:

```
cluster1::> volume mount -vserver vs1 -volume vol1 -junction-path /sales
```

## Establezca el tiempo de retención

Se puede establecer el tiempo de retención de un archivo explícitamente o se puede usar el período de retención predeterminado para el volumen a fin de obtener el tiempo de retención. A menos que se establezca el tiempo de retención explícitamente, SnapLock utiliza el período de retención predeterminado para calcular el tiempo de retención. También es posible configurar la retención de archivos después de un evento.

### Acerca del período de retención y del tiempo de retención

El *retention period* para un archivo WORM especifica la cantidad de tiempo que debe conservarse el archivo después de comprometerse al estado WORM. El *retention time* para un archivo WORM es el tiempo a partir del cual ya no es necesario retener el archivo. Un período de retención de 20 años para un archivo comprometido con EL estado WORM el 10 de noviembre a las 2020 6:00, por ejemplo, daría como resultado un período de retención de 10 de noviembre a las 2040 6:00 a.m.



A partir de ONTAP 9.10.1, se puede establecer un tiempo de retención hasta el 26 de octubre de 3058 y un período de retención de hasta 100 años. Al ampliar las fechas de retención, las directivas más antiguas se convierten automáticamente. En ONTAP 9.9.1 y versiones anteriores, a menos que se establezca el período de retención predeterminado en infinito, el tiempo de retención máximo admitido es el 19 2071 de enero (GMT).

### Consideraciones importantes sobre la replicación

Cuando se establece una relación de SnapMirror con un volumen de origen de SnapLock con una fecha de retención posterior al 19 de enero de 2071 (GMT), el clúster de destino debe ejecutar ONTAP 9.10.1 o una versión posterior, o se producirá un error en la transferencia de SnapMirror.

### Consideraciones importantes sobre la reversión

ONTAP impide que se pueda revertir un clúster de ONTAP 9.10.1 a una versión de ONTAP anterior cuando hay archivos con un período de retención posterior a "19 de enero de 2071 8:44:07 AM".

Descripción de los periodos de retención

Los volúmenes de empresa o de cumplimiento de normativas de SnapLock tienen cuatro periodos de retención:

- Periodo de retención mínimo (min), con un valor predeterminado de 0
- Periodo de retención máximo (max), con un valor por defecto de 30 años
- Periodo de retención predeterminado, con un valor predeterminado igual a min Tanto para el modo de cumplimiento como para el modo de empresa a partir de ONTAP 9.10.1. En las versiones de ONTAP anteriores a ONTAP 9.10.1, el periodo de retención predeterminado depende del modo:
  - Para el modo de cumplimiento, el valor predeterminado es igual a max.
  - Para el modo Enterprise, el valor predeterminado es igual a min.
- Periodo de retención no especificado.

A partir de ONTAP 9.8, es posible establecer el periodo de retención en los archivos de un volumen en unspecified, para permitir que el archivo se conserve hasta que se establezca un tiempo de retención absoluto. Puede establecer un archivo con tiempo de retención absoluto en retención no especificada y volver a la retención absoluta siempre y cuando el nuevo tiempo de retención absoluto sea posterior al tiempo absoluto establecido anteriormente.

A partir de ONTAP 9.12.1, archivos WORM con el periodo de retención establecido en unspecified Estén garantizados para que el periodo de retención se haya establecido en el periodo de retención mínimo configurado para el volumen de SnapLock. Al cambiar el periodo de retención de archivos de unspecified para un tiempo de retención absoluto, el nuevo tiempo de retención especificado debe ser superior al tiempo de retención mínimo establecido en el archivo.

Por lo tanto, si no establece el tiempo de retención explícitamente antes de confirmar un archivo de modo de cumplimiento en el estado WORM y no modifica los valores predeterminados, el archivo se conservará durante 30 años. Del mismo modo, si no establece el tiempo de retención explícitamente antes de comprometer un archivo de modo empresarial con el estado WORM, y no modifica los valores predeterminados, el archivo se conservará durante 0 años o, efectivamente, De nada.

Establecer el periodo de retención predeterminado


Puede utilizar el volume snaplock modify Comando para establecer el periodo de retención predeterminado para los archivos de un volumen de SnapLock.

Lo que necesitará

El volumen SnapLock debe estar en línea.

Acerca de esta tarea

En la siguiente tabla se muestran los posibles valores para la opción de periodo de retención predeterminado:



El periodo de retención predeterminado debe ser mayor o igual que (>=) el periodo de retención mínimo y menor o igual que (<=) el periodo de retención máximo.

| Valor     | Unidad   | Notas |
|-----------|----------|-------|
| 0 - 65535 | segundos |       |

| Valor           | Unidad | Notas                                                                             |
|-----------------|--------|-----------------------------------------------------------------------------------|
| 0 - 24          | horas  |                                                                                   |
| 0 - 365         | días   |                                                                                   |
| 0 - 12          | meses  |                                                                                   |
| 0 - 100         | años   | A partir de ONTAP 9.10.1, Para versiones anteriores de ONTAP, el valor es 0 - 70. |
| capacidad       | -      | Usar el período de retención máximo.                                              |
| espacio         | -      | Use el período de retención mínimo.                                               |
| infinita        | -      | Conserve los archivos para siempre.                                               |
| sin especificar | -      | Conserve los archivos hasta que se defina un período de retención absoluto.       |

Los valores y los rangos para los períodos de retención máximo y mínimo son idénticos, excepto para `max` y `min`, que no son aplicables. Para obtener más información acerca de esta tarea, consulte ["Establezca la visión general de la hora de retención"](#).

Puede utilizar el `volume snaplock show` comando para ver la configuración del período de retención del volumen. Para obtener más información, consulte la página man del comando.



Después de que un archivo se haya comprometido con el estado WORM, puede ampliar el período de retención, pero no acortar.

## Pasos

1. Establezca el período de retención predeterminado para los archivos en un volumen de SnapLock:

```
volume snaplock modify -vserver SVM_name -volume volume_name -default
-retention-period default_retention_period -minimum-retention-period
min_retention_period -maximum-retention-period max_retention_period
```

Para obtener una lista completa de las opciones, consulte la página de manual del comando.



En los siguientes ejemplos se asume que los períodos de retención mínimo y máximo no se han modificado previamente.

El siguiente comando establece el período de retención predeterminado para un volumen de Compliance o Enterprise en 20 días:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period 20days
```

El siguiente comando establece el período de retención predeterminado para un volumen de cumplimiento en 70 años:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -maximum
-retention-period 70years
```

El comando siguiente establece el período de retención predeterminado para un volumen de Enterprise en 10 años:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period max -maximum-retention-period 10years
```

Los siguientes comandos establecen el período de retención predeterminado para un volumen de empresa en 10 días:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -minimum
-retention-period 10days
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period min
```

El siguiente comando establece el período de retención predeterminado para un volumen de cumplimiento en infinito:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period infinite -maximum-retention-period infinite
```

### Establezca explícitamente el tiempo de retención de un archivo

Puede establecer explícitamente el tiempo de retención de un archivo modificando su última hora de acceso. Puede usar cualquier comando o programa adecuado a través de NFS o CIFS para modificar la última hora de acceso.

#### Acerca de esta tarea

Después de haber comprometido un archivo con WORM, puede ampliar el tiempo de retención, pero no reducir este. El tiempo de retención se almacena en la `atime` para el archivo.



No se puede establecer explícitamente el tiempo de retención de un archivo en `infinite`. Ese valor solo está disponible cuando se utiliza el período de retención predeterminado para calcular el tiempo de retención.

## Pasos

1. Utilice un comando o programa adecuado para modificar la última hora de acceso para el archivo cuyo tiempo de retención desee establecer.

En un shell de UNIX, utilice el comando siguiente para establecer una hora de retención de 21 de noviembre de 2020 6:00 a.m. en un archivo llamado `document.txt`:

```
touch -a -t 202011210600 document.txt
```



Puede utilizar cualquier comando o programa adecuado para modificar la última hora de acceso en Windows.

## Establezca el período de retención de archivos después de un evento

A partir de ONTAP 9.3, puede definir cuánto tiempo se retiene un archivo después de que se produzca un evento mediante la función *SnapLock Event Based Retention (EBR)*.

### Lo que necesitará

- Debe ser un administrador de SnapLock para realizar esta tarea.

["Cree una cuenta de administrador de SnapLock"](#)

- Debe haber iniciado sesión en una conexión segura (SSH, Console o ZAPI).

### Acerca de esta tarea

La directiva *event retention* define el período de retención del archivo después de que se produzca el evento. La directiva se puede aplicar a un único archivo o a todos los archivos de un directorio.

- Si un archivo no es UN archivo WORM, se comprometerá con el estado WORM para el período de retención definido en la política.
- Si un archivo es UN archivo WORM o un archivo ampliable WORM, su período de retención se extenderá por el período de retención que se define en la política.

Puede usar un volumen de modo de cumplimiento o de modo empresarial.



Las políticas de EBR no se pueden aplicar a los archivos de una retención legal.

Para un uso avanzado, consulte ["Almacenamiento WORM conforme a la normativa con SnapLock de NetApp"](#).

**usar EBR para ampliar el período de retención de archivos WORM ya existentes**

EBR resulta muy práctico cuando se desea ampliar el período de retención de archivos WORM ya existentes. Por ejemplo, podría ser la política de su empresa retener los registros del empleado W-4 en forma no modificada durante tres años después de que el empleado cambie una elección de retención. Otra política de la empresa podría requerir que los registros W-4 se retengan durante cinco años después de que el empleado haya terminado.

En este caso, podría crear una política EBR con un período de retención de cinco años. Una vez que el empleado ha terminado (el "evento"), aplicaría la política de EBR al registro W-4 del empleado, lo que provocaría que se ampliara su período de retención. Esto suele ser más sencillo que ampliar el período de retención manualmente, especialmente cuando se trata de un gran número de archivos.

## Pasos

1. Crear una política EBR:

```
snaplock event-retention policy create -vserver SVM_name -name policy_name -retention-period retention_period
```

El siguiente comando crea la política EBR `employee_exit` encendido `vs1` con un período de retención de diez años:

```
cluster1::>snaplock event-retention policy create -vserver vs1 -name employee_exit -retention-period 10years
```

2. Aplicar una política EBR:

```
snaplock event-retention apply -vserver SVM_name -name policy_name -volume volume_name -path path_name
```

El siguiente comando aplica la política EBR `employee_exit` encendido `vs1` a todos los archivos del directorio `d1`:

```
cluster1::>snaplock event-retention apply -vserver vs1 -name employee_exit -volume vol1 -path /d1
```

## Cree un registro de auditoría

Si utiliza ONTAP 9.9.1 o una versión anterior, primero debe crear un agregado de SnapLock y, a continuación, debe crear un registro de auditoría protegido por SnapLock antes de ejecutar una eliminación con privilegios o mover volúmenes de SnapLock. El registro de auditoría registra la creación y eliminación de cuentas de administrador de SnapLock, las modificaciones realizadas en el volumen de registro, si la eliminación con privilegios está habilitada, las operaciones de eliminación con privilegios y las operaciones de movimiento de volúmenes SnapLock.

A partir de ONTAP 9.10.1, ya no se crea un agregado de SnapLock. Debe utilizar la opción `-snaplock-type` a. ["Crear explícitamente un volumen SnapLock"](#) Especificando `Compliance` o `Enterprise` como tipo SnapLock.

## Antes de empezar

Si se utiliza ONTAP 9.9.1 o una versión anterior, debe ser un administrador de clústeres para crear un agregado de SnapLock.

## Acerca de esta tarea

No se puede eliminar un registro de auditoría hasta que haya transcurrido el período de retención del archivo de registro. No es posible modificar un registro de auditoría incluso después de transcurrido el período de retención. Esto es así tanto para el modo de cumplimiento de normativas SnapLock como para el modo de empresa.



En ONTAP 9.4 y versiones anteriores, no se puede usar un volumen de empresa SnapLock para el registro de auditoría. Se debe usar un volumen de cumplimiento de normativas de SnapLock. En ONTAP 9.5 y versiones posteriores, se puede usar un volumen de empresa SnapLock o un volumen de cumplimiento de SnapLock para el registro de auditoría. En todos los casos, el volumen de registro de auditoría debe montarse en la ruta de unión `/snaplock_audit_log`. Ningún otro volumen puede utilizar esta ruta de unión.

Los registros de auditoría de SnapLock se pueden encontrar en la `/snaplock_log` directorio en la raíz del volumen de registro de auditoría, en subdirectorios denominados `privdel_log` (operaciones de eliminación con privilegios) y `system_log` (todo lo demás). Los nombres de archivos de registro de auditoría contienen la Marca de hora de la primera operación de registro, lo que facilita la búsqueda de registros en el momento aproximado en que se ejecutaron las operaciones.

- Puede utilizar el `snaplock log file show` comando para ver los archivos de registro en el volumen del registro de auditoría.
- Puede utilizar el `snaplock log file archive` para archivar el archivo de registro actual y crear uno nuevo, lo que resulta útil en los casos en los que se necesita registrar la información del registro de auditoría en un archivo independiente.

Para obtener más información, consulte las páginas de manual de los comandos.



No se puede usar un volumen de protección de datos como volumen de registro de auditoría de SnapLock.

## Pasos

1. Cree un agregado de SnapLock.

[Cree un agregado de SnapLock](#)

2. En la SVM que desee configurar para el registro de auditoría, cree un volumen de SnapLock.

[Cree un volumen de SnapLock](#)

3. Configure la SVM para el registro de auditoría:

```
snaplock log create -vserver SVM_name -volume snaplock_volume_name -max-log
-size size -retention-period default_retention_period
```



El período de retención mínimo predeterminado para archivos de registro de auditoría es de seis meses. Si el período de retención de un archivo afectado es más largo que el período de retención del registro de auditoría, el período de retención del registro hereda el período de retención del archivo. Por lo tanto, si el período de retención de un archivo eliminado mediante eliminación privilegiada es de 10 meses y el período de retención del registro de auditoría de 8 meses, el período de retención del registro se extiende a 10 meses. Para obtener más información sobre el tiempo de retención y el período de retención predeterminado, consulte ["Establezca el tiempo de retención"](#).

Se configura el siguiente comando SVM1 Para el registro de auditoría mediante el volumen SnapLock logVol. El registro de auditoría tiene un tamaño máximo de 20 GB y se conserva durante ocho meses.

```
SVM1::> snaplock log create -vserver SVM1 -volume logVol -max-log-size 20GB -retention-period 8months
```

4. En la SVM que haya configurado para el registro de auditoría, monte el volumen SnapLock en la ruta de unión /snaplock\_audit\_log.

[Montar un volumen de SnapLock](#)

## Comprobar la configuración de SnapLock

Puede utilizar el `volume file fingerprint start y. volume file fingerprint dump` Comandos para ver información clave sobre archivos y volúmenes, incluido el tipo de archivo (normal, WORM o WORM, que puede adaptarse a ellas), la fecha de caducidad del volumen, etc.

### Pasos

1. Generar una huella digital de archivo:

```
volume file fingerprint start -vserver SVM_name -file file_path
```

```
svm1::> volume file fingerprint start -vserver svm1 -file /vol/sle/vol/f1
File fingerprint operation is queued. Run "volume file fingerprint show -session-id 16842791" to view the fingerprint session status.
```

El comando genera un ID de sesión que puede usar como entrada en el `volume file fingerprint dump` comando.



Puede utilizar el `volume file fingerprint show` Comando con el ID de sesión para supervisar el progreso de la operación de huella digital. Asegúrese de que la operación haya finalizado antes de intentar mostrar la huella.

2. Mostrar la huella digital del archivo:

```
volume file fingerprint dump -session-id session_ID
```



```
svml:> volume file fingerprint dump -session-id 33619976
Vserver:svml
Session-ID:33619976
Volume:slc_vol
Path:/vol/slc_vol/fl
Data
Fingerprint:MOFJVEvxNSJm3C/4Bn5oEEYH5lCrudOzZYK4r5Cfylg=Metadata

Fingerprint:8iMjqJXiNcqqXT5XuRhLiEwIrJEihDmwS0hrexnjgmc=Fingerprint
Algorithm:SHA256
 Fingerprint Scope:data-and-metadata
 Fingerprint Start Time:1460612586
 Formatted Fingerprint Start Time:Thu Apr 14 05:43:06 GMT 2016
 Fingerprint Version:3
 SnapLock License:available
 Vserver UUID:acf7ae64-00d6-11e6-a027-0050569c55ae
 Volume MSID:2152884007
 Volume DSID:1028
 Hostname:my_host
 Filer ID:5f18eda2-00b0-11e6-914e-6fb45e537b8d
 Volume Containing Aggregate:slc_aggr1
 Aggregate ID:c84634aa-c757-4b98-8f07-eefe32565f67
 **SnapLock System ComplianceClock:1460610635
 Formatted SnapLock System ComplianceClock:Thu Apr 14 05:10:35
GMT 2016
 Volume SnapLock Type:compliance
 Volume ComplianceClock:1460610635
 Formatted Volume ComplianceClock:Thu Apr 14 05:10:35 GMT 2016
 Volume Expiry Date:1465880998**
 Is Volume Expiry Date Wraparound:false
 Formatted Volume Expiry Date:Tue Jun 14 05:09:58 GMT 2016
 Filesystem ID:1028
 File ID:96
 File Type:worm
 File Size:1048576
 Creation Time:1460612515
 Formatted Creation Time:Thu Apr 14 05:41:55 GMT 2016
 Modification Time:1460612515
 Formatted Modification Time:Thu Apr 14 05:41:55 GMT 2016
 Changed Time:1460610598
 Is Changed Time Wraparound:false
 Formatted Changed Time:Thu Apr 14 05:09:58 GMT 2016
 Retention Time:1465880998
 Is Retention Time Wraparound:false
 Formatted Retention Time:Tue Jun 14 05:09:58 GMT 2016
```

```
Access Time:-
Formatted Access Time:-
Owner ID:0
Group ID:0
Owner SID:-
Fingerprint End Time:1460612586
Formatted Fingerprint End Time:Thu Apr 14 05:43:06 GMT 2016
```

## Gestione los archivos WORM

### Gestione los archivos WORM

Puede gestionar archivos WORM de las siguientes formas:

- ["Los archivos cumplen CON WORM"](#)
- ["Confirmar copias Snapshot a WORM en un destino de almacén"](#)
- ["Refleje los archivos WORM para la recuperación ante desastres"](#)
- ["Conserve los archivos WORM durante su proceso de litigio"](#)
- ["Eliminar los archivos WORM"](#)

### Los archivos cumplen CON WORM

Puede confirmar archivos a WORM (escritura única y lectura múltiple) o bien manualmente, o bien conserva los archivos automáticamente. También puede crear archivos flexibles WORM.

#### Confirmar los archivos a WORM manualmente

Los archivos se comprometen a WORM manualmente haciendo que el archivo sea de solo lectura. Puede utilizar cualquier comando o programa adecuado a través de NFS o CIFS para cambiar el atributo de lectura y escritura de un archivo a sólo lectura. Puede optar por confirmar los archivos manualmente si desea garantizar que una aplicación haya terminado de escribir en un archivo de modo que el archivo no se confirme prematuramente o si hay problemas de escalado para el analizador de compromiso automático debido a un gran número de volúmenes.

#### Lo que necesitará

- El archivo que desea confirmar debe residir en un volumen de SnapLock.
- El archivo debe ser editable.

#### Acerca de esta tarea

El tiempo de la instancia de ComplianceClock del volumen se escribe en `ctime` campo del archivo cuando se ejecuta el comando o el programa. La hora de la instancia de ComplianceClock determina cuándo se ha alcanzado el tiempo de retención del archivo.

#### Pasos

1. Utilice un comando o programa adecuado para cambiar el atributo de lectura y escritura de un archivo a sólo lectura.

En un shell UNIX, utilice el siguiente comando para crear un archivo denominado `document.txt` solo lectura:

```
chmod -w document.txt
```

En un shell de Windows, utilice el siguiente comando para crear un archivo denominado `document.txt` solo lectura:


```
attrib +r document.txt
```

**Confirmar archivos a WORM automáticamente**

La función de compromiso automático de SnapLock le permite confirmar los archivos automáticamente a WORM. La función de compromiso automático confirma un archivo en estado WORM en un volumen SnapLock si el archivo no cambió en el período de compromiso automático duración. La función de compromiso automático está deshabilitada de forma predeterminada.

**Lo que necesitará**

- Los archivos que desea confirmar automáticamente deben residir en un volumen de SnapLock.
- El volumen SnapLock debe estar en línea.
- El volumen SnapLock debe ser un volumen de lectura/escritura.



La función SnapLock autocommit analiza todos los archivos del volumen y confirma un archivo si cumple con el requisito de compromiso automático. Es posible que haya un intervalo de tiempo entre cuando el archivo esté listo para la confirmación automática y cuando el escáner de confirmación automática de SnapLock lo confirme realmente. Sin embargo, el sistema de archivos sigue protegiendo el archivo de las modificaciones y eliminaciones en cuanto sea apto para la confirmación automática.

**Acerca de esta tarea**

El *autocommit Period* especifica la cantidad de tiempo que los archivos deben permanecer sin cambios antes de que se autocomprometan. Al cambiar un archivo antes de que haya transcurrido el período de compromiso automático, se reinicia el período de compromiso automático del archivo.

En la siguiente tabla se muestran los posibles valores para el período de compromiso automático:

| Valor       | Unidad  | Notas                    |
|-------------|---------|--------------------------|
| ninguno     | -       | El valor predeterminado. |
| 5 - 5256000 | minutos | -                        |
| 1 - 87600   | horas   | -                        |
| 1 - 3650    | días    | -                        |

| Valor   | Unidad | Notas |
|---------|--------|-------|
| 1 - 120 | meses  | -     |
| 1 - 10  | años   | -     |



El valor mínimo es de 5 minutos y el valor máximo es de 10 años.

## Pasos

1. Los archivos de confirmación automática en un volumen SnapLock a WORM:

```
volume snaplock modify -vserver SVM_name -volume volume_name -autocommit
-period autocommit_period
```

Para obtener una lista completa de las opciones, consulte la página de manual del comando.

El siguiente comando confirma automáticamente los archivos en el volumen `vol1` De SVM `vs1`, siempre y cuando los archivos permanezcan inalterados durante 5 horas:

```
cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -autocommit
-period 5hours
```

## Crear un archivo ampliable WORM

Un archivo ampliable WORM conserva los datos escritos de forma incremental, como las entradas del registro. Puede utilizar cualquier comando o programa adecuado para crear un archivo que pueda adaptarse A WORM o la función SnapLock *volume append mode* para crear archivos WORM adaptados de forma predeterminada.

### Utilice un comando o programa para crear un archivo que puede adaptarse A WORM

Puede utilizar cualquier comando o programa adecuado a través de NFS o CIFS para crear un archivo ampliable WORM. Un archivo ampliable WORM conserva los datos escritos de forma incremental, como las entradas del registro. Los datos se agregan al archivo en fragmentos de 256 KB. A medida que se escribe cada fragmento, el fragmento anterior se convierte en CON protección WORM. No se puede eliminar el archivo hasta que haya transcurrido el período de retención.

### Lo que necesitará

El archivo ampliable WORM debe residir en un volumen SnapLock.

### Acerca de esta tarea

Los datos no tienen que escribirse secuencialmente en el fragmento de 256 KB activo. Cuando se escriben datos en el byte  $n \times 256KB + 1$  del archivo, el segmento de 256 KB anterior se protege WORM.

## Pasos

1. Utilice un comando o programa adecuado para crear un archivo de longitud cero con el tiempo de retención deseado.

En un shell de UNIX, utilice el comando siguiente para establecer una hora de retención de 21 de

noviembre de 2020 6:00 a.m. en un archivo de longitud cero denominado `document.txt`:

```
touch -a -t 202011210600 document.txt
```

2. Utilice un comando o programa adecuado para cambiar el atributo de lectura y escritura del archivo a sólo lectura.

En un shell UNIX, utilice el siguiente comando para crear un archivo denominado `document.txt` solo lectura:

```
chmod 444 document.txt
```

3. Utilice un comando o programa adecuado para cambiar el atributo de lectura y escritura del archivo a grabable.



Este paso no se considera un riesgo de cumplimiento de normativas porque no hay datos en el archivo.

En un shell UNIX, utilice el siguiente comando para crear un archivo denominado `document.txt` modificable:

```
chmod 777 document.txt
```

4. Utilice un comando o programa adecuado para iniciar la escritura de datos en el archivo.

En un shell UNIX, utilice el comando siguiente para escribir datos en `document.txt`:

```
echo test data >> document.txt
```



Vuelva a cambiar los permisos de archivo a sólo lectura cuando ya no necesite agregar datos al archivo.

### Use el modo de adición de volúmenes para crear archivos WORM flexibles

A partir de ONTAP 9.3, se puede utilizar la función SnapLock *volume append mode* (VAM) para crear archivos WORM flexibles de forma predeterminada. Un archivo ampliable WORM conserva los datos escritos de forma incremental, como las entradas del registro. Los datos se agregan al archivo en fragmentos de 256 KB. A medida que se escribe cada fragmento, el fragmento anterior se convierte en CON protección WORM. No se puede eliminar el archivo hasta que haya transcurrido el período de retención.

### Lo que necesitará

- El archivo ampliable WORM debe residir en un volumen SnapLock.
- El volumen SnapLock debe estar desmontado y vacío de las copias Snapshot y los archivos creados por el usuario.

## Acerca de esta tarea

Los datos no tienen que escribirse secuencialmente en el fragmento de 256 KB activo. Cuando se escriben datos en el byte  $n \times 256\text{KB} + 1$  del archivo, el segmento de 256 KB anterior se protege WORM.

Si se especifica un período de compromiso automático para el volumen, se comprometen a WORM los archivos flexibles que no se modifican durante un período superior al período de compromiso automático a WORM.



No se admite el VAM en los volúmenes de registros de auditoría de SnapLock.

## Pasos

1. Activar VAM:

```
volume snaplock modify -vserver SVM_name -volume volume_name -is-volume-append
-mode-enabled true|false
```

Para obtener una lista completa de las opciones, consulte la página de manual del comando.

El siguiente comando habilita VAM sobre el volumen vol1 de SVM vs1:

```
cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -is-volume
-append-mode-enabled true
```

2. Utilice un comando o programa adecuado para crear archivos con permisos de escritura.

De forma predeterminada, los archivos se pueden APPWORM.

## Confirmar copias Snapshot a WORM en un destino de almacén

Puede usar SnapLock para SnapVault para proteger CON WORM las copias Snapshot en el almacenamiento secundario. Todas las tareas básicas de SnapLock se realizan en el destino del almacén. El volumen de destino es de solo lectura montado automáticamente, por lo que no es necesario confirmar explícitamente las copias Snapshot a WORM; por lo tanto, no se admiten la creación de copias Snapshot programadas en el volumen de destino mediante políticas de SnapMirror.

### Antes de empezar

- El clúster de origen debe ejecutar ONTAP 8.2.2 o una versión posterior.
- Los agregados de origen y destino deben tener 64 bits.
- El volumen de origen no puede ser un volumen de SnapLock.
- Los volúmenes de origen y destino deben crearse en clústeres con una relación entre iguales con SVM.

Para obtener más información, consulte ["Conexión de clústeres entre iguales"](#).

- Si se deshabilita el crecimiento automático de un volumen, el espacio libre en el volumen de destino debe ser al menos un cinco por ciento mayor que el espacio usado en el volumen de origen.

## Acerca de esta tarea

El volumen de origen puede usar almacenamiento de NetApp o de terceros. Para el almacenamiento que no

sea de NetApp, debe usar la virtualización de FlexArray.



No puede cambiar el nombre de una copia Snapshot que esté comprometida con el estado WORM.

Es posible clonar volúmenes de SnapLock, pero no es posible clonar archivos en un volumen de SnapLock.



Los LUN no son compatibles con los volúmenes de SnapLock. Los LUN se admiten en volúmenes de SnapLock solo en casos en los que las copias de Snapshot creadas en un volumen distinto de SnapLock se transfieren a un volumen de SnapLock para la protección como parte de la relación de almacén de SnapLock. Los LUN no son compatibles con los volúmenes de SnapLock de lectura/escritura. Las copias Snapshot a prueba de manipulaciones son compatibles tanto con los volúmenes de origen como con los volúmenes de destino de SnapMirror que contienen LUN.

A partir de ONTAP 9.14.1, puede especificar períodos de retención para etiquetas de SnapMirror específicas en la política de SnapMirror de la relación de SnapMirror, de modo que las copias Snapshot replicadas del volumen de origen al de destino se conserven durante el período de retención especificado en la regla. Si no se especifica ningún período de retención, se utiliza el período de retención predeterminado del volumen de destino.

A partir de ONTAP 9.13.1, puede restaurar instantáneamente una copia Snapshot bloqueada en el volumen SnapLock de destino de una relación de almacén de SnapLock mediante la creación de un FlexClone con el `snaplock-type` Opción establecida en «non-snaplock» y especificando la copia Snapshot como la «parent-snapshot» al ejecutar la operación de creación de clones de volúmenes. Más información acerca de ["Creación de un volumen FlexClone con un tipo de SnapLock"](#).

Para las configuraciones de MetroCluster, debe tener en cuenta lo siguiente:

- Solo puede crear relaciones de SnapVault entre varias SVM sincronizada en origen, no entre una SVM sincronizada en origen y una SVM sincronizada en destino.
- Puede crear una relación de SnapVault entre un volumen en una SVM sincronizada en origen y una SVM que sirva datos.
- Puede crear una relación de SnapVault entre un volumen en una SVM que sirva datos y un volumen de DP en una SVM sincronizada en origen.

En la siguiente ilustración, se muestra el procedimiento para inicializar una relación de almacén de SnapLock:

## Pasos

1. Identifique el clúster de destino.
2. En el clúster de destino, ["Instale la licencia de SnapLock"](#), ["Inicie el reloj de cumplimiento"](#), Y, si está utilizando una versión de ONTAP anterior a 9.10.1, ["Cree un agregado de SnapLock"](#).
3. En el clúster de destino, cree un volumen de destino de SnapLock de tipo DP que tiene el mismo tamaño o mayor que el volumen de origen:

```
volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name
-snaplock-type compliance|enterprise -type DP -size size
```



A partir de ONTAP 9.10.1, los volúmenes de SnapLock y otros de SnapLock pueden existir en el mismo agregado; por lo tanto, ya no es necesario crear un agregado de SnapLock separado si se utiliza ONTAP 9.10.1. La opción `volume -snaplock-type` se utiliza para especificar el tipo de volumen Compliance o Enterprise SnapLock. En las versiones de ONTAP anteriores a ONTAP 9.10.1, el modo SnapLock, Compliance o Enterprise, se hereda del agregado. No se admiten los volúmenes de destino con versión flexible. La configuración de idioma del volumen de destino debe coincidir con la configuración de idioma del volumen de origen.

El siguiente comando crea una SnapLock de 2 GB Compliance volumen denominado `dstvolB` pulg SVM2 en el agregado `node01_aggr`:

```
cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate
node01_aggr -snaplock-type compliance -type DP -size 2GB
```

4. En el clúster de destino, establezca el período de retención predeterminado, tal como se describe en [Establecer el período de retención predeterminado](#).



Un volumen SnapLock que es un destino de almacén tiene asignado un período de retención predeterminado. El valor correspondiente a este período se establece inicialmente en un mínimo de 0 años para volúmenes de SnapLock Enterprise y un máximo de 30 años para volúmenes de SnapLock Compliance. Cada copia de Snapshot de NetApp se compromete con el primer período de retención predeterminado. El período de retención se puede ampliar más adelante, si fuera necesario. Para obtener más información, consulte [Establecer información general sobre el tiempo de retención](#).

5. [Cree una nueva relación de replicación](#) Entre el origen que no es de SnapLock y el nuevo destino de SnapLock que creó en el paso 3.

En este ejemplo, se crea una nueva relación de SnapMirror con el volumen de SnapLock de destino `dstvolB` utilizar una política de `XDPDefault` Para almacenar las copias snapshot etiquetadas como diaria y semanal en una programación horaria:

```
cluster2::> snapmirror create -source-path SVM1:srcvolA -destination
-path SVM2:dstvolB -vserver SVM2 -policy XDPDefault -schedule hourly
```



[Cree una política de replicación personalizada](#) o a [programación personalizada](#) si los valores predeterminados disponibles no son adecuados.

6. En la SVM de destino, inicialice la relación de SnapVault creada en el paso 5:

**`snapmirror initialize -destination-path destination_path`**

El siguiente comando inicializa la relación entre el volumen de origen `srcvolA` encendido SVM1 y el volumen de destino `dstvolB` encendido SVM2:

```
cluster2::> snapmirror initialize -destination-path SVM2:dstvolB
```



7. Después de inicializar y de estar inactiva la relación, utilice `snapshot show` Comando en el destino para comprobar el tiempo de caducidad de la SnapLock aplicado a las copias Snapshot replicadas.

En este ejemplo, se enumeran las copias Snapshot en el volumen `dstvolB` Que tienen la etiqueta de SnapMirror y la fecha de caducidad de SnapLock:

```
cluster2::> snapshot show -vserver SVM2 -volume dstvolB -fields
snapmirror-label, snaplock-expiry-time
```

### Información relacionada

["Relaciones entre iguales de clústeres y SVM"](#)

["Backup de volúmenes mediante SnapVault"](#)

### Refleje los archivos WORM para la recuperación ante desastres

Puede usar SnapMirror para replicar archivos WORM a otra ubicación geográfica a efectos de recuperación ante desastres y otros fines. Tanto el volumen de origen como el de destino deben configurarse para SnapLock, y ambos volúmenes deben tener el mismo modo SnapLock, Compliance o Enterprise. Se replican todas las propiedades clave de la SnapLock del volumen y los archivos.

### Requisitos previos

Los volúmenes de origen y destino deben crearse en clústeres con una relación entre iguales con SVM. Para obtener más información, consulte ["Relaciones entre iguales de clústeres y SVM"](#).

### Acerca de esta tarea

- A partir de ONTAP 9.5, puede replicar archivos WORM con la relación de tipo XDP (protección de datos ampliada) de SnapMirror en lugar de la relación de tipo DP (protección de datos). El modo XDP es independiente de las versiones de ONTAP y es capaz de diferenciar los archivos almacenados en el mismo bloque, facilitando de este modo la resincronización de los volúmenes replicados de modo de cumplimiento. Para obtener información sobre cómo convertir una relación de tipo DP existente a una relación de tipo XDP, consulte ["Protección de datos"](#).
- Una operación de resincronización de tipo DP relación SnapMirror genera un error en un volumen de modo de cumplimiento si SnapLock determina que provocará la pérdida de datos. Si una operación de resincronización falla, puede utilizar el `volume clone create` comando para crear un clon del volumen de destino. A continuación, puede volver a sincronizar el volumen de origen con el clon.
- Una relación de SnapMirror del tipo XDP entre volúmenes compatibles con SnapLock admite una resincronización después de una interrupción aunque los datos del destino hayan divergido del origen posterior a la interrupción.

En un resincronización, cuando se detecta una divergencia de datos entre el destino de origen más allá de la instantánea común, se corta una nueva instantánea en el destino para capturar esta divergencia. La nueva snapshot y la snapshot común están bloqueadas con un tiempo de retención de la siguiente manera:

- La hora de caducidad del volumen del destino
- Si el tiempo de caducidad del volumen es pasado o no se ha establecido, la copia de Snapshot se bloquea durante un período de 30 días

- Si el destino tiene retenciones legales, el período de caducidad real del volumen se oculta y aparece como "indefinido", sin embargo la instantánea se bloquea durante el período de caducidad real del volumen.

Si el volumen de destino tiene un período de caducidad posterior al origen, se conserva el período de caducidad del destino y no se sobrescribe con el período de caducidad del volumen de origen posterior a la resincronización.

Si el destino tiene retenciones legales en él que difieren de la fuente, no se permite una resincronización. El origen y el destino deben tener idénticas retenciones legales o todas las retenciones legales del destino deben liberarse antes de intentar realizar una resincronización.

Una copia Snapshot bloqueada en el volumen de destino creada para capturar los datos divergentes se puede copiar en el origen con la CLI ejecutando el `snapmirror update -s snapshot` comando. La instantánea una vez copiada seguirá bloqueada en la fuente.


- No se admiten las relaciones de protección de datos de SVM.
- No se admiten las relaciones de protección de datos con uso compartido de carga.

En la siguiente ilustración, se muestra el procedimiento para inicializar una relación de SnapMirror:

## System Manager

A partir de ONTAP 9.12.1, puede usar System Manager para configurar la replicación de SnapMirror de archivos WORM.

### Pasos

1. Vaya a **almacenamiento > volúmenes**.
2. Haga clic en **Mostrar/Ocultar** y seleccione **Tipo de SnapLock** para visualizar la columna en la ventana **volúmenes**.
3. Busque un volumen de SnapLock.
4. Haga clic en  Y seleccione **proteger**.
5. Elija el clúster de destino y la máquina virtual de almacenamiento de destino.
6. Haga clic en **más opciones**.
7. Seleccione **Mostrar políticas heredadas** y seleccione **DPDefault (Legacy)**.
8. En la sección **Detalles de la configuración de destino**, seleccione **Anular programa de transferencia** y seleccione **por hora**.
9. Haga clic en **Guardar**.
10. A la izquierda del nombre del volumen de origen, haga clic en la flecha para expandir los detalles del volumen y, en el lado derecho de la página, consulte los detalles de la protección remota de SnapMirror.
11. En el clúster remoto, vaya a **Relaciones de protección**.
12. Busque la relación y haga clic en el nombre del volumen de destino para ver los detalles de la relación.
13. Compruebe que el tipo de SnapLock del volumen de destino y otra información de SnapLock.

### CLI

1. Identifique el clúster de destino.
2. En el clúster de destino, ["Instale la licencia de SnapLock"](#), ["Inicialice el reloj de cumplimiento"](#), Y, si está utilizando una versión de ONTAP anterior a 9.10.1, ["Cree un agregado de SnapLock"](#).
3. En el clúster de destino, cree un volumen de destino de SnapLock de tipo DP es el mismo tamaño que el volumen de origen o mayor:

```
volume create -vserver SVM_name -volume volume_name -aggregate
aggregate_name -snaplock-type compliance|enterprise -type DP -size size
```



A partir de ONTAP 9.10.1, los volúmenes de SnapLock y otros de SnapLock pueden existir en el mismo agregado; por lo tanto, ya no es necesario crear un agregado de SnapLock separado si se utiliza ONTAP 9.10.1. La opción `volume -snaplock-type` se utiliza para especificar el tipo de volumen Compliance o Enterprise SnapLock. En las versiones de ONTAP anteriores a ONTAP 9.10.1, el modo SnapLock (Compliance o Enterprise) se hereda del agregado. No se admiten los volúmenes de destino con versión flexible. La configuración de idioma del volumen de destino debe coincidir con la configuración de idioma del volumen de origen.

El siguiente comando crea una SnapLock de 2 GB Compliance volumen denominado `dstvolB` en el agregado `node01_aggr`:

```
cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate
node01_aggr -snaplock-type compliance -type DP -size 2GB
```

4. En la SVM de destino, cree una política de SnapMirror:

```
snapmirror policy create -vserver SVM_name -policy policy_name
```

El siguiente comando crea la política de toda la SVM SVM1-mirror:

```
SVM2::> snapmirror policy create -vserver SVM2 -policy SVM1-mirror
```

5. En la SVM de destino, cree una programación de SnapMirror:

```
job schedule cron create -name schedule_name -dayofweek day_of_week -hour
hour -minute minute
```

El siguiente comando crea una programación de SnapMirror con el nombre weekendcron:

```
SVM2::> job schedule cron create -name weekendcron -dayofweek
"Saturday, Sunday" -hour 3 -minute 0
```

6. En la SVM de destino, cree una relación de SnapMirror:

```
snapmirror create -source-path source_path -destination-path
destination_path -type XDP|DP -policy policy_name -schedule schedule_name
```

El siguiente comando crea una relación de SnapMirror entre el volumen de origen srcvolA encendido SVM1 y el volumen de destino dstvolB encendido SVM2, y asigna la directiva SVM1-mirror y el programa weekendcron:

```
SVM2::> snapmirror create -source-path SVM1:srcvolA -destination
-path SVM2:dstvolB -type XDP -policy SVM1-mirror -schedule
weekendcron
```



El tipo XDP está disponible en ONTAP 9.5 y posterior. Debe usar el tipo de DP en ONTAP 9.4 y versiones anteriores.

7. En la SVM de destino, inicialice la relación de SnapMirror:

```
snapmirror initialize -destination-path destination_path
```

El proceso de inicialización realiza una *transferencia basal* al volumen de destino. SnapMirror realiza una copia Snapshot del volumen de origen y, a continuación, transfiere la copia y todos los bloques de datos que hace referencia al volumen de destino. También transfiere cualquier otra copia Snapshot del volumen de origen al volumen de destino.

El siguiente comando inicializa la relación entre el volumen de origen `srcvolA` encendido SVM1 y el volumen de destino `dstvolB` encendido SVM2:

```
SVM2::> snapmirror initialize -destination-path SVM2:dstvolB
```

### Información relacionada

["Relaciones entre iguales de clústeres y SVM"](#)

["Preparación para la recuperación ante desastres de volúmenes"](#)

["Protección de datos"](#)

### Conserve los archivos WORM durante su litigio gracias a su conservación legal

A partir de ONTAP 9.3, puede conservar archivos WORM en modo de cumplimiento durante un litigio con la función *Legal Hold*.

#### Lo que necesitará

- Debe ser un administrador de SnapLock para realizar esta tarea.

["Cree una cuenta de administrador de SnapLock"](#)

- Debe haber iniciado sesión en una conexión segura (SSH, Console o ZAPI).

#### Acerca de esta tarea

Un archivo de retención legal se comporta como un archivo WORM con un período de retención indefinido. Es su responsabilidad especificar cuándo termina el período de retención legal.

El número de archivos que se pueden colocar en una conservación legal depende del espacio disponible en el volumen.

#### Pasos

1. Inicie una conservación legal:

```
snaplock legal-hold begin -litigation-name litigation_name -volume volume_name -path path_name
```

El siguiente comando inicia una retención legal para todos los archivos de `vol1`:

```
cluster1::> snaplock legal-hold begin -litigation-name litigation1 -volume vol1 -path /
```

2. Terminar una conservación legal:

```
snaplock legal-hold end -litigation-name litigation_name -volume volume_name -path path_name
```

El siguiente comando finaliza una retención legal para todos los archivos de `vol1`:

```
cluster1::>snaplock legal-hold end -litigation-name litigation1 -volume
vol1 -path /
```

## Información general acerca de Delete WORM files

Puede eliminar archivos WORM en modo de empresa durante el período de retención mediante la función de eliminación con privilegios.

Antes de poder usar esta función, debe crear una cuenta de administrador de SnapLock y, a continuación, utilizar la cuenta, habilitar la función.

### Cree una cuenta de administrador de SnapLock

Para realizar una eliminación con privilegios, debe tener privilegios de administrador de SnapLock. Estos privilegios se definen en el rol vsadmin-snaplock. Si todavía no ha asignado ese rol, puede solicitar al administrador de clúster que cree una cuenta de administrador de SVM con el rol de administrador de SnapLock.

### Lo que necesitará

- Para realizar esta tarea, debe ser un administrador de clústeres.
- Debe haber iniciado sesión en una conexión segura (SSH, Console o ZAPI).

### Pasos

1. Cree una cuenta de administrador de SVM con el rol de administrador de SnapLock:

```
security login create -vserver SVM_name -user-or-group-name user_or_group_name
-application application -authmethod authentication_method -role role -comment
comment
```

El siguiente comando habilita la cuenta de administrador de SVM SnapLockAdmin con los predefinidos vsadmin-snaplock función a la que acceder SVM1 con una contraseña:

```
cluster1::> security login create -vserver SVM1 -user-or-group-name
SnapLockAdmin -application ssh -authmethod password -role vsadmin-
snaplock
```

### Active la función de eliminación con privilegios

Debe habilitar explícitamente la función de eliminación con privilegios en el volumen de Enterprise que contiene los archivos WORM que desea eliminar.

### Acerca de esta tarea

El valor de `-privileged-delete` la opción determina si la eliminación con privilegios está habilitada. Los valores posibles son `enabled`, `disabled`, y `permanently-disabled`.



`permanently-disabled` es el estado del terminal. No se puede habilitar la eliminación con privilegios en el volumen después de establecer el estado en `permanently-disabled`.

## Pasos

1. Habilitar la eliminación con privilegios para un volumen de SnapLock Enterprise:

```
volume snaplock modify -vserver SVM_name -volume volume_name -privileged
-delete disabled|enabled|permanently-disabled
```

El siguiente comando habilita la función de eliminación con privilegios para el volumen de empresa dataVol encendido SVM1:

```
SVM1::> volume snaplock modify -vserver SVM1 -volume dataVol -privileged
-delete enabled
```

## Elimine los archivos WORM de modo empresarial

Puede utilizar la función de eliminación con privilegios para eliminar archivos WORM en modo de empresa durante el período de retención.

### Lo que necesitará

- Debe ser un administrador de SnapLock para realizar esta tarea.
- Debe haber creado un registro de auditoría de SnapLock y habilitado la función de eliminación privilegiada en el volumen empresarial.

### Acerca de esta tarea

No puede utilizar una operación de eliminación privilegiada para eliminar un archivo WORM caducado. Puede utilizar el `volume file retention show` Comando para ver el tiempo de retención del archivo WORM que desea eliminar. Para obtener más información, consulte la página man del comando.

## Paso

1. Eliminar un archivo WORM en un volumen empresarial:

```
volume file privileged-delete -vserver SVM_name -file file_path
```

El siguiente comando elimina el archivo /vol/dataVol/f1 En la SVM SVM1:

```
SVM1::> volume file privileged-delete -file /vol/dataVol/f1
```

## Mover un volumen de SnapLock

A partir de ONTAP 9.8, puede mover un volumen SnapLock a un agregado de destino del mismo tipo, ya sea de empresa a empresa o de cumplimiento de normativas. Debe

tener asignado el rol de seguridad SnapLock para mover un volumen de SnapLock.

## Cree una cuenta de administrador de seguridad de SnapLock

Debe tener privilegios de administrador de seguridad de SnapLock para realizar un movimiento de volúmenes de SnapLock. Este privilegio se le concede con el rol *SnapLock*, introducido en ONTAP 9.8. Si todavía no ha recibido ese rol, puede solicitar al administrador del clúster que cree un usuario de seguridad SnapLock con este rol de seguridad SnapLock.

### Lo que necesitará

- Para realizar esta tarea, debe ser un administrador de clústeres.
- Debe haber iniciado sesión en una conexión segura (SSH, Console o ZAPI).

### Acerca de esta tarea

El rol SnapLock se asocia con la SVM de administrador, a diferencia del rol vsadmin-snaplock, que está asociada con la SVM de datos.

### Paso

1. Cree una cuenta de administrador de SVM con el rol de administrador de SnapLock:

```
security login create -vserver SVM_name -user-or-group-name user_or_group_name
-application application -authmethod authentication_method -role role -comment
comment
```

El siguiente comando habilita la cuenta de administrador de SVM SnapLockAdmin con los predefinidos snaplock Rol para acceder a la SVM de administrador cluster1 con una contraseña:

```
cluster1::> security login create -vserver cluster1 -user-or-group-name
SnapLockAdmin -application ssh -authmethod password -role snaplock
```

## Mover un volumen de SnapLock

Puede utilizar el `volume move` Comando para mover un volumen de SnapLock a un agregado de destino.

### Lo que necesitará

- Debe haber creado un registro de auditoría protegido en SnapLock antes de ejecutar el movimiento de volúmenes de SnapLock.

["Cree un registro de auditoría"](#).

- Si utiliza una versión de ONTAP anterior a ONTAP 9.10.1, el agregado de destino debe ser el mismo tipo de SnapLock que el volumen de SnapLock que desea mover: Compliance to Compliance o Enterprise to Enterprise. A partir de ONTAP 9.10.1, esta restricción se elimina y un agregado puede incluir volúmenes SnapLock de Compliance y Enterprise, así como volúmenes que no son de SnapLock.
- Debe haberse registrado como usuario con el rol de seguridad SnapLock.

### Pasos

1. Con una conexión segura, inicie sesión en la LIF de gestión de clústeres de ONTAP:

```
ssh snaplock_user@cluster_mgmt_ip
```



## 2. Mover un volumen de SnapLock:

```
volume move start -vserver SVM_name -volume SnapLock_volume_name -destination
-aggregate destination_aggregate_name
```

## 3. Compruebe el estado de la operación de movimiento de volúmenes:

```
volume move show -volume SnapLock_volume_name -vserver SVM_name -fields
volume,phase,vserver
```

## Bloquee una copia Snapshot para obtener protección contra ataques de ransomware

A partir de ONTAP 9.12.1, puede bloquear una copia Snapshot en un volumen que no sea de SnapLock para proporcionar protección contra ataques de ransomware. El bloqueo de las copias Snapshot garantiza que no se puedan eliminar accidental o con malas intenciones.

La función de reloj de cumplimiento de normativas de SnapLock le permite bloquear las copias Snapshot durante un período determinado para que no se puedan eliminar hasta que llegue el momento de caducidad. Bloquear copias Snapshot las protege a prueba de manipulaciones e impedir las amenazas de ransomware. Puede usar copias Snapshot bloqueadas para recuperar los datos si un volumen se ve afectado por un ataque de ransomware.

A partir de ONTAP 9.14.1, el bloqueo de copias Snapshot admite copias Snapshot de retención a largo plazo en destinos de almacenes SnapLock y en volúmenes de destino que no sean de SnapMirror de SnapLock. El bloqueo de copia de Snapshot se habilita configurando el período de retención mediante las reglas de políticas de SnapMirror asociadas a un [etiqueta de política existente](#). La regla anula el período de retención predeterminado establecido en el volumen. Si no existe un período de retención asociado con la etiqueta de SnapMirror, se utiliza el período de retención predeterminado del volumen.

### Requisitos y consideraciones sobre copias Snapshot a prueba de manipulaciones

- Si utiliza la CLI de ONTAP, todos los nodos del clúster deben ejecutar ONTAP 9.12.1 o una versión posterior. Si utiliza System Manager, todos los nodos deben ejecutar ONTAP 9.13.1 o una versión posterior.
- ["La licencia de SnapLock debe instalarse en el clúster"](#). Esta licencia está incluida en ["ONTAP One"](#).
- ["Es necesario inicializar el reloj de cumplimiento de normativas del clúster"](#).
- Cuando se habilita el bloqueo de snapshots en un volumen, es posible actualizar los clústeres a una versión de ONTAP posterior a ONTAP 9.12.1; Sin embargo, no puede revertir a una versión anterior de ONTAP hasta que todas las copias snapshot bloqueadas hayan alcanzado su fecha de caducidad y se eliminen, y el bloqueo de la copia snapshot se ha deshabilitado.
- Cuando se bloquea una instantánea, el tiempo de caducidad del volumen se establece en el tiempo de caducidad de la copia snapshot. Si más de una copia Snapshot está bloqueada, el tiempo de caducidad del volumen refleja el mayor tiempo de caducidad de todas las copias Snapshot.
- El período de retención para las copias Snapshot bloqueadas tiene prioridad sobre el número de copias de Snapshot conservadas; esto significa que no se respeta el límite de conservación de recuento si no ha caducado el período de retención de copia de Snapshot para copias Snapshot bloqueadas.
- En una relación de SnapMirror, puede establecer un período de retención en una regla de política de reflejo-almacén y el período de retención se aplica a las copias Snapshot replicadas en el destino si el volumen de destino tiene la función de bloqueo de copias Snapshot habilitada. El período de retención

tiene prioridad sobre el recuento de retenciones; por ejemplo, las copias Snapshot que no hayan sobrepasado su vencimiento se retendrán aunque se supere el recuento de retenciones.

- Puede cambiar el nombre de una copia Snapshot en un volumen que no sea de SnapLock. Las operaciones de cambio de nombre de Snapshot en el volumen primario de una relación de SnapMirror se reflejan en el volumen secundario solo si la política es MirrorAllSnapshots. Para otros tipos de políticas, la copia Snapshot cuyo nombre se ha cambiado no se propaga durante las actualizaciones.
- Si utiliza la CLI de ONTAP, puede restaurar una copia Snapshot bloqueada con el `volume snapshot restore` Comando solo si la copia snapshot bloqueada es la más reciente. Si hay alguna copia Snapshot sin expirar más adelante que la que se va a restaurar, se produce un error en la operación de restauración de la copia de Snapshot.

### Funciones compatibles con copias Snapshot a prueba de manipulaciones

- Volúmenes de FlexGroup

Los volúmenes de FlexGroup admiten el bloqueo de copias Snapshot. El bloqueo de instantáneas solo se realiza en la copia snapshot que forma parte del componente raíz. Solo se permite eliminar el volumen FlexGroup si ha transcurrido el tiempo de caducidad del componente raíz.

- Conversión de FlexVol a FlexGroup

Puede convertir un volumen FlexVol con copias snapshot bloqueadas en un volumen FlexGroup. Las copias snapshot permanecen bloqueadas después de la conversión.

- Clon de volumen y clon de archivo

Es posible crear clones de volúmenes y clones de archivos a partir de una copia Snapshot bloqueada.

### Funciones no admitidas

En la actualidad, las siguientes funciones no son compatibles con las copias Snapshot a prueba de manipulaciones:

- Cloud Volumes ONTAP
- Grupos de consistencia
- FabricPool
- Volúmenes de FlexCache
- SMTape
- Continuidad del negocio de SnapMirror (SM-BC)
- Reglas de política de SnapMirror mediante el `-schedule` parámetro
- SnapMirror síncrono
- Movilidad de datos de SVM (se usa para migrar o reubicar una SVM desde un clúster de origen a un clúster de destino)

### Habilite el bloqueo de las copias snapshot al crear un volumen

A partir de ONTAP 9.12.1, se puede habilitar el bloqueo de copias snapshot cuando se crea un volumen nuevo o se modifica un volumen existente mediante el `-snapshot-locking-enabled` con la `volume create` y `volume modify` Comandos de la CLI. A partir de ONTAP 9.13.1, puede usar System Manager para habilitar el bloqueo de copias de SnapVault.

## System Manager

1. Navegue hasta **Almacenamiento > Volúmenes** y seleccione **Agregar**.
2. En la ventana **Añadir volumen**, seleccione **Más opciones**.
3. Introduzca el nombre del volumen, el tamaño, la política de exportación y el nombre del recurso compartido.
4. Seleccione **Habilitar Bloqueo de instantáneas**. Esta selección no se muestra si la licencia de SnapLock no está instalada.
5. Si aún no está habilitado, seleccione **Inicializar reloj de cumplimiento de SnapLock**.
6. Guarde los cambios.
7. En la ventana **Volúmenes**, seleccione el volumen que actualizaste y seleccione **Resumen**.
8. Verifique que **SnapLock Bloqueo de copia instantánea** se muestre como **habilitado**.

## CLI

1. Para crear un nuevo volumen y habilitar el bloqueo de copias Snapshot, introduzca el siguiente comando:

```
volume create -vserver vs1 -volume volume_name -snapshot-locking-enabled true
```


El siguiente comando habilita el bloqueo de copias Snapshot en un nuevo volumen denominado vol1:

```
> volume create -volume vol1 -aggregate aggr1 -size 100m -snapshot-locking-enabled true
Warning: Snapshot copy locking is being enabled on volume "vol1" in Vserver "vs1". It cannot be disabled until all locked Snapshot copies are past their expiry time. A volume with unexpired locked Snapshot copies cannot be deleted.
Do you want to continue: {yes|no}: y
[Job 32] Job succeeded: Successful
```

## Habilite el bloqueo de copias snapshot en un volumen existente

A partir de ONTAP 9.12.1, puede habilitar el bloqueo de copia de snapshot en un volumen existente mediante la interfaz de línea de comandos de ONTAP. A partir de ONTAP 9.13.1, puede usar System Manager para habilitar el bloqueo de copias de Snapshot en un volumen existente.

## System Manager

1. Vaya a **almacenamiento > volúmenes**.
2. Seleccione  Y elija **Editar > Volumen**.
3. En la ventana **Editar volumen**, localice la sección Configuración de copias snapshot (locales) y seleccione **Habilitar bloqueo de instantáneas**.

Esta selección no se muestra si la licencia de SnapLock no está instalada.

4. Si aún no está habilitado, selecciona **Inicializar reloj de cumplimiento de SnapLock**.
5. Guarde los cambios.
6. En la ventana **Volúmenes**, selecciona el volumen que actualizaste y selecciona **Resumen**.
7. Verifique que **SnapLock Bloqueo de copia instantánea** se muestre como **habilitado**.

## CLI

1. Para modificar un volumen existente para habilitar el bloqueo de copias Snapshot, introduzca el siguiente comando:


```
volume modify -vserver vserver_name -volume volume_name -snapshot-locking
-enabled true
```

## Cree una política de copia de Snapshot bloqueada y aplique retención

A partir de ONTAP 9.12.1, puede crear políticas de copias de Snapshot para aplicar un período de retención de copias de Snapshot y aplicar la política a un volumen para bloquear las copias de Snapshot durante el período especificado. También puede bloquear una copia Snapshot mediante la configuración manual de un período de retención. A partir de ONTAP 9.13.1, puede usar System Manager para crear políticas de bloqueo de copias de Snapshot y aplicarlas a un volumen.

### Cree una política de bloqueo de copias snapshot

## System Manager

1. Vaya a **Storage > Storage VMs** y seleccione una VM de almacenamiento.
2. Seleccione **Ajustes**.
3. Localice **Políticas de instantánea** y seleccione .
4. En la ventana **Add Snapshot Policy**, introduzca el nombre de la política.
5. Seleccione  **Add**.
6. Proporcione los detalles de la programación de la copia de Snapshot, incluido el nombre de la programación, el número máximo de copias de Snapshot que se deben conservar y el período de retención de SnapLock.
7. En la columna **SnapLock Retention Period**, introduzca el número de horas, días, meses o años que se van a conservar las copias snapshot. Por ejemplo, una política de copia de Snapshot con un período de retención de 5 días bloquea una copia de Snapshot por 5 días desde el momento en que se creó y no puede eliminarse durante ese período. Se admiten los siguientes rangos de períodos de retención:
  - Años: 0 - 100
  - Meses: 0 - 1200
  - Días: 0 - 36500
  - Horario: 0 - 24
8. Guarde los cambios.

## CLI

1. Para crear una política de copias Snapshot, introduzca el siguiente comando:

```
volume snapshot policy create -policy policy_name -enabled true -schedule1
schedule1_name -count1 maximum_Snapshot_copies -retention-period1
_retention_period
```


El siguiente comando crea una política de bloqueo de copias de Snapshot:

```
cluster1> volume snapshot policy create -policy policy_name -enabled
true -schedule1 hourly -count1 24 -retention-period1 "1 days"
```

No se reemplaza una copia Snapshot si se encuentra sujeta a una retención activa; es decir, el número de retención no se respetará si hay copias Snapshot bloqueadas que aún no han caducado.

## Aplicar una política de bloqueo a un volumen

### System Manager

1. Vaya a **almacenamiento > volúmenes**.
2. Seleccione  Y elija **Editar > Volumen**.
3. En la ventana **Editar volumen**, seleccione **Programar copias snapshot**.
4. Seleccione la política de copias de Snapshot bloqueadas de la lista.
5. Si el bloqueo de copias snapshot no está activado, seleccione **Activar bloqueo de instantáneas**.
6. Guarde los cambios.

### CLI

1. Para aplicar una política de bloqueo de copias Snapshot a un volumen existente, introduzca el siguiente comando:

```
volume modify -volume volume_name -vserver vserver_name -snapshot-policy
policy_name
```

### Aplicación del período de retención durante la creación manual de las copias de Snapshot

Es posible aplicar un período de retención de copia Snapshot cuando se crea manualmente una copia Snapshot. Debe habilitarse el bloqueo de copia de snapshot en el volumen; de lo contrario, se ignorará la configuración del período de retención.

## System Manager

1. Navegue hasta **Almacenamiento > Volúmenes** y seleccione un volumen.
2. En la página de detalles del volumen, seleccione la pestaña **Copias de instantánea**.
3. Seleccione **+ Add**.
4. Introduzca el nombre de la copia Snapshot y la hora de caducidad de SnapLock. Puede seleccionar el calendario para elegir la fecha y la hora de caducidad de la retención.
5. Guarde los cambios.
6. En la página **Volúmenes > Copias de instantáneas**, seleccione **Mostrar/Ocultar** y elija **Tiempo de caducidad de SnapLock** para mostrar la columna **Tiempo de caducidad de SnapLock** y verifique que el tiempo de retención esté establecido.

## CLI

1. Para crear una copia Snapshot manualmente y aplicar un período de retención de bloqueo, introduzca el siguiente comando:


```
volume snapshot create -volume volume_name -snapshot snapshot_copy_name
-snaplock-expiry-time expiration_date_time
```

El siguiente comando crea una nueva copia Snapshot y establece el período de retención:

```
cluster1> volume snapshot create -vserver vs1 -volume vol1 -snapshot
snap1 -snaplock-expiry-time "11/10/2022 09:00:00"
```

## Aplique el período de retención a una copia Snapshot existente

## System Manager

1. Navegue hasta **Almacenamiento > Volúmenes** y seleccione un volumen.
2. En la página de detalles del volumen, seleccione la pestaña **Copias de instantánea**.
3. Seleccione la copia Snapshot y seleccione , Y elija **Modificar tiempo de caducidad de SnapLock**. Puede seleccionar el calendario para elegir la fecha y la hora de caducidad de la retención.
4. Guarde los cambios.
5. En la página **Volúmenes > Copias de instantáneas**, seleccione **Mostrar/Ocultar** y elija **Tiempo de caducidad de SnapLock** para mostrar la columna **Tiempo de caducidad de SnapLock** y verifique que el tiempo de retención esté establecido.

## CLI

1. Para aplicar manualmente un período de retención a una copia Snapshot existente, introduzca el siguiente comando:

```
volume snapshot modify-snaplock-expiry-time -volume volume_name -snapshot snapshot_copy_name -expiry-time expiration_date_time
```

En el siguiente ejemplo se aplica un período de retención a una copia Snapshot existente:

```
cluster1> volume snapshot modify-snaplock-expiry-time -volume vol1
-snapshot snap2 -expiry-time "11/10/2022 09:00:00"
```

## Modifique una política existente para aplicar la retención a largo plazo

A partir de ONTAP 9.14.1, puede modificar una política de SnapMirror existente añadiendo una regla para establecer una retención a largo plazo de copias Snapshot. La regla se utiliza para anular el período de retención de volúmenes predeterminado en destinos de almacén de SnapLock y en volúmenes de destino que no son de SnapMirror de SnapLock.

1. Agregue una regla a una política de SnapMirror existente:

```
snapmirror policy add-rule -vserver <SVM name> -policy <policy name>
-snapmirror-label <label name> -keep <number of Snapshot copies> -retention
-period [<integer> days|months|years]
```

En el siguiente ejemplo se crea una regla que aplica un período de retención de 6 meses a la política existente denominada «lockvault»:

```
snapmirror policy add-rule -vserver vs1 -policy lockvault -snapmirror
-label test1 -keep 10 -retention-period "6 months"
```

## API de SnapLock

Puede utilizar las API de Zephyr para integrar la funcionalidad de SnapLock en scripts o automatización de flujos de trabajo. Las API utilizan mensajería XML a través de HTTP,



HTTPS y DCE/RPC de Windows. Para obtener más información, consulte ["Documentación de automatización de ONTAP"](#).

#### **archivo-huella-abortar**

Anular una operación de huellas digitales de archivo.

#### **volcado de huellas digitales de archivo**

Mostrar información de huellas digitales del archivo.

#### **file-fingerprint-get-iter**

Muestra el estado de las operaciones de huella digital de archivos.

#### **inicio de la huella digital de archivo**

Genere una huella digital de archivo.

#### **snaplock-archive-vserver-log**

Archive el archivo de registro de auditoría activo.

#### **snaplock-create-vserver-log**

Cree una configuración de registro de auditoría para una SVM.

#### **snaplock-delete-vserver-log**

Eliminar una configuración de registro de auditoría para una SVM.

#### **snaplock-file-privileged-delete**

Ejecute una operación de eliminación privilegiada.

#### **snaplock-get-file-retention**

Obtenga el período de retención de un archivo.

#### **snaplock-get-node-compliance-clock**

Obtenga la fecha y la hora de la instancia de ComplianceClock del nodo.

#### **snaplock-get-vserver-activo-log-files-iter**

Mostrar el estado de los archivos de registro activos.

#### **snaplock-get-vserver-log-iter**

Muestre la configuración del registro de auditoría.

### **snaplock-modify-vserver-log**

Modifique la configuración del registro de auditoría para una SVM.

### **retención de conjuntos de archivos de snaplock**

Establezca el tiempo de retención de un archivo.

### **snaplock-set-node-compliance-clock**

Establezca la fecha y la hora de la instancia de ComplianceClock del nodo.

### **snaplock-volume-set-privileged-delete**

Establezca la opción Privileged-delete en un volumen SnapLock Enterprise.

### **volume-get-snaplock-attrs**

Obtenga los atributos de un volumen de SnapLock.

### **volume-set-snaplock-attrs**

Configure los atributos de un volumen SnapLock.

## **Grupos de consistencia**

### **Información general sobre los grupos de consistencia**

Un grupo de coherencia es una recogida de volúmenes que se gestionan como una sola unidad. En ONTAP, los grupos de coherencia proporcionan una gestión fácil y una garantía de protección para una carga de trabajo de la aplicación que abarca varios volúmenes.

Puede utilizar grupos de consistencia para simplificar la gestión del almacenamiento. Imagine que dispone de una base de datos importante que abarca veinte LUN. Puede administrar las LUN de forma individual o tratar las LUN como un conjunto de datos solitario, organizándolas en un único grupo de consistencia.

Los grupos de coherencia facilitan la gestión de cargas de trabajo de aplicaciones, proporcionando políticas de protección local y remota fáciles de configurar, y copias de Snapshot simultáneas consistentes con las aplicaciones y con los fallos de una colección de volúmenes en un momento específico. Las copias Snapshot de un grupo de coherencia permiten restaurar una carga de trabajo de la aplicación completa.

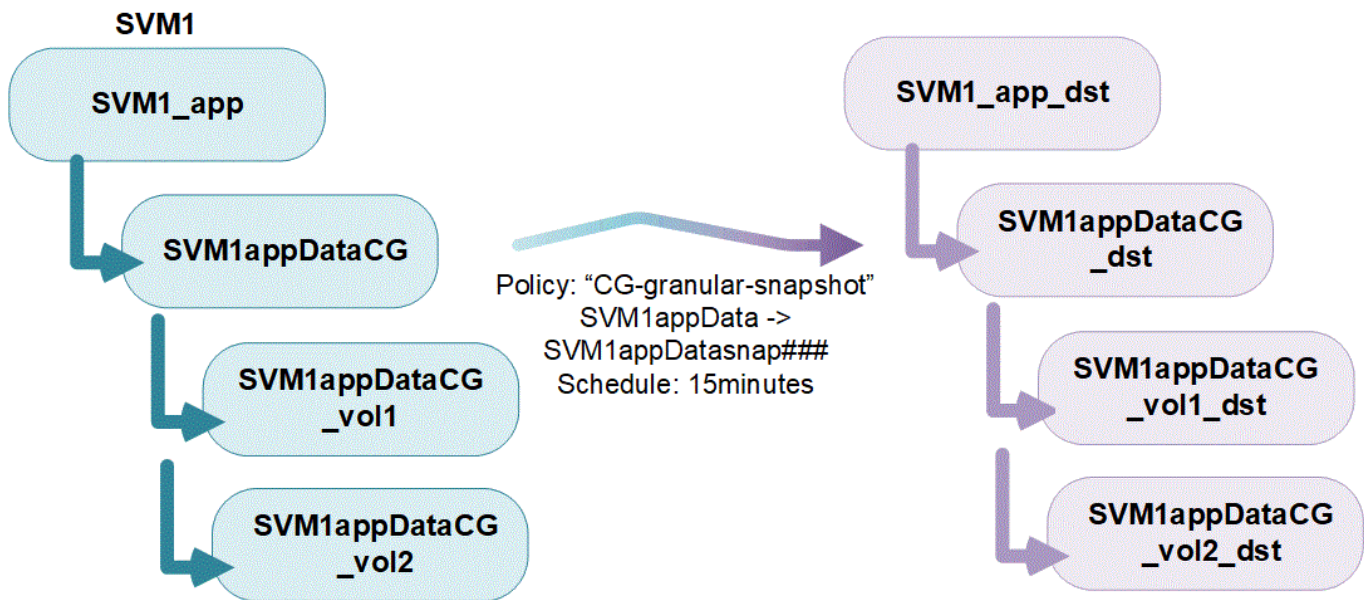
### **Obtenga más información sobre los grupos de consistencia**

Los grupos de consistencia admiten cualquier volumen de FlexVol independientemente del protocolo (NAS, SAN o NVMe) y pueden gestionarse a través de la API REST de ONTAP o en System Manager, en el elemento de menú **almacenamiento > grupos de consistencia**. A partir de ONTAP 9.14.1, los grupos de consistencia se pueden administrar con la CLI de ONTAP.

Los grupos de consistencia pueden existir como entidades individuales (como una colección de volúmenes) o en una relación jerárquica, que consiste en otros grupos de consistencia. Los volúmenes individuales pueden tener su propia política de copias Snapshot granulares de volúmenes. Además, puede haber una política de Snapshot para todo el grupo de consistencia. El grupo de consistencia solo puede tener una relación de

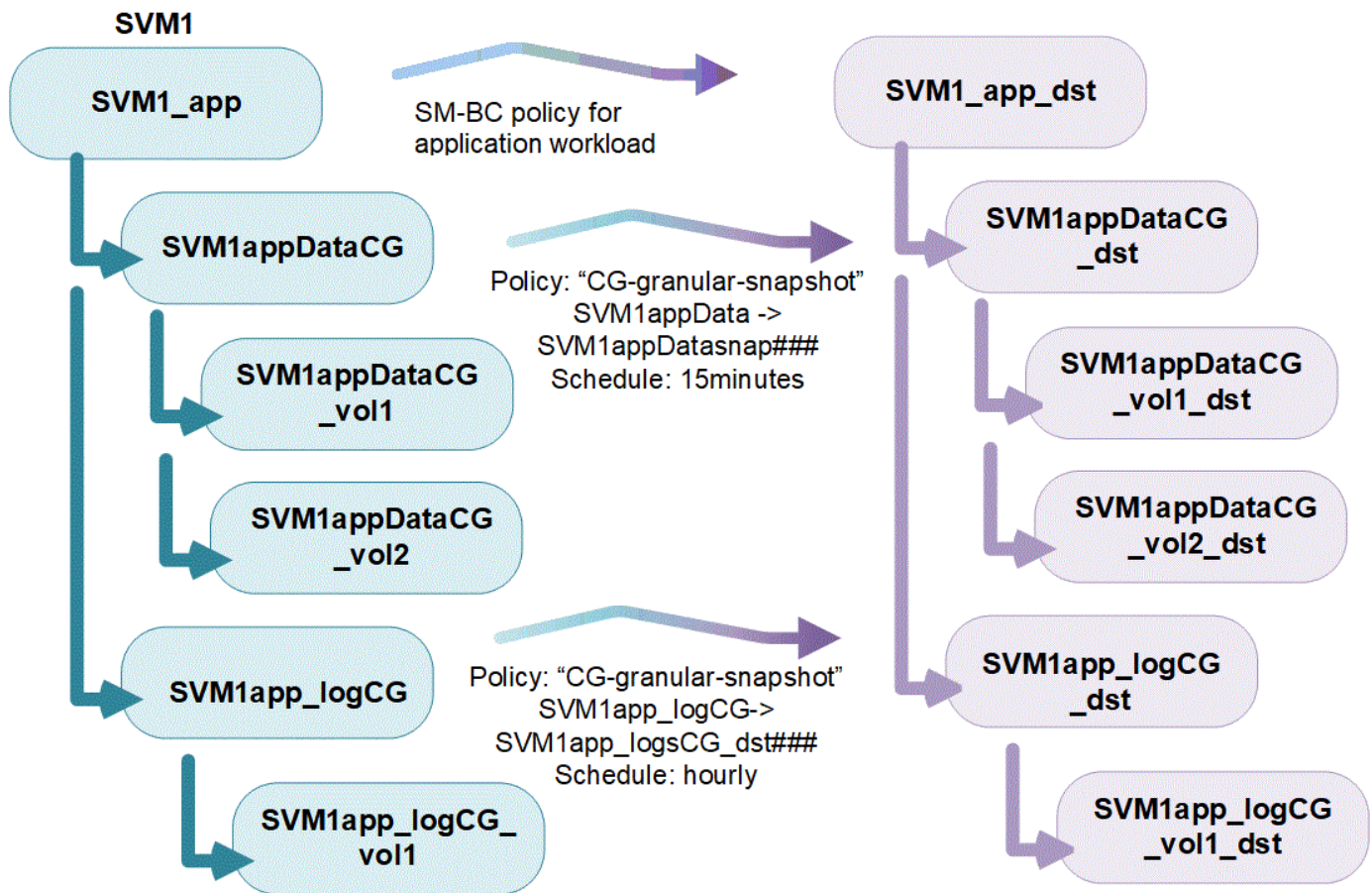
continuidad del negocio de SnapMirror (SM-BC) y una política de SM-BC compartida, que puede utilizarse para recuperar todo el grupo de consistencia.

En el siguiente diagrama se muestra cómo se puede utilizar un grupo de consistencia individual. Los datos de una aplicación alojada en SVM1 abarca dos volúmenes: vol1 y vol2. Una política de Snapshot en el grupo de consistencia captura copias Snapshot de los datos cada 15 minutos.



Las cargas de trabajo de aplicaciones más grandes pueden requerir varios grupos de coherencia. En estas situaciones, puede crear grupos de consistencia jerárquicos, donde un solo grupo de consistencia se convierte en componentes secundarios de un grupo de coherencia primario. El grupo de consistencia primario puede incluir hasta cinco grupos de consistencia secundarios. Al igual que en grupos de consistencia individuales, se puede aplicar una política de protección de SM-BC remota a toda la configuración de los grupos de consistencia (principal y secundario) para recuperar la carga de trabajo de la aplicación.

En el siguiente ejemplo, una aplicación se aloja en SVM1. El administrador ha creado un grupo de consistencia primario, SVM1\_app, que incluye dos grupos de consistencia secundarios: SVM1appDataCG para los datos y SVM1app\_logCG para los registros. Cada grupo de consistencia secundario tiene su propia política de Snapshot. Copias Snapshot de los volúmenes en SVM1appDataCG se toman cada 15 minutos. Copias Snapshot de SVM1app\_logCG se toman cada hora. El grupo de consistencia primario SVM1\_app Tiene una política de SM-BC que replica los datos para garantizar un servicio continuado en caso de desastre.



A partir de ONTAP 9.12.1, admiten los grupos de consistencia [clonado](#) y modificar los miembros de la consistencia por [agregar o quitar volúmenes](#). Tanto en System Manager como en la API DE REST de ONTAP. A partir de ONTAP 9.12.1, la API de REST DE ONTAP también admite:

- Creación de grupos de coherencia con volúmenes NFS o SMB o espacios de nombres NVMe nuevos.
- Añadir volúmenes NFS o SMB o espacios de nombres NVMe nuevos o existentes a grupos de coherencia existentes.

Para obtener más información sobre la API de REST de ONTAP, consulte ["Documentación de referencia de la API DE REST de ONTAP"](#).

## Supervisar grupos de consistencia

A partir de ONTAP 9.13.1, los grupos de consistencia ofrecen supervisión de capacidad y rendimiento en tiempo real e históricos, lo que proporciona información sobre el rendimiento de aplicaciones y grupos de coherencia individuales.

Los datos de supervisión se actualizan cada cinco minutos y se mantienen hasta un año. Puede realizar un seguimiento de las métricas para:

- Rendimiento: IOPS, latencia y rendimiento
- Capacidad: Tamaño, lógico utilizado, disponible

Puede ver los datos de supervisión en la pestaña **Información general** del menú del grupo de consistencia de System Manager o solicitándolos en la API DE REST. A partir de ONTAP 9.14.1, puede ver las métricas del grupo de consistencia con la CLI mediante el `consistency-group metrics show` comando.



En ONTAP 9.13.1, solo puede recuperar métricas históricas mediante la API de REST. A partir de ONTAP 9.14.1, las métricas históricas también están disponibles en System Manager.

## Proteger los grupos de consistencia

Los grupos de consistencia ofrecen protección mediante:

- Políticas de Snapshot
- [Continuidad del negocio de SnapMirror \(SM-BC\)](#)
- [\[mcc\]](#) (A partir de ONTAP 9.11.1)
- [SnapMirror asíncrono](#) (A partir de ONTAP 9.13.1)
- ["Recuperación ante desastres de SVM"](#) (A partir de ONTAP 9.14.1)

La creación de un grupo de consistencia no habilita la protección automáticamente. Las políticas de protección local y remota se pueden establecer al crear o después de crear un grupo de coherencia.

Para configurar la protección en un grupo de consistencia, consulte ["Proteja un grupo de consistencia"](#).

Para poder utilizar la protección remota, debe cumplir los requisitos de [Puestas en marcha de continuidad del negocio con SnapMirror](#).



No se pueden establecer relaciones de SM-BC en volúmenes montados para el acceso NAS.

## Grupos de consistencia en configuraciones de MetroCluster

A partir de ONTAP 9.11.1, puede aprovisionar grupos de consistencia con nuevos volúmenes en un clúster dentro de una configuración de MetroCluster. Estos volúmenes se aprovisionan en agregados reflejados.

Después de que se hayan aprovisionado, puede mover los volúmenes asociados con grupos de coherencia entre los agregados reflejados y no reflejados. Por lo tanto, los volúmenes asociados con grupos de coherencia pueden ubicarse en agregados reflejados, agregados no reflejados o en ambos. Es posible modificar los agregados reflejados que contienen volúmenes asociados con grupos de coherencia para que no se reflejen. De igual manera, se pueden modificar los agregados no reflejados que contienen volúmenes asociados con grupos de coherencia para habilitar el mirroring.

Los volúmenes y las copias Snapshot asociados con grupos de consistencia ubicados en agregados reflejados se replican en el sitio remoto (sitio B). El contenido de los volúmenes del sitio B ofrece una garantía de escritura para el grupo de coherencia, lo que le permite recuperar desde el sitio B en caso de desastre. Puede acceder a copias de Snapshot de los grupos de consistencia mediante un grupo de consistencia con la API de REST y System Manager en los clústeres que ejecutan ONTAP 9.11.1 o una versión posterior. A partir de ONTAP 9.14.1, también puede acceder a las copias Snapshot con la CLI de ONTAP.

Si algunos o todos los volúmenes asociados con un grupo de consistencia se encuentran en agregados no reflejados a los que no se puede acceder actualmente, las operaciones GET o DELETE en el grupo de coherencia se comportan como si los volúmenes locales o los agregados de alojamiento están sin conexión.

## Configuraciones del grupo de consistencia para la replicación

Si el sitio B ejecuta ONTAP 9.10.1 o una versión anterior, solo se replican los volúmenes asociados con los grupos de coherencia ubicados en agregados reflejados al sitio B. Las configuraciones del grupo de consistencia solo se replican en el sitio B, si ambos sitios ejecutan ONTAP 9.11.1 o una versión posterior. Una vez que el sitio B se actualiza a ONTAP 9.11.1, los datos de los grupos de consistencia del sitio A que tienen

todos los volúmenes asociados ubicados en agregados reflejados se replican en el sitio B.



Se recomienda mantener al menos un 20% de espacio libre para agregados reflejados para lograr un rendimiento y una disponibilidad de almacenamiento óptimos. Aunque la recomendación es del 10% para agregados no duplicados, el sistema de archivos puede utilizar el 10% adicional del espacio para absorber cambios incrementales. Los cambios incrementales aumentan el aprovechamiento del espacio para agregados reflejados gracias a la arquitectura basada en Snapshot de copia en escritura de ONTAP. Si no se siguen estas mejores prácticas, puede tener un impacto negativo en el rendimiento.

## Consideraciones de renovación

Los grupos de coherencia creados con SM-BC en ONTAP 9,8 y 9.9.1 se actualizarán automáticamente y se podrán gestionar en **Almacenamiento > Grupos de consistencia** en System Manager o la API REST DE ONTAP cuando se actualice a ONTAP 9.10.1 o una versión posterior. Para obtener más información sobre la actualización desde ONTAP 9,8 o 9,9.1, consulte ["Consideraciones sobre la actualización y reversión de SM-BC"](#).

Las copias de Snapshot de grupo de consistencia creadas en la API de REST pueden gestionarse a través de la interfaz del grupo de consistencia de System Manager y mediante extremos de la API de REST del grupo de consistencia. A partir de ONTAP 9.14.1, las copias Snapshot de grupo de consistencia también se pueden gestionar con la CLI de ONTAP.



Copias Snapshot creadas con los comandos ONTAPI `cg-start` y `cg-commit` Se reconocen como las copias Snapshot de grupo de consistencia y, por lo tanto, no se pueden gestionar a través de la interfaz del grupo de consistencia de System Manager ni los extremos del grupo de consistencia en la API DE REST DE ONTAP. A partir de ONTAP 9.14.1, estas copias Snapshot se pueden reflejar en el volumen de destino si utiliza una política de SnapMirror asíncrono. Para obtener más información, consulte [Configurar la protección asíncrona de SnapMirror](#).

## Funciones compatibles por versión

|                                             | ONTAP<br>9.14.1 | ONTAP<br>9.13.1 | ONTAP<br>9.12.1  | ONTAP<br>9.11.1 | ONTAP<br>9.10.1 |
|---------------------------------------------|-----------------|-----------------|------------------|-----------------|-----------------|
| Grupos de consistencia jerárquicos          | ✓               | ✓               | ✓                | ✓               | ✓               |
| Protección local con copias Snapshot        | ✓               | ✓               | ✓                | ✓               | ✓               |
| Continuidad del negocio de SnapMirror       | ✓               | ✓               | ✓                | ✓               | ✓               |
| Soporte de MetroCluster                     | ✓               | ✓               | ✓                | ✓               |                 |
| Confirmaciones bifásicas (solo API de REST) | ✓               | ✓               | ✓                | ✓               |                 |
| Etiquetas de aplicaciones y componentes     | ✓               | ✓               | ✓                |                 |                 |
| Clonar grupos de consistencia               | ✓               | ✓               | ✓                |                 |                 |
| Añadir y quitar volúmenes                   | ✓               | ✓               | ✓                |                 |                 |
| Cree CG con los nuevos volúmenes NAS        | ✓               | ✓               | Solo API DE REST |                 |                 |



|                                                                               | ONTAP<br>9.14.1 | ONTAP<br>9.13.1 | ONTAP<br>9.12.1  | ONTAP<br>9.11.1 | ONTAP<br>9.10.1 |
|-------------------------------------------------------------------------------|-----------------|-----------------|------------------|-----------------|-----------------|
| Crear CG con nuevos espacios de nombres NVMe                                  | ✓               | ✓               | Solo API DE REST |                 |                 |
| Mueva volúmenes entre grupos de coherencia secundarios                        | ✓               | ✓               |                  |                 |                 |
| Modificar la geometría del grupo de consistencia                              | ✓               | ✓               |                  |                 |                 |
| Supervisión                                                                   | ✓               | ✓               |                  |                 |                 |
| SnapMirror asíncrono (solo grupos de consistencia individuales)               | ✓               | ✓               |                  |                 |                 |
| Recuperación ante desastres de SVM (solo grupos de consistencia individuales) | ✓               |                 |                  |                 |                 |
| Compatibilidad con CLI                                                        | ✓               |                 |                  |                 |                 |

## Más información sobre los grupos de consistencia

### Consistency Groups for Application Management & Protection

With NetApp ONTAP 9.10.1 + System Manager

© 2022 NetApp, Inc. All rights reserved.





## Más información

- ["Documentación de automatización de ONTAP"](#)
- [Continuidad del negocio de SnapMirror](#)
- [Conceptos básicos de la recuperación ante desastres de SnapMirror asíncrono](#)
- ["Documentación de MetroCluster"](#)

## Límites del grupo de consistencia

Al planificar y administrar los grupos de consistencia, tenga en cuenta los límites de objetos en el ámbito del clúster y del grupo de consistencia primario o secundario.

### Límites impuestos

La siguiente tabla captura los límites de los grupos de coherencia. Se aplican límites separados para los grupos de coherencia que utilizan SnapMirror Business Continuity (SM-BC). Para obtener más información, consulte ["Restricciones y limitaciones de SM-BC"](#).

| Límite                                                                                                                                  | Ámbito                           | Mínimo                  | Máximo                                                |
|-----------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|-------------------------|-------------------------------------------------------|
| Número de grupos de consistencia                                                                                                        | Clúster                          | 0                       | Igual que el número máximo de volúmenes en el clúster |
| Número de grupos de consistencia primarios                                                                                              | Clúster                          | 0                       | Igual que el número máximo de volúmenes en el clúster |
| Número de grupos de consistencia individuales y primarios                                                                               | Clúster                          | 0                       | Igual que el número máximo de volúmenes en el clúster |
| Número de volúmenes en un grupo de consistencia                                                                                         | Grupo de consistencia único      | 1 tb de volumen         | 80 volúmenes                                          |
| El número de volúmenes en el secundario de un grupo de consistencia primario                                                            | Grupo de consistencia primario   | 1 tb de volumen         | 80 volúmenes                                          |
| El número de volúmenes en un grupo de coherencia secundario                                                                             | Grupo de consistencia secundario | 1 tb de volumen         | 80 volúmenes                                          |
| Número de grupos de consistencia secundarios de un grupo de consistencia primario                                                       | Grupo de consistencia primario   | 1 grupo de consistencia | 5 grupos de consistencia                              |
| Número de relaciones de recuperación ante desastres de SVM donde existe un grupo de consistencia (disponible a partir de ONTAP 9.14.1). | Clúster                          | 0                       | 32                                                    |

### Límites no aplicados

La programación mínima de copias Snapshot admitida para grupos de consistencia es de 30 minutos. Esta opción está basada en ["Prueba para FlexGroups"](#), Que comparten la misma infraestructura Snapshot que los grupos de consistencia.



## Configure un único grupo de consistencia

Los grupos de consistencia se pueden crear con volúmenes existentes o con LUN o volúmenes nuevos (según la versión de ONTAP). Un volumen o LUN solo pueden asociarse a un grupo de coherencia a la vez.

### Acerca de esta tarea

- No se admite la modificación de los volúmenes miembro de un grupo de coherencia después de su creación en ONTAP 9.10.1 a 9.11.1.

A partir de ONTAP 9.12.1, es posible modificar los volúmenes miembro de un grupo de coherencia. Para obtener más información sobre este proceso, consulte [Modificar un grupo de consistencia](#).

### Cree un grupo de consistencia con nuevas LUN o volúmenes

En ONTAP 9.10.1 a 9.12.1, puede crear un grupo de consistencia utilizando nuevas LUN. A partir de ONTAP 9.13.1, System Manager también admite la creación de un grupo de consistencia con espacios de nombres NVMe nuevos o volúmenes NAS nuevos. (También es compatible con la API REST DE ONTAP a partir de ONTAP 9.12.1).

## System Manager

### Pasos

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione **+Agregar** y, a continuación, seleccione el protocolo para el objeto de almacenamiento.

En ONTAP 9.10.1 a 9.12.1, la única opción para un nuevo objeto de almacenamiento es **utilizando nuevas LUN**. A partir de ONTAP 9.13.1, System Manager admite la creación de grupos de consistencia con espacios de nombres NVMe nuevos y volúmenes NAS nuevos.

3. Asigne un nombre al grupo de consistencia. Designe el número de volúmenes o LUN y la capacidad por volumen o LUN.
  - a. **Tipo de aplicación:** Si está utilizando ONTAP 9.12.1 o posterior, seleccione un tipo de aplicación. Si no se selecciona ningún valor, se asignará al grupo de consistencia el tipo de **Other** de forma predeterminada. Obtenga más información sobre la coherencia de etiquetado en [Etiquetas de aplicaciones y componentes](#). Si planea crear un grupo de consistencia con una política de protección remota, debe usar **Other**.
  - b. Para **Nuevas LUN**: Seleccione el sistema operativo del host y el formato de LUN. Introduzca la información del iniciador del host.
  - c. Para **Nuevos volúmenes NAS**: Elija la opción de exportación apropiada (NFS o SMB/CIFS) según la configuración NAS de su SVM.
  - d. Para **Nuevos espacios de nombres NVMe**: Seleccione el sistema operativo del host y el subsistema NVMe.
4. Para configurar políticas de protección, agregar un grupo de consistencia secundario o permisos de acceso, seleccione **Más opciones**.
5. Seleccione **Guardar**.
6. Para confirmar que se ha creado el grupo de consistencia, vuelva al menú del grupo de consistencia principal, donde aparecerá una vez que se complete el trabajo. Si establece una política de protección, sabrá que se ha aplicado cuando ve un escudo verde bajo la directiva apropiada, remoto o local.

### CLI

A partir de ONTAP 9.14.1, puede crear un grupo de consistencia nuevo con volúmenes nuevos mediante la CLI de ONTAP. Los parámetros específicos dependen de si los volúmenes son SAN, NVMe o NFS.

#### Crear un grupo de consistencia con volúmenes de NFS

1. Cree el grupo de consistencia:

```
consistency-group create -vserver SVM_name -consistency-group consistency-group-name -volume volume-prefix -volume-count number -size size -export-policy policy_name
```

#### Crear un grupo de consistencia con volúmenes SAN

1. Cree el grupo de consistencia:

```
consistency-group create -vserver SVM_name -consistency-group consistency-group-name -lun lun_name -size size -lun-count number -igroup igroup_name
```

#### Cree un grupo de consistencia con espacios de nombres NVMe

1. Cree el grupo de consistencia:

```
consistency-group create -vserver SVM_name -consistency-group
consistency_group_name -namespace namespace_name -volume-count number
-namespace-count number -size size -subsystem subsystem_name
```

**Después de terminar**

1. Confirme que el grupo de consistencia se ha creado mediante el `consistency-group show` comando.

**Cree un grupo de coherencia con volúmenes existentes**

Es posible utilizar volúmenes existentes para crear un grupo de coherencia.

## System Manager

### Pasos

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione **+Agregar y utilizando volúmenes existentes**.
3. Asigne un nombre al grupo de consistencia y seleccione la máquina virtual de almacenamiento.
  - a. **Tipo de aplicación:** Si está utilizando ONTAP 9.12.1 o posterior, seleccione un tipo de aplicación. Si no se selecciona ningún valor, se asignará al grupo de consistencia el tipo de **Other** de forma predeterminada. Obtenga más información sobre la coherencia de etiquetado en [Etiquetas de aplicaciones y componentes](#). Si el grupo de consistencia tiene una relación SM-BC, debe utilizar **otros**.
4. Seleccione los volúmenes existentes que desea incluir. Solo se podrá seleccionar los volúmenes que todavía no sean parte de un grupo de coherencia.



Si crea un grupo de coherencia con volúmenes existentes, el grupo de coherencia es compatible con volúmenes FlexVol. Los volúmenes con relaciones de SnapMirror asíncrono o síncrono se pueden añadir a grupos de coherencia, pero no tienen en cuenta los grupos de consistencia. Los grupos de consistencia no admiten bloques S3 ni máquinas virtuales de almacenamiento con relaciones de SVMDR.

5. Seleccione **Guardar**.
6. Para confirmar que se ha creado el grupo de coherencia, vuelva al menú del grupo de consistencia principal, donde aparecerá una vez que se complete el trabajo de ONTAP. Si ha elegido una política de protección, confirme que se configuró correctamente al seleccionar un grupo de coherencia en el menú. Si establece una política de protección, sabrá que se ha aplicado cuando ve un escudo verde bajo la directiva apropiada, remoto o local.

### CLI

A partir de ONTAP 9.14.1, puede crear un grupo de consistencia con volúmenes existentes mediante la CLI de ONTAP.

### Pasos

1. Emita el `consistency-group create` comando. La `-volumes` parameter acepta una lista de nombres de volúmenes separados por comas.

```
consistency-group create -vserver SVM_name -consistency-group consistency-group-name -volume volumes
```

2. Vea el grupo de consistencia mediante la `consistency-group show` comando.

### Siguientes pasos

- [Proteja un grupo de consistencia](#)
- [Modificar un grupo de consistencia](#)
- [Clonar un grupo de consistencia](#)

## Configurar un grupo de consistencia jerárquico

Los grupos de coherencia jerárquicos permiten gestionar cargas de trabajo grandes que

abarcan varios volúmenes, creando un grupo de coherencia primario que funciona como un paraguas para los grupos de coherencia secundarios.

Los grupos de consistencia jerárquicos tienen un primario que puede incluir hasta cinco grupos de consistencia individuales. Los grupos de coherencia jerárquicos pueden admitir diferentes políticas Snapshot locales en grupos de coherencia o volúmenes individuales. Si utiliza una política de protección remota, que se aplicará a todo el grupo de consistencia jerárquico (primario y secundario).

A partir de ONTAP 9.13.1, puede hacerlo [modifique la geometría de sus grupos de consistencia](#) y.. [mueva volúmenes entre grupos de coherencia secundarios](#).

Para obtener información sobre los límites de objetos en los grupos de consistencia, consulte [Límites de objetos para los grupos de consistencia](#).

### **Cree un grupo de consistencia jerárquico con nuevas LUN o volúmenes**

Al crear un grupo de consistencia jerárquico, puede rellenarlo con nuevas LUN. A partir de ONTAP 9.13.1, también se pueden usar nuevos espacios de nombres NVMe y volúmenes NAS.

## System Manager

### Pasos

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione **+Agregar** y, a continuación, seleccione el protocolo para el objeto de almacenamiento.

En ONTAP 9.10.1 a 9.12.1, la única opción para un nuevo objeto de almacenamiento es **utilizando nuevas LUN**. A partir de ONTAP 9.13.1, System Manager admite la creación de grupos de consistencia con espacios de nombres NVMe nuevos y volúmenes NAS nuevos.

3. Asigne un nombre al grupo de consistencia. Designe el número de volúmenes o LUN y la capacidad por volumen o LUN.
  - a. **Tipo de aplicación:** Si está utilizando ONTAP 9.12.1 o posterior, seleccione un tipo de aplicación. Si no se selecciona ningún valor, se asignará al grupo de consistencia el tipo de **Other** de forma predeterminada. Obtenga más información sobre la coherencia de etiquetado en [Etiquetas de aplicaciones y componentes](#). Si planea usar una política de protección remota, debe elegir **Otro**.
4. Seleccione el sistema operativo del host y el formato de LUN. Introduzca la información del iniciador del host.
  - a. Para **Nuevas LUN**: Seleccione el sistema operativo del host y el formato de LUN. Introduzca la información del iniciador del host.
  - b. Para **Nuevos volúmenes NAS**: Elija la opción de exportación apropiada (NFS o SMB/CIFS) según la configuración NAS de su SVM.
  - c. Para **Nuevos espacios de nombres NVMe**: Seleccione el sistema operativo del host y el subsistema NVMe.
5. Para agregar un grupo de consistencia hijo, seleccione **Más opciones** y luego **+Agregar grupo de consistencia hijo**.
6. Seleccione el nivel de rendimiento, el número de LUN o volúmenes y la capacidad por LUN o volumen. Designe las configuraciones de exportación adecuadas o la información del sistema operativo en función del protocolo que esté utilizando.
7. Opcionalmente, seleccione una política de Snapshot local y establezca los permisos de acceso.
8. Repita desde un máximo de cinco grupos de consistencia secundarios.
9. Seleccione **Guardar**.
10. Para confirmar que se ha creado el grupo de coherencia, vuelva al menú del grupo de consistencia principal, donde aparecerá una vez que se complete el trabajo de ONTAP. Si establece una directiva de protección, mire bajo la directiva apropiada, remota o local, que debe mostrar un escudo verde con una Marca de verificación en ella.

### CLI

A partir de ONTAP 9.14.1, puede crear un nuevo grupo de consistencia jerárquico mediante la CLI.

### Paso

1. Cree el nuevo grupo de consistencia mediante el `consistency-group create` comando.

La `volume-count` parameter configura la cantidad de volúmenes en cada grupo de coherencia secundario. Se puede crear un grupo de coherencia primario con un máximo de cinco grupos de consistencia secundarios.

```
consistency-group create -vserver SVM_name -consistency-group
consistency_group_name -parent-consistency-group
parent_consistency_group_name -cg-count number_of_child_consistency_groups
-volume volume_prefix -volume-count number -size size -export-policy
policy_name -storage-service extreme
```

### **Cree un grupo de coherencia jerárquico con volúmenes existentes**

Se pueden organizar los volúmenes existentes en un grupo de coherencia jerárquico.

## System Manager

### Pasos

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione **+Agregar y utilizando volúmenes existentes**.
3. Seleccione la máquina virtual de almacenamiento.
4. Seleccione los volúmenes existentes que desea incluir. Solo se podrá seleccionar los volúmenes que todavía no sean parte de un grupo de coherencia.
5. Para agregar un grupo de consistencia hijo, seleccione **+Agregar grupo de consistencia hijo**. Cree los grupos de consistencia necesarios, que se nombrarán automáticamente.
  - a. **Tipo de componente:** Si está utilizando ONTAP 9.12.1 o posterior, seleccione un tipo de componente de "datos", "registros" u "otro". Si no se selecciona ningún valor, se asignará al grupo de consistencia el tipo de **Other** de forma predeterminada. Obtenga más información sobre la coherencia de etiquetado en [Etiquetas de aplicaciones y componentes](#). Si planea usar una política de protección remota, debe usar **Otro**.
6. Asigne volúmenes existentes a cada grupo de coherencia.
7. Opcionalmente, seleccione una política de Snapshot local.
8. Repita desde un máximo de cinco grupos de consistencia secundarios.
9. Seleccione **Guardar**.
10. Para confirmar que se ha creado el grupo de coherencia, vuelva al menú del grupo de consistencia principal, donde aparecerá una vez que se complete el trabajo de ONTAP. Si ha elegido una política de protección, confirme que se ha configurado correctamente seleccionando su grupo de consistencia en el menú; en el tipo de política correspondiente, verá un escudo verde con una Marca de verificación en el interior de la misma.

### CLI

A partir de ONTAP 9.14.1, puede crear un grupo de consistencia jerárquico mediante la CLI.

### Pasos

1. Aprovechone un nuevo grupo de coherencia primario y asigne volúmenes a un nuevo grupo de consistencia secundario:

```
consistency-group create -vserver svm_name -consistency-group
child_consistency_group_name -parent-consistency-group
parent_consistency_group_name -volumes volume_names
```

2. Introduzca **y** para confirmar que desea crear un nuevo grupo de consistencia primario y secundario.

### Siguientes pasos

- [Modificar la geometría de un grupo de consistencia](#)
- [Modificar un grupo de consistencia](#)
- [Proteja un grupo de consistencia](#)

## Proteger los grupos de consistencia

Los grupos de coherencia ofrecen una protección local y remota de fácil gestión para



aplicaciones SAN, NAS y NVMe que abarcan varios volúmenes.

La creación de un grupo de consistencia no habilita la protección automáticamente. Las políticas de protección se pueden establecer en el momento de la creación o después de crear el grupo de consistencia. Puede proteger grupos de consistencia mediante:

- Copias Snapshot locales
- Continuidad del negocio de SnapMirror (SM-BC)
- [MetroCluster \(principios de 9.11.1\)](#)
- SnapMirror asíncrono (inicio de 9.13.1)
- Recuperación ante desastres asíncrona de SVM (comenzando 9.14.1)

Si utiliza grupos de consistencia anidados, puede establecer políticas de protección distintas para los grupos de coherencia primario y secundario.

A partir de ONTAP 9.11.1, se ofrecen los grupos de consistencia [Creación de copias Snapshot de grupo de consistencia en dos fases](#). La operación Snapshot de dos fases ejecuta una comprobación previa para garantizar que la copia Snapshot se capture correctamente.

Se puede producir la recuperación de un grupo de consistencia completo, de un solo grupo de consistencia en una configuración jerárquica o de volúmenes individuales en el grupo de consistencia. Para lograr la recuperación, seleccione el grupo de consistencia del que desea recuperar, seleccione el tipo de copia Snapshot y, a continuación, identifique la copia Snapshot en la que se basa la restauración. Para obtener más información acerca de este proceso, consulte ["Restaurar un volumen de una copia de Snapshot anterior"](#).

### **Configurar una política de Snapshot local**


Configurar una política de protección Snapshot local permite crear una política que abarque todos los volúmenes en un grupo de coherencia.

#### **Acerca de esta tarea**

La programación mínima de copias Snapshot admitida para grupos de consistencia es de 30 minutos. Esta opción está basada en ["Prueba para FlexGroups"](#), Que comparten la misma infraestructura Snapshot que los grupos de consistencia.

## System Manager

### Pasos

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione el grupo de consistencia que ha creado en el menú del grupo de consistencia.
3. En la parte superior derecha de la página de descripción general del grupo de consistencia, seleccione **Editar**.
4. Marque la casilla junto a **programar copias Snapshot (local)**.
5. Seleccione una política de Snapshot. Para configurar una directiva nueva y personalizada, consulte ["Cree una política de protección de datos personalizada"](#).
6. Seleccione **Guardar**.
7. Volver al menú de descripción general del grupo de consistencia. En la columna izquierda bajo **copias Snapshot (local)**, el estado dirá protegido al lado .

### CLI

A partir de ONTAP 9.14.1, puede modificar la política de protección de un grupo de consistencia con la CLI.

### Paso

1. Ejecute el siguiente comando para establecer o modificar la política de protección:

Si modifica la política de protección de una consistencia secundaria, debe identificar el grupo de consistencia primario mediante el `-parent-consistency-group` *parent\_consistency\_group\_name* parámetro.

```
consistency-group modify -vserver svm_name -consistency-group
consistency_group_name -snapshot-policy policy_name
```

## Cree una copia Snapshot bajo demanda

Si necesita crear una copia Snapshot del grupo de consistencia fuera de una política normalmente programada, puede crear una bajo demanda.

## System Manager

### Pasos

1. Vaya a **Almacenamiento > Grupos de consistencia**.
2. Seleccione el grupo de coherencia para el que desea crear una copia Snapshot bajo demanda.
3. Cambie a la pestaña **Copias de instantánea** y seleccione **+Agregar**.
4. Proporcione un **Nombre** y una **Etiqueta de SnapMirror**. En el menú desplegable de **Consistencia**, seleccione **Consistente a la aplicación** o **Consistente a la caída**.
5. Seleccione **Guardar**.

### CLI

A partir de ONTAP 9.14.1, puede crear una copia Snapshot bajo demanda de un grupo de consistencia utilizando la CLI.

### Paso

1. Cree la copia Snapshot:

De forma predeterminada, el tipo de Snapshot es coherente con los fallos. Puede modificar el tipo de instantánea con el opcional `-type` parámetro.

```
consistency-group snapshot create -vserver svm_name -consistency-group
consistency_group_name -snapshot snapshot_name
```

## Cree Snapshots de grupo de consistencia de dos fases

A partir de ONTAP 9.11.1, los grupos de consistencia admiten confirmaciones de dos fases para la creación de Snapshot de grupos de consistencia (CG), que ejecutan una comprobación previa antes de confirmar la copia Snapshot. Esta función solo está disponible con la API de REST de ONTAP.

La creación de snapshots de dos fases de CG solo está disponible para la creación de snapshots, no para el aprovisionamiento de grupos de consistencia ni para la restauración de grupos de consistencia.

Una Snapshot CG de dos fases divide el proceso de creación de Snapshot en dos fases:

1. En la primera fase, la API ejecuta comprobaciones previas y activa la creación de copias Snapshot. La primera fase incluye un parámetro de tiempo de espera, lo que designa la cantidad de tiempo que tarda la copia Snapshot en realizarse correctamente.
2. Si la solicitud en la primera fase se completa correctamente, puede invocar la segunda fase dentro del intervalo designado desde la primera fase, confirmando la copia Snapshot en el punto final correspondiente.

### Antes de empezar

- Para utilizar la creación Snapshot de CG de dos fases, todos los nodos del clúster deben ejecutar ONTAP 9.11.1 o una versión posterior.
- Solo se admite una llamada activa de una operación Snapshot de grupo de consistencia en una instancia de grupo de consistencia a la vez, ya sea una fase o dos fases. Al intentar invocar una operación de Snapshot mientras otra está en curso, se produce un error.
- Cuando invoca la creación de Snapshot, puede configurar un valor de tiempo de espera opcional de entre 5 y 120 segundos. Si no se proporciona ningún valor de tiempo de espera, se agota el tiempo de espera

de la operación en el valor predeterminado de 7 segundos. En la API, configure el valor de tiempo de espera en `action_timeout` parámetro. En la CLI, utilice `-timeout` bandera.

### Pasos

Es posible completar una Snapshot en dos fases con la API de REST o, a partir de ONTAP 9.14.1, la CLI de ONTAP. Esta operación no es compatible con System Manager.



Si invoca la creación de Snapshot con la API, debe confirmar la copia Snapshot con la API. Si invoca la creación de Snapshot con la CLI, debe confirmar la copia Snapshot con la CLI. No se admiten métodos de mezcla.

## CLI

A partir de ONTAP 9.14.1, puede crear una copia Snapshot de dos fases con la CLI.

### Pasos

1. Inicie la instantánea:

```
consistency-group snapshot start -vserver svm_name -consistency-group
consistency_group_name -snapshot snapshot_name [-timeout time_in_seconds
-write-fence {true|false}]
```

2. Compruebe que la instantánea se ha realizado:

```
consistency-group snapshot show
```

3. Confirme la instantánea:

```
consistency-group snapshot commit svm_name -consistency-group
consistency_group_name -snapshot snapshot_name
```

## API

1. Invoque la creación de la instantánea. Envíe una solicitud POST al extremo del grupo de consistencia mediante el `action=start` parámetro.

```
curl -k -X POST 'https://<IP_address>/application/consistency-
groups/<cg-uuid>/snapshots?action=start&action_timeout=7' -H
"accept: application/hal+json" -H "content-type: application/json"
-d '
{
 "name": "<snapshot_name>",
 "consistency_type": "crash",
 "comment": "<comment>",
 "snapmirror_label": "<SnapMirror_label>"
}'
```

2. Si la solicitud POST se realiza correctamente, el resultado incluye un uuid de Snapshot. Con ese uuid, envíe una solicitud de REVISIÓN para confirmar la copia Snapshot.

```
curl -k -X PATCH 'https://<IP_address>/application/consistency-groups/<cg_uuid>/snapshots/<snapshot_id>?action=commit' -H "accept: application/hal+json" -H "content-type: application/json"
```

For more information about the ONTAP REST API, see [link:https://docs.netapp.com/us-en/ontap-automation/reference/api\\_reference.html](https://docs.netapp.com/us-en/ontap-automation/reference/api_reference.html) [API reference^] or the [link:https://devnet.netapp.com/restapi.php](https://devnet.netapp.com/restapi.php) [ONTAP REST API page^] at the NetApp Developer Network for a complete list of API endpoints.

## Configurar la protección remota para un grupo de coherencia

Los grupos de coherencia ofrecen protección remota mediante SM-BC y, a partir de ONTAP 9.13.1, SnapMirror asíncrono.

### Configurar la protección con SM-BC

Puede utilizar SM-BC para garantizar que las copias Snapshot de los grupos de consistencia creados en el grupo de consistencia se copien el destino. Para obtener más información sobre SM-BC o sobre cómo configurar SM-BC mediante la CLI, consulte [Configure la protección para la continuidad del negocio](#).

#### Antes de empezar

- No se pueden establecer relaciones de SM-BC en volúmenes montados para el acceso NAS.
- Las etiquetas de políticas del clúster de origen y destino deben coincidir.
- SM-BC no replicará las copias Snapshot de forma predeterminada a menos que se añada una regla con una etiqueta de SnapMirror al valor predefinido `AutomatedFailOver`. La política y las copias de Snapshot se crean con esa etiqueta.

Para obtener más información sobre este proceso, consulte ["Proteja con SM-BC"](#).

- [Implementaciones en cascada](#) No son compatibles con SM-BC.
- A partir de ONTAP 9.13.1, se puede sin interrupciones [añada volúmenes a un grupo de coherencia](#) Con una relación SM-BC activa. Cualquier otro cambio en un grupo de consistencia requiere que rompa la relación de SM-BC, que modifique el grupo de consistencia y, a continuación, vuelva a establecer y resincronizar la relación.



Para configurar SM-BC con la CLI, consulte [Proteja con SM-BC](#).

### Pasos para System Manager

1. Asegúrese de haber cumplido con el ["Requisitos previos para usar SM-BC"](#).
2. Seleccione **almacenamiento > grupos de consistencia**.
3. Seleccione el grupo de consistencia que ha creado en el menú del grupo de consistencia.
4. En la parte superior derecha de la página de descripción general, seleccione **más** y, a continuación, **proteger**.
5. System Manager rellena automáticamente la información del origen. Seleccione la máquina virtual de almacenamiento y clúster apropiado para el destino. Seleccione una política de protección. Asegúrese de

que **Initialize Relationship** está activada.

6. Seleccione **Guardar**.

7. El grupo de consistencia debe inicializar y sincronizar. Confirme que la sincronización se ha completado correctamente volviendo al menú **Grupo de consistencia**. Se muestra el estado **SnapMirror (Remote)**

Protected junto a. .

### Configurar la protección asíncrona de SnapMirror

A partir de ONTAP 9.13.1, puede configurar la protección SnapMirror asíncrona para un único grupo de consistencia. A partir de ONTAP 9.14.1, se puede usar SnapMirror asíncrono para replicar copias Snapshot granulares de volúmenes en el clúster de destino mediante la relación del grupo de coherencia.

#### Acerca de esta tarea

Para replicar copias Snapshot granulares del volumen, debe ejecutar ONTAP 9.14.1 o una versión posterior. Para las políticas de MirrorAndVault y Vault, la etiqueta de SnapMirror de la política de Snapshot granular de volumen debe coincidir con la regla de política de SnapMirror del grupo de coherencia. Las snapshots granulares del volumen rigen el valor conservar de la política de SnapMirror del grupo de consistencia, que se calcula independientemente de las snapshots del grupo de consistencia. Por ejemplo, si tiene una política para conservar dos copias Snapshot en el destino, puede tener dos copias Snapshot granulares de volumen y dos copias Snapshot de grupo de consistencia.

Al volver a sincronizar la relación de SnapMirror con copias Snapshot granulares de volúmenes, se pueden conservar copias de Snapshot granulares de volúmenes con el `-preserve` bandera. Se conservan las copias Snapshot granulares de volúmenes más recientes que las copias Snapshot de grupo de consistencia. Si no existe una copia de Snapshot de grupo de consistencia, no se pueden transferir copias de Snapshot granulares de volumen en la operación de resincronización.

#### Antes de empezar

- La protección asíncrona SnapMirror solo está disponible para grupos de consistencia individuales. No se admite para grupos de coherencia jerárquicos. Para convertir un grupo de consistencia jerárquico en un grupo de consistencia único, consulte [modificar la arquitectura del grupo de consistencia](#).
- Las etiquetas de políticas del clúster de origen y destino deben coincidir.
- Puede sin interrupciones [añada volúmenes a un grupo de coherencia](#) Con una relación de SnapMirror asíncrona activa. Cualquier otro cambio en un grupo de consistencia requiere que rompa la relación de SnapMirror, modifique el grupo de consistencia y, a continuación, vuelva a establecer y vuelva a sincronizar la relación.
- Si se configuró una relación de protección de SnapMirror asíncrono para varios volúmenes individuales, puede convertir dichos volúmenes en un grupo de coherencia y mantener las copias de Snapshot existentes. Para convertir volúmenes correctamente:
  - Debe haber una copia de Snapshot común de los volúmenes.
  - Debe interrumpir la relación de SnapMirror existente. [añada los volúmenes a un único grupo de consistencia](#), a continuación, vuelva a sincronizar la relación mediante el siguiente flujo de trabajo.

#### Pasos

1. En el clúster de destino, seleccione **Almacenamiento > Grupos de consistencia**.
2. Seleccione el grupo de consistencia que ha creado en el menú del grupo de consistencia.
3. En la parte superior derecha de la página de descripción general, seleccione **más** y, a continuación, **proteger**.
4. System Manager rellena automáticamente la información del origen. Seleccione la máquina virtual de

almacenamiento y clúster apropiado para el destino. Seleccione una política de protección. Asegúrese de que **Initialize Relationship** está activada.

Al seleccionar una política asíncrona, tiene la opción de **Anular horario de transferencia**.



La programación mínima admitida (objetivo de punto de recuperación o objetivo de punto de recuperación) para los grupos de consistencia con SnapMirror asíncrono es de 30 minutos.

5. Seleccione **Guardar**.

6. El grupo de consistencia debe inicializar y sincronizar. Confirme que la sincronización se ha completado correctamente volviendo al menú **Grupo de consistencia**. Se muestra el estado **SnapMirror (Remote)**

Protected junto a .

### Configurar la recuperación ante desastres de la SVM

A partir de ONTAP 9.14.1, [Recuperación ante desastres de SVM](#) admite grupos de coherencia, lo que permite reflejar información del grupo de coherencia del origen al clúster de destino.

Si va a habilitar la recuperación ante desastres de SVM en una SVM que ya contiene un grupo de consistencia, a continuación los flujos de trabajo de configuración de la SVM para [System Manager](#) o la [CLI de ONTAP](#).

Si va a añadir un grupo de coherencia a una SVM que esté en una relación de recuperación ante desastres de SVM activa y en buen estado, debe actualizar la relación de recuperación ante desastres de SVM desde el clúster de destino. Para obtener más información, consulte [Actualice manualmente una relación de replicación](#). Debe actualizar la relación cada vez que expanda el grupo de consistencia.

### Limitaciones

- La recuperación ante desastres de SVM no admite grupos de consistencia jerárquicos.
- La recuperación ante desastres de SVM no admite grupos de consistencia protegidos con SnapMirror asíncrono. Debe interrumpir la relación de SnapMirror antes de configurar la recuperación ante desastres de SVM.
- Ambos clústeres deben ejecutar ONTAP 9.14.1 o una versión posterior.
- Las relaciones de dispersión no se admiten para las configuraciones de recuperación ante desastres de SVM que contienen grupos de coherencia.
- Para ver otros límites, consulte [límites del grupo de consistencia](#).

### Visualizar relaciones

System Manager visualiza los mapas de LUN en el menú **Protección > Relaciones**. Cuando selecciona una relación de origen, System Manager muestra una visualización de las relaciones de origen. Al seleccionar un volumen, puede profundizar en estas relaciones para ver una lista de las LUN contenidas y las relaciones con el iGroup. Esta información se puede descargar como un libro de Excel desde la vista de volumen individual; la operación de descarga se ejecuta en segundo plano.

### Información relacionada

- ["Clonar un grupo de consistencia"](#)
- ["Configure las copias Snapshot"](#)
- ["Cree políticas de protección de datos personalizadas"](#)



- ["Recuperar desde copias Snapshot"](#)
- ["Restaurar un volumen de una copia de Snapshot anterior"](#)
- ["Información general sobre SM-BC"](#)
- ["Documentación de automatización de ONTAP"](#)
- [Conceptos básicos de la recuperación ante desastres de SnapMirror asíncrono](#)

## Modificar los volúmenes miembro en un grupo de coherencia

A partir de ONTAP 9.12.1, puede modificar un grupo de coherencia quitando volúmenes o añadiendo volúmenes (expandiendo el grupo de coherencia). A partir de ONTAP 9.13.1, se pueden mover volúmenes entre grupos de coherencia secundarios si comparten un volumen primario común.

### Añadir volúmenes a un grupo de coherencia

A partir de ONTAP 9.12.1, es posible añadir volúmenes a un grupo de coherencia sin interrupciones.

#### Acerca de esta tarea

- No es posible añadir volúmenes asociados con otro grupo de coherencia.
- Los grupos de consistencia admiten los protocolos NAS, SAN y NVMe.
- Puede añadir hasta 16 volúmenes a la vez a un grupo de coherencia si los ajustes se encuentran dentro de la configuración general [límites del grupo de consistencia](#).
- A partir de ONTAP 9.13.1, se pueden añadir volúmenes sin interrupciones a un grupo de coherencia con una política de continuidad del negocio con SnapMirror (SM-BC) activa o una política de protección SnapMirror asíncrona.
- Cuando se añaden volúmenes a un grupo de coherencia protegido por SM-BC, el estado de la relación de SM-BC cambiará a «Expansión» hasta que el mirroring y la protección se configuren para el volumen nuevo. Si se produce un desastre en el clúster primario antes de que se complete este proceso, el grupo de consistencia revierte a su composición original como parte de la operación de conmutación al nodo de respaldo.
- En ONTAP 9.12.1 y versiones anteriores, *no puede* añadir volúmenes a un grupo de coherencia de una relación SM-BC. Primero, debe interrumpir la relación de SM-BC, modificar el grupo de consistencia y, a continuación, restaurar la protección con SM-BC.
- A partir de ONTAP 9.12.1, la API DE REST DE ONTAP admite la adición *new* o volúmenes existentes a un grupo de coherencia. Para obtener más información sobre la API de REST de ONTAP, consulte ["Documentación de referencia de la API DE REST de ONTAP"](#).

A partir de ONTAP 9.13.1, esta funcionalidad es compatible con System Manager.

- Al expandir un grupo de consistencia, las copias Snapshot del grupo de consistencia capturado antes de la modificación se considerarán parciales. Cualquier operación de restauración basada en esa copia Snapshot reflejará el grupo de consistencia en el momento específico de la Snapshot.
- Si utiliza ONTAP 9.10.1 a 9.11.1, no puede modificar un grupo de consistencia. Para cambiar la configuración de un grupo de coherencia en ONTAP 9.10.1 o 9.11.1, debe eliminar el grupo de coherencia y, a continuación, crear un nuevo grupo de coherencia con los volúmenes que desea incluir.
- A partir de ONTAP 9.14.1, se pueden replicar copias Snapshot granulares del volumen en el clúster de destino cuando se utiliza SnapMirror asíncrono. Cuando se amplía un grupo de consistencia con SnapMirror asíncrono, las copias Snapshot granulares de volúmenes solo se replican después de

expandir el grupo de coherencia cuando la política de SnapMirror es MirrorAll o MirrorAndVault. Solo se replican las copias Snapshot granulares del volumen más recientes que las copias Snapshot del grupo de consistencia base.

- Si añade volúmenes a un grupo de consistencia en una relación de recuperación ante desastres de SVM (compatible a partir de ONTAP 9.14.1), debe actualizar la relación de recuperación ante desastres de SVM desde el clúster de destino tras expandir el grupo de consistencia. Para obtener más información, consulte [Actualice manualmente una relación de replicación](#).

## Ejemplo 22. Pasos

### System Manager

A partir de ONTAP 9.12.1, puede realizar esta operación con System Manager.

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione el grupo de coherencia que desea modificar.
3. Si va a modificar un solo grupo de consistencia, en la parte superior del menú **Volumes**, seleccione **más y**, a continuación, **ampliar** para añadir un volumen.

Si va a modificar un grupo de consistencia secundario, identifique el grupo de consistencia primario que desea modificar. Seleccione el botón **>** para ver los grupos de consistencia hijo y, a continuación, seleccione **⋮** junto al nombre del grupo de consistencia secundario que desea modificar. En ese menú, seleccione **ampliar**.

4. Seleccione hasta 16 volúmenes para añadir al grupo de coherencia.
5. Seleccione **Guardar**. Cuando la operación se complete, vea los volúmenes recién agregados en el menú **Volúmenes** del grupo de consistencia.

### CLI

A partir de ONTAP 9.14.1, puede añadir volúmenes a un grupo de coherencia mediante la CLI de ONTAP.

#### Añadir volúmenes existentes

1. Ejecute el siguiente comando. La `-volumes` el parámetro acepta una lista de volúmenes separados por comas.



Incluya sólo el `-parent-consistency-group` el parámetro si el grupo de coherencia está en una relación jerárquica.

```
consistency-group volume add -vserver svm_name -consistency-group
consistency_group_name -parent-consistency-group parent_consistency_group
-volume volumes
```

#### Añadir volúmenes nuevos

El procedimiento para añadir volúmenes nuevos depende del protocolo que utilice.



Incluya sólo el `-parent-consistency-group` el parámetro si el grupo de coherencia está en una relación jerárquica.

- Para añadir volúmenes nuevos sin exportarlos, realice lo siguiente:

```
consistency-group volume create -vserver SVM_name -consistency-group
child_consistency_group -parent-consistency-group existingParentCg -volume
volume_name -size size
```

- Para añadir volúmenes NFS nuevos:

```
consistency-group volume create -vserver SVM_name -consistency-group
consistency_group_name -volume volume-prefix -volume-count number -size
```

```
size -export-policy policy_name
```

- Para añadir nuevos volúmenes de SAN:

```
consistency-group volume create -vserver SVM_name -consistency-group
consistency_group_name -lun lun_name -size size -lun-count number -igroup
igroup_name
```

- Para añadir nuevos espacios de nombres de NVMe:

```
consistency-group volume create -vserver SVM_name -consistency-group
consistency_group_name -namespace namespace_name -volume-count number
-namespace-count number -size size -subsystem subsystem_name
```

## Quite volúmenes de un grupo de coherencia

Los volúmenes que se quitan de un grupo de consistencia no se eliminan. Permanecen activos en el clúster.

### Acerca de esta tarea

- No se pueden quitar volúmenes de un grupo de coherencia de una relación de recuperación ante desastres de SM-BC o SVM. Primero, debe romper la relación de SM-BC para modificar el grupo de consistencia y, a continuación, volver a establecer la relación.
- Si un grupo de coherencia no tiene volúmenes en él después de la operación de eliminación, se eliminará el grupo de coherencia.
- Cuando un volumen se elimina de un grupo de consistencia, las Snapshot existentes del grupo de consistencia permanecen, pero se consideran no válidas. Las snapshots existentes no se pueden utilizar para restaurar el contenido del grupo de consistencia. Siguen siendo válidas las copias Snapshot granulares en volúmenes.
- Si elimina un volumen del clúster, se elimina automáticamente del grupo de coherencia.
- Para cambiar la configuración de un grupo de coherencia en ONTAP 9.10.1 o 9.11.1, debe eliminar el grupo de coherencia y, a continuación, crear un grupo de coherencia nuevo con los volúmenes miembro deseados.
- Al eliminar un volumen del clúster, automáticamente lo quitará el grupo de coherencia.

## System Manager

A partir de ONTAP 9.12.1, puede realizar esta operación con System Manager.

### Pasos

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione el grupo de consistencia único o secundario que desea modificar.
3. En el menú **volúmenes**, seleccione las casillas de verificación junto a los volúmenes individuales que desea quitar del grupo de consistencia.
4. Seleccione **Eliminar volúmenes del grupo de coherencia**.
5. Confirmar que comprende la eliminación de los volúmenes hará que todas las copias snapshot del grupo de consistencia no sean válidas y seleccione **Quitar**.

### CLI

A partir de ONTAP 9.14.1, puede quitar volúmenes de un grupo de consistencia mediante la CLI.

### Paso

1. Quite los volúmenes. La `-volumes` el parámetro acepta una lista de volúmenes separados por comas.

Incluya sólo el `-parent-consistency-group` el parámetro si el grupo de coherencia está en una relación jerárquica.

```
consistency-group volume remove -vserver SVM_name -consistency-group
consistency_group_name -parent-consistency-group
parent_consistency_group_name -volume volumes
```

## Mover volúmenes entre grupos de coherencia

A partir de ONTAP 9.13.1, se pueden mover volúmenes entre grupos de coherencia secundarios que comparten un volumen primario.

### Acerca de esta tarea

- Solo puede mover volúmenes entre grupos de coherencia anidados bajo el mismo grupo de consistencia primario.
- Las snapshots de grupo de consistencia existentes quedan no válidas y ya no se puede acceder a ellas como snapshots de grupo de consistencia. Las copias de Snapshot de volumen individuales siguen siendo válidas.
- Las copias Snapshot del grupo de consistencia primario siguen siendo válidas.
- Si mueve todos los volúmenes de un grupo de consistencia secundario, se eliminará ese grupo de coherencia.
- Las modificaciones a un grupo de consistencia deben respetar [límites del grupo de consistencia](#).

## System Manager

A partir de ONTAP 9.12.1, puede realizar esta operación con System Manager.

### Pasos

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione el grupo de coherencia primario que contiene los volúmenes que desea mover. Encuentre el grupo de consistencia secundario y luego expanda el menú **VOLUMES**. Seleccione los volúmenes que desea mover.
3. Seleccione **Mover**.
4. Seleccione si desea mover los volúmenes a un grupo de coherencia nuevo o a un grupo existente.
  - a. Para desplazarse a un grupo de consistencia existente, seleccione **Grupo de consistencia secundario existente** y, a continuación, elija el nombre del grupo de consistencia en el menú desplegable.
  - b. Para desplazarse a un nuevo grupo de consistencia, seleccione **Nuevo grupo de consistencia secundario**. Introduzca un nombre para el nuevo grupo de consistencia secundario y seleccione un tipo de componente.
5. Seleccione **Mover**.

### CLI

A partir de ONTAP 9.14.1, puede mover volúmenes entre grupos de consistencia mediante la interfaz de línea de comandos de ONTAP.

#### Mueva volúmenes a un nuevo grupo de coherencia secundario

1. El siguiente comando crea un nuevo grupo de coherencia secundario que contiene los volúmenes designados.

Cuando se crea el nuevo grupo de coherencia, se pueden designar nuevas políticas de Snapshot, calidad de servicio y organización en niveles.

```
consistency-group volume reassign -vserver SVM_name -consistency-group
source_child_consistency_group -parent-consistency-group
parent_consistency_group -volume volumes -new-consistency-group
consistency_group_name [-snapshot-policy policy -qos-policy policy -tiering
-policy policy]
```

#### Mueva volúmenes a un grupo de coherencia secundario existente

1. Reasigne los volúmenes. La `-volumes` parameter acepta una lista de nombres de volúmenes separados por comas.

```
consistency-group volume reassign -vserver SVM_name -consistency-group
source_child_consistency_group -parent-consistency-group
parent_consistency_group -volume volumes -to-consistency-group
target_consistency_group
```

### Información relacionada

- [Límites del grupo de consistencia](#)

- [Clonar un grupo de consistencia](#)

## Modificar la geometría del grupo de consistencia

A partir de ONTAP 9.13.1, puede modificar la geometría de un grupo de consistencia. Modificar la geometría de un grupo de coherencia permite modificar la configuración de grupos de coherencia secundarios o primarios sin interrupciones en las operaciones de I/O en curso.

La modificación de la geometría del grupo de coherencia afectará a las copias Snapshot existentes.



No puede modificar la geometría de un grupo de consistencia configurado con una política de protección remota. Primero debe romper la relación de protección, modificar la geometría y, a continuación, restaurar la protección remota.

## Agregue un nuevo grupo de consistencia secundario

A partir de ONTAP 9.13.1, puede agregar un nuevo grupo de consistencia secundario a un grupo de consistencia primario existente.

### Antes de empezar

- Un grupo de coherencia primario puede contener un máximo de cinco grupos de coherencia secundarios. Consulte [límites del grupo de consistencia](#) para otros límites.
- No puede agregar un grupo de consistencia secundario a un grupo de consistencia único. Usted debe primero [\[promocionar\]](#) el grupo de consistencia, luego puede agregar un grupo de consistencia secundario.
- Las copias Snapshot existentes del grupo de consistencia capturadas antes de la operación de ampliación se considerarán parciales. Cualquier operación de restauración basada en esa copia Snapshot reflejará el grupo de consistencia en el momento específico de la copia Snapshot.

## Ejemplo 23. Pasos

### System Manager

A partir de ONTAP 9.13.1, puede realizar esta operación con System Manager.

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione el grupo de consistencia primario al que desea añadir un grupo de consistencia secundario.
3. Junto al nombre del grupo de consistencia primario, seleccione **Más** y luego **Agregar nuevo grupo de consistencia secundario**.
4. Introduzca un nombre para su grupo de consistencia.
5. Seleccione si desea añadir volúmenes nuevos o existentes.
  - a. Si va a agregar volúmenes existentes, seleccione **Volúmenes existentes** y, a continuación, elija los volúmenes en el menú desplegable.
  - b. Si va a agregar nuevos volúmenes, seleccione **Nuevos volúmenes** y luego designe el número de volúmenes y su tamaño.
6. Seleccione **Agregar**.

### CLI

A partir de ONTAP 9.14.1, puede agregar un grupo de consistencia secundario mediante la CLI de ONTAP.

#### Añada un grupo de coherencia secundario con volúmenes nuevos

1. Cree el nuevo grupo de consistencia. Proporcionar valores para el nombre del grupo de coherencia, el prefijo del volumen, la cantidad de volúmenes, el tamaño de volumen, el servicio de almacenamiento, y el nombre de la política de exportación:

```
consistency-group create -vserver SVM_name -consistency-group
consistency_group -parent-consistency-group parent_consistency_group
-volume-prefix prefix -volume-count number -size size -storage-service
service -export-policy policy_name
```

#### Añada un grupo de coherencia secundario con volúmenes existentes

1. Cree el nuevo grupo de consistencia. La `volumes` parameter acepta una lista de nombres de volúmenes separados por comas.

```
consistency-group create -vserver SVM_name -consistency-group
new_consistency_group -parent-consistency-group parent_consistency_group
-volumes volume
```

## Desvincular un grupo de consistencia secundario

A partir de ONTAP 9.13.1, puede quitar un grupo de consistencia secundario de su primario, convirtiéndolo en un grupo de consistencia individual.

### Antes de empezar

- Al desvincular un grupo de coherencia secundario, las snapshots del grupo de coherencia primario dejan de ser válidas y no se puede acceder a ellas. Las copias Snapshot granulares de volúmenes siguen



siendo válidas.

- Las copias Snapshot existentes del grupo de consistencia individual siguen siendo válidas.
- Se producirá un error en esta operación si existe un grupo de coherencia único existente con el mismo nombre que el grupo de coherencia secundario que se pretende desvincular. Si se encuentra con esta situación, debe cambiar el nombre del grupo de consistencia al desconectarlo.

## Ejemplo 24. Pasos

### System Manager

A partir de ONTAP 9.13.1, puede realizar esta operación con System Manager.

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione el grupo de consistencia primario que contiene el secundario que desea desvincular.
3. Junto al grupo de consistencia hijo que desea separar, seleccione **Más** y luego **Desasociar del padre**.
4. Opcionalmente, cambie el nombre del grupo de coherencia y seleccione un tipo de aplicación.
5. Seleccione **Desasociar**.

### CLI

A partir de ONTAP 9.14.1, puede desvincular un grupo de consistencia secundario mediante la CLI de ONTAP.

1. Desvincule el grupo de consistencia. De manera opcional, cambie el nombre del grupo de consistencia desvinculado con `-new-name` parámetro.

```
consistency-group detach -vserver SVM_name -consistency-group
child_consistency_group -parent-consistency-group parent_consistency_group
[-new-name new_name]
```

## Mueva un grupo de consistencia único existente bajo un grupo de consistencia primario

A partir de ONTAP 9.13.1, puede convertir un grupo de consistencia único existente en un grupo de consistencia secundario. Puede mover el grupo de consistencia por un grupo de consistencia primario existente o crear un grupo de consistencia primario nuevo durante la operación de movimiento.

### Antes de empezar

- El grupo de coherencia primario debe tener cuatro o menos hijos. Un grupo de coherencia primario puede contener un máximo de cinco grupos de coherencia secundarios. Consulte [límites del grupo de consistencia](#) para otros límites.
- Las copias Snapshot existentes del grupo de consistencia *parent* capturadas antes de esta operación se considerarán parciales. Cualquier operación de restauración basada en una de esas copias Snapshot reflejará el grupo de consistencia en el momento específico de la copia Snapshot.
- Las copias de Snapshot de grupo de consistencia existentes del grupo de consistencia único siguen siendo válidas.

## Ejemplo 25. Pasos

### System Manager

A partir de ONTAP 9.13.1, puede realizar esta operación con System Manager.

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione el grupo de consistencia que desea convertir.
3. Seleccione **Más** y luego **Mover bajo diferente grupo de consistencia**.
4. De manera opcional, introduzca un nuevo nombre para el grupo de consistencia y seleccione un tipo de componente. De forma predeterminada, el tipo de componente será Otro.
5. Elija si desea migrar a un grupo de consistencia primario existente o crear un nuevo grupo de consistencia primario:
  - a. Para migrar a un grupo de consistencia primario existente, seleccione **Grupo de consistencia existente** y, a continuación, elija el grupo de consistencia en el menú desplegable.
  - b. Para crear un grupo de consistencia primario nuevo, seleccione **Nuevo grupo de consistencia** y, a continuación, proporcione un nombre para el nuevo grupo de consistencia.
6. Selecciona **Mover**.

### CLI

A partir de ONTAP 9.14.1, puede mover un solo grupo de consistencia debajo de un grupo de consistencia primario mediante la CLI de ONTAP.

#### Mover un grupo de consistencia debajo de un nuevo grupo de consistencia primario

1. Cree el nuevo grupo de consistencia primario. La `-consistency-groups` el parámetro migrará cualquier grupo de consistencia existente al nuevo elemento principal.

```
consistency-group attach -vserver svm_name -consistency-group
parent_consistency_group -consistency-groups child_consistency_group
```

#### Mueva un grupo de consistencia bajo un grupo de consistencia existente

1. Mueva el grupo de consistencia:

```
consistency-group add -vserver SVM_name -consistency-group
consistency_group -parent-consistency-group parent_consistency_group
```

## Promover un grupo de consistencia secundario

A partir de ONTAP 9.13.1, puede promover un grupo de consistencia a un grupo de consistencia primario. Cuando se promociona el grupo de coherencia único a un elemento primario, también se crea un nuevo grupo de coherencia secundario que hereda todos los volúmenes del grupo de coherencia único original.

### Antes de empezar

- Si desea convertir un grupo de consistencia secundario en un grupo de consistencia primario, primero debe [\[detach\]](#) el grupo de consistencia secundario y, a continuación, siga este procedimiento.
- Las copias Snapshot existentes del grupo de consistencia siguen siendo válidas después de promocionar el grupo de consistencia.

## Ejemplo 26. Pasos

### System Manager

A partir de ONTAP 9.13.1, puede realizar esta operación con System Manager.

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione el grupo de coherencia que desea promocionar.
3. Seleccione **Más** y luego **Promocionar al grupo de consistencia primario**.
4. Introduzca un **Nombre** y seleccione un **Tipo de componente** para el grupo de consistencia hijo.
5. Seleccione **Promocionar**.

### CLI

A partir de ONTAP 9.14.1, puede mover un solo grupo de consistencia debajo de un grupo de consistencia primario mediante la CLI de ONTAP.

1. Promocione el grupo de consistencia. Este comando creará un grupo de coherencia primario y un secundario.

```
consistency-group promote -vserver SVM_name -consistency-group
existing_consistency_group -new-name new_child_consistency_group
```

## Degrade un elemento principal a un solo grupo de consistencia

A partir de ONTAP 9.13.1, puede degradar un grupo de consistencia primario a un solo grupo de consistencia. Al degradar el elemento primario, se abre la jerarquía del grupo de consistencia y se eliminan todos los grupos de coherencia secundarios asociados. Todos los volúmenes del grupo de coherencia permanecerán bajo el nuevo grupo de coherencia único.

### Antes de empezar

- Las copias Snapshot existentes del grupo de consistencia primario siguen siendo válidas después de degradarlas a una sola consistencia. Las copias Snapshot existentes de cualquiera de los grupos de consistencia secundarios asociados de dicho grupo principal dejarán de ser válidas, pero las snapshots de volúmenes individuales que contienen siguen siendo accesibles como snapshots granulares para el volumen.

## Ejemplo 27. Pasos

### System Manager

A partir de ONTAP 9.13.1, puede realizar esta operación con System Manager.

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione el grupo de consistencia primario que desea degradar.
3. Seleccione **Más** y luego **Descender a un solo grupo de consistencia**.
4. Una advertencia le aconsejará que se eliminen todos los grupos de coherencia secundarios asociados y que sus volúmenes se muevan al nuevo grupo de consistencia único. Seleccione **Descenso** para confirmar que entiendes el impacto.

### CLI

A partir de ONTAP 9.14.1, puede degradar un grupo de consistencia mediante la CLI de ONTAP.

1. Degrade el grupo de consistencia. Utilice el opcional `-new-name` parámetro para cambiar el nombre del grupo de consistencia.

```
consistency-group demote -vserver SVM_name -consistency-group
parent_consistency_group [-new-name new_consistency_group_name]
```

## Modificar etiquetas de aplicación y componentes

A partir de ONTAP 9.12.1, los grupos de consistencia admiten el etiquetado de componentes y aplicaciones. Las etiquetas de aplicaciones y componentes son una herramienta de gestión que le permite filtrar e identificar diferentes cargas de trabajo en sus grupos de consistencia.

### Acerca de esta tarea

Los grupos de consistencia ofrecen dos tipos de etiquetas:

- **Etiquetas de aplicación:** Estas se aplican a grupos de consistencia individuales y padre. Las etiquetas de las aplicaciones proporcionan etiquetas para cargas de trabajo como MongoDB, Oracle o SQL Server. La etiqueta de aplicación predeterminada para los grupos de consistencia es otra.
- **Etiquetas de componentes:** Los niños de los grupos de consistencia jerárquicos tienen etiquetas de componentes en lugar de etiquetas de aplicación. Las opciones para etiquetas de componentes son "datos", "registros" u "otros". El valor predeterminado es Other.

Puede aplicar las etiquetas al crear grupos de consistencia o después de crear los grupos de consistencia.




Si el grupo de consistencia tiene una relación SM-BC, debe utilizar **otros** como la aplicación o etiqueta de componente.

### Pasos

A partir de ONTAP 9.12.1, puede modificar las etiquetas de componentes y aplicaciones mediante System Manager. A partir de ONTAP 9.14.1, puede modificar la aplicación y las etiquetas de los componentes mediante la CLI de ONTAP.

## System Manager

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione el grupo de consistencia cuya etiqueta desea modificar. Seleccione la  Junto al nombre del grupo de consistencia luego **Editar**.
3. En el menú desplegable, seleccione la aplicación o etiqueta de componente adecuada.
4. Seleccione **Guardar**.

## CLI

A partir de ONTAP 9.14.1, puede modificar la aplicación o la etiqueta de componente de un grupo de consistencia existente mediante la CLI de ONTAP.

### Modifique la etiqueta de aplicación

1. Las etiquetas de aplicación aceptan un número limitado de cadenas predefinidas. Para ver la lista de cadenas aceptadas, ejecute el siguiente comando:

```
consistency-group modify -vserver svm_name -consistency-group
consistency_group -application-type ?
```

2. Elija la cadena adecuada del resultado, el modifique el grupo de consistencia:

```
consistency-group modify -vserver svm_name -consistency-group
consistency_group -application-type application_type
```

### Modifique la etiqueta de componente

1. Modifique el tipo de componente. El tipo de componente puede ser datos, registros u otros. Si está utilizando SM-BC, debe ser "Otro".

```
consistency-group modify -vserver svm -consistency-group
child_consistency_group -parent-consistency-group parent_consistency_group
-application-component-type [data|logs|other]
```

## Clonar un grupo de consistencia

A partir de ONTAP 9.12.1, puede clonar un grupo de consistencia para crear una copia de un grupo de consistencia y su contenido. La clonación de un grupo de coherencia crea una copia de la configuración del grupo de coherencia, sus metadatos, como el tipo de aplicación, y todos los volúmenes y su contenido, como archivos, directorios, LUN o espacios de nombres NVMe.

### Acerca de esta tarea

Al clonar un grupo de consistencia, puede clonarlo con su configuración actual, pero con el contenido del volumen como son o basado en una snapshot de grupo de consistencia existente.

La clonación de un grupo de consistencia solo se admite para todo el grupo de consistencia. No puede clonar un grupo de consistencia secundario individual en una relación jerárquica: Solo se puede clonar la configuración completa del grupo de consistencia.

Cuando clona un grupo de consistencia, no se clonan los siguientes componentes:

- Grupos de iniciadores
- Mapas de LUN

- Subsistemas NVMe
- Asignaciones del subsistema de espacio de nombres de NVMe

#### **Antes de empezar**

- Cuando se clona un grupo de coherencia, ONTAP no creará recursos compartidos de SMB para los volúmenes clonados si no se especifica un nombre de recurso compartido. \* Los grupos de consistencia clonados no están montados si no se especifica una ruta de unión.
- Si intenta clonar un grupo de consistencia basado en una snapshot que no refleja los volúmenes constituyentes actuales del grupo de consistencia, se producirá un error en la operación.
- Después de clonar un grupo de consistencia, debe realizar la operación de asignación adecuada.

Consulte [Asigne iGroups a varias LUN](#) o [Asignar un espacio de nombres NVMe a un subsistema](#) si quiere más información.

- No se admite la clonación de un grupo de consistencia en una relación de continuidad empresarial de SnapMirror o con ningún volumen de DP asociado.

## System Manager

### Pasos

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione el grupo de consistencia que desea clonar en el menú **Grupo de consistencia**.
3. En la parte superior derecha de la página de descripción general del grupo de consistencia, seleccione **Clonar**.
4. Introduzca un nombre para el nuevo grupo de consistencia clonado o acepte el nombre predeterminado.
  - a. Elija si desea habilitar **"Thin Provisioning"**.
  - b. Elija **Split Clone** si desea disociar el grupo de consistencia de su origen y asignar espacio en disco adicional para el grupo de consistencia clonado.
5. Para clonar el grupo de consistencia en su estado actual, elija **Agregar una nueva copia Snapshot**.

Para clonar el grupo de consistencia basado en una instantánea, seleccione **utilizar una copia Snapshot** existente. Si selecciona esta opción, se abrirá un nuevo submenú. Elija la copia de Snapshot que desea usar como base para la operación de clonado.

6. Seleccione **Clonar**.
7. Vuelva al menú **Grupo de consistencia** para confirmar que el grupo de consistencia ha sido clonado.

### CLI

A partir de ONTAP 9.14.1, puede clonar un grupo de consistencia mediante la CLI.

#### Clonar un grupo de consistencia

1. La `consistency-group clone create` el comando clona el grupo de coherencia en su estado actual de un momento específico. Para basar la operación de clonación en una instantánea, incluya la `-source-snapshot` parámetro.

```
consistency-group clone create -vserver svm_name -consistency-group
clone_name -source-consistency-group consistency_group_name [-source-
snapshot snapshot_name]
```

### Siguientes pasos

- [Asigne iGroups a varias LUN](#)
- [Asignar un espacio de nombres NVMe a un subsistema](#)

## Eliminar un grupo de consistencia

Si decide que ya no necesita un grupo de consistencia, puede eliminarlo.

### Acerca de esta tarea


- Al eliminar un grupo de coherencia se elimina la instancia del grupo de coherencia y *no* afecta a los volúmenes constituyentes o las LUN. La eliminación de un grupo de consistencia no elimina las instantáneas presentes en cada volumen, pero ya no será accesible como copias Snapshot de grupo de consistencia. Sin embargo, las copias Snapshot pueden seguir gestionándose como snapshots granulares

de volumen normales.

- ONTAP elimina automáticamente un grupo de coherencia si todos los volúmenes del grupo de coherencia se eliminan.
- Al eliminar un grupo de consistencia primario, se eliminan todos los grupos de consistencia secundarios asociados.
- Si utiliza una versión de ONTAP entre 9.10.1 y 9.12.0, los volúmenes solo se pueden eliminar de un grupo de coherencia si el volumen se elimina, en cuyo caso, el volumen se elimina automáticamente del grupo de coherencia. A partir de ONTAP 9.12.1, es posible quitar volúmenes de un grupo de consistencia sin eliminar el grupo de consistencia. Para obtener más información sobre este proceso, consulte [Modificar un grupo de consistencia](#).

## Ejemplo 28. Pasos

### System Manager

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione el grupo de coherencia que desea eliminar.
3. Junto al nombre del grupo de consistencia, seleccione  Luego **Eliminar**.

### CLI

A partir de ONTAP 9.14.1, puede eliminar un grupo de consistencia mediante la CLI.

### Eliminar un grupo de consistencia

1. Elimine el grupo de consistencia:

```
consistency-group delete -vserver svm_name -consistency-group
consistency_group_name
```

# Continuidad del negocio de SnapMirror

## Información general sobre la continuidad del negocio de SnapMirror

SnapMirror Business Continuity (SM-BC), también conocido como SnapMirror sincronización activa, permite que los servicios empresariales continúen funcionando incluso si se produce un fallo completo en el sitio, lo que permite que las aplicaciones conmuten por error de forma transparente usando una copia secundaria. No se requiere intervención manual ni secuencias de comandos adicionales para activar una recuperación tras fallos con SM-BC.

SM-BC está disponible a partir de ONTAP 9.8. SM-BC se admite en clústeres AFF o en clústeres de cabinas all-flash de SAN (ASA), donde los clústeres primario y secundario pueden ser AFF o ASA. SM-BC protege las aplicaciones con LUN iSCSI o FCP.

### Beneficios

SM-BC ofrece las siguientes ventajas:

- Disponibilidad continua para aplicaciones vitales para el negocio



- Capacidad de alojar aplicaciones críticas alternativamente desde la ubicación principal y la secundaria
- Gestión de aplicaciones simplificada usando grupos de consistencia para mantener la coherencia de los pedidos de escritura dependiente
- La capacidad de probar la recuperación tras fallos para cada aplicación
- Creación instantánea de clones duplicados sin afectar a la disponibilidad de las aplicaciones
- A partir de ONTAP 9.11.1, SM-BC admite [SnapRestore de archivo único](#).
- A partir de ONTAP 9.14.1, SM-BC es compatible con los clústeres de conmutación al nodo de respaldo de Windows y ["Reservas persistentes de SCSI 3"](#), mejorando la alta disponibilidad.

## Casos de uso

### Puesta en marcha de aplicaciones para objeto de tiempo de recuperación cero (RTO)

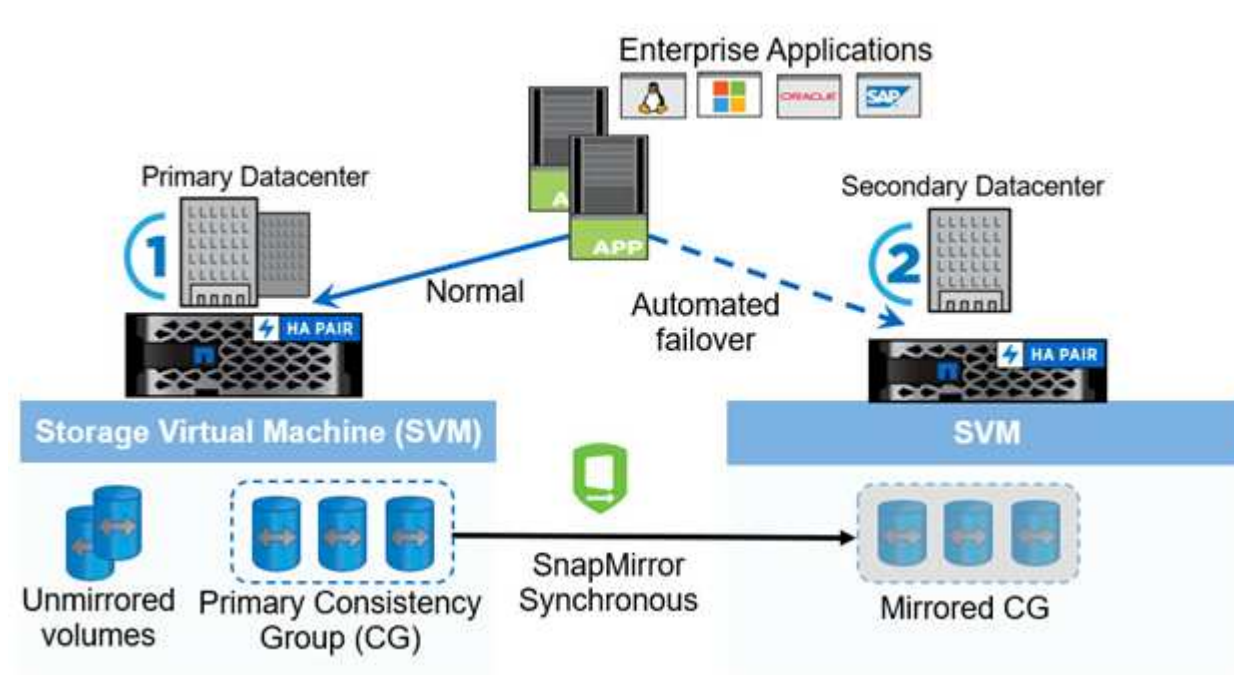
En una implementación de SM-BC, tendrá un clúster primario y secundario. Una LUN en el clúster primario (LP) tendrá un espejo (L1S) en el volumen secundario; ambas LUN comparten el mismo ID de serie y se notifican como LUN de lectura y escritura en el host. Sin embargo, las operaciones de lectura y escritura solo se realizan en la LUN principal, LP. Cualquier escritura en el reflejo L1S son servidas por proxy.

### Situación de desastre

Con SM-BC, puede replicar de forma síncrona varios volúmenes para una aplicación entre sitios en ubicaciones geográficamente dispersas. Puede conmutar automáticamente por respaldo a la copia secundaria en caso de interrupción del almacenamiento primario, con lo que se permite la continuidad del negocio para aplicaciones de nivel uno.

## Arquitectura

La siguiente figura muestra el funcionamiento de la función de continuidad de negocio de SnapMirror a grandes rasgos.



En la sección uno del diagrama, se pone en marcha una aplicación en una SVM del centro de datos principal. Los volúmenes que se han añadido al grupo de coherencia primario están protegidos con SM-BC y se reflejan

en un grupo de coherencia secundario en un centro de datos secundario. Los volúmenes del grupo de coherencia primario se conmutarán al nodo de respaldo al grupo de coherencia reflejado en caso de interrupción. Los volúmenes que no están en un grupo de consistencia reflejada no se proporcionan en caso de conmutación al nodo de respaldo.

## Más información

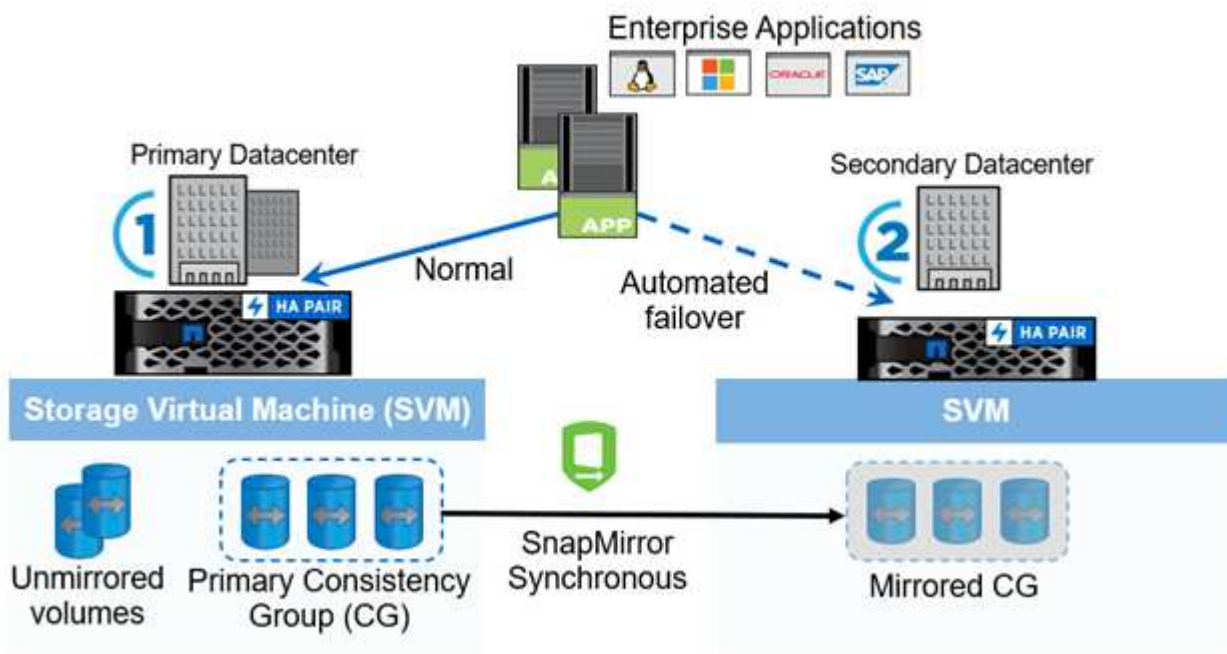
- ["TR-4878: Continuidad del negocio de SnapMirror"](#)

## Conceptos clave

La continuidad del negocio de SnapMirror (SM-BC) utiliza funciones tales como grupos de consistencia y el mediador de ONTAP para garantizar que sus datos se repliquen y se sirvan incluso en caso de desastre. A la hora de planificar la implementación de SM-BC, es importante comprender los conceptos básicos de SM-BC y su arquitectura.

## Arquitectura

En la siguiente figura se muestra una descripción general de la implementación de SM-BC.



El diagrama muestra una aplicación empresarial alojada en una máquina virtual de almacenamiento (SVM) en el centro de datos principal. La SVM contiene cinco volúmenes, tres de los cuales forman parte de un grupo de coherencia. Los tres volúmenes del grupo de coherencia se reflejan en un centro de datos secundario. En circunstancias normales, todas las operaciones de escritura se realizan en el centro de datos primario; en efecto, este centro de datos sirve como origen de operaciones de I/O, mientras que el centro de datos secundario sirve como destino.

En caso de que se produzca un desastre en el centro de datos primario, ONTAP Mediator dirigirá al centro de datos secundario para que actúe como primario y sirva todas las operaciones de I/O. Solo se servirá los volúmenes reflejados en el grupo de coherencia. Cualquier operación que pertenezca a los otros dos volúmenes en la SVM se verá afectada por el evento de desastre.

## Conceptos esenciales

Comprender los siguientes términos le ayudará a implementar SM-BC.

### Grupo de consistencia

Un grupo de coherencia es una colección de volúmenes o LUN que proporcionan una garantía de coherencia en orden de escritura para la carga de trabajo de la aplicación que debe protegerse para la continuidad del negocio. Un grupo de consistencia garantiza que todos los volúmenes de este conjunto de datos se pongan en modo inactivo y, a continuación, se snappean en el mismo momento específico, lo que proporciona un punto de restauración coherente con los datos en todos los volúmenes para ese conjunto de datos.

En SM-BC, creará un grupo de consistencia principal y secundario para la replicación y la protección de datos. El grupo de consistencia secundario servirá sus datos en caso de interrupción.

Para obtener más información sobre los grupos de consistencia, consulte ["Información general sobre los grupos de consistencia"](#).

### Componente

Un volumen o LUN individual que forma parte de un grupo de coherencia, que está protegido por la relación de SM-BC.

### Mediador ONTAP

Los mediadores de ONTAP supervisan los dos clústeres ONTAP y orquestan la conmutación por error en caso de que se produzca un error en el sistema de almacenamiento principal. Con Mediador de ONTAP, su aplicación se vuelve a conectar automáticamente con los recursos del sistema de almacenamiento secundario.

Con la información de estado de ONTAP Mediator, los clústeres pueden diferenciar entre fallos de LIF entre clústeres y fallos del sitio. Cuando el sitio falla, ONTAP Mediator transmite la información de estado al clúster del mismo nivel bajo demanda, lo que facilita el clúster del mismo nivel a la conmutación por error.

Obtenga más información sobre la ["Mediador ONTAP"](#).

### Conmutación al respaldo planificada

Operación manual para cambiar los roles de las copias en una relación SM-BC. Los sitios primarios se convierten en los secundarios y los secundarios se convierten en los primarios.

### Conmutación automática al respaldo no planificada (AUFO)

Una operación automática para ejecutar una conmutación por error a la copia de mirroring. La operación requiere ayuda de Mediator para detectar que la copia primaria no está disponible.

### Fuera de sincronización (OOS)

Cuando las operaciones de I/O de aplicaciones no se replican en el sistema de almacenamiento secundario, se informará como **fuera de sincronización**. Un estado fuera de sincronización significa que los volúmenes secundarios no se sincronizan con el primario (origen) y que no se está produciendo la replicación de SnapMirror.

Si el estado de reflejo es `Snapmirrored`, esto indica un error de transferencia o un fallo debido a una operación no soportada.

### RPO cero

RPO es la sigla en inglés para el objetivo de punto de recuperación, que es la cantidad de pérdida de datos que se considera aceptable durante un período de tiempo dado. El RPO de cero significa que no es aceptable ninguna pérdida de datos.

## RTO CERO

El objetivo de tiempo de recuperación es el objetivo de tiempo de recuperación, que es la cantidad de tiempo que se considera aceptable para que una aplicación regrese a las operaciones normales tras una interrupción del servicio, un fallo u otro evento de pérdida de datos. El objetivo de tiempo de recuperación cero significa que no se acepta ningún tiempo de inactividad.

## Planificación

### Requisitos previos

Cuando planifique la puesta en marcha de continuidad del negocio de SnapMirror, asegúrese de haber cumplido los distintos requisitos de configuración de hardware, software y sistema.

### Hardware subyacente

- Solo se admiten clústeres de alta disponibilidad de dos nodos
- Ambos clústeres deben ser AFF (incluido AFF C-Series) o ASA (sin combinación)

### De NetApp

- ONTAP 9,8 o posterior
- Mediador ONTAP 1.2 o posterior
- Un servidor Linux o máquina virtual para el Mediador ONTAP que ejecuta uno de los siguientes:

| Versión de ONTAP Mediator | Versiones de Linux compatibles                                                                                                                              |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1,7                       | <ul style="list-style-type: none"><li>• Red Hat Enterprise Linux: 8,5, 8,6, 8,7, 8,8, 8,9, 9,0, 9,1, 9,2 y 9,3</li><li>• Rocky Linux 8 y 9</li></ul>        |
| 1,6                       | <ul style="list-style-type: none"><li>• Red Hat Enterprise Linux: 8,4, 8,5, 8,6, 8,7, 8,8, 9,0, 9,1, 9,2</li><li>• Rocky Linux 8 y 9</li></ul>              |
| 1,5                       | <ul style="list-style-type: none"><li>• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 7.9, 8.1 8.2, 8.3, 8.4, 8.5</li><li>• CentOS: 7.6, 7.7, 7.8, 7.9</li></ul> |
| 1,4                       | <ul style="list-style-type: none"><li>• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 7.9, 8.1 8.2, 8.3, 8.4, 8.5</li><li>• CentOS: 7.6, 7.7, 7.8, 7.9</li></ul> |
| 1,3                       | <ul style="list-style-type: none"><li>• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 7.9, 8.1 8.2, 8.3</li><li>• CentOS: 7.6, 7.7, 7.8, 7.9</li></ul>           |
| 1,2                       | <ul style="list-style-type: none"><li>• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 8.1</li><li>• CentOS: 7.6, 7.7, 7.8</li></ul>                              |

## Licencia

- Debe aplicarse la licencia síncrona de SnapMirror (SM-S) en ambos clústeres
- Debe aplicarse la licencia de SnapMirror en ambos clústeres



Si sus sistemas de almacenamiento de ONTAP se adquirieron antes de junio de 2019, consulte ["Claves de licencia maestra de ONTAP de NetApp"](#) Para obtener la licencia SM-S necesaria.

Las licencias de SnapMirror Synchronous y SnapMirror Synchronous se incluyen en ["ONTAP One"](#).

## Entorno de red

- El tiempo de ida y vuelta (RTT) de latencia entre clústeres debe ser inferior a 10 milisegundos.
- Las reservas persistentes SCSI-3 son **no** compatibles con SM-BC.

## Protocolos compatibles

- Solo son compatibles los protocolos SAN (no NFS/SMB).
- Solo se admiten los protocolos Fibre Channel e iSCSI.
- El espacio IP predeterminado es necesario por SM-BC para las relaciones de paridad de clústeres. No se admite el espacio IP personalizado.

## Estilo de seguridad NTFS

El estilo de seguridad NTFS **no** se admite en volúmenes SM-BC.

## Mediador ONTAP

- El mediador ONTAP se aprovisiona externamente y se conecta a ONTAP para una recuperación transparente tras fallos de aplicaciones.
- Para que funcione completamente y habilitar la conmutación automática al respaldo no planificada, el mediador externo ONTAP se debería aprovisionar y configurar con clústeres de ONTAP.
- ONTAP Mediator debe instalarse en un tercer dominio de fallo, independiente de los dos clústeres de ONTAP.
- Al instalar el Mediador ONTAP, debe sustituir el certificado autofirmado por un certificado válido firmado por una CA confiable convencional.
- Para obtener más información sobre el Mediador ONTAP, consulte ["Prepare la instalación del servicio Mediador ONTAP"](#).

## Volúmenes de destino de lectura y escritura

- No se admiten las relaciones de SM-BC en los volúmenes de destino de lectura/escritura. Para poder usar un volumen de lectura/escritura, debe convertirlo en un volumen de DP. Para ello, cree una relación de SnapMirror en el nivel de volumen y elimine la relación. Para obtener más información, consulte ["Conversión de relaciones existentes a relaciones SM-BC"](#)

## Grandes LUN y grandes volúmenes

La compatibilidad con LUN de gran tamaño y volúmenes de gran tamaño (más de 100 TB) depende de la versión de ONTAP que utilice y de su plataforma.

### ONTAP 9.12.1P2 y posterior

- Para ONTAP 9.12.1 P2 y versiones posteriores, SMBC admite LUN grandes y volúmenes grandes mayores de 100TB en ASA y AFF (incluido C-Series).



Para las versiones 9.12.1P2 de ONTAP y versiones posteriores, debe asegurarse de que los clústeres primario y secundario sean cabinas All Flash SAN o cabina All Flash, y que ambos tengan instalado ONTAP 9.12.1 P2 o una versión posterior. Si el clúster secundario ejecuta una versión anterior a ONTAP 9.12.1P2, o si el tipo de cabina no es el mismo que el clúster primario, la relación síncrona puede desincronizarse si el volumen primario crece más de 100 TB.

### ONTAP 9,8 - 9.12.1P1

- Para las versiones de ONTAP entre ONTAP 9,8 y 9.12.1 P1 (inclusive), las cabinas SAN all-flash solo admiten LUN de gran tamaño y volúmenes grandes superiores a 100TB TB.



Para versiones de ONTAP entre ONTAP 9,8 y 9.12.1 P2, debe asegurarse de que los clústeres primario y secundario sean cabinas all-flash SAN, y que ambos tengan ONTAP 9,8 o una versión posterior instalada. Si el clúster secundario ejecuta una versión anterior a ONTAP 9,8, o si no es una cabina all-flash SAN, la relación síncrona puede desincronizarse si el volumen primario crece más de 100 TB.

### Más información

- ["Hardware Universe"](#)
- ["Descripción general de ONTAP Mediator"](#)

### Configuraciones y funciones compatibles

SnapMirror Business Continuity es compatible con numerosos sistemas operativos y otras funciones incluidas en ONTAP. Obtenga información sobre detalles y configuraciones recomendadas.

### Configuraciones admitidas

SM-BC es compatible con numerosos sistemas operativos, incluyendo:

- AIX (a partir de ONTAP 9.11.1)
- HP-UX (a partir de ONTAP 9.10.1)
- Solaris 11,4 (a partir de ONTAP 9.10.1)

### AIX

A partir de ONTAP 9.11.1, AIX es compatible con SM-BC. Con una configuración AIX, el clúster primario es el clúster "activo".

En una configuración AIX, las recuperaciones tras fallos son disruptivas. Con cada conmutación al nodo de respaldo, deberá realizar un nuevo análisis en el host para que se reanuden las operaciones de I/O.

Para configurar un host AIX con SM-BC, consulte el artículo de la base de conocimientos ["Cómo configurar un](#)

[host AIX para la continuidad del negocio de SnapMirror \(SM-BC\)".](#)

## HP-UX

A partir de ONTAP 9.10.1, se admite SM-BC para HP-UX.

### Limitaciones de HP-UX

Un evento de failover no planificado automático (AUFO) en el cluster maestro aislado puede deberse a un fallo de evento doble cuando se pierde la conexión entre el cluster primario y el secundario y también se pierde la conexión entre el cluster primario y el mediador. Esto se considera un evento raro, a diferencia de otros eventos de AUFO.

- En este escenario, podría tardar más de 120 segundos en reanudarse la E/S en el host HP-UX. En función de las aplicaciones que se estén ejecutando, esto puede no provocar ninguna interrupción de I/O o mensajes de error.
- Para remediar, debe reiniciar las aplicaciones en el host de HP-UX que tengan una tolerancia de interrupción inferior a 120 segundos.

### Recomendación de configuración de host de Solaris

A partir de ONTAP 9.10.1, SM-BC admite Solaris 11.4.

Para garantizar que las aplicaciones cliente de Solaris no son disruptivas cuando se produce una conmutación por error de sitio no planificada en un entorno SM-BC, modifique la configuración predeterminada del sistema operativo Solaris. Para configurar Solaris con la configuración recomendada, consulte el artículo de la base de conocimientos ["Ajustes recomendados para el soporte de host Solaris en la configuración de continuidad empresarial de SnapMirror \(SM-BC\)".](#)

### Clustering de conmutación al nodo de respaldo de Windows

A partir de ONTAP 9.14.1, SM-BC es compatible con los clústeres de conmutación por error de Windows. Para obtener más información, consulte ["TR-4878: Continuidad del negocio de SnapMirror"](#).

### Integraciones de ONTAP

SM-BC ofrece compatibilidad con otras funciones de ONTAP, como:

- Configuraciones de dispersión
- Copia NDMP (a partir de ONTAP 9.13.1)
- Restauración parcial de archivos (a partir de ONTAP 9.12.1)

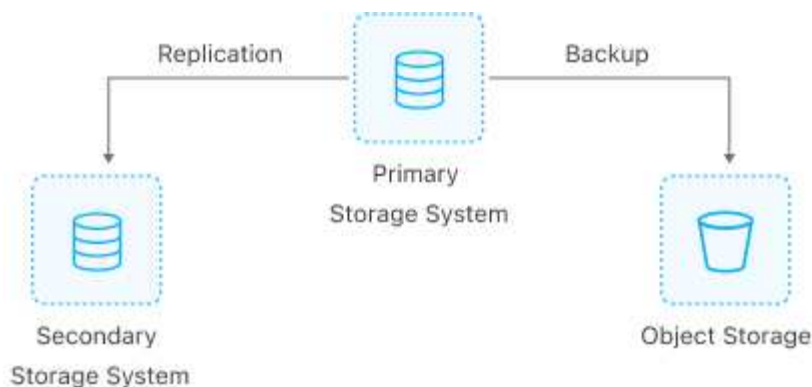
### FabricPool

SM-BC admite los volúmenes de origen y destino en agregados de FabricPool con la política de organización en niveles: Ninguno, Snapshot o Automático. SM-S SM-BC no es compatible con agregados FabricPool utilizando una política de organización en niveles de todos.

### Configuraciones de dispersión

En una [configuraciones de dispersión](#), Su volumen de origen se puede duplicar en un extremo de destino de SM-BC y en una o más relaciones asíncronas de SnapMirror.





Soportes SM-BC [configuraciones de dispersión](#) con la MirrorAllSnapshots Política y, a partir de ONTAP 9.11.1, el MirrorAndVault política. SM-BC no admite configuraciones de salida de ventilador con el XDPDefault política.

Si experimenta una conmutación al nodo de respaldo en el destino de SM-BC en una configuración de dispersión, deberá hacerlo de forma manual [reanude la protección en la configuración de fan-out](#).

## Restauración de NDMP

A partir de ONTAP 9.13.1, se puede usar NDMP para copiar y restaurar datos con SM-BC. El uso de NDMP permite mover datos a la fuente SM-BC para realizar una restauración sin pausar la protección. Esto resulta especialmente útil en configuraciones ramificadas.

Para obtener más información sobre este proceso, consulte [Transferencia de datos mediante la copia ndmp](#).

## Restauración parcial de archivos

A partir de ONTAP 9.12.1, se admite una restauración de LUN parcial para los volúmenes de SM-BC. Para obtener información sobre este proceso, consulte ["Restaurar parte de un archivo desde una copia snapshot"](#).

## Límites de objetos para la continuidad del negocio de SnapMirror

Cuando se prepare para utilizar y gestionar SnapMirror Business Continuity, tenga en cuenta las siguientes limitaciones.

### Grupos de consistencia en un clúster

Los límites de los grupos de consistencia para un clúster con SM-BC se calculan en función de las relaciones y dependen de la versión de ONTAP utilizada. Los límites son independientes de la plataforma.

| Versión de ONTAP                     | Número máximo de relaciones |
|--------------------------------------|-----------------------------|
| ONTAP 9.8-9.9.1                      | 5                           |
| ONTAP 9.10.1                         | 20                          |
| ONTAP 9.11.1 y versiones posteriores | 50                          |

### Volúmenes por grupo de coherencia

El número máximo de volúmenes por grupo de coherencia con SM-BC es independiente de la plataforma.



| <b>Versión de ONTAP</b>    | <b>Cantidad máxima de volúmenes admitidos en una relación de grupo de consistencia</b> |
|----------------------------|----------------------------------------------------------------------------------------|
| ONTAP 9,8-9.9.1            | 12                                                                                     |
| ONTAP 9.10.1 y posteriores | 16                                                                                     |

### Volúmenes

Los límites de volumen en SM-BC se calculan en función del número de puntos finales, no del número de relaciones. Un grupo de consistencia con 12 volúmenes contribuye con 12 extremos en el clúster primario y secundario. Tanto las relaciones de SM-BC como de SnapMirror Synchronous contribuyen al número total de extremos.

En la siguiente tabla se incluyen los puntos finales máximos por plataforma.

| <b>S. No</b> | <b>Plataforma</b> | <b>Extremos por ha para SM-BC</b> |              |                                      | <b>Sincronización general y extremos SM-BC por alta disponibilidad</b> |              |                                      |
|--------------|-------------------|-----------------------------------|--------------|--------------------------------------|------------------------------------------------------------------------|--------------|--------------------------------------|
|              |                   | ONTAP 9,8-9.9.1                   | ONTAP 9.10.1 | ONTAP 9.11.1 y versiones posteriores | ONTAP 9,8-9.9.1                                                        | ONTAP 9.10.1 | ONTAP 9.11.1 y versiones posteriores |
| 1            | AFF               | 60                                | 200          | 400                                  | 80                                                                     | 200          | 400                                  |
| 2            | ASA               | 60                                | 200          | 400                                  | 80                                                                     | 200          | 400                                  |

### Límites DE objetos DE SAN

En la siguiente tabla se incluyen los límites de objetos SAN. Los límites se aplican independientemente de la plataforma.

| <b>Objeto en una relación SM-BC</b>                         | <b>Cuente</b>                                                                                                              |
|-------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| LUN por volumen                                             | 256                                                                                                                        |
| Mapas de LUN por nodo                                       | <ul style="list-style-type: none"> <li>• 4096 (ONTAP 9,10 y posterior)</li> <li>• 2048 (ONTAP 9.9.1 y anterior)</li> </ul> |
| Mapas de LUN por clúster                                    | <ul style="list-style-type: none"> <li>• 8192 (ONTAP 9,10 y posterior)</li> <li>• 4096 (ONTAP 9.9.1 y anterior)</li> </ul> |
| LIF por SVM (con al menos un volumen en una relación SM-BC) | 256                                                                                                                        |
| LIF entre clústeres por nodo                                | 4                                                                                                                          |
| LIF entre clústeres por clúster                             | 8                                                                                                                          |

### Información relacionada

- ["Hardware Universe"](#)
- ["Límites del grupo de consistencia"](#)

## Instalar y configurar

### Configurar el mediador de ONTAP y los clústeres para la continuidad del negocio con SnapMirror

SnapMirror Business Continuity (SM-BC) utiliza clústeres con conexión entre iguales para garantizar que los datos están disponibles en caso de conmutación por error. ONTAP Mediator es un recurso clave que garantiza la continuidad del negocio y supervisa el estado de cada clúster. Para configurar SM-BC, primero debe instalar ONTAP Mediator y asegurarse de que los clústeres primario y secundario están configurados correctamente.

Una vez que haya instalado ONTAP Mediator y configurado los clústeres, debe hacerlo [\[initialize-the-ontap-mediator\]](#) Mediator ONTAP para uso con SM-BC. Entonces debe hacerlo [Cree, inicialice y asigne el grupo de consistencia para SM-BC](#)

#### Mediador ONTAP

El Mediador ONTAP establece un quórum para los clústeres de ONTAP en una relación de SM-BC. Coordina la conmutación automática al nodo de respaldo cuando se detecta un fallo, al determinar qué clúster actúa como principal y garantizar que se sirven los datos a y desde el destino correcto.

#### Requisitos previos para el Mediador ONTAP

- El Mediador ONTAP incluye su propio conjunto de requisitos previos. Debe cumplir con estos requisitos previos antes de instalar el mediador.

Para obtener más información, consulte ["Prepare la instalación del servicio Mediador ONTAP"](#).

- De forma predeterminada, el Mediador ONTAP proporciona servicio a través del puerto TCP 31784. Debe asegurarse de que el puerto 31784 esté abierto y disponible entre los clústeres de ONTAP y el mediador.

#### Instale ONTAP Mediator y confirme la configuración del cluster

Continúe con cada uno de los pasos siguientes. Para cada paso, debe confirmar que se ha realizado la configuración específica. Utilice el enlace que se incluye después de cada paso para obtener más información según sea necesario.

#### Pasos

1. Instale el servicio Mediator de ONTAP antes de asegurarse de que los clústeres de origen y destino están configurados correctamente.

[Prepárese para instalar o actualizar el servicio de Mediador de ONTAP](#)

2. Confirme que existe una relación de paridad entre los clústeres.



El espacio IP predeterminado es necesario por SM-BC para las relaciones de paridad de clústeres. No se admite un espacio IP personalizado.

[Configure las relaciones de paridad](#)

3. Confirmar que las máquinas virtuales de almacenamiento se crean en cada clúster.

[Creación de una SVM](#)

4. Confirmar que existe una relación entre iguales entre las máquinas virtuales de almacenamiento en cada clúster.

[Creación de una relación de paridad de SVM](#)

5. Confirme que los volúmenes existen para sus LUN.

[Creación de un volumen](#)

6. Confirmar que se crea al menos un LIF SAN en cada nodo del clúster.

["Consideraciones para los LIF en un entorno SAN de clúster"](#)

["Crear una LIF"](#)

7. Confirmar que las LUN necesarias se crean y asignan a un igroup, que se utiliza para asignar las LUN al iniciador en el host de la aplicación.

[Cree LUN y asigne iGroups](#)

8. Vuelva a analizar el host de la aplicación para detectar todos los LUN nuevos.

#### **Inicialice el mediador ONTAP para SM-BC**

Una vez que haya instalado ONTAP Mediator y confirmado la configuración del clúster, debe inicializar ONTAP Mediator para la supervisión del clúster. Puede inicializar ONTAP Mediator mediante System Manager o la CLI de ONTAP.

## System Manager

Con System Manager, puede configurar el servidor ONTAP Mediator para una conmutación automática al respaldo. También puede reemplazar SSL y CA autofirmados por el certificado SSL y CA validados de terceros si aún no lo ha hecho.

### Pasos

1. Vaya a **Protección > Descripción general > Mediator > Configurar**.
2. Seleccione **Agregar** e introduzca la siguiente información del servidor de ONTAP Mediator:
  - Dirección IPv4
  - Nombre de usuario
  - Contraseña
  - Certificado

### CLI

Puede inicializar el mediador de ONTAP desde el clúster primario o secundario mediante la CLI de ONTAP. Cuando emita el `mediator add` Comando en un clúster, el Mediator ONTAP se agrega automáticamente al otro clúster.

### Pasos

1. Inicialice Mediator en uno de los grupos:

```
snapmirror mediator add -mediator-address IP_Address -peer-cluster
cluster_name -username user_name
```

### ejemplo

```
cluster1::> snapmirror mediator add -mediator-address 192.168.10.1
-peer-cluster cluster2 -username mediatoradmin
Notice: Enter the mediator password.

Enter the password: *****
Enter the password again: *****
```

2. Compruebe el estado de la configuración del Mediator:

```
snapmirror mediator show
```

| Mediator Address | Peer Cluster | Connection Status | Quorum Status |
|------------------|--------------|-------------------|---------------|
| 192.168.10.1     | cluster-2    | connected         | true          |

Quorum Status Indica si las relaciones del grupo de coherencia SnapMirror se sincronizan con el mediador, un estado de `true` indica una sincronización correcta.

## Protección con SnapMirror Business Continuity

La configuración de la protección mediante SnapMirror Business Continuity implica seleccionar las LUN en el clúster de origen de ONTAP y añadirlas a un grupo de consistencia.

### Antes de empezar

- Debe tener un ["Licencia de SnapMirror Synchronous"](#).
- Debe ser un administrador de clústeres o máquinas virtuales de almacenamiento.
- Todos los volúmenes constituyentes de un grupo de coherencia deben estar en una única máquina virtual de almacenamiento (SVM).
  - Los LUN pueden residir en distintos volúmenes.
- Los clústeres de origen y destino no pueden ser los mismos.
- No es posible establecer relaciones de grupos de consistencia SM-BC entre clústeres de ASA y clústeres no-ASA.
- El espacio IP predeterminado es necesario por SM-BC para las relaciones de paridad de clústeres. No se admite el espacio IP personalizado.
- El nombre del grupo de coherencia debe ser único.
- Los volúmenes en el clúster secundario (de destino) deben ser del tipo DP.
- Las SVM principales y secundarias deben estar en una relación entre iguales.

### Pasos

Puede configurar un grupo de coherencia con la CLI de ONTAP o System Manager.

A partir de ONTAP 9.10.1, ONTAP ofrece un extremo y un menú de grupo de consistencia en System Manager, y ofrece utilidades de gestión adicionales. Si utiliza ONTAP 9.10.1 o posterior, consulte ["Configurar un grupo de consistencia"](#) a continuación ["configure la protección"](#) Para crear una relación SM-BC.

## System Manager

1. En el clúster principal, navegue hasta **Protección > Descripción general > Proteger para continuidad empresarial > Proteger LUN**.
2. Seleccione las LUN que desea proteger y añádalas a un grupo de protección.
3. Seleccione el clúster y la SVM de destino.
4. **La opción inicializar relación** está seleccionada de forma predeterminada. Haga clic en **Guardar** para comenzar la protección.
5. Vaya a **Consola > rendimiento** para verificar la actividad de IOPS de las LUN.
6. En el clúster de destino, utilice System Manager para comprobar que la protección de la relación de continuidad de negocio está sincronizada: **Protección > Relaciones**.

## CLI

1. Cree una relación de grupo de coherencia a partir del clúster de destino.  
``destination::> snapmirror create -source-path source-path -destination-path destination-path -cg-item -maps volume-paths -policy policy-name`

Puede asignar hasta 12 volúmenes constituyentes mediante el `cg-item-mappings` parámetro en la `snapmirror create` comando.

El siguiente ejemplo crea dos grupos de consistencia: `cg_src_` on the source with ``vol1 y. vol2` y un grupo de consistencia de destino de mirroring, `cg_dst`.

```
destination::> snapmirror create -source-path vs1_src:/cg/cg_src
-destination-path vs1_dst:/cg/cg_dst -cg-item-mappings
vol_src1:@vol_dst1,vol_src2:@vol_dst2 -policy AutomatedFailOver
```

2. Desde el clúster de destino, inicialice el grupo de coherencia.

```
destination::> snapmirror initialize -destination-path destination-
consistency-group
```

3. Confirme que la operación de inicialización se ha realizado correctamente. El estado debe ser InSync.

```
snapmirror show
```

4. En cada clúster, cree un igroup para poder asignar las LUN al iniciador en el host de la aplicación.  
`lun igroup create -igroup name -protocol fc|iscsi -ostype os -initiator initiator_name`
5. En cada clúster, asigne las LUN al igroup:

```
lun map -path path_name -igroup igroup_name
```

6. Compruebe que la asignación de LUN se ha completado correctamente con el `lun map` comando. Luego, puede detectar las nuevas LUN en el host de la aplicación.

## Gestión de SM-BC y protección de los datos

### Cree una copia Snapshot común

Además de las operaciones de copia de Snapshot programadas regularmente, puede crear un común de forma manual "[Copia Snapshot](#)". Entre los volúmenes del grupo de coherencia de SnapMirror primario y los volúmenes en el grupo de coherencia de SnapMirror secundario.

#### Acerca de esta tarea

- En ONTAP 9.8, el intervalo de creación de snapshot programado es de una hora.

A partir de ONTAP 9.9.1, ese intervalo es de 12 horas.

#### Antes de empezar

- La relación de grupo SnapMirror debe estar sincronizada.

#### Pasos

1. Cree una copia Snapshot común:

```
destination::>snapmirror update -destination-path vs1_dst:/cg/cg_dst
```

2. Supervise el progreso de la actualización:

```
destination::>snapmirror show -fields -newest-snapshot
```

### Realizar una conmutación al respaldo planificada

En una conmutación al respaldo planificada, debe cambiar los roles de los clústeres primario y secundario, de modo que el clúster secundario asuma el control del clúster principal. Durante una conmutación por error, lo que normalmente funciona el clúster secundario procesa las solicitudes de entrada y salida localmente sin interrumpir las operaciones del cliente.

Quizás desee realizar una conmutación al respaldo planificada para probar el estado de la configuración de recuperación de desastres o realizar tareas de mantenimiento del clúster principal.

#### Acerca de esta tarea

El administrador del clúster secundario inicia una conmutación al respaldo planificada. La operación requiere cambiar los roles primario y secundario de manera que el clúster secundario asuma el control del primario. Después, el nuevo clúster principal puede comenzar a procesar solicitudes de entrada y salida de forma local sin interrumpir las operaciones del cliente.

#### Antes de empezar

- La relación SM-BC debe estar sincronizada.
- No puede iniciar una conmutación al respaldo planificada cuando hay una operación no disruptiva en proceso. Las operaciones no disruptivas incluyen movimientos de volúmenes, reubicaciones de agregaciones y recuperación tras fallos de almacenamiento.
- El mediador ONTAP debe estar configurado, conectado y en quórum.

## Pasos

Puede realizar una conmutación al respaldo planificada con la interfaz de línea de comandos de ONTAP o System Manager.

### System Manager

1. En System Manager, seleccione **Protección > Descripción general > Relaciones**.
2. Identifique la relación de SM-BC que desea conmutar al nodo de respaldo. Junto a su nombre, seleccione la ... Junto al nombre de la relación, luego seleccione **Failover**.
3. Para supervisar el estado de la conmutación por error, utilice `snapmirror failover show` En la CLI de ONTAP.

### CLI

1. Desde el clúster de destino, inicie la operación de conmutación por error:

```
destination::>snapmirror failover start -destination-path
vs1_dst:/cg/cg_dst
```

2. Supervise el progreso de la conmutación por error:

```
destination::>snapmirror failover show
```

3. Una vez finalizada la operación de conmutación por error, puede supervisar el estado de la relación de protección de SnapMirror síncrono desde el destino:

```
destination::>snapmirror show
```

## Recuperarse de operaciones de conmutación al respaldo automáticas no planificadas

Una operación de conmutación por error no planificada automática (AUFO) se produce cuando el clúster primario está inactivo o aislado. El mediador ONTAP detecta cuándo se produce una conmutación por error y ejecuta una conmutación por error automática no planificada en el clúster secundario. El clúster secundario se convierte al principal y comienza a prestar servicio a los clientes. Esta operación se realiza sólo con la ayuda del Mediador ONTAP.



Después de la conmutación automática al respaldo no planificada, es importante volver a analizar las rutas de I/O del LUN del host para que no se pierda las rutas de I/O.


## Restablecer la relación de protección tras una conmutación al respaldo no planificada

Puede volver a establecer la relación de protección mediante System Manager o la CLI de ONTAP.



## System Manager

### Pasos

1. Vaya a **Protección > Relaciones** y espere a que el estado de la relación muestre "InSync".
2. Para reanudar las operaciones en el clúster de origen original, haga clic en  Y seleccione **Failover**.

### CLI

Puede supervisar el estado de la conmutación automática al respaldo no planificada mediante `snapmirror failover show` comando.

Por ejemplo:

```
ClusterB::> snapmirror failover show -instance
Start Time: 9/23/2020 22:03:29
 Source Path: vs1:/cg/scg3
Destination Path: vs3:/cg/dcg3
Failover Status: completed
 Error Reason:
 End Time: 9/23/2020 22:03:30
Primary Data Cluster: cluster-2
Last Progress Update: -
 Failover Type: unplanned
Error Reason codes: -
```

Consulte la "[Referencia EMS](#)" para obtener más información acerca de los mensajes de eventos y las acciones correctivas.

### Reanude la protección en una configuración ramificada después de una conmutación al nodo de respaldo

Si experimenta una conmutación al respaldo en el clúster secundario en la relación de SM-BC, el destino asíncrono de SnapMirror queda en mal estado. Debe restaurar manualmente la protección eliminando y volviendo a crear la relación con el extremo asíncrono de SnapMirror.

### Pasos

1. Compruebe que la conmutación por error se ha realizado correctamente:  
`snapmirror failover show`
2. En el extremo asíncrono de SnapMirror, elimine el extremo de dispersión:  
`snapmirror delete -destination-path destination_path`
3. En el tercer sitio, cree una relación asíncrona de SnapMirror entre el nuevo volumen primario de SM-BC y el volumen de destino de dispersión asíncrono:  
`snapmirror create -source-path source_path -destination-path destination_path -policy MirrorAllSnapshots -schedule schedule`
4. Resincronice la relación:  
`snapmirror resync -destination-path destination_path`
5. Verifique el estado y el estado de la relación:  
`snapmirror show`

## Supervisar las operaciones de continuidad del negocio de SnapMirror

Puede supervisar las siguientes operaciones de continuidad del negocio de SnapMirror (SM-BC) para garantizar el estado de la configuración de SM-BC:

- Mediador ONTAP
- Operaciones de conmutación por error planificadas
- Operaciones automáticas de conmutación al respaldo no planificadas
- Disponibilidad de SM-BC

### Mediador ONTAP

Durante las operaciones normales, el estado Mediador de ONTAP debe estar conectado. Si está en cualquier otro estado, esto puede indicar una condición de error. Puede revisar el ["Mensajes del sistema de gestión de eventos \(EMS\)"](#) para determinar el error y las acciones correctivas apropiadas.

### Operaciones de conmutación por error planificadas

Puede supervisar el estado y el progreso de una operación de conmutación al nodo de respaldo planificada mediante el `snapmirror failover show` comando. Por ejemplo:

```
ClusterB::> snapmirror failover start -destination-path vs1:/cg/dcg1
```

Una vez finalizada la operación de conmutación al nodo de respaldo, puede supervisar el estado de protección de SnapMirror síncrono desde el nuevo clúster de destino. Por ejemplo:

```
ClusterA::> snapmirror show
```

Consulte la ["Referencia EMS"](#) para obtener más información acerca de los mensajes de eventos y las acciones correctivas.

### Operaciones automáticas de conmutación al respaldo no planificadas

Durante una conmutación al respaldo automática no planificada, puede supervisar el estado de la operación mediante el `snapmirror failover show` comando.

```
ClusterB::> snapmirror failover show -instance
Start Time: 9/23/2020 22:03:29
 Source Path: vs1:/cg/scg3
 Destination Path: vs3:/cg/dcg3
 Failover Status: completed
 Error Reason:
 End Time: 9/23/2020 22:03:30
Primary Data Cluster: cluster-2
Last Progress Update: -
 Failover Type: unplanned
Error Reason codes: -
```

Consulte la "[Referencia EMS](#)" para obtener más información acerca de los mensajes de eventos y las acciones correctivas.

### Disponibilidad de SM-BC

Puede comprobar la disponibilidad de la relación SM-BC mediante una serie de comandos, ya sea en el clúster principal, el clúster secundario o ambos.

Entre los comandos que utiliza se incluyen los `snapmirror mediator show` comando en el clúster principal y secundario para comprobar la conexión y el estado de quórum, la `snapmirror show` y la `volume show` comando. Por ejemplo:

```

SMBC_A::*> snapmirror mediator show
Mediator Address Peer Cluster Connection Status Quorum Status

10.236.172.86 SMBC_B connected true

SMBC_B::*> snapmirror mediator show
Mediator Address Peer Cluster Connection Status Quorum Status

10.236.172.86 SMBC_A connected true

SMBC_B::*> snapmirror show -expand

Progress
Source Destination Mirror Relationship Total
Last
Path Type Path State Status Progress Healthy
Updated

vs0:/cg/cg1 XDP vs1:/cg/cg1_dp Snapmirrored InSync - true -
vs0:vol1 XDP vs1:vol1_dp Snapmirrored InSync - true -
2 entries were displayed.

SMBC_A::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1
vserver volume is-smbc-master is-smbc-failover-capable smbc-consensus

vs0 vol1 true false Consensus

SMBC_B::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1_dp
vserver volume is-smbc-master is-smbc-failover-capable smbc-consensus

vs1 vol1_dp false true No-consensus

```

### Añada o quite volúmenes a un grupo de coherencia

A medida que cambian los requisitos de carga de trabajo de la aplicación, es posible que deba añadir o quitar volúmenes de un grupo de coherencia para garantizar la continuidad del negocio. El proceso de añadir y quitar volúmenes en una relación de SM-BC activa depende de la versión de ONTAP que utilice.

En la mayoría de los casos, este es un proceso disruptivo que requiere que se rompa la relación de SnapMirror, se modifique el grupo de consistencia y, a continuación, se reanude la protección. A partir de ONTAP 9.13.1, añadir volúmenes a un grupo de coherencia con una relación de SM-BC activa es una operación no disruptiva.

### Acerca de esta tarea

- En ONTAP 9,8 a 9,9.1, es posible añadir o quitar volúmenes a un grupo de consistencia mediante la CLI de ONTAP.
- A partir de ONTAP 9.10.1, se recomienda que los gestione ["grupos de consistencia"](#) A través de System Manager o con la API DE REST de ONTAP.

Si desea cambiar la composición del grupo de coherencia. Para ello, añada o quite un volumen, primero debe eliminar la relación original y, a continuación, volver a crear el grupo de coherencia con la nueva composición.

- A partir de ONTAP 9.13.1, se pueden añadir volúmenes a un grupo de coherencia con una relación de SM-BC activa desde el origen o el destino.

Eliminar volúmenes es una operación disruptiva. Debe interrumpir la relación de SnapMirror antes de continuar eliminando los volúmenes.

## ONTAP 9,8-9.13.0

### Antes de empezar

- No puede comenzar a modificar el grupo de consistencia mientras está en la InSync estado.
- El volumen de destino debe ser del tipo DP.
- El nuevo volumen que añada para expandir el grupo de coherencia debe tener un par de copias de Snapshot comunes entre los volúmenes de origen y de destino.

### Pasos

Los ejemplos que se muestran en dos asignaciones de volúmenes: `vol_src1 ↔ vol_dst1` y..  
`vol_src2 ↔ vol_dst2`, en una relación de grupo de coherencia entre los puntos finales  
`vs1_src:/cg/cg_src` y..`vs1_dst:/cg/cg_dst`.

1. En los clústeres de origen y destino, compruebe que hay una Snapshot común entre los clústeres de origen y destino con el comando `snapshot show -vserver svm_name -volume volume_name -snapshot snapmirror`

```
source::>snapshot show -vserver vs1_src -volume vol_src3 -snapshot
snapmirror*
```

```
destination::>snapshot show -vserver vs1_dst -volume vol_dst3 -snapshot
snapmirror*
```

2. Si no existe ninguna copia Snapshot común, cree e inicialice una relación de SnapMirror de FlexVol:

```
destination::>snapmirror initialize -source-path vs1_src:vol_src3
-destination-path vs1_dst:vol_dst3
```

3. Elimine la relación del grupo de consistencia:

```
destination::>snapmirror delete -destination-path vs1_dst:vol_dst3
```

4. Libere la relación de SnapMirror de origen y conserve las copias Snapshot comunes:

```
source::>snapmirror release -relationship-info-only true -destination-path
vs1_dst:vol_dst3
```

5. Desasigne las LUN y elimine la relación de grupo de consistencia existente:

```
destination::>lun mapping delete -vserver vs1_dst -path <lun_path> -igroup
<igroup_name>
```



Se anula la asignación de las LUN de destino, mientras que las LUN de la copia principal siguen sirviendo la I/O del host

```
destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst
```

```
source::>snapmirror release -destination-path vs1_dst:/cg/cg_dst
-relationship-info-only true
```

6. Si está utilizando ONTAP 9.10.1 a 9.13.0, elimine y recree y el grupo de consistencia en la fuente

con la composición correcta. Siga los pasos de [Eliminar un grupo de consistencia](#) y después [Configure un único grupo de consistencia](#). En ONTAP 9.10.1 y versiones posteriores, debe realizar las operaciones de eliminación y creación en System Manager o con la API DE REST de ONTAP; no existe un procedimiento de la CLI.

**Si está utilizando ONTAP 9.8, 9.0 o 9.9.1, vaya al paso siguiente.**

7. Cree el nuevo grupo de consistencia en el destino con la nueva composición:

```
destination::>snapmirror create -source-path vs1_src:/cg/cg_src
-destination-path vs1_dst:/cg/cg_dst -cg-item-mappings vol_src1:@vol_dst1,
vol_src2:@vol_dst2, vol_src3:@vol_dst3
```

8. Resincronice la relación del grupo de consistencia de objetivo de tiempo de recuperación cero para garantizar que está sincronizada:

```
destination::>snapmirror resync -destination-path vs1_dst:/cg/cg_dst
```

9. Reasigne las LUN no asignadas en el paso 5:

```
destination::> lun map -vserver vs1_dst -path lun_path -igroup igroup_name
```


10. Vuelva a analizar las rutas de I/O del LUN del host para restaurar todas las rutas a los LUN.

### ONTAP 9.13.1 y versiones posteriores

A partir de ONTAP 9.13.1, es posible añadir volúmenes de forma no disruptiva a un grupo de coherencia con una relación de SM-BC activa. SM-BC admite la adición de volúmenes de origen y destino.

Para obtener detalles sobre cómo añadir volúmenes del grupo de coherencia de origen, consulte [Modificar un grupo de consistencia](#).

### Añada un volumen desde el clúster de destino

1. En el clúster de destino, seleccione **Protección > Relaciones**.
2. Busque la relación de SM-BC a la que desea añadir volúmenes. Seleccione  Luego **Expandir**.
3. Seleccione las relaciones de volumen cuyos volúmenes se añadirán al grupo de coherencia
4. Seleccione **Expandir**.

## Convertir relaciones existentes en relaciones SM-BC

Si tiene una relación de SnapMirror síncrono entre un clúster de origen y de destino, puede convertirlo en una relación de SM-BC. De este modo, se pueden asociar los volúmenes reflejados a un grupo de coherencia, garantizando un objetivo de punto de recuperación cero en una carga de trabajo de varios volúmenes. Además, puede conservar los snapshots de SnapMirror existentes si necesita revertir a un momento específico antes de establecer la relación SM-BC.

### Antes de empezar

- Debe haber una relación de SnapMirror síncrono con un objetivo de punto de recuperación cero entre el clúster primario y el secundario.
- Se deben anular la asignación de todas las LUN del volumen de destino antes de crear la relación de

SnapMirror con objetivo de tiempo de recuperación cero.

- SM-BC solo admite protocolos SAN (no NFS/CIFS). Asegúrese de que no hay ningún componente del grupo de consistencia montado para el acceso NAS.

#### Acerca de esta tarea

- Debe ser un administrador de clústeres y de SVM en los clústeres principales y secundarios.
- No se puede convertir un objetivo de punto de recuperación de cero en una sincronización de objetivo de tiempo de recuperación de cero cambiando la política de SnapMirror.
- Debe asegurarse de quitar la asignación de las LUN antes de emitir el `snapmirror create` comando.

Si las LUN existentes en el volumen secundario se asignan y el AutomatedFailover la política se configura, la `snapmirror create` desencadenará un error.

#### Pasos

1. Desde el clúster secundario, realice una actualización de SnapMirror en la relación existente:

```
destination::>snapmirror update -destination-path vs1_dst:vol1
```

2. Compruebe que la actualización de SnapMirror se ha realizado correctamente:

```
destination::>snapmirror show
```

3. Desactive cada una de las relaciones síncronas de RPO cero:

```
destination::>snapmirror quiesce -destination-path vs1_dst:vol1
```

```
destination::>snapmirror quiesce -destination-path vs1_dst:vol2
```

4. Elimine cada una de las relaciones síncronas de RPO cero:

```
destination::>snapmirror delete -destination-path vs1_dst:vol1
```

```
destination::>snapmirror delete -destination-path vs1_dst:vol2
```

5. Libere la relación de SnapMirror de origen, pero conserve las copias Snapshot comunes:

```
source::>snapmirror release -relationship-info-only true -destination-path
vs1_dst:vol1
```

```
source::>snapmirror release -relationship-info-only true -destination-path
vs1_dst:vol2
```

6. Cree un objetivo de tiempo de recuperación cero para grupo relación de SnapMirror síncrono:

```
destination::> snapmirror create -source-path vs1_src:/cg/cg_src -destination
-path vs1_dst:/cg/cg_dst -cg-item-mappings vol1:@vol1,vol2:@vol2 -policy
AutomatedFailover
```

7. Resincronice el grupo de consistencia:

```
destination::> snapmirror resync -destination-path vs1_dst:/cg/cg_dst
```



8. Vuelva a analizar las rutas de I/O del LUN del host para restaurar todas las rutas a los LUN.

## Actualice y revierta ONTAP con SM-BC

La continuidad del negocio con SnapMirror (SM-BC) es compatible a partir de ONTAP 9,8. Actualizar y revertir el clúster de ONTAP tiene implicaciones en su relación SM-BC dependiendo de la versión de ONTAP a la que actualice o revierta.

### Actualice ONTAP con SM-BC

Para usar SM-BC, todos los nodos de los clústeres de origen y destino deben ejecutar ONTAP 9,8 o una versión posterior.

Al actualizar ONTAP con relaciones activas de SM-BC, debe utilizar [Actualización automatizada no disruptiva \(ANDU\)](#). El uso de ANDU garantiza que sus relaciones de SM-BC estén sincronizadas y en buen estado durante el proceso de actualización.

No hay pasos de configuración para preparar las implementaciones de SM-BC para las actualizaciones de ONTAP. Sin embargo, se recomienda que antes y después de la actualización, compruebe que:

- Las relaciones de SM-BC están sincronizadas.
- No hay errores relacionados con SnapMirror en el registro de eventos.
- El Mediador está en línea y en buen estado desde ambos clusters.
- Todos los hosts pueden ver todas las rutas correctamente para proteger los LUN.



Cuando se actualizan clústeres de ONTAP 9,8 o 9.9.1 a ONTAP 9.10.1 y versiones posteriores, ONTAP crea nuevos [grupos de consistencia](#) En los clústeres de origen y de destino para las relaciones de SM-BC que se pueden configurar mediante System Manager.



La `snapmirror quiesce` y `snapmirror resume` Los comandos no son compatibles con SM-BC.

### Vuelva a ONTAP 9.9.1 desde ONTAP 9.10.1

Para revertir las relaciones de la versión 9.10.1 a la 9.9.1, deben eliminarse las relaciones de SM-BC, seguido por la instancia del grupo de consistencia 9.10.1. Los grupos de consistencia con una relación de SM-BC activa no se pueden eliminar. Todos los volúmenes de FlexVol que se hayan actualizado a 9.10.1 asociados previamente con otro contenedor inteligente o aplicación empresarial en la versión 9.9.1 o anterior ya no se asociarán al revertir. Al eliminar grupos de consistencia no se eliminan los volúmenes constituyentes ni las snapshots granulares de volúmenes. Consulte ["Eliminar un grupo de consistencia"](#) Para obtener más información sobre esta tarea en ONTAP 9.10.1 y versiones posteriores.

### Vuelva a ONTAP 9,7 desde ONTAP 9,8



SM-BC no es compatible con clústeres mixtos de ONTAP 9.7 y ONTAP 9.8.

Al cambiar de ONTAP 9.8 a ONTAP 9.7, debe tener en cuenta lo siguiente:

- Si el clúster aloja un destino de SM-BC, no se permite revertir a ONTAP 9,7 hasta que se rompa y se elimine la relación.

- Si el clúster aloja un origen de SM-BC, no se permite revertir a ONTAP 9.7 hasta que se libere la relación.
- Todas las políticas personalizadas de SM-BC SnapMirror creadas por el usuario deben eliminarse antes de revertir a ONTAP 9.7.

Para cumplir estos requisitos, consulte ["Quitar una configuración de SM-BC"](#).

## Pasos

1. Realice una comprobación de reversión desde uno de los clústeres de la relación de SM-BC:

```
cluster::*> system node revert-to -version 9.7 -check-only
```

Ejemplo:

```
cluster::*> system node revert-to -version 9.7 -check-only
Error: command failed: The revert check phase failed. The following
issues must be resolved before revert can be completed. Bring the data
LIFs down on running vservers. Command to list the running vservers:
vserver show -admin-state running Command to list the data LIFs that are
up: network interface show -role data -status-admin up Command to bring
all data LIFs down: network interface modify {-role data} -status-admin
down
Disable snapshot policies.
 Command to list snapshot policies: "snapshot policy show".
 Command to disable snapshot policies: "snapshot policy modify
-vserver
 * -enabled false"

 Break off the initialized online data-protection (DP) volumes and
delete
 Uninitialized online data-protection (DP) volumes present on the
local
 node.
 Command to list all online data-protection volumes on the local
node:
 volume show -type DP -state online -node <local-node-name>
 Before breaking off the initialized online data-protection volumes,
quiesce and abort transfers on associated SnapMirror relationships
and
 wait for the Relationship Status to be Quiesced.
 Command to quiesce a SnapMirror relationship: snapmirror quiesce
 Command to abort transfers on a SnapMirror relationship: snapmirror
abort
 Command to see if the Relationship Status of a SnapMirror
relationship
 is Quiesced: snapmirror show
 Command to break off a data-protection volume: snapmirror break
 Command to break off a data-protection volume which is the
```

```

destination
 of a SnapMirror relationship with a policy of type "vault":
snapmirror
 break -delete-snapshots
 Uninitialized data-protection volumes are reported by the
"snapmirror
 break" command when applied on a DP volume.
 Command to delete volume: volume delete

Delete current version snapshots in advanced privilege level.
 Command to list snapshots: "snapshot show -fs-version 9.8"
 Command to delete snapshots: "snapshot prepare-for-revert -node
<nodename>"

Delete all user-created policies of the type active-strict-sync-
mirror
and active-sync-mirror.
The command to see all active-strict-sync-mirror and active-sync-
mirror
type policies is:
 snapmirror policy show -type
 active-strict-sync-mirror,active-sync-mirror
The command to delete a policy is :
 snapmirror policy delete -vserver <SVM-name> -policy <policy-name>

```

Para obtener información sobre cómo revertir los clústeres, consulte ["Revierte ONTAP"](#).

## Quitar una configuración de SM-BC

Si ya no necesita protección SnapMirror sincronizada con un objetivo de tiempo de recuperación cero, puede eliminar su relación SM-BC.

### Acerca de esta tarea

- Antes de eliminar la relación SM-BC, se debe quitar la asignación de todas las LUN del clúster de destino.
- Una vez que se anula la asignación de las LUN y se vuelve a analizar el host, el destino SCSI notifica a los hosts que ha cambiado el inventario de LUN. Las LUN existentes en los volúmenes secundarios con objetivo de tiempo de recuperación cero cambian para reflejar una identidad nueva después de eliminar la relación con objetivo de tiempo de recuperación cero. Los hosts detectan los LUN del volumen secundario como nuevos LUN que no tienen relación con los LUN del volumen de origen.
- Los volúmenes secundarios permanecen en los volúmenes de recuperación ante desastres una vez que se elimina la relación. Puede emitir el `snapmirror break` comando para convertirlos a lectura/escritura.
- No se permite eliminar la relación en el estado fallido cuando no se invierte la relación.

### Pasos

1. En el clúster secundario, quite la relación del grupo de consistencia de SM-BC entre el extremo de origen y el extremo de destino:

```
destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst
```

2. En el clúster principal, liberar la relación del grupo de consistencia y las copias Snapshot creadas para la relación:

```
source::>snapmirror release -destination-path vs1_dst:/cg/cg_dst
```

3. Realice una detección repetida del host para actualizar el inventario de LUN.
4. A partir de ONTAP 9.10.1, al eliminar la relación SnapMirror no se elimina el grupo de consistencia. Si desea eliminar el grupo de coherencia, debe usar System Manager o la API DE REST de ONTAP. Consulte [Eliminar un grupo de consistencia](#) si quiere más información.

## Retire el Mediador ONTAP

Si desea eliminar una configuración de Mediador ONTAP existente de los clústeres de ONTAP, puede hacerlo mediante el `snapmirror mediator remove` comando.

### Pasos

1. Eliminar Mediador ONTAP:

```
snapmirror mediator remove -mediator-address 12.345.678.90 -peer-cluster
cluster_xyz
```

## Solucionar problemas

### Se produce un error en la operación de eliminación de SnapMirror en estado de takeover

#### Tema:

Cuando se instala ONTAP 9.9.1 en un clúster, se ejecuta el `snapmirror delete` Error del comando cuando la relación del grupo de consistencia SM-BC se encuentra en estado de toma de control.

```
C2_cluster::> snapmirror delete vs1:/cg/dd
```

```
Error: command failed: RPC: Couldn't make connection
```

#### Solución

Cuando los nodos de una relación SM-BC se encuentran en estado de toma de control, realice la operación de eliminación y lanzamiento de SnapMirror con la opción "-force" establecida en true.

```
C2_cluster::> snapmirror delete vs1:/cg/dd -force true

Warning: The relationship between source "vs0:/cg/ss" and destination
 "vs1:/cg/dd" will be deleted, however the items of the
destination
 Consistency Group might not be made writable, deletable, or
modifiable
 after the operation. Manual recovery might be required.
Do you want to continue? {y|n}: y
Operation succeeded: snapmirror delete for the relationship with
destination "vs1:/cg/dd".
```

## Error al crear una relación de SnapMirror e inicializar el grupo de consistencia

### Tema:

Se produce un error en la creación de la relación de SnapMirror y en la inicialización del grupo de consistencia.

### Solución:


Asegúrese de no haber superado el límite de grupos de consistencia por clúster. Los límites de los grupos de consistencia en SM-BC son independientes de la plataforma y difieren en función de la versión de ONTAP. Consulte ["Restricciones y limitaciones adicionales"](#) Para limitaciones basadas en la versión de ONTAP.

### Error

Si el grupo de consistencia está inicializando, compruebe el estado de sus inicializaciones de grupo de consistencia con la API REST de ONTAP, System Manager o el comando `sn show -expand`.

### Solución:

Si los grupos de consistencia no se inician, elimine la relación SM-BC, elimine el grupo de consistencia y luego vuelva a crear la relación e inicializarla. Este flujo de trabajo varía en función de la versión de ONTAP que se utilice.

| Si utiliza ONTAP 9.8-9.9.1                                                                                                                                                                                                                              | Si utiliza ONTAP 9.10.1 o una versión posterior                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ol style="list-style-type: none"> <li>1. <a href="#">"Retire la configuración de SM-BC"</a></li> <li>2. <a href="#">"Cree una relación de grupo de coherencia"</a></li> <li>3. <a href="#">"Inicie la relación del grupo de coherencia"</a></li> </ol> | <ol style="list-style-type: none"> <li>1. En <b>Protección &gt; Relaciones</b>, encuentre la relación SM-BC en el grupo de consistencia. Seleccione , Luego <b>Eliminar</b> para eliminar la relación SM-BC.</li> <li>2. <a href="#">"Elimine el grupo de consistencia"</a></li> <li>3. <a href="#">"Configure el grupo de consistencia"</a></li> </ol> |

## Conmutación al nodo de respaldo planificada incorrecta

### Tema:

Después de ejecutar el `snapmirror failover start` comando, el resultado del `snapmirror failover show` el comando muestra un mensaje que indica que hay

una operación no disruptiva en curso.

```
Cluster1::> snapmirror failover show
Source Destination Error
Path Path Type Status start-time end-time Reason

vs1:/cg/cg vs0:/cg/cg planned failed 10/1/2020 10/1/2020 SnapMirror
Failover cannot start because a volume move is running. Retry the command
once volume move has finished.
08:35:04 08:35:04
```

**Causa:**

Una conmutación al respaldo planificada no puede comenzar cuando exista una operación no disruptiva en curso, incluyendo el movimiento de volúmenes, la reubicación de agregados y la conmutación al respaldo de almacenamiento.

**Solución:**

Se debe esperar a que finalice la operación no disruptiva y volver a intentar la operación de conmutación al nodo de respaldo.

**No se puede acceder a mediador ONTAP o el estado del quórum de mediador es FALSE**

**Tema:**

Después de ejecutar el `snapmirror failover start` comando, el resultado del `snapmirror failover show` Comando muestra un mensaje que indica que Mediator no está configurado.

Consulte "[Inicialice el Mediador ONTAP](#)".

```
Cluster1::> snapmirror failover show
Source Destination Error
Path Path Type Status start-time end-time Reason

vs0:/cg/cg vs1:/cg/cg planned failed 10/1/2020 10/1/2020 SnapMirror
failover cannot start because the source-side precheck failed. reason:
Mediator not configured.
05:50:42 05:50:43
```

**Causa:**

Mediador no está configurado o existen problemas de conectividad de red.

**Solución:**

Si el Mediador ONTAP no está configurado, debe configurar el Mediador ONTAP antes de poder establecer una relación SM-BC. Solucione cualquier problema de conectividad de red. Asegúrese de que Mediator está conectado y que el estado de quórum es verdadero en el sitio de origen y de destino mediante el comando

snapmirror mediator show. Para obtener más información, consulte [Configure el Mediador ONTAP](#).

```
cluster::> snapmirror mediator show
Mediator Address Peer Cluster Connection Status Quorum Status

10.234.10.143 cluster2 connected true
```

## Recuperación tras fallos no planificada automática no activada en el sitio B

### Tema:

Un error en el sitio A no activa una conmutación por error no planificada en el sitio B.

### Causa posible n.o 1:

El Mediador ONTAP no está configurado. Para determinar si esta es la causa, emita el `snapmirror mediator show` Comando en el clúster del sitio B.

```
Cluster2::*> snapmirror mediator show
This table is currently empty.
```

Este ejemplo indica que ONTAP Mediator no está configurado en el sitio B.

### Solución:

Asegúrese de que ONTAP Mediator está configurado en ambos clusters, que el estado es Conectado y que el quórum está definido en Verdadero.

### Posible causa n.o 2:

El grupo de consistencia de SnapMirror no está sincronizado. Para determinar si esta es la causa, consulte el registro de eventos para ver si el grupo de consistencia estaba sincronizado durante el momento en el que se produjo un error en el sitio.

```
cluster::*> event log show -event *out.of.sync*

Time Node Severity Event

10/1/2020 23:26:12 sti42-vsims-ucs511w ERROR sms.status.out.of.sync:
Source volume "vs0:zrto_cg_556844_511u_RW1" and destination volume
"vs1:zrto_cg_556881_511w_DP1" with relationship UUID "55ab7942-03e5-11eb-
ba5a-005056a7dc14" is in "out-of-sync" status due to the following reason:
"Transfer failed."
```

### Solución:

Realice los pasos siguientes para realizar una conmutación por error forzada en el sitio B.

1. Desasigne todas las LUN que pertenecen al grupo de consistencia desde el sitio B.

2. Elimine la relación del grupo de coherencia SnapMirror mediante `force` opción.
3. Introduzca el `snapmirror break` Comando en los volúmenes constituyentes del grupo de coherencia para convertir volúmenes de DP a R/W para habilitar I/o del sitio B.
4. Arranque los nodos del sitio A para crear una relación de objetivo de tiempo de recuperación cero desde el sitio B al sitio A.
5. Libere el grupo de consistencia con `relationship-info-only` En el sitio A para conservar una copia Snapshot común y desasignar las LUN que pertenecen al grupo de consistencia.
6. Convierta los volúmenes en el sitio A de R/W a DP mediante la configuración de una relación de nivel de volumen con la política de sincronización o la política asíncrona.
7. Emita el `snapmirror resync` para sincronizar las relaciones.
8. Elimine las relaciones de SnapMirror con la política de sincronización en el sitio A.
9. Libere las relaciones de SnapMirror con la política de Sync mediante `relationship-info-only true` En el sitio B.
10. Cree una relación de grupo de consistencia del Sitio B al Sitio A.
11. Realice una resincronización del grupo de consistencia del sitio A y, a continuación, compruebe que el grupo de consistencia está sincronizado.
12. Vuelva a analizar las rutas de I/o del LUN del host para restaurar todas las rutas a los LUN.

#### **Enlace entre el sitio B y el mediador caído y el sitio A caído**

Para comprobar la conexión del Mediador ONTAP, utilice el `snapmirror mediator show` comando. Si el estado de conexión es inaccesible y el sitio B no puede acceder al sitio A, tendrá una salida similar a la que se muestra a continuación. Siga los pasos de la solución para restaurar la conexión



```

cluster::*> snapmirror mediator show
Mediator Address Peer Cluster Connection Status Quorum Status

10.237.86.17 C1_cluster unreachable true
SnapMirror consistency group relationship status is out of sync.

C2_cluster::*> snapmirror show -expand
Source Destination Mirror Relationship Total
Last
Path Type Path State Status Progress Healthy
Updated

vs0:/cg/src_cg_1 XDP vs1:/cg/dst_cg_1 Snapmirrored OutOfSync - false -
vs0:zrto_cg_655724_188a_RW1 XDP vs1:zrto_cg_655755_188c_DP1 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655733_188a_RW2 XDP vs1:zrto_cg_655762_188c_DP2 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655739_188b_RW1 XDP vs1:zrto_cg_655768_188d_DP1 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655748_188b_RW2 XDP vs1:zrto_cg_655776_188d_DP2 Snapmirrored
OutOfSync - false -
5 entries were displayed.

Site B cluster is unable to reach Site A.
C2_cluster::*> cluster peer show
Peer Cluster Name Cluster Serial Number Availability
Authentication

C1_cluster 1-80-000011 Unavailable ok

```

## Solución

Forzar una conmutación al respaldo para habilitar la I/O en el sitio B y, a continuación, establecer una relación de objetivo de tiempo de recuperación cero en el sitio B al sitio A. Realice los pasos siguientes para realizar una conmutación por error forzada en el sitio B.

1. Desasigne todas las LUN que pertenecen al grupo de consistencia desde el sitio B.
2. Elimine la relación del grupo de coherencia SnapMirror con la opción force.
3. Introduzca el comando `snapmirror break` (`snapmirror break -destination_path svm:_volume_`) En los volúmenes constituyentes del grupo de coherencia para convertir volúmenes de DP a RW, para habilitar I/O del sitio B.

Debe emitir el comando `snapmirror break` para cada relación del grupo de coherencia. Por ejemplo, si hay tres volúmenes en el grupo de coherencia, emitirá el comando para cada volumen.

4. Arranque los nodos del sitio A para crear una relación de objetivo de tiempo de recuperación cero desde el sitio B al sitio A.
5. Libere el grupo de consistencia con Relationship-info-only en el sitio A para conservar una copia Snapshot común y desasignar las LUN que pertenecen al grupo de consistencia.
6. Convierta los volúmenes en el sitio A de RW a DP configurando una relación de nivel de volumen mediante una política de sincronización o una política asíncrona.
7. Emita el `snapmirror resync` comando para sincronizar las relaciones.
8. Elimine las relaciones de SnapMirror con la política de sincronización en el sitio A.
9. Lance las relaciones de SnapMirror con la política Sync mediante la relación-info-only true en el sitio B.
10. Cree una relación de grupo de consistencia entre el sitio B y el sitio A.
11. En el clúster de origen, resincronice el grupo de consistencia. Compruebe que el estado del grupo de consistencia esté sincronizado.
12. Vuelva a analizar las rutas de I/O del LUN del host para restaurar todas las rutas a las LUN.

### Enlace entre el sitio A y el mediador caído y el sitio B caído

Cuando use SM-BC, puede perder la conectividad entre ONTAP Mediator o sus clústeres con conexión entre iguales. Puede diagnosticar el problema comprobando la conexión, la disponibilidad y el estado de consenso de las diferentes partes de la relación SM-BC y, a continuación, reanudando la conexión con fuerza.

| Qué comprobar                        | Comando CLI                                                 | Indicador                                                                      |
|--------------------------------------|-------------------------------------------------------------|--------------------------------------------------------------------------------|
| Mediador del Sitio A                 | <code>snapmirror mediator show</code>                       | El estado de la conexión será <code>unreachable</code>                         |
| Conectividad del centro B.           | <code>cluster peer show</code>                              | Se ofrecerá disponibilidad <code>unavailable</code>                            |
| Estado de consenso del volumen SM-BC | <code>volume show volume_name -fields smbc-consensus</code> | La <code>sm-bc consensus</code> el campo leerá <code>Awaiting-consensus</code> |

Para obtener información adicional acerca del diagnóstico y la resolución de este problema, consulte el artículo de la base de conocimientos ["Enlace entre el Sitio A y el Mediador abajo y el Sitio B inactivo al utilizar SM-BC"](#).

**Se produce un error en la operación de eliminación de SM-BC de SnapMirror cuando se establece la cerca en el volumen de destino**

**Tema:**

Se produce un error en la operación de eliminación de SnapMirror cuando alguno de los volúmenes de destino tiene un conjunto de cerca de redirección.

### Solución

Realizar las siguientes operaciones para volver a intentar la redirección y eliminar la cerca del volumen de destino.

- Resincronización de SnapMirror
- Actualización de SnapMirror

## La operación de movimiento de volúmenes se atasca cuando la opción primaria está inactiva

### Tema:

Una operación de movimiento de volumen se bloquea indefinidamente en un estado de transposición diferida cuando el sitio primario está inactivo en una relación de SM-BC. Cuando el sitio primario está inactivo, el sitio secundario realiza una conmutación por error automática no planificada (AUFO). Cuando hay una operación de movimiento de volumen en curso cuando se activa el AUFO, el movimiento de volumen se queda atascado.

### Solución:

Cancele la instancia de movimiento de volumen que está bloqueada y reinicie la operación de movimiento de volumen.

## Se produce un error en la versión de SnapMirror cuando no se puede eliminar la copia de Snapshot

### Tema:

Se produce un error en la operación de versión de SnapMirror cuando no se puede eliminar la copia de Snapshot.

### Solución:

La copia Snapshot contiene una etiqueta transitoria. Utilice la `snapshot delete` con el `-ignore-owners` Opción para quitar la copia Snapshot puntual.

```
snapshot delete -volume <volume_name> -snapshot <snapshot_name> -ignore-owners true -force true
```

Vuelva a intentar el `snapmirror release` comando.

## La copia Snapshot de referencia de traslado de volúmenes se muestra como la más reciente

### Tema:

Después de ejecutar una operación de movimiento de volumen en un volumen de grupo de coherencia, la copia de Snapshot de referencia para movimiento de volumen puede aparecer como la más reciente de la relación de SnapMirror.

Puede ver la copia Snapshot más reciente con el siguiente comando:

```
snapmirror show -fields newest-snapshot status -expand
```

### Solución:

Realizar manualmente un `snapmirror resync` también puede esperar a la próxima operación de resincronización automática una vez que finalice la operación de movimiento de volumen.

## Servicio mediador para la continuidad empresarial de MetroCluster y SnapMirror

## Descripción general de ONTAP Mediator

El Mediador ONTAP proporciona varias funciones para las funciones de ONTAP:

- Proporciona un almacén persistente y cercado para metadatos de alta disponibilidad.
- Funciona como proxy ping para la vida útil de la controladora.
- Proporciona funcionalidad de consulta de estado de nodo síncrono para ayudar a determinar el quórum.

ONTAP Mediator proporciona dos servicios adicionales de systemctl:

- **ontap\_mediator.service**

Mantiene el servidor API REST para gestionar las relaciones ONAP.

- **mediator-scst.service**

Controla el inicio y el apagado del módulo iSCSI (SCST).

## Herramientas proporcionadas para el administrador del sistema

Herramientas proporcionadas para el administrador del sistema:

- **/usr/local/bin/mediator\_change\_password**

Establece una nueva contraseña de API cuando se proporcionan el nombre de usuario y la contraseña actuales de la API.

- **/usr/local/bin/mediator\_change\_user**

Establece un nuevo nombre de usuario de API cuando se proporcionan el nombre de usuario y la contraseña actuales de la API.

- **/usr/local/bin/mediator\_generate\_support\_bundle**

Genera un archivo tgz local con toda la información de soporte útil necesaria para la comunicación con el soporte al cliente de NetApp. Esto incluye la configuración de la aplicación, los registros y cierta información del sistema. Los paquetes se generan en el disco local y se pueden transferir manualmente, según sea necesario. Ubicación de almacenamiento: /Opt/netapp/data/support\_bundles/

- **/usr/local/bin/uninstall\_ontap\_mediator**

Elimina el paquete ONTAP Mediator y el módulo del núcleo SCST. Esto incluye todos los datos de configuración, registros y buzón de correo.

- **/usr/local/bin/mediator\_unlock\_user**

Libera un bloqueo en la cuenta de usuario de la API si se alcanzó el límite de reintentos de autenticación. Esta función se utiliza para evitar la derivación de contraseña de fuerza bruta. Solicita al usuario el nombre de usuario y la contraseña correctos.

- **/usr/local/bin/mediator\_add\_user**

(Solo soporte) Se utiliza para agregar el usuario de la API durante la instalación.

## Notas especiales

ONTAP Mediator confía en SCST para proporcionar iSCSI (consulte <http://scst.sourceforge.net/index.html>). Este paquete es un módulo del núcleo que se compila durante la instalación específicamente para el núcleo. Es posible que cualquier actualización del núcleo requiera la reinstalación de SCST. Como alternativa, desinstale y vuelva a instalar ONTAP Mediator y, a continuación, vuelva a configurar la relación ONTAP.



Cualquier actualización del kernel del sistema operativo del servidor se debe coordinar con una ventana de mantenimiento de ONTAP.

## Novedades del Mediador ONTAP

En cada versión se incluyen nuevas mejoras del Mediador de ONTAP. Esto es lo nuevo.

### Mejoras

| Versión de ONTAP Mediator | Mejoras                                                                                                                                                                                                                                             |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1,7                       | <ul style="list-style-type: none"><li>• Compatibilidad con RHEL 8,5, 8,6, 8,7, 8,8, 8,9, 9,0, 9,1, 9,2 y 9,3</li><li>• Compatibilidad con Rocky Linux 8 y 9</li></ul>                                                                               |
| 1,6                       | <ul style="list-style-type: none"><li>• Actualizaciones de Python 3,9.</li><li>• Compatibilidad con RHEL 8,4-8,8, 9,0-9,2, Rocky Linux 8 y 9.</li><li>• Interrupción del soporte para RHEL 7.x / CentOS todas las versiones.</li></ul>              |
| 1,5                       | <ul style="list-style-type: none"><li>• Optimiza la velocidad para sistemas SMBC a gran escala.</li><li>• Firma de código criptográfico añadida al instalador.</li><li>• Incluye advertencias de amortización para RHEL 7.x / CentOS 7.x.</li></ul> |
| 1,4                       | <ul style="list-style-type: none"><li>• Compatibilidad con RHEL 8,4 y 8,5.</li><li>• Incluye SCST versión 3,6.0.</li><li>• Se ha añadido soporte para Secure Boot (SB) del firmware basado en UEFI.</li></ul>                                       |
| 1,3                       | <ul style="list-style-type: none"><li>• Compatibilidad con RHEL/CentOS 8,2 y 8,3.</li><li>• Incluye SCST versión 3,5.0.</li></ul>                                                                                                                   |
| 1,2                       | <ul style="list-style-type: none"><li>• Compatibilidad con buzones HTTPS.</li><li>• Para uso con ONTAP 9,8+ MCC-IP AUSO y SM-BC ZRTO.</li><li>• Incluye SCST versión 3,4.0.</li></ul>                                                               |
| 1,1                       | <ul style="list-style-type: none"><li>• Compatibilidad con RHEL/CentOS 7,6, 7,7, 8,0 y 8,1.</li><li>• Elimina las dependencias de Perl.</li><li>• Incluye SCST versión 3,4.0.</li></ul>                                                             |

|     |                                                                                                                                                                                                |
|-----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1,0 | <ul style="list-style-type: none"> <li>• Compatibilidad con buzones de correo iSCSI.</li> <li>• Para uso con ONTAP 9,7+ MCC-IP AUSO.</li> <li>• Compatibilidad con RHEL/CentOS 7,6.</li> </ul> |
|-----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Matriz de compatibilidad de SO

| OS for<br>ONTAP<br>Mediator | 1,7      | 1,6      | 1,5 | 1,4 | 1,3 | 1,2       | 1,1 | 1,0            |
|-----------------------------|----------|----------|-----|-----|-----|-----------|-----|----------------|
| 7,6                         | Obsoleto | Obsoleto | Sí  | Sí  | Sí  | Sí        | Sí  | Sí (solo RHEL) |
| 7,7                         | Obsoleto | Obsoleto | Sí  | Sí  | Sí  | Sí        | No  | No             |
| 7,8                         | Obsoleto | Obsoleto | Sí  | Sí  | Sí  | Sí        | No  | No             |
| 7,9                         | Obsoleto | Obsoleto | Sí  | Sí  | Sí  | Implícita | No  | No             |
| RHEL 8,0                    | Obsoleto | Obsoleto | Sí  | Sí  | Sí  | Sí        | Sí  | No             |
| RHEL 8,1                    | Obsoleto | Obsoleto | Sí  | Sí  | Sí  | Sí        | No  | No             |
| RHEL 8,2                    | Obsoleto | Obsoleto | Sí  | Sí  | Sí  | No        | No  | No             |
| RHEL 8,3                    | Obsoleto | Obsoleto | Sí  | Sí  | Sí  | No        | No  | No             |
| RHEL 8,4                    | Obsoleto | Sí       | Sí  | Sí  | No  | No        | No  | No             |
| RHEL 8,5                    | Sí       | Sí       | Sí  | Sí  | No  | No        | No  | No             |
| RHEL 8,6                    | Sí       | Sí       | No  | No  | No  | No        | No  | No             |
| RHEL 8,7                    | Sí       | Sí       | No  | No  | No  | No        | No  | No             |
| RHEL 8,8                    | Sí       | Sí       | No  | No  | No  | No        | No  | No             |
| RHEL 9,0                    | Sí       | Sí       | No  | No  | No  | No        | No  | No             |
| RHEL 9,1                    | Sí       | Sí       | No  | No  | No  | No        | No  | No             |
| RHEL 9,2                    | Sí       | Sí       | No  | No  | No  | No        | No  | No             |
| RHEL 9,3                    | Sí       | No       | No  | No  | No  | No        | No  | No             |

|                   |    |    |      |      |      |      |      |      |
|-------------------|----|----|------|------|------|------|------|------|
| CentOS 8 y STREAM | No | No | No   | No   | No   | N.A. | N.A. | N.A. |
| Rocky Linux 8     | Sí | Sí | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. |
| Rocky Linux 9     | Sí | Sí | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. |

- OS hace referencia a las versiones RedHat y CentOS, a menos que se especifique lo contrario.
- “No” significa que el sistema operativo y el Mediador ONTAP no son compatibles.
- CentOS 8 se eliminó para todas las versiones debido a su rerafirmación. CentOS Stream no se consideró un sistema operativo de destino de producción adecuado. No se ha planificado ningún soporte.
- ONTAP Mediator 1,5 fue la última versión admitida para los sistemas operativos de sucursal RHEL 7.x.
- ONTAP Mediator 1,6 añade soporte para Rocky Linux 8 y 9.

### Problemas resueltos

| Fecha del cambio      | Cambiar ID | Descripción                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10 de enero de 2023   | 6567145    | Se realizaron los siguientes cambios: <ul style="list-style-type: none"> <li>• Se ha añadido soporte para sistemas operativos adicionales para ONTAP Mediator: RHEL 9,6, 8,7, 9,0 y 9,1.</li> <li>• Se ha añadido la nueva versión 3.7.0 de SCST para desbloquear los problemas de los nuevos sistemas operativos admitidos.</li> <li>• Añadido soporte para Rocky Linux: Rocky 8 y 9.</li> </ul> |
| 24 de enero de 2023   | 6621319    | Se permite la biblioteca SCST preinstalada para instalaciones de ONTAP Mediator.                                                                                                                                                                                                                                                                                                                  |
| 27 de febrero de 2023 | 6623764    | Se han implementado cambios para cargar siempre el módulo del núcleo scst_DISK cuando se reinicia el servicio mediator-scst. Estos cambios garantizan que el servicio siempre estará listo para crear nuevos destinos iSCSI utilizando la lógica estándar.                                                                                                                                        |
| 28 de febrero de 2023 | 6625194    | Se ha añadido una nueva opción al instalador de ONTAP Mediator: <code>--skip-yum-dependencies</code>                                                                                                                                                                                                                                                                                              |
| 24 de marzo de 2023   | 6652840    | Se ha actualizado el instalador de ONTAP Mediator para que pueda reinstalar o reparar la instalación de SCST.                                                                                                                                                                                                                                                                                     |

|                     |         |                                                                                                                              |
|---------------------|---------|------------------------------------------------------------------------------------------------------------------------------|
| 27 de marzo de 2023 | 6655179 | Se corrigió un problema de análisis que se produjo al activar la recogida del bundle de soporte con una contraseña compleja. |
| 28 de marzo de 2023 | 6656739 | Se ha cambiado la lógica de comparación de SCST para que se instale la versión correcta cuando se actualice ONTAP Mediator.  |

## Instale o actualice

### Prepárese para instalar o actualizar el servicio de Mediador de ONTAP

Para instalar el servicio ONTAP Mediator, debe asegurarse de que se cumplen todos los requisitos previos, obtener el paquete de instalación y ejecutar el instalador en el host. Este procedimiento se utiliza para una instalación o actualización de una instalación existente.

#### Acerca de esta tarea

- A partir de ONTAP 9.7, puede utilizar cualquier versión de Mediator de ONTAP para supervisar una configuración IP de MetroCluster.
- A partir de ONTAP 9.8, puede utilizar cualquier versión de Mediator de ONTAP para supervisar una relación SM-BC.

#### Antes de empezar

Debe cumplir con los siguientes requisitos previos.

| Versión de ONTAP Mediator | Versiones de Linux compatibles                                                                                                                                 |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1,7                       | <ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux: 8,5, 8,6, 8,7, 8,8, 8,9, 9,0, 9,1, 9,2 y 9,3</li> <li>• Rocky Linux 8 y 9</li> </ul>        |
| 1,6                       | <ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux: 8,4, 8,5, 8,6, 8,7, 8,8, 9,0, 9,1, 9,2</li> <li>• Rocky Linux 8 y 9</li> </ul>              |
| 1,5                       | <ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 7.9, 8.1 8.2, 8.3, 8.4, 8.5</li> <li>• CentOS: 7.6, 7.7, 7.8, 7.9</li> </ul> |
| 1,4                       | <ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 7.9, 8.1 8.2, 8.3, 8.4, 8.5</li> <li>• CentOS: 7.6, 7.7, 7.8, 7.9</li> </ul> |
| 1,3                       | <ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 7.9, 8.1 8.2, 8.3</li> <li>• CentOS: 7.6, 7.7, 7.8, 7.9</li> </ul>           |
| 1,2                       | <ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 8.1</li> <li>• CentOS: 7.6, 7.7, 7.8</li> </ul>                              |





La versión del kernel debe coincidir con la versión del sistema operativo.

- instalación física de 64 bits o máquina virtual
- 8 GB DE MEMORIA RAM
- 1 GB de espacio en disco (utilizado para la instalación de aplicaciones, registros del servidor y la base de datos)
- Usuario: Acceso raíz

Cualquier paquete de biblioteca, excepto el núcleo, se puede actualizar de forma segura, pero es posible que sea necesario reiniciarlo para que se vea afectado dentro de la aplicación ONTAP Mediator. Se recomienda una ventana de servicio cuando es necesario reiniciar.

Si instala el `yum-utils` paquete, puede utilizar el `needs-restarting` comando.

El núcleo central del núcleo se puede actualizar si se está actualizando a una versión que aún es compatible con la matriz de versiones de ONTAP Mediator. Un reinicio será obligatorio, por lo que se requiere una ventana de servicio.

El módulo del núcleo SCST debe desinstalarse antes del reinicio y, a continuación, volver a instalarse después del reinicio.



No se admite la actualización a un núcleo más allá de la versión de SO admitida para la versión de ONTAP Mediator específica. (Esto probablemente indica que el módulo SCST probado no se compilará).

#### Registre una clave de seguridad cuando el arranque seguro de UEFI esté habilitado

Si el inicio seguro de UEFI está activado, para instalar ONTAP Mediator, tendrá que registrar una clave de seguridad antes de que el servicio ONTAP Mediator pueda iniciarse. Para determinar si el sistema está habilitado para UEFI y Secure Boot está activado, realice los siguientes pasos:

#### Pasos

1. Si `mokutil` no está instalado, ejecute el siguiente comando:

```
yum install mokutil
```

2. Para determinar si UEFI Secure Boot está habilitado en su sistema, ejecute el siguiente comando:

```
mokutil --sb-state
```

Los resultados muestran si UEFI Secure Boot está habilitado en este sistema.



ONTAP Mediator 1.2.0 y las versiones anteriores no admiten este modo.

#### Desactive UEFI Secure Boot

También puede optar por deshabilitar el arranque seguro de UEFI antes de instalar ONTAP Mediator.

#### Pasos

1. En la configuración del BIOS de la máquina física, desactive la opción «Arranque seguro UEFI».

2. En la configuración de VMware para la máquina virtual, desactive la opción de inicio seguro para vSphere 6.x o la opción de arranque seguro para vSphere 7.x.

## Actualice el sistema operativo del host y, a continuación, el Mediador de ONTAP

Para actualizar el sistema operativo host para ONTAP Mediator a una versión posterior, primero debe desinstalar ONTAP Mediator.

### Antes de empezar

A continuación se enumeran las mejores prácticas para instalar Red Hat Enterprise Linux o Rocky Linux y los repositorios asociados en su sistema. Los sistemas instalados o configurados de forma diferente pueden requerir pasos adicionales.

- Debe instalar Red Hat Enterprise Linux o Rocky Linux de acuerdo con las mejores prácticas de Red Hat. Debido al soporte final de su vida útil para las versiones CentOS 8.x, no se recomienda utilizar versiones compatibles de CentOS 8.x.
- Al instalar el servicio ONTAP Mediator en Red Hat Enterprise Linux o Rocky Linux, el sistema debe tener acceso al repositorio adecuado para que el programa de instalación pueda acceder e instalar todas las dependencias de software necesarias.
- Para que el instalador de yum encuentre software dependiente en los repositorios de Red Hat Enterprise Linux, debe haber registrado el sistema durante la instalación de Red Hat Enterprise Linux o después mediante una suscripción válida de Red Hat.

Consulte la documentación de Red Hat para obtener información acerca de Red Hat Subscription Manager.

- Los siguientes puertos deben no utilizarse y estar disponibles para el Mediator:
  - 31784
  - 3260
- Si utiliza un firewall de terceros: Consulte ["Requisitos de firewall para ONTAP Mediator"](#)
- Si el host Linux se encuentra en una ubicación sin acceso a Internet, debe asegurarse de que los paquetes requeridos estén disponibles en un repositorio local.

Si utiliza el protocolo de control de agregación de enlaces (LACP) en un entorno de Linux, debe configurar correctamente el kernel y asegurarse de que `sysctl net.ipv4.conf.all.arp_ignore` está configurado en "2".

### Lo que necesitará

El servicio Mediator de ONTAP requiere los siguientes paquetes:

|                                 |                                                    |                                                    |
|---------------------------------|----------------------------------------------------|----------------------------------------------------|
| Todas las versiones RHEL/CentOS | Paquetes adicionales para RHEL 8.x / Rocky Linux 8 | Paquetes adicionales para RHEL 9.x / Rocky Linux 9 |
|---------------------------------|----------------------------------------------------|----------------------------------------------------|

|                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                  |                                                                                                                                                                                     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• openssl</li> <li>• openssl</li> <li>• kernel-devel-\$(uname -r)</li> <li>• gcc</li> <li>• marca</li> <li>• libselinux-utils</li> <li>• parche</li> <li>• bzip2</li> <li>• perl-Data-Dumper</li> <li>• perl-ExtLibs-MakeMaker</li> <li>• efibootmgr</li> <li>• mokutil</li> </ul> | <ul style="list-style-type: none"> <li>• python3-pip</li> <li>• elfutils-libelf-devel</li> <li>• pollicoreutils-python-utils</li> <li>• redhat-lsb-core</li> <li>• python39</li> <li>• python39-devel</li> </ul> | <ul style="list-style-type: none"> <li>• python3-pip</li> <li>• elfutils-libelf-devel</li> <li>• pollicoreutils-python-utils</li> <li>• python3</li> <li>• python3-devel</li> </ul> |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

El paquete de instalación de Mediator es un archivo tar comprimido autoextraíble que incluye:

- Un archivo RPM que contiene todas las dependencias que no pueden obtenerse del repositorio de la versión compatible.
- Una secuencia de comandos de instalación.

Se recomienda una certificación SSL válida.

#### Acerca de esta tarea

Al actualizar el sistema operativo host para ONTAP Mediator a una versión principal posterior (por ejemplo, de 7.x a 8.x) con la herramienta leapp-upgrade, Debe desinstalar ONTAP Mediator porque la herramienta intenta detectar nuevas versiones de los RPM instalados en los repositorios registrados con el sistema.

Como se instaló un archivo .rpm como parte del instalador de ONTAP Mediator, se incluye en esa búsqueda. Sin embargo, como ese archivo .rpm se desempaquetó como parte del instalador y no se descargó de un repositorio registrado, no se puede encontrar una actualización. En este caso, la herramienta leapp-upgrade desinstala el paquete.

Para conservar los archivos de registro, que se utilizarán para clasificar los casos de soporte, debe realizar una copia de seguridad de los archivos antes de realizar una actualización del sistema operativo y restaurarlos después de una reinstalación del paquete ONTAP Mediator. Debido a que ONTAP Mediator se está reinstalando, todos los clústeres de ONTAP que estén conectados a él deberán volver a conectarse después de la nueva instalación.



Los siguientes pasos deben realizarse en orden. Inmediatamente después de reinstalar ONTAP Mediator, debe detener el servicio ontap\_mediator, reemplazar los archivos de registro y reiniciar el servicio. Esto asegurará que no se pierdan los registros.

#### Pasos

1. Realice una copia de seguridad de los archivos de registro.

```
[rootmediator-host ~]# tar -czf ontap_mediator_file_backup.tgz -C
/opt/netapp/lib/ontap_mediator ./log
./ontap_mediator/server_config/ontap_mediator.user_config.yaml
[rootmediator-host ~]# tar -tf ontap_mediator_file_backup.tgz
./log/
./log/ontap_mediator.log
./log/scstadmin.log
./log/ontap_mediator_stdout.log
./log/ontap_mediator_requests.log
./log/install_20230419134611.log
./log/scst.log
./log/ontap_mediator_syslog.log
./ontap_mediator/server_config/ontap_mediator.user_config.yaml
[rootmediator-host ~]#
```

## 2. Realice la actualización con la herramienta leapp-upgrade.

```
[rootmediator-host ~]# leapp preupgrade --target 8.4
..<snip upgrade checks>..
..<fix issues found>..
[rootmediator-host ~]# leapp upgrade --target 8.4
..<snip upgrade>..
[rootmediator-host ~]# cat /etc/os-release | head -2
NAME="Red Hat Enterprise Linux"
VERSION="8.4 (Ootpa)"
[rootmediator-host ~]#
```

## 3. Vuelva a instalar ONTAP Mediator.



Realice el resto de los pasos inmediatamente después de volver a instalar ONTAP Mediator para evitar la pérdida de archivos de registro.

```
[rootmediator-host ~]# ontap-mediator-1.6.0/ontap-mediator-1.6.0

ONTAP Mediator: Self Extracting Installer

..<snip installation>..
[rootmediator-host ~]#
```

## 4. Detenga el servicio ontap\_mediator.

```
[rootmediator-host ~]# systemctl stop ontap_mediator
[rootmediator-host ~]#
```

5. Sustituya los archivos de registro.

```
[rootmediator-host ~]# tar -xf ontap_mediator_log_backup.tgz -C
/opt/netapp/lib/ontap_mediator
[rootmediator-host ~]#
```

6. Inicie el servicio ontap\_mediator.

```
[rootmediator-host ~]# systemctl start ontap_mediator
[rootmediator-host ~]#
```

7. Vuelva a conectar todos los clústeres de ONTAP con el Mediador de ONTAP actualizado

```

siteA::> metrocluster configuration-settings mediator show
Mediator IP Port Node Configuration
Connection
Status Status

172.31.40.122
31784 siteA-node2 true false
 siteA-nod1 true false
 siteB-node2 true false
 siteB-node2 true false

siteA::> metrocluster configuration-settings mediator remove
Removing the mediator and disabling Automatic Unplanned Switchover.
It may take a few minutes to complete.
Please enter the username for the mediator: mediatoradmin
Please enter the password for the mediator:
Confirm the mediator password:
Automatic Unplanned Switchover is disabled for all nodes...
Removing mediator mailboxes...
Successfully removed the mediator.

siteA::> metrocluster configuration-settings mediator add -mediator
-address 172.31.40.122
Adding the mediator and enabling Automatic Unplanned Switchover. It
may take a few minutes to complete.
Please enter the username for the mediator: mediatoradmin
Please enter the password for the mediator:
Confirm the mediator password:
Successfully added the mediator.

siteA::> metrocluster configuration-settings mediator show
Mediator IP Port Node Configuration
Connection
Status Status

172.31.40.122
31784 siteA-node2 true true
 siteA-nod1 true true
 siteB-node2 true true
 siteB-node2 true true

siteA::>

```

## Procedimiento de Continuidad del negocio con SnapMirror

Para la continuidad del negocio con SnapMirror, si instaló su certificado TLS fuera del directorio /opt/netapp, no será necesario reinstalarlo. Si estaba utilizando el certificado autofirmado generado por defecto o colocó el certificado personalizado en el directorio /opt/netapp, deberá realizar un backup y restaurarlo.

```
peer1::> snapmirror mediator show
Mediator Address Peer Cluster Connection Status Quorum Status

172.31.49.237 peer2 unreachable true

peer1::> snapmirror mediator remove -mediator-address 172.31.49.237
-peer-cluster peer2

Info: [Job 39] 'mediator remove' job queued

peer1::> job show -id 39
Job ID Name Owning
Vserver Node State

39 mediator remove peer1 peer1-nodel Success
Description: Removing entry in mediator

peer1::> security certificate show -common-name ONTAPMediatorCA
Vserver Serial Number Certificate Name
Type

peer1
4A790360081F41145E14C5D7CE721DC6C210007F
ONTAPMediatorCA
server-ca
Certificate Authority: ONTAP Mediator CA
Expiration Date: Mon Apr 17 10:27:54 2013

peer1::> security certificate delete -common-name ONTAPMediatorCA *
1 entry was deleted.

peer1::> security certificate install -type server-ca -vserver
peer1

Please enter Certificate: Press <Enter> when done
..<snip ONTAP Mediator CA public key>..

You should keep a copy of the CA-signed digital certificate for
future reference.
```

The installed certificate's CA and serial number for reference:

CA: ONTAP Mediator CA

serial: 44786524464C5113D5EC966779D3002135EA4254

The certificate's generated name for reference: ONTAPMediatorCA

```
peer2::> security certificate delete -common-name ONTAPMediatorCA *
1 entry was deleted.
```

```
peer2::> security certificate install -type server-ca -vserver peer2
```

```
Please enter Certificate: Press <Enter> when done
..
..<snip ONTAP Mediator CA public key>..
```

You should keep a copy of the CA-signed digital certificate for future reference.

The installed certificate's CA and serial number for reference:

CA: ONTAP Mediator CA

serial: 44786524464C5113D5EC966779D3002135EA4254

The certificate's generated name for reference: ONTAPMediatorCA

```
peer1::> snapmirror mediator add -mediator-address 172.31.49.237
-peer-cluster peer2 -username mediatoradmin
```

Notice: Enter the mediator password.

Enter the password:

Enter the password again:

Info: [Job: 43] 'mediator add' job queued

```
peer1::> job show -id 43
```

| Job ID                                 | Name         | Owning<br>Vserver | Node        | State   |
|----------------------------------------|--------------|-------------------|-------------|---------|
| 43                                     | mediator add | peer1             | peer1-node2 | Success |
| Description: Creating a mediator entry |              |                   |             |         |

```
peer1::> snapmirror mediator show
```

| Mediator Address | Peer Cluster | Connection Status | Quorum Status |
|------------------|--------------|-------------------|---------------|
| 172.31.49.237    | peer2        | connected         | true          |



```
peer1::>
```

## Habilite el acceso a los repositorios

Debe activar el acceso a los repositorios para que ONTAP Mediator pueda acceder a los paquetes necesarios durante el proceso de instalación

### Pasos

1. Determine a qué repositorios se debe acceder, como se muestra en la siguiente tabla:

| Si su sistema operativo es... | Debe proporcionar acceso a estos repositorios...                                                                           |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| RHEL 7.x                      | <ul style="list-style-type: none"><li>• rhel-7-server-optional-rpms</li></ul>                                              |
| RHEL 8.x                      | <ul style="list-style-type: none"><li>• rhel-8-for-x86_64-baseos-rpms</li><li>• rhel-8-for-x86_64-appstream-rpms</li></ul> |
| RHEL 9.x                      | <ul style="list-style-type: none"><li>• rhel-9-for-x86_64-baseos-rpms</li><li>• rhel-9-for-x86_64-appstream-rpms</li></ul> |
| CentOS 7.x                    | <ul style="list-style-type: none"><li>• C7.6.1810 - repositorio base</li></ul>                                             |
| Rocky Linux 8                 | <ul style="list-style-type: none"><li>• flujo de aplicación</li><li>• baseos</li></ul>                                     |
| Rocky Linux 9                 | <ul style="list-style-type: none"><li>• flujo de aplicación</li><li>• baseos</li></ul>                                     |

2. Utilice uno de los siguientes procedimientos para habilitar el acceso a los repositorios enumerados anteriormente para que ONTAP Mediator pueda acceder a los paquetes necesarios durante el proceso de instalación.

## Procedimiento para el sistema operativo RHEL 7.x.

Utilice este procedimiento si su sistema operativo es **RHEL 7.x** para permitir el acceso a los repositorios:

### Pasos

1. Suscríbase al repositorio deseado:

```
subscription-manager repos --enable rhel-7-server-optional-rpms
```

En el ejemplo siguiente se muestra la ejecución de este comando:

```
[root@localhost ~]# subscription-manager repos --enable rhel-7-
server-optional-rpms
Repository 'rhel-7-server-optional-rpms' is enabled for this system.
```

2. Ejecute el `yum repolist` comando.

En el siguiente ejemplo, se muestra la ejecución de este comando. El repositorio "rhel-7-Server-optional-rpms" debe aparecer en la lista.

```
[root@localhost ~]# yum repolist
Loaded plugins: product-id, search-disabled-repos, subscription-
manager
rhel-7-server-optional-rpms | 3.2 kB 00:00:00
rhel-7-server-rpms | 3.5 kB 00:00:00
(1/3): rhel-7-server-optional-rpms/7Server/x86_64/group
| 26 kB 00:00:00
(2/3): rhel-7-server-optional-rpms/7Server/x86_64/updateinfo
| 2.5 MB 00:00:00
(3/3): rhel-7-server-optional-rpms/7Server/x86_64/primary_db
| 8.3 MB 00:00:01
repo id repo name
status
rhel-7-server-optional-rpms/7Server/x86_64 Red Hat Enterprise
Linux 7 Server - Optional (RPMs) 19,447
rhel-7-server-rpms/7Server/x86_64 Red Hat Enterprise
Linux 7 Server (RPMs) 26,758
repolist: 46,205
[root@localhost ~]#
```

## Procedimiento para el sistema operativo RHEL 8.x.

Utilice este procedimiento si su sistema operativo es **RHEL 8.x** para permitir el acceso a los repositorios:

### Pasos

1. Suscríbase al repositorio deseado:

```
subscription-manager repos --enable rhel-8-for-x86_64-baseos-rpms
```

```
subscription-manager repos --enable rhel-8-for-x86_64-appstream-rpms
```

En el ejemplo siguiente se muestra la ejecución de este comando:

```
[root@localhost ~]# subscription-manager repos --enable rhel-8-for-
x86_64-baseos-rpms
Repository 'rhel-8-for-x86_64-baseos-rpms' is enabled for this
system.
[root@localhost ~]# subscription-manager repos --enable rhel-8-for-
x86_64-appstream-rpms
Repository 'rhel-8-for-x86_64-appstream-rpms' is enabled for this
system.
```

2. Ejecute el `yum repolist` comando.

Los repositorios recientemente suscritos deben aparecer en la lista.

## Procedimiento para el sistema operativo RHEL 9.x.

Utilice este procedimiento si su sistema operativo es **RHEL 9.x** para permitir el acceso a los repositorios:

### Pasos

1. Suscríbase al repositorio deseado:

```
subscription-manager repos --enable rhel-9-for-x86_64-baseos-rpms
```

```
subscription-manager repos --enable rhel-9-for-x86_64-appstream-rpms
```

En el ejemplo siguiente se muestra la ejecución de este comando:

```
[root@localhost ~]# subscription-manager repos --enable rhel-9-for-
x86_64-baseos-rpms
Repository 'rhel-9-for-x86_64-baseos-rpms' is enabled for this
system.
[root@localhost ~]# subscription-manager repos --enable rhel-9-for-
x86_64-appstream-rpms
Repository 'rhel-9-for-x86_64-appstream-rpms' is enabled for this
system.
```

2. Ejecute el `yum repolist` comando.

Los repositorios recientemente suscritos deben aparecer en la lista.

## Procedimiento para el sistema operativo CentOS 7.x.

Utilice este procedimiento si su sistema operativo es **CentOS 7.x** para permitir el acceso a los repositorios:



Los siguientes ejemplos muestran un repositorio para CentOS 7,6 y es posible que no funcione para otras versiones de CentOS. Utilice el repositorio base para su versión de CentOS.

### Pasos

1. Agregue el repositorio base C7.6.1810. El repositorio de almacén base C7,6.1810 contiene el paquete «kernel-devel» necesario para ONTAP Mediator.
2. Agregue las siguientes líneas a `/etc/yum.repos.d/CentOS-Vault.repo`.

```
[C7.6.1810-base]
name=CentOS-7.6.1810 - Base
baseurl=http://vault.centos.org/7.6.1810/os/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
enabled=1
```

3. Ejecute el `yum repolist` comando.

En el siguiente ejemplo, se muestra la ejecución de este comando. El repositorio de CentOS-7.6.1810 - base debería aparecer en la lista.

```
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
* base: distro.ibiblio.org
* extras: distro.ibiblio.org
* updates: ewr.edge.kernel.org
C7.6.1810-base | 3.6 kB 00:00:00
(1/2): C7.6.1810-base/x86_64/group_gz | 166 kB 00:00:00
(2/2): C7.6.1810-base/x86_64/primary_db | 6.0 MB 00:00:04
repo id repo name status
C7.6.1810-base/x86_64 CentOS-7.6.1810 - Base 10,019
base/7/x86_64 CentOS-7 - Base 10,097
extras/7/x86_64 CentOS-7 - Extras 307
updates/7/x86_64 CentOS-7 - Updates 1,010
repolist: 21,433
[root@localhost ~]#
```

## Procedimiento para sistemas operativos Rocky Linux 8 o 9

Utilice este procedimiento si su sistema operativo es **Rocky Linux 8** o **Rocky Linux 9** para permitir el acceso a los repositorios:

### Pasos

1. Suscríbase a los repositorios requeridos:

```
dnf config-manager --set-enabled baseos

dnf config-manager --set-enabled appstream
```

2. Realice una clean operación:

```
dnf clean all
```

3. Verifique la lista de repositorios:

```
dnf repolist
```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id repo name
appstream Rocky Linux 8 - AppStream
baseos Rocky Linux 8 - BaseOS
[root@localhost ~]#
```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id repo name
appstream Rocky Linux 9 - AppStream
baseos Rocky Linux 9 - BaseOS
[root@localhost ~]#
```

## Descargue el paquete de instalación de Mediator

Descargue el paquete de instalación de Mediator como parte del proceso de instalación.

### Pasos

1. Descargue el paquete de instalación del Mediator desde la página Mediator de ONTAP.

["Página de descarga de Mediator ONTAP"](#)

2. Confirme que el paquete de instalación de Mediator se encuentra en el directorio de trabajo actual:

ls

```
[root@mediator-host ~]#ls
ontap-mediator-1.7.0.tgz
```



Para las versiones 1.4 y anteriores de Mediator de ONTAP, se denomina al instalador `ontap-mediator`.

Si se encuentra en una ubicación sin acceso a Internet, debe asegurarse de que el instalador tiene acceso a los paquetes necesarios.

3. Si es necesario, mueva el paquete de instalación de Mediator del directorio de descarga al directorio de instalación del host Linux Mediator.
4. Descomprima el paquete del instalador:

```
tar xvfz ontap-mediator-1.7.0.tgz
```

```
[root@scs000099753 ~]# tar xvfz ontap-mediator-1.7.0.tgz
ontap-mediator-1.7.0/
ontap-mediator-1.7.0/ONTAP-Mediator-production.pub
ontap-mediator-1.7.0/tsa-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.7.0/tsa-prod-ONTAP-Mediator.pem
ontap-mediator-1.7.0/csc-prod-ONTAP-Mediator.pem
ontap-mediator-1.7.0/csc-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.7.0/ontap-mediator-1.7.0
ontap-mediator-1.7.0/ontap-mediator-1.7.0.sig.tsr
ontap-mediator-1.7.0/ontap-mediator-1.7.0.tsr
ontap-mediator-1.7.0/ontap-mediator-1.7.0.sig
```

## Verifique la firma del código del Mediator ONTAP

Antes de instalar el paquete de instalación del Mediator, debe comprobar la firma del código del Mediator ONTAP.

### Antes de empezar

Antes de comprobar la firma del código del Mediator, el sistema debe cumplir los siguientes requisitos.

- versiones de openssl 1.0.2 a 3.0 para verificación básica
- la versión de openssl 1.1.0 o posterior para las operaciones de la Autoridad de fijación temporal (TSA)
- Acceso público a Internet para verificación OCSP

En el paquete de descarga se incluyen los siguientes archivos:

| Archivo                           | Descripción                                                                           |
|-----------------------------------|---------------------------------------------------------------------------------------|
| ONTAP-Mediator-development.pub    | Clave pública utilizada para verificar la firma                                       |
| csc-prod-chain-ONTAP-Mediator.pem | La cadena de confianza de CA de certificación pública                                 |
| csc-prod-ONTAP-Mediator.pem       | El certificado utilizado para generar la clave                                        |
| ontap-mediator-1.7.0              | Ejecutable de instalación del producto para la versión 1.7.0                          |
| ontap-mediator-1.7.0.sig          | El SHA-256 hash, luego RSA-firmado usando la clave csc-prod, firma para el instalador |
| ontap-mediator-1.7.0.sig.tsr      | La solicitud de revocación para el uso por parte de OCSP para la firma del instalador |
| tsc-prod-ONTAP-Mediator.pem       | El certificado público para la TSR                                                    |
| tsc-prod-chain-ONTAP-Mediator.pem | El certificado público CA Chain para la TSR                                           |

## Pasos

1. Realice la comprobación de revocación activada `csc-prod-ONTAP-Mediator.pem` Mediante el protocolo de estado de certificado en línea (OCSP).
  - a. Busque la URL de OCSP utilizada para registrar el certificado porque los certificados de desarrollador pueden no proporcionar un uri.

```
openssl x509 -noout -ocsp_uri -in csc-prod-chain-ONTAP-Mediator.pem
```

- b. Genere una solicitud OCSP para el certificado.

```
openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem -reqout req.der
```

- c. Conéctese al administrador de OCSP para enviar la solicitud OCSP:

```
openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem -url ${ocsp_uri} -resp_text -respout resp.der -verify_other csc-prod-chain-ONTAP-Mediator.pem
```



2. Verifique la cadena de confianza del CSC y las fechas de vencimiento con respecto al host local:

```
openssl verify
```



La openssl La versión de LA RUTA de ACCESO debe ser válida cert.pem (no autofirmado).

```
openssl verify -untrusted csc-prod-chain-ONTAP-Mediator.pem -CApath
${OPENSSLDIR} csc-prod-ONTAP-Mediator.pem # Failure action: The Code-
Signature-Check certificate has expired or is invalid. Download a newer
version of the ONTAP Mediator.
openssl verify -untrusted tsa-prod-chain-ONTAP-Mediator.pem -CApath
${OPENSSLDIR} tsa-prod-ONTAP-Mediator.pem # Failure action: The Time-
Stamp certificate has expired or is invalid. Download a newer version of
the ONTAP Mediator.
```

3. Compruebe el ontap-mediator-1.6.0.sig.tsr y. ontap-mediator-1.7.0.tsr archivos que utilizan los certificados asociados:

```
openssl ts -verify
```



.tsr los archivos contienen la respuesta de marca de tiempo asociada con el instalador y la firma del código. El procesamiento confirma que la Marca de tiempo tiene una firma válida de TSA y que su archivo de entrada no ha cambiado. La verificación se realiza de forma local en su máquina. Independientemente, no hay necesidad de acceder a los servidores TSA.

```
openssl ts -verify -data ontap-mediator-1.7.0.sig -in ontap-mediator-
1.7.0.sig.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-
prod-ONTAP-Mediator.pem
openssl ts -verify -data ontap-mediator-1.7.0 -in ontap-mediator-
1.7.0.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-prod-
ONTAP-Mediator.pem
```

4. Verificar firmas con respecto a la clave:

```
openssl dgst -verify
```

```
openssl dgst -sha256 -verify ONTAP-Mediator-production.pub -signature
ontap-mediator-1.7.0.sig ontap-mediator-1.7.0
```

## Ejemplo de verificación de la firma del código del Mediador ONTAP (salida de consola)

```
[root@scspa2695423001 ontap-mediator-1.7.0]# pwd
/root/ontap-mediator-1.7.0
[root@scspa2695423001 ontap-mediator-1.7.0]# ls -l
total 63660
-r--r--r-- 1 root root 8582 Feb 19 15:02 csc-prod-chain-ONTAP-
Mediator.pem
-r--r--r-- 1 root root 2373 Feb 19 15:02 csc-prod-ONTAP-
Mediator.pem
-r-xr-xr-- 1 root root 65132818 Feb 20 15:17 ontap-mediator-1.7.0
-rw-r--r-- 1 root root 384 Feb 20 15:17 ontap-mediator-1.7.0.sig
-rw-r--r-- 1 root root 5437 Feb 20 15:17 ontap-mediator-
1.7.0.sig.tsr
-rw-r--r-- 1 root root 5436 Feb 20 15:17 ontap-mediator-1.7.0.tsr
-r--r--r-- 1 root root 625 Feb 19 15:02 ONTAP-Mediator-
production.pub
-r--r--r-- 1 root root 3323 Feb 19 15:02 tsa-prod-chain-ONTAP-
Mediator.pem
-r--r--r-- 1 root root 1740 Feb 19 15:02 tsa-prod-ONTAP-
Mediator.pem
[root@scspa2695423001 ontap-mediator-1.7.0]#
[root@scspa2695423001 ontap-mediator-1.7.0]#
/root/verify_ontap_mediator_signatures.sh
++ openssl version -d
++ cut -d '"' -f2
+ OPENSSLDIR=/etc/pki/tls
+ openssl version
OpenSSL 1.1.1k FIPS 25 Mar 2021
++ openssl x509 -noout -ocsp_uri -in csc-prod-chain-ONTAP-Mediator.pem
+ ocsp_uri=http://ocsp.entrust.net
+ echo http://ocsp.entrust.net
http://ocsp.entrust.net
+ openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem -reqout
req.der
+ openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem -url
http://ocsp.entrust.net -resp_text -respout resp.der -verify_other csc-
prod-chain-ONTAP-Mediator.pem
OCSP Response Data:
 OCSP Response Status: successful (0x0)
 Response Type: Basic OCSP Response
 Version: 1 (0x0)
 Responder Id: C = US, O = "Entrust, Inc.", CN = Entrust Extended
Validation Code Signing CA - EVCS2
```

Produced At: Feb 28 05:01:00 2023 GMT

Responses:

Certificate ID:

Hash Algorithm: sha1

Issuer Name Hash: 69FA640329AB84E27220FE0927647B8194B91F2A

Issuer Key Hash: CE894F8251AA15A28462CA312361D261F8FE78

Serial Number: 511A542B57522AEB7295A640DC6200E5

Cert Status: good

This Update: Feb 28 05:00:00 2023 GMT

Next Update: Mar 4 04:59:59 2023 GMT

Signature Algorithm: sha512WithRSAEncryption

3c:1d:49:b0:93:62:37:3e:c7:38:e3:9f:9f:62:82:73:ed:f4:  
ea:00:6b:f1:01:cd:79:57:92:f1:9d:5d:85:9b:60:59:f8:6c:  
e6:f4:50:51:f3:4c:8a:51:dd:50:68:16:8f:20:24:7e:39:b0:  
44:94:8d:b0:61:da:b9:08:36:74:2d:44:55:62:fb:92:be:4a:  
e7:6c:8c:49:dd:0c:fd:d8:ce:20:08:0d:0f:5a:29:a3:19:03:  
9f:d3:df:41:f4:89:0f:73:18:3f:ac:bb:a7:a3:96:7d:c5:70:  
4c:57:cd:17:17:c6:8a:60:d1:37:c9:2d:81:07:2a:d7:a6:02:  
ee:ce:88:16:22:db:e3:43:64:1e:9b:0d:4d:31:66:fa:ab:a5:  
52:99:94:4a:4a:d0:52:c5:34:f5:18:c7:15:5b:ce:74:c2:fc:  
61:ea:55:aa:f1:2f:82:a3:6a:95:8d:7e:2b:38:49:4f:bf:b1:  
68:7b:1b:24:8b:1f:4d:c5:77:f0:71:af:9c:34:c8:7a:82:50:  
09:a2:19:6e:c6:30:4f:da:a2:79:08:f9:d0:ff:85:d9:2a:84:  
cf:0c:aa:75:8f:72:c9:a7:a2:83:e8:8b:cf:ed:0c:69:75:b6:  
2a:7b:6b:58:99:01:d8:34:ad:e1:89:25:27:1b:fa:d9:6d:32:  
97:3a:0b:0a:8e:a3:9e:e3:f4:e0:d6:1a:c9:b5:14:8c:3e:54:  
3b:37:17:1a:93:44:84:8b:4a:87:97:1e:76:43:3e:d3:ec:8b:  
7e:56:4a:3f:01:31:c0:e5:58:fb:50:ce:6f:b1:e7:35:f9:b7:  
a3:ef:6b:3b:21:95:37:a6:5b:8f:f0:15:18:36:65:89:a1:9c:  
9b:69:00:b4:b1:65:6a:bc:11:2d:d4:9b:b4:97:cc:cb:7a:0c:  
16:11:c1:75:58:7e:13:ab:56:3c:3f:93:5b:95:24:c6:54:52:  
1f:86:a9:16:ce:d9:ea:8b:3a:f3:4f:c4:8f:ad:de:e8:3e:3c:  
d2:51:51:ad:33:7f:d8:c5:33:24:26:f1:2d:9d:0e:9f:55:d0:  
68:bf:af:bd:68:4a:40:08:bc:92:a0:62:54:7d:16:7b:36:29:  
15:b1:cd:58:8e:fb:4a:f2:3e:94:8b:fe:56:95:cc:24:32:af:  
5f:71:99:18:ed:0c:64:94:f7:54:48:87:48:d0:6d:b3:42:04:  
96:03:73:a2:8e:8a:6a:b2:af:ee:56:19:a1:c6:35:12:59:ad:  
19:6a:fe:e0:f1:27:cc:96:4e:f0:4f:fb:6a:bd:ce:05:2c:aa:  
79:7c:df:02:5c:ca:53:7d:60:12:88:7c:ce:15:c7:d4:02:27:  
c1:ab:cf:71:30:1e:14:ba

WARNING: no nonce in response

Response verify OK

csc-prod-ONTAP-Mediator.pem: good

This Update: Feb 28 05:00:00 2023 GMT

Next Update: Mar 4 04:59:59 2023 GMT

```

+ openssl verify -untrusted csc-prod-chain-ONTAP-Mediator.pem -CApath
/etc/pki/tls csc-prod-ONTAP-Mediator.pem
csc-prod-ONTAP-Mediator.pem: OK
+ openssl verify -untrusted tsa-prod-chain-ONTAP-Mediator.pem -CApath
/etc/pki/tls tsa-prod-ONTAP-Mediator.pem
tsa-prod-ONTAP-Mediator.pem: OK
+ openssl ts -verify -data ontap-mediator-1.7.0.sig -in ontap-mediator-
1.7.0.sig.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-
prod-ONTAP-Mediator.pem
Using configuration from /etc/pki/tls/openssl.cnf
Verification: OK
+ openssl ts -verify -data ontap-mediator-1.7.0 -in ontap-mediator-
1.7.0.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-
prod-ONTAP-Mediator.pem
Using configuration from /etc/pki/tls/openssl.cnf
Verification: OK
+ openssl dgst -sha256 -verify ONTAP-Mediator-production.pub -signature
ontap-mediator-1.7.0.sig ontap-mediator-1.7.0
Verified OK
[root@scspa2695423001 ontap-mediator-1.7.0]#

```

## Instale el paquete de instalación del Mediador ONTAP

Para instalar el servicio ONTAP Mediator, debe obtener el paquete de instalación y ejecutar el instalador en el host.

### Pasos

1. Ejecute el instalador y responda a las indicaciones según sea necesario:

```
./ontap-mediator-1.7.0/ontap-mediator-1.7.0 -y
```

```
[root@scs000099753 ~]# ./ontap-mediator-1.5.0/ontap-mediator-1.7.0 -y
```

El proceso de instalación permite crear las cuentas necesarias e instalar los paquetes necesarios. Si tiene instalada una versión anterior de Mediator en el host, se le pedirá que confirme que desea actualizar.

2. A partir de ONTAP Mediator 1.4, el mecanismo de arranque seguro está activado en los sistemas UEFI. Cuando Secure Boot está activado, debe realizar pasos adicionales para registrar la clave de seguridad después de la instalación:

- Siga las instrucciones del archivo README para firmar el módulo del núcleo SCST.:

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.module-
signing
```

- Localice las claves que desee:

/opt/netapp/lib/ontap\_mediator/ontap\_mediator/SCST\_mod\_keys



Después de la instalación, los archivos README y la ubicación de la clave también se proporcionan en la salida del sistema.

## Ejemplo de instalación de ONTAP Mediator 1,6 (salida de la consola)

```
[root@scs000099753 ~]# ./ontap-mediator-1.6.0/ontap-mediator-1.6.0 -y
ONTAP Mediator: Self Extracting Installer

+ Extracting the ONTAP Mediator installation/upgrade archive
+ Performing the ONTAP Mediator run-time code signature check
 Using openssl from the path: /usr/bin/openssl configured for
 CApath:/etc/pki/tls

+ Unpacking the ONTAP Mediator installer
ONTAP Mediator requires two user accounts. One for the service
(netapp), and one for use by ONTAP to the mediator API (mediatoradmin).
Using default account names: netapp + mediatoradmin

Enter ONTAP Mediator user account (mediatoradmin) password:

Re-Enter ONTAP Mediator user account (mediatoradmin) password:

+ Checking if SELinux is in enforcing mode

+ Checking for default Linux firewall
success
success
success

#####
Preparing for installation of ONTAP Mediator packages.

+ Installing required packages.

Last metadata expiration check: 0:25:24 ago on Fri 21 Oct 2022 04:00:13
PM EDT.
Package openssl-1:1.1.1k-4.el8.x86_64 is already installed.
Package gcc-8.4.1-1.el8.x86_64 is already installed.
Package python36-3.6.8-2.module+el8.1.0+3334+5cb623d7.x86_64 is already
installed.
Package libselinux-utils-2.9-5.el8.x86_64 is already installed.
Package perl-Data-Dumper-2.167-399.el8.x86_64 is already installed.
Package efibootmgr-16-1.el8.x86_64 is already installed.
Package mokutil-1:0.3.0-11.el8.x86_64 is already installed.
```

Package python3-pip-9.0.3-19.el8.noarch is already installed.  
 Package polycoreutils-python-utils-2.9-14.el8.noarch is already installed.  
 Dependencies resolved.

```
=====
```

| Package                                | Architecture | Repository  |
|----------------------------------------|--------------|-------------|
| Version                                |              |             |
| Size                                   |              |             |
| =====                                  |              |             |
| =====                                  |              |             |
| =====                                  |              |             |
| Installing:                            |              |             |
| bzip2                                  | x86_64       |             |
| 1.0.6-26.el8                           |              | rhel-8-for- |
| x86_64-baseos-rpms                     | 60 k         |             |
| elfutils-libelf-devel                  | x86_64       |             |
| 0.186-1.el8                            |              | rhel-8-for- |
| x86_64-baseos-rpms                     | 60 k         |             |
| kernel-devel                           | x86_64       |             |
| 4.18.0-348.el8                         |              | rhel-8-for- |
| x86_64-baseos-rpms                     | 20 M         |             |
| make                                   | x86_64       |             |
| 1:4.2.1-11.el8                         |              | rhel-8-for- |
| x86_64-baseos-rpms                     | 498 k        |             |
| openssl-devel                          | x86_64       |             |
| 1:1.1.1k-7.el8_6                       |              | rhel-8-for- |
| x86_64-baseos-rpms                     | 2.3 M        |             |
| patch                                  | x86_64       |             |
| 2.7.6-11.el8                           |              | rhel-8-for- |
| x86_64-baseos-rpms                     | 138 k        |             |
| perl-ExtUtils-MakeMaker                | noarch       |             |
| 1:7.34-1.el8                           |              | rhel-8-for- |
| x86_64-appstream-rpms                  | 301 k        |             |
| python36-devel                         | x86_64       |             |
| 3.6.8-38.module+el8.5.0+12207+5c5719bc |              | rhel-8-for- |
| x86_64-appstream-rpms                  | 17 k         |             |
| redhat-lsb-core                        | x86_64       |             |
| 4.1-47.el8                             |              | rhel-8-for- |
| x86_64-appstream-rpms                  | 45 k         |             |
| Upgrading:                             |              |             |
| cpp                                    | x86_64       |             |
| 8.5.0-10.1.el8_6                       |              | rhel-8-for- |
| x86_64-appstream-rpms                  | 10 M         |             |
| elfutils-libelf                        | x86_64       |             |

|                                        |       |        |             |
|----------------------------------------|-------|--------|-------------|
| 0.186-1.el8                            |       |        | rhel-8-for- |
| x86_64-baseos-rpms                     | 229 k |        |             |
| elfutils-libs                          |       | x86_64 |             |
| 0.186-1.el8                            |       |        | rhel-8-for- |
| x86_64-baseos-rpms                     | 295 k |        |             |
| gcc                                    |       | x86_64 |             |
| 8.5.0-10.1.el8_6                       |       |        | rhel-8-for- |
| x86_64-appstream-rpms                  | 23 M  |        |             |
| libgcc                                 |       | x86_64 |             |
| 8.5.0-10.1.el8_6                       |       |        | rhel-8-for- |
| x86_64-baseos-rpms                     | 80 k  |        |             |
| libgomp                                |       | x86_64 |             |
| 8.5.0-10.1.el8_6                       |       |        | rhel-8-for- |
| x86_64-baseos-rpms                     | 207 k |        |             |
| libsemanage                            |       | x86_64 |             |
| 2.9-8.el8                              |       |        | rhel-8-for- |
| x86_64-baseos-rpms                     | 168 k |        |             |
| mokutil                                |       | x86_64 |             |
| 1:0.3.0-11.el8_6.1                     |       |        | rhel-8-for- |
| x86_64-baseos-rpms                     | 46 k  |        |             |
| openssl                                |       | x86_64 |             |
| 1:1.1.1k-7.el8_6                       |       |        | rhel-8-for- |
| x86_64-baseos-rpms                     | 709 k |        |             |
| openssl-libs                           |       | x86_64 |             |
| 1:1.1.1k-7.el8_6                       |       |        | rhel-8-for- |
| x86_64-baseos-rpms                     | 1.5 M |        |             |
| platform-python-pip                    |       | noarch |             |
| 9.0.3-22.el8                           |       |        | rhel-8-for- |
| x86_64-baseos-rpms                     | 1.6 M |        |             |
| policycoreutils                        |       | x86_64 |             |
| 2.9-19.el8                             |       |        | rhel-8-for- |
| x86_64-baseos-rpms                     | 374 k |        |             |
| policycoreutils-python-utils           |       | noarch |             |
| 2.9-19.el8                             |       |        | rhel-8-for- |
| x86_64-baseos-rpms                     | 253 k |        |             |
| python3-libsemanage                    |       | x86_64 |             |
| 2.9-8.el8                              |       |        | rhel-8-for- |
| x86_64-baseos-rpms                     | 128 k |        |             |
| python3-pip                            |       | noarch |             |
| 9.0.3-22.el8                           |       |        | rhel-8-for- |
| x86_64-appstream-rpms                  | 20 k  |        |             |
| python3-policycoreutils                |       | noarch |             |
| 2.9-19.el8                             |       |        | rhel-8-for- |
| x86_64-baseos-rpms                     | 2.2 M |        |             |
| python36                               |       | x86_64 |             |
| 3.6.8-38.module+el8.5.0+12207+5c5719bc |       |        | rhel-8-for- |



```

x86_64-appstream-rpms 19 k
Installing dependencies:
 annobin x86_64
10.29-3.el8 rhel-8-for-
x86_64-appstream-rpms 117 k
 at x86_64
3.1.20-11.el8 rhel-8-for-
x86_64-baseos-rpms 81 k
 bc x86_64
1.07.1-5.el8 rhel-8-for-
x86_64-baseos-rpms 129 k
 cups-client x86_64
1:2.2.6-38.el8 rhel-8-for-
x86_64-appstream-rpms 169 k
 dwz x86_64
0.12-10.el8 rhel-8-for-
x86_64-appstream-rpms 109 k
 ed x86_64
1.14.2-4.el8 rhel-8-for-
x86_64-baseos-rpms 82 k
 efi-srpm-macros noarch
3-3.el8 rhel-8-for-
x86_64-appstream-rpms 22 k
 esmtplib x86_64
1.2-15.el8 EPEL-8
57 k
 glibc-srpm-macros noarch
1.4.2-7.el8 rhel-8-for-
x86_64-appstream-rpms 9.4 k
 go-srpm-macros noarch
2-17.el8 rhel-8-for-
x86_64-appstream-rpms 13 k
 keyutils-libs-devel x86_64
1.5.10-6.el8 rhel-8-for-
x86_64-baseos-rpms 48 k
 krb5-devel x86_64
1.18.2-14.el8 rhel-8-for-
x86_64-baseos-rpms 560 k
 libcom_err-devel x86_64
1.45.6-2.el8 rhel-8-for-
x86_64-baseos-rpms 38 k
 libesmtplib x86_64
1.0.6-18.el8 EPEL-8
70 k
 libkadm5 x86_64
1.18.2-14.el8 rhel-8-for-

```

|                       |       |        |             |
|-----------------------|-------|--------|-------------|
| x86_64-baseos-rpms    | 187 k |        |             |
| libblockfile          |       | x86_64 |             |
| 1.14-1.el8            |       |        | rhel-8-for- |
| x86_64-appstream-rpms | 32 k  |        |             |
| libselinux-devel      |       | x86_64 |             |
| 2.9-5.el8             |       |        | rhel-8-for- |
| x86_64-baseos-rpms    | 200 k |        |             |
| libsepol-devel        |       | x86_64 |             |
| 2.9-3.el8             |       |        | rhel-8-for- |
| x86_64-baseos-rpms    | 87 k  |        |             |
| libverto-devel        |       | x86_64 |             |
| 0.3.0-5.el8           |       |        | rhel-8-for- |
| x86_64-baseos-rpms    | 18 k  |        |             |
| m4                    |       | x86_64 |             |
| 1.4.18-7.el8          |       |        | rhel-8-for- |
| x86_64-baseos-rpms    | 223 k |        |             |
| mailx                 |       | x86_64 |             |
| 12.5-29.el8           |       |        | rhel-8-for- |
| x86_64-baseos-rpms    | 257 k |        |             |
| ncurses-compat-libs   |       | x86_64 |             |
| 6.1-9.20180224.el8    |       |        | rhel-8-for- |
| x86_64-baseos-rpms    | 328 k |        |             |
| ocaml-srpm-macros     |       | noarch |             |
| 5-4.el8               |       |        | rhel-8-for- |
| x86_64-appstream-rpms | 9.5 k |        |             |
| openblas-srpm-macros  |       | noarch |             |
| 2-2.el8               |       |        | rhel-8-for- |
| x86_64-appstream-rpms | 8.0 k |        |             |
| pcre2-devel           |       | x86_64 |             |
| 10.32-2.el8           |       |        | rhel-8-for- |
| x86_64-baseos-rpms    | 605 k |        |             |
| pcre2-utf16           |       | x86_64 |             |
| 10.32-2.el8           |       |        | rhel-8-for- |
| x86_64-baseos-rpms    | 229 k |        |             |
| pcre2-utf32           |       | x86_64 |             |
| 10.32-2.el8           |       |        | rhel-8-for- |
| x86_64-baseos-rpms    | 220 k |        |             |
| perl-CPAN-Meta-YAML   |       | noarch |             |
| 0.018-397.el8         |       |        | rhel-8-for- |
| x86_64-appstream-rpms | 34 k  |        |             |
| perl-ExtUtils-Command |       | noarch |             |
| 1:7.34-1.el8          |       |        | rhel-8-for- |
| x86_64-appstream-rpms | 19 k  |        |             |
| perl-ExtUtils-Install |       | noarch |             |
| 2.14-4.el8            |       |        | rhel-8-for- |
| x86_64-appstream-rpms | 46 k  |        |             |

|                        |       |        |             |
|------------------------|-------|--------|-------------|
| perl-ExtUtils-Manifest |       | noarch |             |
| 1.70-395.el8           |       |        | rhel-8-for- |
| x86_64-appstream-rpms  | 37 k  |        |             |
| perl-ExtUtils-ParseXS  |       | noarch |             |
| 1:3.35-2.el8           |       |        | rhel-8-for- |
| x86_64-appstream-rpms  | 83 k  |        |             |
| perl-JSON-PP           |       | noarch |             |
| 1:2.97.001-3.el8       |       |        | rhel-8-for- |
| x86_64-appstream-rpms  | 68 k  |        |             |
| perl-Math-BigInt       |       | noarch |             |
| 1:1.9998.11-7.el8      |       |        | rhel-8-for- |
| x86_64-baseos-rpms     | 196 k |        |             |
| perl-Math-Complex      |       | noarch |             |
| 1.59-421.el8           |       |        | rhel-8-for- |
| x86_64-baseos-rpms     | 109 k |        |             |
| perl-Test-Harness      |       | noarch |             |
| 1:3.42-1.el8           |       |        | rhel-8-for- |
| x86_64-appstream-rpms  | 279 k |        |             |
| perl-devel             |       | x86_64 |             |
| 4:5.26.3-419.el8_4.1   |       |        | rhel-8-for- |
| x86_64-appstream-rpms  | 599 k |        |             |
| perl-srpm-macros       |       | noarch |             |
| 1-25.el8               |       |        | rhel-8-for- |
| x86_64-appstream-rpms  | 11 k  |        |             |
| perl-version           |       | x86_64 |             |
| 6:0.99.24-1.el8        |       |        | rhel-8-for- |
| x86_64-appstream-rpms  | 67 k  |        |             |
| platform-python-devel  |       | x86_64 |             |
| 3.6.8-41.el8           |       |        | rhel-8-for- |
| x86_64-appstream-rpms  | 249 k |        |             |
| python-rpm-macros      |       | noarch |             |
| 3-41.el8               |       |        | rhel-8-for- |
| x86_64-appstream-rpms  | 15 k  |        |             |
| python-srpm-macros     |       | noarch |             |
| 3-41.el8               |       |        | rhel-8-for- |
| x86_64-appstream-rpms  | 15 k  |        |             |
| python3-pyparsing      |       | noarch |             |
| 2.1.10-7.el8           |       |        | rhel-8-for- |
| x86_64-baseos-rpms     | 142 k |        |             |
| python3-rpm-generators |       | noarch |             |
| 5-7.el8                |       |        | rhel-8-for- |
| x86_64-appstream-rpms  | 25 k  |        |             |
| python3-rpm-macros     |       | noarch |             |
| 3-41.el8               |       |        | rhel-8-for- |
| x86_64-appstream-rpms  | 14 k  |        |             |
| qt5-srpm-macros        |       | noarch |             |

|                                      |       |        |             |
|--------------------------------------|-------|--------|-------------|
| 5.15.2-1.el8                         |       |        | rhel-8-for- |
| x86_64-appstream-rpms                | 11 k  |        |             |
| redhat-lsb-submod-security           |       | x86_64 |             |
| 4.1-47.el8                           |       |        | rhel-8-for- |
| x86_64-appstream-rpms                | 22 k  |        |             |
| redhat-rpm-config                    |       | noarch |             |
| 125-1.el8                            |       |        | rhel-8-for- |
| x86_64-appstream-rpms                | 87 k  |        |             |
| rust-srpm-macros                     |       | noarch |             |
| 5-2.el8                              |       |        | rhel-8-for- |
| x86_64-appstream-rpms                | 9.3 k |        |             |
| spax                                 |       | x86_64 |             |
| 1.5.3-13.el8                         |       |        | rhel-8-for- |
| x86_64-baseos-rpms                   | 217 k |        |             |
| systemtap-sdt-devel                  |       | x86_64 |             |
| 4.6-4.el8                            |       |        | rhel-8-for- |
| x86_64-appstream-rpms                | 86 k  |        |             |
| time                                 |       | x86_64 |             |
| 1.9-3.el8                            |       |        | rhel-8-for- |
| x86_64-baseos-rpms                   | 54 k  |        |             |
| unzip                                |       | x86_64 |             |
| 6.0-46.el8                           |       |        | rhel-8-for- |
| x86_64-baseos-rpms                   | 196 k |        |             |
| util-linux-user                      |       | x86_64 |             |
| 2.32.1-28.el8                        |       |        | rhel-8-for- |
| x86_64-baseos-rpms                   | 100 k |        |             |
| zip                                  |       | x86_64 |             |
| 3.0-23.el8                           |       |        | rhel-8-for- |
| x86_64-baseos-rpms                   | 270 k |        |             |
| zlib-devel                           |       | x86_64 |             |
| 1.2.11-17.el8                        |       |        | rhel-8-for- |
| x86_64-baseos-rpms                   | 58 k  |        |             |
| Installing weak dependencies:        |       |        |             |
| perl-CPAN-Meta                       |       | noarch |             |
| 2.150010-396.el8                     |       |        | rhel-8-for- |
| x86_64-appstream-rpms                | 191 k |        |             |
| perl-CPAN-Meta-Requirements          |       | noarch |             |
| 2.140-396.el8                        |       |        | rhel-8-for- |
| x86_64-appstream-rpms                | 37 k  |        |             |
| perl-Encode-Locale                   |       | noarch |             |
| 1.05-10.module+el8.3.0+6498+9eecfe51 |       |        | rhel-8-for- |
| x86_64-appstream-rpms                | 22 k  |        |             |
| perl-Time-HiRes                      |       | x86_64 |             |
| 4:1.9758-2.el8                       |       |        | rhel-8-for- |
| x86_64-appstream-rpms                | 61 k  |        |             |

## Transaction Summary

Install 69 Packages

Upgrade 17 Packages

Total download size: 72 M

Is this ok [y/N]: y

Downloading Packages:

(1/86): perl-ExtUtils-Install-2.14-4.el8.noarch.rpm

735 kB/s | 46 kB 00:00

(2/86): libesmtplib-1.0.6-18.el8.x86\_64.rpm

1.0 MB/s | 70 kB 00:00

(3/86): esmtplib-1.2-15.el8.x86\_64.rpm

747 kB/s | 57 kB 00:00

(4/86): rust-srpm-macros-5-2.el8.noarch.rpm

308 kB/s | 9.3 kB 00:00

(5/86): perl-ExtUtils-Manifest-1.70-395.el8.noarch.rpm

781 kB/s | 37 kB 00:00

(6/86): perl-CPAN-Meta-2.150010-396.el8.noarch.rpm

2.7 MB/s | 191 kB 00:00

(7/86): ocaml-srpm-macros-5-4.el8.noarch.rpm

214 kB/s | 9.5 kB 00:00

(8/86): perl-JSON-PP-2.97.001-3.el8.noarch.rpm

1.2 MB/s | 68 kB 00:00

(9/86): perl-ExtUtils-MakeMaker-7.34-1.el8.noarch.rpm

5.8 MB/s | 301 kB 00:00

(10/86): ghc-srpm-macros-1.4.2-7.el8.noarch.rpm

317 kB/s | 9.4 kB 00:00

(11/86): perl-Test-Harness-3.42-1.el8.noarch.rpm

4.5 MB/s | 279 kB 00:00

(12/86): perl-ExtUtils-Command-7.34-1.el8.noarch.rpm

520 kB/s | 19 kB 00:00

...

15 MB/s | 1.5 MB 00:00

Total

35 MB/s | 72 MB 00:02

Running transaction check

Transaction check succeeded.

Running transaction test

```

Transaction test succeeded.
Running transaction
 Preparing :
1/1
 Running scriptlet: openssl-libs-1:1.1.1k-7.el8_6.x86_64
1/1
 Upgrading : openssl-libs-1:1.1.1k-7.el8_6.x86_64
1/103
 Running scriptlet: openssl-libs-1:1.1.1k-7.el8_6.x86_64
1/103
 Upgrading : libgcc-8.5.0-10.1.el8_6.x86_64
2/103
 Running scriptlet: libgcc-8.5.0-10.1.el8_6.x86_64
2/103
 Upgrading : elfutils-libelf-0.186-1.el8.x86_64
3/103
 Installing : perl-version-6:0.99.24-1.el8.x86_64
4/103
 Installing : perl-CPAN-Meta-Requirements-2.140-396.el8.noarch
5/103
 Upgrading : libsemanage-2.9-8.el8.x86_64
6/103
 Installing : zlib-devel-1.2.11-17.el8.x86_64
7/103
 Installing : python-srpm-macros-3-41.el8.noarch
8/103
 Installing : python-rpm-macros-3-41.el8.noarch
9/103
 Installing : python3-rpm-macros-3-41.el8.noarch
10/103
 Installing : perl-Time-HiRes-4:1.9758-2.el8.x86_64
11/103
 Installing : perl-ExtUtils-ParseXS-1:3.35-2.el8.noarch
12/103
 Installing : perl-Test-Harness-1:3.42-1.el8.noarch
13/103
 Upgrading : python3-libsemanage-2.9-8.el8.x86_64
14/103
 Upgrading : polycoreutils-2.9-19.el8.x86_64
15/103
 Running scriptlet: polycoreutils-2.9-19.el8.x86_64
15/103
 Upgrading : python3-polycoreutils-2.9-19.el8.noarch
16/103
 Installing : dwz-0.12-10.el8.x86_64
17/103

```

```

Installing : ncurses-compat-libs-6.1-9.20180224.el8.x86_64
18/103
Installing : libesmtplib-1.0.6-18.el8.x86_64
19/103
Installing : mailx-12.5-29.el8.x86_64
20/103
Installing : libkadm5-1.18.2-14.el8.x86_64
21/103
Upgrading : libgomp-8.5.0-10.1.el8_6.x86_64
22/103
Running scriptlet: libgomp-8.5.0-10.1.el8_6.x86_64
22/103
Upgrading : platform-python-pip-9.0.3-22.el8.noarch
23/103
Upgrading : python3-pip-9.0.3-22.el8.noarch
24/103
Upgrading : python36-3.6.8-
38.module+el8.5.0+12207+5c5719bc.x86_64
25/103
Running scriptlet: python36-3.6.8-
38.module+el8.5.0+12207+5c5719bc.x86_64
25/103
Upgrading : cpp-8.5.0-10.1.el8_6.x86_64
26/103
Running scriptlet: cpp-8.5.0-10.1.el8_6.x86_64
26/103
Upgrading : gcc-8.5.0-10.1.el8_6.x86_64
27/103
Running scriptlet: gcc-8.5.0-10.1.el8_6.x86_64
27/103
Installing : annobin-10.29-3.el8.x86_64
28/103
Installing : unzip-6.0-46.el8.x86_64
29/103
Installing : zip-3.0-23.el8.x86_64
30/103
Installing : perl-Math-Complex-1.59-421.el8.noarch
31/103
Installing : perl-Math-BigInt-1:1.9998.11-7.el8.noarch
32/103
Installing : perl-JSON-PP-1:2.97.001-3.el8.noarch
33/103
Installing : make-1:4.2.1-11.el8.x86_64
34/103
Running scriptlet: make-1:4.2.1-11.el8.x86_64
34/103

```

```

Installing : libcom_err-devel-1.45.6-2.el8.x86_64
35/103
Installing : util-linux-user-2.32.1-28.el8.x86_64
36/103
Installing : libsepol-devel-2.9-3.el8.x86_64
37/103
Installing : pcre2-utf32-10.32-2.el8.x86_64
38/103
Installing : pcre2-utf16-10.32-2.el8.x86_64
39/103
Installing : pcre2-devel-10.32-2.el8.x86_64
40/103
Installing : libselinux-devel-2.9-5.el8.x86_64
41/103
Installing : patch-2.7.6-11.el8.x86_64
42/103
Installing : python3-pyparsing-2.1.10-7.el8.noarch
43/103
Installing : systemtap-sdt-devel-4.6-4.el8.x86_64
44/103
Installing : spax-1.5.3-13.el8.x86_64
45/103
Running scriptlet: spax-1.5.3-13.el8.x86_64
45/103
Installing : m4-1.4.18-7.el8.x86_64
46/103
Running scriptlet: m4-1.4.18-7.el8.x86_64
46/103
Installing : libverto-devel-0.3.0-5.el8.x86_64
47/103
Installing : bc-1.07.1-5.el8.x86_64
48/103
Running scriptlet: bc-1.07.1-5.el8.x86_64
48/103
Installing : at-3.1.20-11.el8.x86_64
49/103
Running scriptlet: at-3.1.20-11.el8.x86_64
49/103
Installing : keyutils-libs-devel-1.5.10-6.el8.x86_64
50/103
Installing : krb5-devel-1.18.2-14.el8.x86_64
51/103
Installing : time-1.9-3.el8.x86_64
52/103
Running scriptlet: time-1.9-3.el8.x86_64
52/103

```



```

Upgrading : polycoreutils-python-utils-2.9-19.el8.noarch
80/103
Installing : elfutils-libelf-devel-0.186-1.el8.x86_64
81/103
Upgrading : elfutils-libs-0.186-1.el8.x86_64
82/103
Upgrading : mokutil-1:0.3.0-11.el8_6.1.x86_64
83/103
Upgrading : openssl-1:1.1.1k-7.el8_6.x86_64
84/103
Installing : kernel-devel-4.18.0-348.el8.x86_64
85/103
Running scriptlet: kernel-devel-4.18.0-348.el8.x86_64

...

85/103
Installing : bzip2-1.0.6-26.el8.x86_64
86/103
Cleanup : polycoreutils-python-utils-2.9-14.el8.noarch
87/103
Cleanup : python3-polycoreutils-2.9-14.el8.noarch
88/103
Cleanup : python36-3.6.8-
2.module+el8.1.0+3334+5cb623d7.x86_64
89/103
Running scriptlet: python36-3.6.8-
2.module+el8.1.0+3334+5cb623d7.x86_64
89/103
Cleanup : elfutils-libs-0.185-1.el8.x86_64
90/103
Cleanup : openssl-1:1.1.1k-4.el8.x86_64
91/103
Cleanup : python3-libsemanage-2.9-6.el8.x86_64
92/103
Running scriptlet: gcc-8.4.1-1.el8.x86_64
93/103
Cleanup : gcc-8.4.1-1.el8.x86_64
93/103
Running scriptlet: polycoreutils-2.9-14.el8.x86_64
94/103
Cleanup : polycoreutils-2.9-14.el8.x86_64
94/103
Cleanup : mokutil-1:0.3.0-11.el8.x86_64
95/103

```

```

Cleanup : python3-pip-9.0.3-19.el8.noarch
96/103
Cleanup : platform-python-pip-9.0.3-19.el8.noarch
97/103
Cleanup : openssl-libs-1:1.1.1k-4.el8.x86_64
98/103
Running scriptlet: openssl-libs-1:1.1.1k-4.el8.x86_64
98/103
Cleanup : libsemanage-2.9-6.el8.x86_64
99/103
Running scriptlet: cpp-8.4.1-1.el8.x86_64
100/103
Cleanup : cpp-8.4.1-1.el8.x86_64
100/103
Cleanup : libgcc-8.5.0-3.el8.x86_64
101/103
Running scriptlet: libgcc-8.5.0-3.el8.x86_64
101/103
Running scriptlet: libgomp-8.4.1-1.el8.x86_64
102/103
Cleanup : libgomp-8.4.1-1.el8.x86_64
102/103
Running scriptlet: libgomp-8.4.1-1.el8.x86_64
102/103
Cleanup : elfutils-libelf-0.185-1.el8.x86_64
103/103
Running scriptlet: elfutils-libelf-0.185-1.el8.x86_64
103/103
Verifying : esmtp-1.2-15.el8.x86_64
1/103
Verifying : libesmtp-1.0.6-18.el8.x86_64

...

Upgraded:
 cpp-8.5.0-10.1.el8_6.x86_64 elfutils-
libelf-0.186-1.el8.x86_64 elfutils-libs-0.186-1.el8.x86_64
gcc-8.5.0-10.1.el8_6.x86_64
 libgcc-8.5.0-10.1.el8_6.x86_64 libgomp-
8.5.0-10.1.el8_6.x86_64 libsemanage-2.9-8.el8.x86_64
mokutil-1:0.3.0-11.el8_6.1.x86_64
 openssl-1:1.1.1k-7.el8_6.x86_64 openssl-
libs-1:1.1.1k-7.el8_6.x86_64 platform-python-pip-9.0.3-22.el8.noarch
policycoreutils-2.9-19.el8.x86_64
 policycoreutils-python-utils-2.9-19.el8.noarch python3-
libsemanage-2.9-8.el8.x86_64 python3-pip-9.0.3-22.el8.noarch

```

```

python3-policycoreutils-2.9-19.el8.noarch
python36-3.6.8-38.module+el8.5.0+12207+5c5719bc.x86_64
Installed:
annobin-10.29-3.el8.x86_64 at-
3.1.20-11.el8.x86_64 bc-1.07.1-5.el8.x86_64
bzip2-1.0.6-26.el8.x86_64
cups-client-1:2.2.6-38.el8.x86_64 dwz-0.12-
10.el8.x86_64
ed-1.14.2-4.el8.x86_64
efi-srpm-macros-3-3.el8.noarch elfutils-libelf-
devel-0.186-1.el8.x86_64
esmtplib-1.2-15.el8.x86_64
ghc-srpm-macros-1.4.2-7.el8.noarch go-srpm-macros-2-
17.el8.noarch
kernel-devel-4.18.0-348.el8.x86_64
keyutils-libs-devel-1.5.10-6.el8.x86_64 krb5-devel-1.18.2-
14.el8.x86_64
libcom_err-devel-1.45.6-2.el8.x86_64
libesmtplib-1.0.6-18.el8.x86_64 libkadm5-1.18.2-
14.el8.x86_64
libblockfile-1.14-1.el8.x86_64
libselinux-devel-2.9-5.el8.x86_64 libsepol-devel-2.9-
3.el8.x86_64
libverto-devel-0.3.0-5.el8.x86_64 m4-
1.4.18-7.el8.x86_64 mailx-12.5-
29.el8.x86_64
make-1:4.2.1-11.el8.x86_64
ncurses-compat-libs-6.1-9.20180224.el8.x86_64 ocaml-srpm-macros-
5-4.el8.noarch
openblas-srpm-macros-2-2.el8.noarch
openssl-devel-1:1.1.1k-7.el8_6.x86_64 patch-2.7.6-
11.el8.x86_64
pcre2-devel-10.32-2.el8.x86_64
pcre2-utf16-10.32-2.el8.x86_64 pcre2-utf32-10.32-
2.el8.x86_64
perl-CPAN-Meta-2.150010-396.el8.noarch
perl-CPAN-Meta-Requirements-2.140-396.el8.noarch perl-CPAN-Meta-
YAML-0.018-397.el8.noarch
perl-Encode-Locale-1.05-10.module+el8.3.0+6498+9eecfe51.noarch
perl-ExtUtils-Command-1:7.34-1.el8.noarch perl-ExtUtils-
Install-2.14-4.el8.noarch
perl-ExtUtils-MakeMaker-1:7.34-1.el8.noarch
perl-ExtUtils-Manifest-1.70-395.el8.noarch perl-ExtUtils-
ParseXS-1:3.35-2.el8.noarch
perl-JSON-PP-1:2.97.001-3.el8.noarch
perl-Math-BigInt-1:1.9998.11-7.el8.noarch perl-Math-Complex-

```

```

1.59-421.el8.noarch
perl-Test-Harness-1:3.42-1.el8.noarch
perl-Time-HiRes-4:1.9758-2.el8.x86_64 perl-devel-
4:5.26.3-419.el8_4.1.x86_64
perl-srpm-macros-1-25.el8.noarch
perl-version-6:0.99.24-1.el8.x86_64 platform-python-
devel-3.6.8-41.el8.x86_64
python-rpm-macros-3-41.el8.noarch
python-srpm-macros-3-41.el8.noarch python3-pyparsing-
2.1.10-7.el8.noarch
python3-rpm-generators-5-7.el8.noarch
python3-rpm-macros-3-41.el8.noarch python36-devel-
3.6.8-38.module+el8.5.0+12207+5c5719bc.x86_64
qt5-srpm-macros-5.15.2-1.el8.noarch
redhat-lsb-core-4.1-47.el8.x86_64 redhat-lsb-submod-
security-4.1-47.el8.x86_64
redhat-rpm-config-125-1.el8.noarch
rust-srpm-macros-5-2.el8.noarch spax-1.5.3-
13.el8.x86_64
systemtap-sdt-devel-4.6-4.el8.x86_64
time-1.9-3.el8.x86_64 unzip-6.0-
46.el8.x86_64
util-linux-user-2.32.1-28.el8.x86_64
zip-3.0-23.el8.x86_64 zlib-devel-1.2.11-
17.el8.x86_64

```

Complete!

OS package installations finished

+ Installing ONTAP Mediator. (Log: /tmp/ontap\_mediator.JixKGP/ontap-mediator-1.6.0/ontap-mediator-1.6.0/install\_20221021155929.log)

This step will take several minutes. Use the log file to view progress.

Sudoer config verified

ONTAP Mediator rsyslog and logging rotation enabled

+ Install successful. (Moving log to /opt/netapp/lib/ontap\_mediator/log/install\_20221021155929.log)

+ WARNING: This system supports UEFI

Secure Boot (SB) is currently disabled on this system.

If SB is enabled in the future, SCST will not work unless the following action is taken:

Using the keys in

/opt/netapp/lib/ontap\_mediator/ontap\_mediator/SCST\_mod\_keys follow instructions in

/opt/netapp/lib/ontap\_mediator/ontap\_mediator/SCST\_mod\_keys/README.module-signing

to sign the SCST kernel module. Note that reboot will be

needed.

SCST will not start automatically when Secure Boot is enabled and not configured properly.

+ Note: ONTAP Mediator uses a kernel module compiled specifically for the current

OS. Using 'yum update' to upgrade the kernel might cause service interruption.

```
For more information, see /opt/netapp/lib/ontap_mediator/README
[root@scs000099753 ~]# cat /etc/redhat-release
Red Hat Enterprise Linux release 8.5 (Ootpa)
[root@scs000099753 ~]#
```

## Compruebe la instalación

Después de instalar ONTAP Mediator, debe verificar que los servicios de ONTAP Mediator se están ejecutando.

### Pasos

1. Ver el estado de los servicios de mediador de ONTAP:

- a. `systemctl status ontap_mediator`

```
[root@scspr1915530002 ~]# systemctl status ontap_mediator

ontap_mediator.service - ONTAP Mediator
Loaded: loaded (/etc/systemd/system/ontap_mediator.service; enabled;
vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:49 EDT; 1 weeks 0
days ago
Process: 286710 ExecStop=/bin/kill -s INT $MAINPID (code=exited,
status=0/SUCCESS)
Main PID: 286712 (uwsgi)
Status: "uWSGI is ready"
Tasks: 3 (limit: 49473)
Memory: 139.2M
CGroup: /system.slice/ontap_mediator.service
├─286712 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
├─286716 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
└─286717 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini

[root@scspr1915530002 ~]#
```

b. `systemctl status mediator-scst`

```
[root@scspr1915530002 ~]# systemctl status mediator-scst
Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:47 EDT; 1
weeks 0 days ago
Process: 286595 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
Main PID: 286662 (iscsi-scstd)
Tasks: 1 (limit: 49473)
Memory: 1.2M
CGroup: /system.slice/mediator-scst.service
└─286662 /usr/local/sbin/iscsi-scstd

[root@scspr1915530002 ~]#
```

2. Confirme los puertos que utiliza el servicio ONTAP Mediator:

`netstat`

```
[root@scspr1905507001 ~]# netstat -anlt | grep -E '3260|31784'

tcp 0 0 0.0.0.0:31784 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:3260 0.0.0.0:* LISTEN
tcp6 0 0 :::3260 :::* LISTEN
```

## Configuración posterior a la instalación

Una vez instalado y en ejecución el servicio ONTAP Mediator, se deben llevar a cabo tareas de configuración adicionales en el sistema de almacenamiento de ONTAP para utilizar las siguientes funciones:

- Para utilizar el servicio Mediator de ONTAP en una configuración IP de MetroCluster, consulte ["Configuración del servicio Mediator ONTAP desde una configuración IP de MetroCluster"](#).
- Para utilizar la continuidad del negocio de SnapMirror, consulte ["Instale el Servicio Mediator ONTAP y confirme la configuración del clúster ONTAP"](#).

## Configurar las políticas de seguridad de ONTAP Mediator

El servidor ONTAP Mediator admite varios ajustes de seguridad configurables. Los valores por defecto para todos los valores se proporcionan en un archivo `low_space_threshold_mib: 10read-only`:

```
/opt/netapp/lib/ontap_mediator/server_config/ontap_mediator.user_config.yaml
```

Todos los valores que se colocan en el `ontap_mediator.user_config.yaml` Sustituirá los valores predeterminados y se mantendrá en todas las actualizaciones de ONTAP Mediator.

Después de modificar `ontap_mediator.user_config.yaml`, Reinicie el servicio ONTAP Mediator:

```
systemctl restart ontap_mediator
```

### Modificar los atributos de ONTAP Mediator

Se pueden configurar los siguientes atributos:



Otros valores predeterminados en la `ontap_mediator.config.yaml` no se debe modificar.

- **Configuración utilizada para instalar certificados SSL de terceros como reemplazos para los certificados autofirmados predeterminados**

```
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_medi
tor_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_medi
tor_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl'
cert_valid_days: '1095' # Used to set the expiration
on client certs to 3 years
x509_passin_pwd: 'pass:ontap' # passphrase for the signed
client cert
```

- **Configuraciones que proporcionan protección contra ataques de adivinación de contraseñas de fuerza bruta**

Para activar la función, configure un valor para `window_seconds` y la `retry_limit`

Ejemplos:

- Proporcione un intervalo de 5 minutos para las conjeturas y, a continuación, restablezca el recuento a cero fallos:

```
authentication_lock_window_seconds: 300
```

- Bloquee la cuenta si se producen cinco fallos dentro del marco temporal de la ventana:

```
authentication_retry_limit: 5
```

- Reduzca el impacto de los ataques de adivinación de contraseñas de fuerza bruta estableciendo un retraso que se produce antes de rechazar cada intento, lo que ralentiza los ataques.

```
authentication_failure_delay_seconds: 5
```

```
authentication_failure_delay_seconds: 0 # seconds (float) to delay
failed auth attempts prior to response, 0 = no delay
authentication_lock_window_seconds: null # seconds (int) since the
oldest failure before resetting the retry counter, null = no window
authentication_retry_limit: null # number of retries to
allow before locking API access, null = unlimited
```

- **Campos que controlan las reglas de complejidad de la contraseña de la cuenta de usuario de la API de Mediator de ONTAP**

```
password_min_length: 8

password_max_length: 64

password_uppercase_chars: 0 # min. uppercase characters
password_lowercase_chars: 1 # min. lowercase character
password_special_chars: 1 # min. non-letter, non-digit
password_nonletter_chars: 2 # min. non-letter characters (digits,
specials, anything)
```

- **Configuración que controla el espacio libre requerido en el `/opt/netapp/lib/ontap_mediator` disco.**

Si el espacio es inferior al umbral establecido, el servicio emitirá un evento de advertencia.

```
low_space_threshold_mib: 10
```

- **Configuración que controla `RESERVE_LOG_SPACE`.**

El servidor de ONTAP Mediator por defecto crea un espacio de disco independiente para los registros. El instalador crea un nuevo archivo de tamaño fijo con un total de 700 MB de espacio en disco que se utilizará explícitamente para el registro de Mediator.

Para desactivar esta función y utilizar el espacio en disco predeterminado, realice los siguientes pasos:

- a. Cambie el valor de `RESERVE_LOG_SPACE` de «1» a «0» en el siguiente archivo:

```
/opt/netapp/lib/ontap_mediator/tools/mediator_env
```



b. Reinicie Mediator:

- i. `cat /opt/netapp/lib/ontap_mediator/tools/mediator_env | grep "RESERVE_LOG_SPACE"`

```
RESERVE_LOG_SPACE=0
```

- ii. `systemctl restart ontap_mediator`

Para volver a habilitar la función, cambie el valor de “0” a “1” y reinicie el Mediator.



Al alternar entre espacios de disco no se depuran los logs existentes. Se realiza una copia de seguridad de todos los registros anteriores y, a continuación, se mueve al espacio de disco actual después de alternar y reiniciar Mediator.

## Gestione el servicio de mediación de ONTAP

Después de instalar el servicio Mediator de ONTAP, es posible que desee cambiar el nombre de usuario o la contraseña. También puede desinstalar el servicio de mediador de ONTAP.

### Cambie el nombre de usuario

#### Acerca de estas tareas

Esta tarea se realiza en el host Linux en el que está instalado el servicio Mediator de ONTAP.

Si no puede alcanzar este comando, puede que deba ejecutar el comando con la ruta completa como se muestra en el ejemplo siguiente:

```
/usr/local/bin/mediator_username
```

#### Procedimiento

Cambie el nombre de usuario eligiendo una de las siguientes opciones:

- Ejecute el comando `mediator_change_user` y responda a las indicaciones como se muestra en el ejemplo siguiente:

```
[root@mediator-host ~]# mediator_change_user
Modify the Mediator API username by entering the following values:
 Mediator API User Name: mediatoradmin
 Password:
New Mediator API User Name: mediator
The account username has been modified successfully.
[root@mediator-host ~]#
```

- Ejecute el siguiente comando:

```
MEDIATOR_USERNAME=mediator MEDIATOR_PASSWORD=mediator2
MEDIATOR_NEW_USERNAME=mediatoradmin mediator_change_user
```

```
[root@mediator-host ~]# MEDIATOR_USERNAME= mediator
MEDIATOR_PASSWORD='mediator2' MEDIATOR_NEW_USERNAME= mediatoradmin
mediator_change_user
The account username has been modified successfully.
[root@mediator-host ~]#
```

## Cambie la contraseña

### Acerca de esta tarea

Esta tarea se realiza en el host Linux en el que está instalado el servicio Mediator de ONTAP.

Si no puede alcanzar este comando, puede que deba ejecutar el comando con la ruta completa como se muestra en el ejemplo siguiente:

```
/usr/local/bin/mediator_change_password
```

### Procedimiento

Cambie la contraseña eligiendo una de las siguientes opciones:

- Ejecute el `mediator_change_password` y responda a las indicaciones como se muestra en el ejemplo siguiente:

```
[root@mediator-host ~]# mediator_change_password
Change the Mediator API password by entering the following values:
 Mediator API User Name: mediatoradmin
 Old Password:
 New Password:
 Confirm Password:
The password has been updated successfully.
[root@mediator-host ~]#
```

- Ejecute el siguiente comando:

```
MEDIATOR_USERNAME= mediatoradmin MEDIATOR_PASSWORD=mediator1
MEDIATOR_NEW_PASSWORD=mediator2 mediator_change_password
```

El ejemplo muestra que la contraseña se cambia de “mediator1” a “mediator2”.

```
[root@mediator-host ~]# MEDIATOR_USERNAME=mediatoradmin
MEDIATOR_PASSWORD=mediator1 MEDIATOR_NEW_PASSWORD=mediator2
mediator_change_password
The password has been updated successfully.
[root@mediator-host ~]#
```

## Detenga el servicio ONTAP Mediator

Para detener el servicio ONTAP Mediator, realice los siguientes pasos:

### Pasos

1. Detenga el Mediator ONTAP.

```
systemctl stop ontap_mediator
```

2. Detener SCST.

```
systemctl stop mediator-scst
```

3. Desactive ONTAP Mediator y SCST.

```
systemctl disable ontap_mediator mediator-scst
```

## Vuelva a habilitar el servicio ONTAP Mediator

Para volver a activar el servicio ONTAP Mediator, realice los siguientes pasos:

### Pasos

1. Active el Mediator ONTAP y el SCST.

```
systemctl enable ontap_mediator mediator-scst
```

2. Inicie SCST.

```
systemctl start mediator-scst
```

3. Inicie Mediator ONTAP.

```
systemctl start ontap_mediator
```

## Compruebe que el mediador ONTAP está en buen estado

Después de instalar ONTAP Mediator, debe verificar que los servicios de ONTAP Mediator se están ejecutando.

### Pasos

1. Ver el estado de los servicios de mediador de ONTAP:

- a. `systemctl status ontap_mediator`

```
[root@scspr1915530002 ~]# systemctl status ontap_mediator

ontap_mediator.service - ONTAP Mediator
Loaded: loaded (/etc/systemd/system/ontap_mediator.service; enabled;
vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:49 EDT; 1 weeks 0
days ago
Process: 286710 ExecStop=/bin/kill -s INT $MAINPID (code=exited,
status=0/SUCCESS)
Main PID: 286712 (uwsgi)
Status: "uWSGI is ready"
Tasks: 3 (limit: 49473)
Memory: 139.2M
CGroup: /system.slice/ontap_mediator.service
├─286712 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
├─286716 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
└─286717 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini

[root@scspr1915530002 ~]#
```

b. `systemctl status mediator-scst`

```
[root@scspr1915530002 ~]# systemctl status mediator-scst

Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:47 EDT; 1
weeks 0 days ago
Process: 286595 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
Main PID: 286662 (iscsi-scstd)
Tasks: 1 (limit: 49473)
Memory: 1.2M
CGroup: /system.slice/mediator-scst.service
└─286662 /usr/local/sbin/iscsi-scstd

[root@scspr1915530002 ~]#
```

2. Confirme los puertos que utiliza el servicio ONTAP Mediator:

`netstat`

```
[root@scspr1905507001 ~]# netstat -anlt | grep -E '3260|31784'
```

```
tcp 0 0 0.0.0.0:31784 0.0.0.0:* LISTEN
```

```
tcp 0 0 0.0.0.0:3260 0.0.0.0:* LISTEN
```

```
tcp6 0 0 :::3260 :::* LISTEN
```

## Desinstale manualmente SCST para realizar el mantenimiento del host

Para desinstalar SCST, necesita el paquete tar de SCST que se utiliza para la versión instalada de ONTAP Mediator.

### Pasos

1. Descargue el paquete SCST adecuado (como se muestra en la siguiente tabla) y desmóntelo.

| Para esta versión... | Usar este paquete tar... |
|----------------------|--------------------------|
| Mediador ONTAP 1,7   | scst-3,7.0.tar.bz2       |
| Mediador ONTAP 1,6   | scst-3,7.0.tar.bz2       |
| Mediador ONTAP 1,5   | scst-3,6.0.tar.bz2       |
| Mediador ONTAP 1,4   | scst-3,6.0.tar.bz2       |
| Mediador ONTAP 1,3   | scst-3,5.0.tar.bz2       |
| Mediador ONTAP 1,1   | scst-3,4.0.tar.bz2       |
| Mediador ONTAP 1,0   | scst-3,3.0.tar.bz2       |

2. Emita los siguientes comandos en el directorio scst:

- a. `systemctl stop mediator-scst`
- b. `make scstadm_uninstall`
- c. `make iscsi_uninstall`
- d. `make usr_uninstall`
- e. `make scst_uninstall`
- f. `depmod`

## Instale manualmente SCST para realizar el mantenimiento del host

Para instalar manualmente SCST, necesita el paquete tar de SCST que se utiliza para la versión instalada de ONTAP Mediator (consulte la [tabla anterior](#)).

1. Emita los siguientes comandos en el directorio scst:

- a. `make 2release`
- b. `make scst_install`
- c. `make usr_install`
- d. `make iscsi_install`
- e. `make scstadm_install`
- f. `depmod`
- g. `cp scst/src/certs/scst_module_key.der /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/.`
- h. `cp scst/src/certs/scst_module_key.der /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/.`
- i. `patch /etc/init.d/scst < /opt/netapp/lib/ontap_mediator/systemd/scst.patch`

2. (Opcional) Si Secure Boot está activado, antes de reiniciar, realice los siguientes pasos:

- a. Determine cada nombre de archivo para los módulos «scst\_vdisk», «scst» e «iscsi\_scst».

```
[root@localhost ~]# modinfo -n scst_vdisk
[root@localhost ~]# modinfo -n scst
[root@localhost ~]# modinfo -n iscsi_scst
```

- b. Determine la versión del kernel.

```
[root@localhost ~]# uname -r
```

- c. Firmar cada archivo con el núcleo.

```
[root@localhost ~]# /usr/src/kernels/<KERNEL-RELEASE>/scripts/sign-
file \sha256 \
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_modu
le_key.priv \
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_modu
le_key.der \
module-filename
```

- d. Instale la clave correcta con el firmware UEFI.

Las instrucciones para instalar la clave UEFI se encuentran en:

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.module-
signing
```

La clave UEFI generada se encuentra en:

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.der
```

### 3. Reinicie.

```
reboot
```

## Desinstale el servicio Mediator de ONTAP

### Antes de empezar

Si es necesario, puede eliminar el servicio Mediator ONTAP. El Mediator debe desconectarse de ONTAP antes de quitar el servicio Mediator.

### Acerca de esta tarea

Esta tarea se realiza en el host Linux en el que está instalado el servicio Mediator de ONTAP.

Si no puede alcanzar este comando, puede que deba ejecutar el comando con la ruta completa como se muestra en el ejemplo siguiente:

```
/usr/local/bin/uninstall_ontap_mediator
```

### Paso

#### 1. Desinstale el servicio Mediator de ONTAP:

```
uninstall_ontap_mediator
```

```
[root@mediator-host ~]# uninstall_ontap_mediator

ONTAP Mediator: Self Extracting Uninstaller

+ Removing ONTAP Mediator. (Log:
/tmp/ontap_mediator.GmRGdA/uninstall_ontap_mediator/remove.log)
+ Remove successful.
[root@mediator-host ~]#
```

## Vuelva a generar un certificado autofirmado temporal

### Acerca de esta tarea

- Esta tarea se realiza en el host Linux en el que está instalado el servicio ONTAP Mediator.
- Puede realizar esta tarea solo si los certificados autofirmados generados se han vuelto obsoletos debido a cambios en el nombre de host o la dirección IP del host después de instalar ONTAP Mediator.
- Una vez que el certificado autofirmado temporal ha sido reemplazado por un certificado de terceros de confianza, *NOT* use esta tarea para regenerar un certificado. La ausencia de un certificado autofirmado provocará que falle este procedimiento.

### Paso

Para regenerar un nuevo certificado autofirmado temporal para el host actual, realice el siguiente paso:

## 1. Reinicie el Mediador ONTAP:

```
./make_self_signed_certs.sh overwrite
```

```
[root@xyz000123456 ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@xyz000123456 server_config]# ./make_self_signed_certs.sh overwrite

Adding Subject Alternative Names to the self-signed server certificate
#
OpenSSL example configuration file.
Generating self-signed certificates
Generating RSA private key, 4096 bit long modulus (2 primes)
.....
.....
.....++++
.....++++
e is 65537 (0x010001)
Generating a RSA private key
.....++++
.....
.....+++
+
writing new private key to 'ontap_mediator_server.key'

Signature ok
subject=C = US, ST = California, L = San Jose, O = "NetApp, Inc.", OU =
ONTAP Core Software, CN = ONTAP Mediator, emailAddress =
support@netapp.com
Getting CA Private Key
```

## Mantener el host del sistema operativo para ONTAP Mediator

Para obtener un rendimiento óptimo, debe mantener regularmente el sistema operativo host para ONTAP Mediator.

### Reinicie el host

Reinicie el host cuando el estado de los clústeres sea bueno. Mientras que ONTAP Mediator no está conectado, los clústeres corren el riesgo de no poder reaccionar correctamente ante fallos. Se recomienda una ventana de servicio si es necesario reiniciar.

ONTAP Mediator se reanuda automáticamente durante un reinicio y volverá a introducir las relaciones que se hayan configurado previamente con los clústeres de ONTAP.



## Actualizaciones del paquete de host

Cualquier biblioteca o paquete yum (excepto el kernel) se puede actualizar de forma segura, pero puede requerir un reinicio para que surta efecto. Se recomienda una ventana de servicio si es necesario reiniciar.

Si instala el `yum-utils` paquete, utilice el `needs-restarting` comando para detectar si algún cambio de paquete requiere un reinicio.

Debe reiniciar si se actualiza alguna de las dependencias de Mediador de ONTAP porque no surtirán efecto inmediato en los procesos en ejecución.

## Actualizaciones del kernel inferiores del sistema operativo host

Se debe compilar SCST para el núcleo que se está utilizando. Para actualizar el sistema operativo, se necesita una ventana de mantenimiento.

### Pasos

Realice los siguientes pasos para actualizar el kernel del sistema operativo host.

1. Detenga el Mediador ONTAP
2. Desinstale el paquete SCST. (SCST no proporciona un mecanismo de actualización.)
3. Actualice el sistema operativo y reinicie.
4. Vuelva a instalar el paquete SCST.
5. Vuelva a habilitar los servicios de ONTAP Mediator.

## El host cambia al nombre de host o IP

### Acerca de esta tarea

- Esta tarea se realiza en el host Linux en el que está instalado el servicio ONTAP Mediator.
- Puede realizar esta tarea solo si los certificados autofirmados generados se han vuelto obsoletos debido a cambios en el nombre de host o la dirección IP del host después de instalar ONTAP Mediator.
- Una vez que el certificado autofirmado temporal ha sido reemplazado por un certificado de terceros de confianza, *NOT* use esta tarea para regenerar un certificado. La ausencia de un certificado autofirmado provocará que falle este procedimiento.

### Paso

Para regenerar un nuevo certificado autofirmado temporal para el host actual, realice el siguiente paso:

1. Reinicie el Mediador ONTAP:

```
./make_self_signed_certs.sh overwrite
```

```

[root@xyz000123456 ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@xyz000123456 server_config]# ./make_self_signed_certs.sh overwrite

Adding Subject Alternative Names to the self-signed server certificate
#
OpenSSL example configuration file.
Generating self-signed certificates
Generating RSA private key, 4096 bit long modulus (2 primes)
.....
.....
.....++++
.....++++
e is 65537 (0x010001)
Generating a RSA private key
.....++++
.....
.....+++
+
writing new private key to 'ontap_mediator_server.key'

Signature ok
subject=C = US, ST = California, L = San Jose, O = "NetApp, Inc.", OU =
ONTAP Core Software, CN = ONTAP Mediator, emailAddress =
support@netapp.com
Getting CA Private Key

[root@xyz000123456 server_config]# systemctl restart ontap_mediator

```

## Gestione sitios de MetroCluster con System Manager

### Información general sobre la gestión de sitios de MetroCluster con System Manager

A partir de ONTAP 9.8, es posible usar System Manager como interfaz simplificado para gestionar una configuración de MetroCluster.

Una configuración MetroCluster permite que dos clústeres reflejen datos entre sí por lo que si un clúster deja de funcionar, los datos no se pierden.

Normalmente, una organización configura los clústeres en dos ubicaciones geográficas independientes. Un administrador en cada ubicación establece un clúster y lo configura. A continuación, uno de los administradores puede configurar la relación entre iguales entre los clústeres para que puedan compartir datos.

La organización también puede instalar un Mediador ONTAP en una tercera ubicación. El servicio Mediador

ONTAP supervisa el estado de cada clúster. Cuando uno de los clústeres detecta que no puede comunicarse con el clúster asociado, consulta al monitor para determinar si el error es un problema con el sistema del clúster o con la conexión de red.

Si el problema está relacionado con la conexión de red, el administrador del sistema realiza métodos de solución de problemas para corregir el error y volver a conectarlo. Si el clúster de partners está inactivo, el otro clúster inicia un proceso de conmutación por sitios para controlar las operaciones de I/O de datos de ambos clústeres.

También puede realizar una conmutación de sitios para desconectar uno de los sistemas de clúster para el mantenimiento planificado. El clúster de partners gestiona todas las operaciones de I/O de datos de ambos clústeres hasta que se ponga en marcha el clúster en el cual usted llevó a cabo el mantenimiento y lleva a cabo una operación de conmutación de estado.

Es posible gestionar las siguientes operaciones:

- ["Configure un sitio MetroCluster IP"](#)
- ["Configurar IP MetroCluster peering"](#)
- ["Configure un sitio MetroCluster IP"](#)
- ["Lleve a cabo conmutación de sitios y conmutación de estado de MetroCluster IP"](#)
- ["Solucionar problemas relacionados con la configuración de MetroCluster IP"](#)
- ["Actualice ONTAP en clústeres de MetroCluster"](#)

## Configure un sitio MetroCluster IP

A partir de ONTAP 9.8, puede usar System Manager para configurar una configuración IP de un sitio de MetroCluster.

Un sitio MetroCluster consta de dos clústeres. Normalmente, los clústeres se encuentran en diferentes ubicaciones geográficas.

### Antes de empezar

- El sistema ya debe estar instalado y cableado de acuerdo con ["Instrucciones de instalación y configuración"](#) eso vino con el sistema.
- Las interfaces de red de clúster se deben configurar en cada nodo de cada clúster para la comunicación dentro del clúster.

## Asigne una dirección IP de gestión de nodos

### Sistema Windows

Debe conectar el equipo con Windows a la misma subred que las controladoras. De este modo se asignará automáticamente una dirección IP de gestión de nodos al sistema.

### Pasos

1. Desde el sistema Windows, abra la unidad **Network** para descubrir los nodos.
2. Haga doble clic en el nodo para iniciar el asistente de configuración de clúster.

## Otros sistemas

Debe configurar la dirección IP de gestión de nodos para uno de los nodos del clúster. Puede usar esta dirección IP de gestión de nodos para iniciar el asistente de configuración del clúster.

Consulte "[Creación del clúster en el primer nodo](#)" Para obtener información sobre la asignación de una dirección IP de gestión de nodos.

## Inicialice y configure el clúster

Para inicializar el clúster, debe establecer una contraseña de administrador para el clúster y configurar las redes de gestión de clústeres y nodos. También puede configurar servicios como un servidor DNS para resolver nombres de host y un servidor NTP para sincronizar la hora.

### Pasos

1. En un navegador web, introduzca la dirección IP de gestión de nodos que haya configurado: "<a href="https://node-management-IP"" class="bare">https://node-management-IP"</a>

System Manager detecta automáticamente los nodos restantes del clúster.

2. En la ventana **inicializar sistema de almacenamiento**, realice lo siguiente:
  - a. Introduzca los datos de configuración de la red de gestión del clúster.
  - b. Introduzca las direcciones IP de gestión de nodos para todos los nodos.
  - c. Proporcione detalles sobre los servidores de nombres de dominio (DNS).
  - d. En la sección **otros**, active la casilla de verificación con la etiqueta **usar servicio de hora (NTP)** para agregar los servidores de hora.

Al hacer clic en **Enviar**, espere a que se cree y configure el clúster. A continuación, se produce un proceso de validación.

### El futuro

Una vez que se hayan configurado, inicializado y configurado ambos clústeres, siga el siguiente procedimiento:

- "[Configurar IP MetroCluster peering](#)"

## Configure ONTAP en un vídeo de clúster nuevo



## Configurar IP MetroCluster peering

A partir de ONTAP 9.8, es posible gestionar una configuración IP de una operación de MetroCluster con System Manager. Después de configurar dos clústeres, debe configurar la configuración de paridad entre ellos.

### Antes de empezar

Debe haber completado el siguiente procedimiento para configurar dos clústeres:

- ["Configure un sitio MetroCluster IP"](#)

Diferentes administradores del sistema ubicados en los sitios geográficos de cada clúster llevan a cabo algunos pasos de este proceso. Para explicar este proceso, los clústeres se denominan "clúster del sitio A" y "clúster del sitio B".

### Realización del proceso de relaciones entre iguales desde el sitio A

Este proceso lo realiza un administrador del sistema en el Sitio A.

#### Pasos

1. Inicie sesión en Site A cluster.
2. En System Manager, seleccione **Dashboard** en la columna de navegación de la izquierda para mostrar la descripción general del clúster.

La consola muestra los detalles de este clúster (Sitio A). En la sección **MetroCluster**, Site A se muestra un clúster a la izquierda.

3. Haga clic en **Adjuntar clúster de partners**.
4. Introduzca los detalles de las interfaces de red que permiten que los nodos del clúster del sitio A se

comuniquen con los nodos del clúster del sitio B.

5. Haga clic en **Guardar y continuar**.
6. En la ventana **Adjuntar clúster de socios**, seleccione **no tengo una contraseña**, lo que le permite generar una frase de contraseña.
7. Copie la frase de contraseña generada y compártela con el administrador del sistema en el sitio B.
8. Seleccione **Cerrar**.

## Realización del proceso de relaciones entre iguales desde el sitio B

Este proceso lo lleva a cabo un administrador del sistema en el Sitio B.

### Pasos

1. Inicie sesión en el clúster del sitio B.
2. En System Manager, seleccione **Dashboard** para mostrar la descripción general del clúster.

La consola muestra los detalles de este clúster (sitio B). En la sección MetroCluster, el clúster del sitio B se muestra a la izquierda.

3. Haga clic en **Adjuntar clúster de socios** para iniciar el proceso de relaciones entre iguales.
4. Introduzca los detalles de las interfaces de red que permiten que los nodos del clúster del sitio B se comuniquen con los nodos del clúster del sitio A.
5. Haga clic en **Guardar y continuar**.
6. En la ventana **Adjuntar clúster de socios**, seleccione **Tengo una contraseña**, que le permite introducir la frase de contraseña que recibió del administrador del sistema en el sitio A.
7. Seleccione **Peer** para completar el proceso de comparación.

### El futuro

Una vez que el proceso de relaciones entre iguales se haya completado correctamente, puede configurar los clústeres. Consulte ["Configure un sitio MetroCluster IP"](#).

## Configure un sitio MetroCluster IP

A partir de ONTAP 9.8, es posible gestionar una configuración IP de una operación de MetroCluster con System Manager. Después de configurar dos clústeres y realizar una conexión entre iguales, debe configurar cada clúster.

### Antes de empezar

Debe haber completado los siguientes procedimientos:

- ["Configure un sitio MetroCluster IP"](#)
- ["Configurar IP MetroCluster peering"](#)

## Configure la conexión entre clústeres

### Pasos

1. Inicie sesión en System Manager en uno de los sitios y seleccione **Panel**.

En la sección **MetroCluster**, el gráfico muestra los dos clústeres que ha configurado y tiene una relación

entre iguales para los sitios MetroCluster. El clúster del que está trabajando desde (clúster local) se muestra a la izquierda.

2. Haga clic en **Configurar MetroCluster**. Desde esta ventana, puede realizar las siguientes tareas:
  - a. Se muestran los nodos para cada clúster en la configuración de MetroCluster. Use las listas desplegables para seleccionar qué nodos del clúster local serán partners de recuperación ante desastres con los que se encuentre el clúster remoto.
  - b. Haga clic en la casilla de verificación si desea configurar un servicio Mediador ONTAP. Consulte [Configure el servicio Mediador de ONTAP](#).
  - c. Si ambos clústeres tienen una licencia para habilitar el cifrado, se muestra la sección **cifrado**.

Para habilitar el cifrado, introduzca una frase de contraseña.

- d. Haga clic en la casilla de verificación si desea configurar MetroCluster con una red de capa 3 compartida.



Los nodos asociados de alta disponibilidad y los switches de red que se conectan a los nodos deben tener una configuración coincidente.

3. Haga clic en **Guardar** para configurar los sitios MetroCluster.

En la sección **Tablero**, en la sección **MetroCluster**, el gráfico muestra una Marca de verificación en el enlace entre los dos grupos, lo que indica una conexión en buen estado.


## Configure el servicio Mediador de ONTAP

El servicio Mediador ONTAP se instala normalmente en una ubicación geográfica independiente de cualquiera de las ubicaciones de los clusters. Los clústeres se comunican regularmente con el servicio para indicar que están activos y en ejecución. Si uno de los clústeres de la configuración de MetroCluster detecta que la comunicación con su clúster asociado está inactiva, se comprueba con el Mediador de ONTAP para determinar si el propio clúster asociado está inactivo.

### Antes de empezar

Los dos clústeres de los sitios de MetroCluster deben tener una relación entre iguales.

### Pasos

1. En el Administrador del sistema de ONTAP 9.8, seleccione **clúster > Configuración**.
2. En la sección **Mediator**, haga clic en .
3. En la ventana **Configurar Mediador**, haga clic en **Agregar+**.
4. Introduzca los detalles de configuración del Mediador ONTAP.

Puede introducir los siguientes detalles al configurar un mediador de ONTAP con System Manager.

- La dirección IP del Mediador.
- El nombre de usuario.
- La contraseña.

## Gestiona el Mediador con System Manager




Con System Manager, puede realizar tareas para gestionar Mediator.

### Acerca de estas tareas

A partir de ONTAP 9,8, puede usar System Manager como una interfaz simplificada para gestionar una configuración IP de cuatro nodos de una configuración de MetroCluster, que puede incluir un Mediator ONTAP instalado en una tercera ubicación.

A partir de ONTAP 9.14.1, se puede usar System Manager para realizar también estas operaciones para una configuración IP de ocho nodos de un sitio MetroCluster. Aunque no puede configurar o expandir un sistema de ocho nodos con System Manager, si ya configuró un sistema MetroCluster IP de ocho nodos, podrá realizar estas operaciones.

Realice las siguientes tareas para gestionar el Mediador.

| Para realizar esta tarea...                                             | Realice estas acciones...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configure el servicio de Mediator                                       | Siga los pasos de <a href="#">"Configure el servicio Mediator de ONTAP"</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Activar o desactivar el cambio automático asistido por mediador (MAUSO) | <ol style="list-style-type: none"><li>1. En System Manager, haga clic en <b>Panel</b>.</li><li>2. Desplácese hasta la sección MetroCluster.</li><li>3. Haga clic en  Junto al nombre del sitio MetroCluster.</li><li>4. Seleccione <b>Activar</b> o <b>Desactivar</b>.</li><li>5. Introduzca el nombre de usuario y la contraseña del administrador, luego haga clic en <b>Habilitar</b> o <b>Deshabilitar</b>.</li></ol> <div> Puede activar o desactivar el Mediador cuando se puede acceder a él y ambos sitios están en modo "Normal". El Mediador sigue estando disponible cuando MAUSO está activado o desactivado si el sistema MetroCluster está en buen estado.</div> |
| Elimine Mediator de la configuración de MetroCluster                    | <ol style="list-style-type: none"><li>1. En System Manager, haga clic en <b>Panel</b>.</li><li>2. Desplácese hasta la sección MetroCluster.</li><li>3. Haga clic en  Junto al nombre del sitio MetroCluster.</li><li>4. Seleccione <b>Eliminar Mediator</b>.</li><li>5. Introduzca el nombre de usuario y la contraseña del administrador, luego haga clic en <b>Eliminar</b>.</li></ol>                                                                                                                                                                                                                                                                                                                                                                        |
| Compruebe el estado del Mediador                                        | Siga los pasos de <a href="#">"Solucionar problemas relacionados con la configuración de MetroCluster IP"</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Realice una conmutación de sitios y una conmutación de retorno          | Siga los pasos de <a href="#">"Lleve a cabo conmutación de sitios y conmutación de estado de MetroCluster IP"</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |



## Lleve a cabo conmutación de sitios y conmutación de estado de MetroCluster IP

Puede conmutar el control de un sitio IP MetroCluster al otro para realizar tareas de mantenimiento o recuperación de un problema.



Los procedimientos de conmutación de sitios y conmutación de estado solo son compatibles con las configuraciones de MetroCluster IP.

### Información general sobre conmutación de sitios y conmutación de estado

Un cambio puede producirse en dos instancias:

- **Un cambio planificado**

Este cambio lo inicia un administrador del sistema mediante System Manager. La conmutación planificada permite al administrador de sistema de un clúster local controlar los switches de manera que los servicios de datos del clúster remoto se puedan gestionar mediante el clúster local. A continuación, un administrador del sistema en la ubicación de clúster remoto puede realizar tareas de mantenimiento en el clúster remoto.

- **Un cambio no planificado**

En algunos casos, cuando un clúster MetroCluster cae o las conexiones entre los clústeres están inhabilitadas, ONTAP iniciará automáticamente un procedimiento de conmutación de modo que el clúster que aún se esté ejecutando gestione las responsabilidades de gestión de datos del clúster inactivo.

Otras veces, cuando ONTAP no puede determinar el estado de uno de los clústeres, el administrador del sistema del sitio que está trabajando inicia el procedimiento de conmutación para tomar el control de las responsabilidades de manejo de datos del otro sitio.

En el caso de cualquier tipo de procedimiento de conmutación, la funcionalidad de servicio de datos vuelve al clúster usando un proceso *regresar*.

Usted lleva a cabo distintos procesos de conmutación de sitios y conmutación de estado para ONTAP 9.7 y 9.8:

- [Use System Manager en ONTAP 9.7 para conmutación y conmutación de estado](#)
- [Utilice System Manager en ONTAP 9,8 para conmutación de sitios y conmutación de estado](#)

### Use System Manager en ONTAP 9.7 para conmutación y conmutación de estado

#### Pasos

1. Inicie sesión en System Manager en ONTAP 9.7.
2. Haga clic en **(Volver a la versión clásica)**.
3. Haga clic en **Configuración > MetroCluster**.

System Manager verifica si es posible una conmutación negociada.


4. Realice uno de los siguientes subpasos cuando el proceso de validación haya finalizado:
  - a. Si la validación falla, pero el sitio B está activo, se ha producido un error. Por ejemplo, es posible que haya un problema con un subsistema o que la duplicación de NVRAM no se sincronice.

- i. Solucione el problema que está causando el error, haga clic en **Cerrar** y, a continuación, vuelva a comenzar en el paso 2.
  - ii. Detenga los nodos del sitio B, haga clic en **Cerrar** y, a continuación, realice los pasos en "[Realizar una conmutación de sitios no planificada](#)".
- b. Si la validación falla y el sitio B está inactivo, lo más probable es que haya un problema de conexión. Compruebe que el sitio B está realmente inactivo y, a continuación, realice los pasos de "[Realizar una conmutación de sitios no planificada](#)".
5. Haga clic en **Cambio del sitio B al sitio A** para iniciar el proceso de cambio.
  6. Haga clic en **Cambiar a la nueva experiencia**.

## Utilice System Manager en ONTAP 9,8 para conmutación de sitios y conmutación de estado

### Realizar una conmutación de sitios planificada (ONTAP 9.8)

#### Pasos

1. Inicie sesión en System Manager en ONTAP 9,8.
2. Seleccione **Panel**. En la sección **MetroCluster**, los dos clústeres se muestran con una conexión.
3. En el clúster local (que se muestra a la izquierda), haga clic en  Y seleccione **Cambio de servicios de datos remotos al sitio local**.

Una vez validada la solicitud de conmutación, el control se transfiere del sitio remoto al sitio local, que ejecuta solicitudes de servicio de datos de ambos clústeres.

El clúster remoto se reinicia, pero los componentes de almacenamiento no están activos y el clúster no ofrece servicio a las solicitudes de datos. Ahora está disponible para el mantenimiento planificado.



El clúster remoto no se debe utilizar para el mantenimiento de datos hasta que lleve a cabo una conmutación de estado.


### Realizar una conmutación de sitios no planificada (ONTAP 9.8)

ONTAP puede iniciar automáticamente un cambio no planificado. Si ONTAP no puede determinar si es necesaria una conmutación de estado, el administrador del sistema del sitio de MetroCluster que aún se ejecuta inicia la conmutación de sitios con los siguientes pasos:

#### Pasos

1. Inicie sesión en System Manager en ONTAP 9,8.
2. Seleccione **Panel**.

En la sección **MetroCluster**, la conexión entre los dos clústeres se muestra con una "X", lo que significa que no se puede detectar una conexión. Las conexiones o el clúster están inactivos.

3. En el clúster local (que se muestra a la izquierda), haga clic en  Y seleccione **Cambio de servicios de datos remotos al sitio local**.

Si se produce un error en la conmutación, haga clic en el enlace "View details" en el mensaje de error y confirme la conmutación no planificada.

Una vez validada la solicitud de conmutación, el control se transfiere del sitio remoto al sitio local, que ejecuta solicitudes de servicio de datos de ambos clústeres.

El clúster se debe reparar antes de que vuelva a estar conectado.



Una vez que el clúster remoto vuelve a estar en línea, no se debe usar para el servicio de datos hasta que vuelva a realizar una conmutación de estado.

### Lleve a cabo una conmutación de estado (ONTAP 9.8)

#### Antes de empezar

Ya sea que el clúster remoto no estaba disponible debido a un mantenimiento planificado o debido a un desastre, ahora debería estar listo y en funcionamiento y esperar a que se produzca la conmutación de estado.

#### Pasos

1. En el clúster local, inicie sesión en System Manager en ONTAP 9.8.
2. Seleccione **Panel**.

En la sección **MetroCluster**, se muestran los dos clústeres.

3. En el clúster local (que se muestra a la izquierda), haga clic en Y seleccione **recuperar control**.

Los datos son *sanated* en primer lugar, para garantizar que los datos se sincronizan y se duplican entre ambos clústeres.

4. Cuando se complete la reparación de los datos, haga clic en Y seleccione **Iniciar regreso**.

Una vez finalizada la conmutación de estado, ambos clústeres están activos y prestan servicio a las solicitudes de datos. Además, los datos se están reflejando y sincronizando entre los clústeres.

### Modificar la dirección, la máscara de red y la pasarela en una IP de MetroCluster

A partir de ONTAP 9.10.1, puede cambiar las siguientes propiedades de una interfaz IP de MetroCluster: Dirección IP, máscara y puerta de enlace. Puede usar cualquier combinación de parámetros para actualizar.

Es posible que deba actualizar estas propiedades, por ejemplo, si se detecta una dirección IP duplicada o si una puerta de enlace necesita cambiar en el caso de una red de capa 3 debido a cambios en la configuración del enrutador. Sólo puede cambiar una interfaz a la vez. Habrá interrupciones en el tráfico en esa interfaz hasta que se actualicen las otras interfaces y se restablezcan las conexiones.



Debe realizar los cambios en cada puerto. De igual modo, los switches de red también deben actualizar su configuración. Por ejemplo, si la puerta de enlace se actualiza, lo ideal es que cambie en ambos nodos de un par de alta disponibilidad, ya que son los mismos. Además, el switch conectado a dichos nodos también debe actualizar su puerta de enlace.

#### Paso

Actualice la dirección IP, la máscara de red y la pasarela de cada nodo e interfaz.

### Solucionar problemas relacionados con la configuración de MetroCluster IP

A partir de ONTAP 9.8, System Manager supervisa el estado de las configuraciones de

MetroCluster IP y ayuda a identificar y corregir los problemas que pueden ocurrir.

## Descripción general de la comprobación del estado de MetroCluster

System Manager comprueba periódicamente el estado de la configuración de MetroCluster IP. Cuando ve la sección MetroCluster en la Consola, normalmente el mensaje es "los sistemas MetroCluster están en buen estado".

Sin embargo, cuando se produce un problema, el mensaje mostrará el número de eventos. Puede hacer clic en ese mensaje y ver los resultados de la comprobación de estado de los siguientes componentes:

- Nodo
- Interfaz de red
- Nivel (almacenamiento)
- Clúster
- Conexión
- Volumen
- Replicación de la configuración

La columna **Estado** identifica qué componentes tienen problemas, y la columna **Detalles** sugiere cómo corregir el problema.

## Resolución de problemas de MetroCluster

### Pasos

1. En System Manager, seleccione **Panel**.
2. En la sección **MetroCluster**, observe el mensaje.
  - a. Si el mensaje indica que la configuración de MetroCluster es correcta y que las conexiones entre los clústeres y el Mediador ONTAP están en buen estado (se muestra con marcas de comprobación), no tiene problemas para corregir.
  - b. Si el mensaje enumera el número de eventos o las conexiones han caído (se muestra con una "X"), continúe con el paso siguiente.
3. Haga clic en el mensaje que muestra el número de eventos.

Aparecerá el Informe de estado de MetroCluster.

4. Solucione los problemas que aparecen en el informe con las sugerencias de la columna **Detalles**.
5. Una vez corregidos todos los problemas, haga clic en **comprobar estado de MetroCluster**.



La comprobación del estado de MetroCluster utiliza una cantidad intensiva de recursos, por lo que se recomienda realizar todas las tareas de solución de problemas antes de ejecutar la comprobación.

La comprobación del estado de MetroCluster se ejecuta en segundo plano. Puede trabajar en otras tareas mientras espera a que finalice.

# Protección de datos mediante backup en cinta

## Información general sobre backup a cinta de volúmenes de FlexVol

ONTAP es compatible con los procesos de backup y restauración a cinta mediante el protocolo de gestión de datos de red (NDMP). NDMP le permite realizar backups de datos en sistemas de almacenamiento directamente en cinta, lo cual resulta en un uso más eficiente del ancho de banda de la red. ONTAP es compatible con los motores de volcado y SMTape para backups a cinta.

Puede realizar backups o restauraciones de volcado o SMTape mediante aplicaciones de backup compatibles con NDMP. Solo se admite la versión 4 de NDMP.

### Copia de seguridad en cinta mediante volcado

Dump es un backup basado en copias snapshot en el cual se realiza un backup de los datos del sistema de archivos en cinta. El motor de volcado ONTAP realiza copias de seguridad de los archivos, directorios y la información de la lista de control de acceso (ACL) aplicable a la cinta. Puede realizar un backup de un volumen completo, de un qtree completo o de un subárbol que no sea un volumen completo o un qtree completo. El volcado admite copias de seguridad de línea base, diferencial e incrementales.

### Backup en cinta con SMTape

SMTape es una solución de recuperación ante desastres basada en copias de Snapshot de ONTAP que realiza backup de bloques de datos a cinta. Puede usar SMTape para realizar backups de volúmenes a las cintas. Sin embargo, no puede realizar un backup en el nivel qtree o subárbol. SMTape admite copias de seguridad de línea base, diferenciales e incrementales.

A partir de ONTAP 9.13.1, el backup en cinta con SMTape admite con [Continuidad del negocio de SnapMirror](#).

## Flujo de trabajo de backup y restauración a cinta

Es posible realizar operaciones de backup y restauración a cinta con una aplicación de backup habilitada para NDMP.

### Acerca de esta tarea

El flujo de trabajo de backup y restauración a cinta ofrece información general de las tareas relacionadas con las operaciones de backup y restauración en cinta. Para obtener información detallada sobre cómo realizar una operación de backup y restauración, consulte la documentación de la aplicación de backup.

### Pasos

1. Configure una biblioteca de cintas eligiendo una topología de cinta compatible con NDMP.
2. Active los servicios NDMP en el sistema de almacenamiento.

Puede habilitar los servicios NDMP en el nivel del nodo o en el nivel de la máquina virtual de almacenamiento (SVM). Esto depende del modo NDMP en el que elija ejecutar las operaciones de backup y restauración a cinta.

3. Utilice las opciones NDMP para gestionar NDMP en su sistema de almacenamiento.

Puede usar las opciones de NDMP a nivel de nodo o de SVM. Esto depende del modo NDMP en el que

elija ejecutar las operaciones de backup y restauración a cinta.

Puede modificar las opciones de NDMP en el nivel de nodo mediante el `system services ndmp modify` Y en el nivel de SVM mediante el `vserver services ndmp modify` comando. Para obtener más información sobre estos comandos, consulte las páginas [man](#).

4. Realizar un backup a cinta o una restauración de datos mediante una aplicación de backup compatible con NDMP.

ONTAP es compatible con los motores de volcado y SMTape para backup y restauración a cinta.

Para obtener más información acerca del uso de la aplicación de copia de seguridad (también denominada *Data Management Applications* o *DMAs*) para realizar operaciones de copia de seguridad o restauración, consulte la documentación de la aplicación de copia de seguridad.

## Información relacionada

[Topologías habituales de backup en cinta NDMP](#)

[Motor de volcado para volúmenes FlexVol](#)

## Casos de uso a la hora de elegir un motor de backup en cinta

ONTAP admite dos motores de respaldo: SMTape y dump. Debe conocer los casos de uso de los motores de copia de seguridad SMTape y de volcado para ayudarle a elegir el motor de copia de seguridad para realizar operaciones de copia de seguridad en cinta y restauración.

El volcado se puede utilizar en los siguientes casos:

- Recuperación de acceso directo (DAR) de ficheros y directorios
- Copia de seguridad de un subconjunto de subdirectorios o archivos en una ruta de acceso específica
- Exclusión de archivos y directorios específicos durante las copias de seguridad
- Conservación del backup a largo plazo

SMTape se puede utilizar en los siguientes casos:

- Solución de recuperación tras siniestros
- Conservación del ahorro de la deduplicación y de la configuración de deduplicación en los datos de backup durante la operación de restauración
- Backup de grandes volúmenes

## Gestión de unidades de cinta

### Descripción general de la administración de unidades de cinta

Puede verificar las conexiones de la biblioteca de cintas y ver la información de la unidad de cinta antes de realizar una operación de backup o restauración de cinta. Puede utilizar una unidad de cinta no cualificada emulando esta unidad a una unidad de cinta cualificada. También puede asignar y eliminar alias de cinta además de ver los alias

existentes.

Cuando se realiza el backup de los datos en cinta, estos se almacenan en archivos de cinta. Las marcas de archivo separan los archivos de cinta y los archivos no tienen nombres. Especifique un archivo de cinta por su posición en la cinta. Se escribe un archivo de cinta mediante un dispositivo de cinta. Cuando lea el archivo de cinta, debe especificar un dispositivo que tenga el mismo tipo de compresión que utilizó para escribir ese archivo de cinta.

### Comandos para gestionar unidades de cinta, cambiadores de medios y operaciones de unidades de cinta

Hay comandos para ver información acerca de las unidades de cinta y los intercambiadores de medios en un clúster, conectar una unidad de cinta y desconectarla, modificar la posición del cartucho de la unidad de cinta, configurar y borrar el nombre del alias de la unidad de cinta y restablecer una unidad de cinta. También es posible ver y restablecer las estadísticas de la unidad de cinta.

| Si desea...                                                                        | Se usa este comando...                                                                                                                                                                                            |
|------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Conectar una unidad de cinta                                                       | <code>storage tape online</code>                                                                                                                                                                                  |
| Borre un nombre de alias para la unidad de cinta o el cambiador de medios          | <code>storage tape alias clear</code>                                                                                                                                                                             |
| Activar o desactivar una operación de rastreo de cinta para una unidad de cinta    | <code>storage tape trace</code>                                                                                                                                                                                   |
| Modifique la posición del cartucho de la unidad de cinta                           | <code>storage tape position</code>                                                                                                                                                                                |
| Restablezca una unidad de cinta                                                    | <div><code>storage tape reset</code></div> <div> Este comando solo está disponible en el nivel de privilegios avanzados.</div> |
| Defina un nombre de alias para la unidad de cinta o el cambiador de medios         | <code>storage tape alias set</code>                                                                                                                                                                               |
| Desconectar una unidad de cinta                                                    | <code>storage tape offline</code>                                                                                                                                                                                 |
| Ver información acerca de todas las unidades de cinta e intercambiadores de medios | <code>storage tape show</code>                                                                                                                                                                                    |
| Ver información acerca de las unidades de cinta conectadas al clúster              | <ul style="list-style-type: none"><li>• <code>storage tape show-tape-drive</code></li><li>• <code>system node hardware tape drive show</code></li></ul>                                                           |

| Si desea...                                                                                                              | Se usa este comando...                                                                                                                                                                      |
|--------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ver información acerca de los cambiadores de medios conectados al clúster                                                | <code>storage tape show-media-changer</code>                                                                                                                                                |
| Ver información de errores sobre las unidades de cinta conectadas al clúster                                             | <code>storage tape show-errors</code>                                                                                                                                                       |
| Ver todas las unidades de cinta cualificadas y compatibles de ONTAP conectadas a cada nodo del clúster                   | <code>storage tape show-supported-status</code>                                                                                                                                             |
| Vea alias de todas las unidades de cinta e intercambiadores de medios conectados a cada nodo del clúster                 | <code>storage tape alias show</code>                                                                                                                                                        |
| Restablece la lectura de estadísticas de una unidad de cinta a cero                                                      | <code>storage stats tape zero tape_name</code><br><br>Debe utilizar este comando en el nodeshell.                                                                                           |
| Vea las unidades de cinta compatibles con ONTAP                                                                          | <code>storage show tape supported [-v]</code><br><br>Debe utilizar este comando en el nodeshell. Puede utilizar el <code>-v</code> opción para ver más detalles sobre cada unidad de cinta. |
| Vea las estadísticas de dispositivos de cinta para comprender el rendimiento de la cinta y comprobar los patrones de uso | <code>storage stats tape tape_name</code><br><br>Debe utilizar este comando en el nodeshell.                                                                                                |

Para obtener más información sobre estos comandos, consulte las páginas man.

### Utilice una unidad de cinta no cualificada

Puede utilizar una unidad de cinta no cualificada en un sistema de almacenamiento si puede emular una unidad de cinta cualificada. Luego se trata como una unidad de cinta cualificada. Para utilizar una unidad de cinta no cualificada, primero debe determinar si emula cualquiera de las unidades de cinta cualificadas.

#### Acerca de esta tarea

Una unidad de cinta no cualificada es una unidad conectada al sistema de almacenamiento, pero que ONTAP no admite ni reconoce.

#### Pasos

1. Consulte las unidades de cinta no cualificadas conectadas a un sistema de almacenamiento mediante la `storage tape show-supported-status` comando.

El siguiente comando muestra las unidades de cinta conectadas al sistema de almacenamiento y el estado de soporte y cualificación de cada unidad de cinta. También se enumeran las unidades de cinta no



cualificadas. `tape_drive_vendor_name` Es una unidad de cinta no cualificada conectada al sistema de almacenamiento, pero que no es compatible con ONTAP.

```
cluster1::> storage tape show-supported-status -node Node1
```

| Node: Node1               | Is        |                         |
|---------------------------|-----------|-------------------------|
| Tape Drive                | Supported | Support Status          |
| -----                     | -----     | -----                   |
| "tape_drive_vendor_name"  | false     | Nonqualified tape drive |
| Hewlett-Packard C1533A    | true      | Qualified               |
| Hewlett-Packard C1553A    | true      | Qualified               |
| Hewlett-Packard Ultrium 1 | true      | Qualified               |
| Sony SDX-300C             | true      | Qualified               |
| Sony SDX-500C             | true      | Qualified               |
| StorageTek T9840C         | true      | Dynamically Qualified   |
| StorageTek T9840D         | true      | Dynamically Qualified   |
| Tandberg LTO-2 HH         | true      | Dynamically Qualified   |

## 2. Emular la unidad de cinta cualificada.

["Descargas de NetApp: Archivos de configuración de dispositivo de cinta"](#)

### Información relacionada

[Qué son las unidades de cinta adecuadas](#)

### Asigne alias de cinta

Para facilitar la identificación del dispositivo, puede asignar alias de cinta a una unidad de cinta o a un cambiador de medios. Los alias proporcionan una correspondencia entre los nombres lógicos de los dispositivos de copia de seguridad y un nombre asignado permanentemente a la unidad de cinta o al cambiador de medios.

### Pasos

1. Asigne un alias a una unidad de cinta o a un cambiador de medios mediante el `storage tape alias set` comando.

Para obtener más información acerca de este comando, consulte las páginas man.

Puede ver la información sobre el número de serie (SN) de las unidades de cinta mediante el `system node hardware tape drive show` y acerca de las bibliotecas de cintas mediante el `system node hardware tape library show` comandos.

El siguiente comando establece un nombre de alias en una unidad de cinta con el número de serie SN[123456]L4 conectado al nodo, cluster1-01:

```
cluster-01::> storage tape alias set -node cluster-01 -name st3
-mapping SN[123456]L4
```

El siguiente comando establece un nombre de alias en un cambiador de medios con el número de serie SN[65432] conectado al nodo, cluster1-01:

```
cluster-01::> storage tape alias set -node cluster-01 -name mc1
-mapping SN[65432]
```

### Información relacionada

[Qué es el solapamiento de cinta](#)

[Eliminación de alias de cinta](#)

### Elimine los alias de cinta

Puede eliminar alias utilizando `storage tape alias clear` comando cuando ya no se necesitan alias persistentes para una unidad de cinta o un cambiador de medios.

### Pasos

1. Retire un alias de una unidad de cinta o de un cambiador de medios mediante el `storage tape alias clear` comando.

Para obtener más información acerca de este comando, consulte las páginas man.

El siguiente comando elimina los alias de todas las unidades de cinta especificando el ámbito de la operación de alias `Clear tape`:

```
cluster-01::>storage tape alias clear -node cluster-01 -clear-scope tape
```

### Después de terminar

Si va a realizar una operación de backup o restauración de cinta mediante NDMP, después de eliminar un alias de una unidad de cinta o un cambiador de medios, debe asignar un nuevo nombre de alias a la unidad de cinta o al cambiador de medios para continuar accediendo al dispositivo de cinta.

### Información relacionada

[Qué es el solapamiento de cinta](#)

[Asignación de alias de cinta](#)

### Activación o desactivación de reservas de cinta

Puede controlar cómo ONTAP administra las reservas de dispositivos de cinta mediante la `tape.reservations` opción. De forma predeterminada, la reserva de cinta está desactivada.

**Acerca de esta tarea**

La activación de la opción de reservas de cintas puede ocasionar problemas si las unidades de cinta, los cambiadores de medios, los puentes o las bibliotecas no funcionan correctamente. Si los comandos de cinta indican que el dispositivo está reservado cuando no hay otros sistemas de almacenamiento que utilicen el dispositivo, esta opción debería estar desactivada.

**Pasos**

1. Para utilizar el mecanismo de reserva/liberación SCSI o la reserva persistente SCSI para desactivar las reservas en cinta, introduzca el siguiente comando en el clustershell:
- options -option-name tape.reservations -option-value {scsi | persistent | off}**

scsi Selecciona el mecanismo de reserva/liberación SCSI.

persistent Selecciona Reservas persistentes SCSI.

off desactiva las reservas de cinta.

**Información relacionada**

[Qué reservas de cinta son](#)

**Comandos para verificar las conexiones de la biblioteca de cintas**

Puede ver información acerca de la ruta de conexión entre un sistema de almacenamiento y una configuración de biblioteca de cintas conectada al sistema de almacenamiento. Puede utilizar esta información para verificar la ruta de conexión a la configuración de la biblioteca de cintas o para solucionar problemas relacionados con las rutas de conexión.

Puede ver los siguientes detalles de la biblioteca de cintas para verificar las conexiones de la biblioteca de cintas después de agregar o crear una biblioteca de cintas nueva, o después de restaurar una ruta de acceso fallida en una ruta única o acceso multivía a una biblioteca de cintas. También puede utilizar esta información al solucionar errores relacionados con la ruta de acceso o si el acceso a una biblioteca de cintas falla.

- Nodo al que está conectada la biblioteca de cintas
- ID del dispositivo
- Ruta NDMP
- Nombre de la biblioteca de cintas
- ID de puerto de destino e puerto de iniciador
- Acceso de ruta única o multivía a una biblioteca de cintas para cada puerto iniciador FC o de destino
- Detalles de la integridad de los datos relacionados con la ruta, como «errores de ruta» y «Manual de ruta».
- Los grupos LUN y el número de LUN

| Si desea...                                                  | Se usa este comando...                              |
|--------------------------------------------------------------|-----------------------------------------------------|
| Ver información sobre una biblioteca de cintas en un clúster | <code>system node hardware tape library show</code> |

| Si desea...                                                                                     | Se usa este comando...                                   |
|-------------------------------------------------------------------------------------------------|----------------------------------------------------------|
| Ver información de ruta de una biblioteca de cintas                                             | <code>storage tape library path show</code>              |
| Vea la información de ruta de una biblioteca de cintas para cada puerto iniciador               | <code>storage tape library path show-by-initiator</code> |
| Vea la información de conectividad entre una biblioteca de cinta de almacenamiento y un clúster | <code>storage tape library config show</code>            |

Para obtener más información sobre estos comandos, consulte las páginas man.

## Acerca de las unidades de cinta

### Descripción general de las unidades de cinta cualificadas

Debe utilizar una unidad de cinta cualificada que se haya probado y encontrado para funcionar correctamente en un sistema de almacenamiento. Puede seguir el solapamiento de cintas y activar reservas de cinta para asegurarse de que sólo un sistema de almacenamiento accede a una unidad de cinta en un momento determinado.

Una unidad de cinta cualificada es una unidad de cinta que se ha probado y que funciona correctamente en sistemas de almacenamiento. Puede calificar las unidades de cinta para las versiones de ONTAP existentes mediante el archivo de configuración de cinta.

### Formato del archivo de configuración de cinta

El formato de archivo de configuración de cinta consta de campos como el ID de proveedor, el ID de producto y los detalles de los tipos de compresión de una unidad de cinta. Este archivo también consta de campos opcionales para activar la función de carga automática de una unidad de cinta y cambiar los valores de tiempo de espera de comando de una unidad de cinta.

La siguiente tabla muestra el formato del archivo de configuración de cinta:

| Elemento                         | Tamaño         | Descripción                                                                |
|----------------------------------|----------------|----------------------------------------------------------------------------|
| <code>vendor_id</code> (cadena)  | hasta 8 bytes  | El ID del proveedor según lo informa la <code>SCSI Inquiry</code> comando. |
| <code>product_id</code> (cadena) | hasta 16 bytes | El ID de producto indicado por la <code>SCSI Inquiry</code> comando.       |

| Elemento                            | Tamaño         | Descripción                                                                                                                                                                                                              |
|-------------------------------------|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>id_match_size(número)</code>  |                | El número de bytes del ID de producto que se va a utilizar para la coincidencia para detectar la unidad de cinta que se va a identificar, comenzando por el primer carácter del ID de producto en los datos de consulta. |
| <code>vendor_pretty (cadena)</code> | hasta 16 bytes | Si este parámetro está presente, se especifica mediante la cadena mostrada por el comando, <code>storage tape show -device -names</code> ; De lo contrario, se mostrará <code>INQ_VENDOR_ID</code> .                     |
| <code>product_pretty(cadena)</code> | hasta 16 bytes | Si este parámetro está presente, se especifica mediante la cadena mostrada por el comando, <code>storage tape show -device -names</code> ; De lo contrario, aparecerá <code>INQ_PRODUCT_ID</code> .                      |




La `vendor_pretty` y.. `product_pretty` los campos son opcionales, pero si uno de estos campos tiene un valor, el otro también debe tener un valor.

En la siguiente tabla se explica la descripción, el código de densidad y el algoritmo de compresión de los distintos tipos de compresión, como l, m, h, y. a:

| Elemento                              | Tamaño         | Descripción                                                                                                                                                         |
|---------------------------------------|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>`{l</code>                      | m              | h                                                                                                                                                                   |
| <code>a}_description=(string)`</code> | hasta 24 bytes | La cadena que se va a imprimir para el comando <code>nodeshell, sysconfig -t</code> , que describe las características de la configuración de densidad determinada. |
| <code>`{l</code>                      | m              | h                                                                                                                                                                   |
| <code>a}_density=(hex codes)`</code>  |                | El código de densidad que se va a establecer en el descriptor de bloque de página del modo SCSI correspondiente al código de densidad deseado para l, m, h o a..    |
| <code>`{l</code>                      | m              | h                                                                                                                                                                   |

| Elemento                  | Tamaño | Descripción                                                                                                                                                           |
|---------------------------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| a}_algorithm=(hex codes)` |        | El algoritmo de compresión que se establecerá en la página del modo de compresión SCSI correspondiente al código de densidad y la característica de densidad deseada. |

En la siguiente tabla se describen los campos opcionales disponibles en el archivo de configuración de cinta:

| Campo                     | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| autoload=(Boolean yes/no) | Este campo está establecido en <code>yes</code> si la unidad de cinta tiene una función de carga automática, es decir, después de insertar el cartucho de cinta, la unidad de cinta estará lista sin necesidad de ejecutar un <code>SCSI load</code> (unidad de arranque/parada). El valor predeterminado de este campo es <code>no</code> .                                                                                                                                                                                                                                  |
| cmd_timeout_0x            | <p>Valor de tiempo de espera individual. Debe utilizar este campo sólo si desea especificar un valor de tiempo de espera diferente del que está utilizando como valor predeterminado el controlador de cinta. El archivo de ejemplo enumera los valores de tiempo de espera predeterminados del comando SCSI que utiliza la unidad de cinta. El valor de tiempo de espera puede expresarse en minutos (m), segundos (s) o milisegundos (ms).</p> <div>  No debe cambiar este campo. </div> |

Puede descargar y ver el archivo de configuración de cinta desde el sitio de soporte de NetApp.

### Ejemplo de formato de archivo de configuración de cinta

El formato de archivo de configuración de cinta para la unidad de cinta HP LTO5 ULTRIUM es el siguiente:

```

vendor_id="HP"

product_id="Ultrium 5-SCSI"

id_match_size=9

vendor_pretty="Hewlett-Packard"

product_pretty="LTO-5"

l_description="LTO-3(ro)/4 4/800 GB"

l_density=0x00

```

```
l_algorithm=0x00

m_description="LTO-3(ro)/4 8/1600 GB cmp"

m_density=0x00

m_algorithm=0x01

h_description="LTO-5 1600 GB"

h_density=0x58

h_algorithm=0x00

a_description="LTO-5 3200 GB cmp"

a_density=0x58

a_algorithm=0x01

autoload="sí"
```

#### **Información relacionada**

["Herramientas de NetApp: Archivos de configuración de dispositivos de cinta"](#)

#### **Cómo el sistema de almacenamiento dota a una nueva unidad de cinta de forma dinámica**

El sistema de almacenamiento califica una unidad de cinta de forma dinámica emparejando su ID de proveedor y su ID de producto con la información contenida en la tabla de calificación de cinta.

Cuando conecta una unidad de cinta al sistema de almacenamiento, busca una identificación del proveedor y una coincidencia de ID de producto entre la información obtenida durante la detección de cinta y la información de la tabla de calificación de cinta interna. Si el sistema de almacenamiento detecta una coincidencia, Marca la unidad de cinta como cualificada y puede acceder a la unidad de cinta. Si el sistema de almacenamiento no encuentra una coincidencia, la unidad de cinta permanece en estado no cualificado y no se accede a ella.

#### **Descripción general de los dispositivos de cinta**

##### **Descripción general de los dispositivos de cinta**

Un dispositivo de cinta es una representación de una unidad de cinta. Es una combinación específica de tipo de rebobinado y capacidad de compresión de una unidad de cinta.

Se crea un dispositivo de cinta para cada combinación de tipo de rebobinado y capacidad de compresión. Por tanto, una unidad de cinta o una biblioteca de cintas pueden tener asociados varios dispositivos de cinta. Debe especificar un dispositivo de cinta para mover, escribir o leer cintas.

Al instalar una unidad de cinta o una biblioteca de cintas en un sistema de almacenamiento, ONTAP crea dispositivos de cinta asociados con la unidad de cinta o la biblioteca de cintas.

ONTAP detecta unidades de cinta y bibliotecas de cintas y asigna números lógicos y dispositivos de cinta a ellos. ONTAP detecta las bibliotecas y unidades de cinta SCSI paralelas, SAS y Fibre Channel cuando están conectadas a los puertos de interfaz. ONTAP detecta estas unidades cuando sus interfaces están habilitadas.

#### Formato de nombre de dispositivo de cinta

Cada dispositivo de cinta tiene un nombre asociado que aparece en un formato definido. El formato incluye información acerca del tipo de dispositivo, el tipo de rebobinado, el alias y el tipo de compresión.

El formato de un nombre de dispositivo de cinta es el siguiente:

```
rewind_type st alias_number compression_type
```

`rewind_type` es el tipo de rebobinado.

En la siguiente lista se describen los distintos valores de tipo de rebobinado:

- **r**

ONTAP rebobina la cinta después de que termine de escribir el archivo de cinta.

- **no**

ONTAP no rebobinará la cinta después de que termine de escribir el archivo de cinta. Debe utilizar este tipo de rebobinado cuando desee escribir varios archivos de cinta en la misma cinta.

- **ur**

Este es el tipo de rebobinado de descarga/recarga. Cuando se utiliza este tipo de rebobinado, la biblioteca de cintas descarga la cinta cuando llega al final de un archivo de cinta y, a continuación, carga la cinta siguiente, si existe una.

Debe utilizar este tipo de rebobinado sólo en las siguientes circunstancias:

- La unidad de cinta asociada con este dispositivo se encuentra en una biblioteca de cintas o en un cambiador de medios que se encuentra en el modo de biblioteca.
- La unidad de cinta asociada con este dispositivo está conectada a un sistema de almacenamiento.
- Las cintas suficientes para la operación que está realizando están disponibles en la secuencia de cintas de biblioteca definida para esta unidad de cinta.



Si graba una cinta con un dispositivo de no rebobinado, debe rebobinar la cinta antes de leerla.

`st` es la designación estándar de una unidad de cinta.

`alias_number` Es el alias que ONTAP asigna a la unidad de cinta. Cuando ONTAP detecta una nueva unidad de cinta, ONTAP asigna un alias a la unidad de cinta.

`compression_type` es un código específico de una unidad para la densidad de datos en la cinta y el tipo de compresión.

La siguiente lista describe los distintos valores para `compression_type`:



- **a**

Mayor compresión

- **h**

Alta compresión

- **m**

Compresión media

- **l**

Baja compresión

## Ejemplos

`nrst0a` especifica un dispositivo sin rebobinar en la unidad de cinta 0 utilizando la compresión más alta.

### Ejemplo de una lista de dispositivos de cinta

En el siguiente ejemplo se muestran los dispositivos de cinta asociados con HP Ultrium 2-SCSI:

```

Tape drive (fc202_6:2.126L1) HP Ultrium 2-SCSI
rst0l - rewind device, format is: HP (200GB)
nrst0l - no rewind device, format is: HP (200GB)
urst0l - unload/reload device, format is: HP (200GB)
rst0m - rewind device, format is: HP (200GB)
nrst0m - no rewind device, format is: HP (200GB)
urst0m - unload/reload device, format is: HP (200GB)
rst0h - rewind device, format is: HP (200GB)
nrst0h - no rewind device, format is: HP (200GB)
urst0h - unload/reload device, format is: HP (200GB)
rst0a - rewind device, format is: HP (400GB w/comp)
nrst0a - no rewind device, format is: HP (400GB w/comp)
urst0a - unload/reload device, format is: HP (400GB w/comp)

```

En la siguiente lista se describen las abreviaturas del ejemplo anterior:

- GB—Gigabytes; esta es la capacidad de la cinta.
- con compresión; esto muestra la capacidad de cinta con compresión.

### Compatible con el número de dispositivos de cinta simultáneos

ONTAP admite un máximo de 64 conexiones simultáneas de unidad de cinta, 16 cambiadores de soporte y 16 dispositivos de puente o router para cada sistema de almacenamiento (por nodo) en cualquier combinación de conexiones Fibre Channel, SCSI o SAS.

Las unidades de cinta o los cambiadores de medios pueden ser dispositivos en bibliotecas de cintas físicas o

virtuales o dispositivos independientes.



Aunque un sistema de almacenamiento puede detectar 64 conexiones a unidades de cinta, la cantidad máxima de sesiones de backup y restauración que pueden realizarse de forma simultánea depende de los límites de escalabilidad del motor de backup.

**Información relacionada**

[Límites de escalabilidad para sesiones de backup y restauración de volcado](#)

**Solapamiento de cinta**

**Descripción general de solapamiento de cinta**

Aliasing simplifica el proceso de identificación del dispositivo. Aliasing enlaza un nombre de ruta física (PPN) o un número de serie (SN) de una cinta o un cambiador de soporte a un nombre de alias persistente pero modificable.

La siguiente tabla describe cómo el aliasing de cinta le permite asegurarse de que una unidad de cinta (o biblioteca de cintas o cambiador de medios) está siempre asociada con un único nombre de alias:

| Situación                                                         | Reasignar el alias                                                                |
|-------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| Cuando se reinicia el sistema                                     | La unidad de cinta se reasigna automáticamente su alias anterior.                 |
| Cuando un dispositivo de cinta se mueve a otro puerto             | El alias se puede ajustar para que apunte a la nueva dirección.                   |
| Cuando más de un sistema utiliza un dispositivo de cinta concreto | El usuario puede configurar el alias para que sea el mismo en todos los sistemas. |



Al actualizar de Data ONTAP 8.1.x a Data ONTAP 8.2.x, la función de alias de cinta de Data ONTAP 8.2.x modifica los nombres de alias de cinta existentes. En tal caso, es posible que tenga que actualizar los nombres de alias de cinta en la aplicación de copia de seguridad.

La asignación de alias de cinta proporciona una correspondencia entre los nombres lógicos de los dispositivos de copia de seguridad (por ejemplo, st0 o mc1) y un nombre asignado permanentemente a un puerto, una unidad de cinta o un cambiador de medios.



st0 y st00 son nombres lógicos diferentes.



Los nombres lógicos y números de serie se utilizan sólo para acceder a un dispositivo. Después de acceder al dispositivo, devuelve todos los mensajes de error utilizando el nombre de ruta física.

Hay dos tipos de nombres disponibles para el solapamiento: Nombre de ruta física y número de serie.

**Qué son los nombres de ruta física**

Los nombres de rutas físicas (PNP) son las secuencias de direcciones numéricas que

ONTAP asigna a unidades de cinta y bibliotecas de cintas basadas en el adaptador o switch SCSI-2/3 (ubicación específica) que están conectados al sistema de almacenamiento. Los PPNS también se conocen como nombres eléctricos.

Los PPNS de dispositivos de conexión directa utilizan el siguiente formato: `host_adapter.device_id_lun`



El valor de LUN se muestra solo para los dispositivos de cinta y cambio medio cuyos valores de LUN no son cero; es decir, si el valor de LUN es cero el `lun` No se muestra parte de la PPN.

Por ejemplo, PPN 8.6 indica que el número de adaptador de host es 8, el ID de dispositivo es 6 y el número de unidad lógica (LUN) es 0.

Los dispositivos de cinta SAS también son dispositivos de conexión directa. Por ejemplo, el PPN 5c.4 indica que en un sistema de almacenamiento, el SAS HBA está conectado en la ranura 5, la cinta SAS está conectada al puerto C del SAS HBA y el identificador de dispositivo es 4.

Los PPNS de los dispositivos conectados mediante conmutador Fibre Channel utilizan el siguiente formato: `switch:port_id.device_id_lun`

Por ejemplo, el PPN MY\_SWITCH:5.3L2 indica que la unidad de cinta conectada al puerto 5 de un switch llamado MY\_SWITCH está establecida con el ID de dispositivo 3 y tiene el LUN 2.

La unidad determina el LUN (número de unidad lógica). Fibre Channel, bibliotecas y unidades de cinta SCSI, así como discos, tienen VPN.

Los PPNS de unidades de cinta y bibliotecas no cambian a menos que cambie el nombre del conmutador, se mueva la unidad de cinta o la biblioteca o se reconfigure la unidad de cinta o la biblioteca. Los PPNS permanecen sin cambios después del reinicio. Por ejemplo, si se retira una unidad de cinta denominada MY\_SWITCH:5.3L2 y se conecta una nueva unidad de cinta con el mismo ID de dispositivo y LUN al puerto 5 del conmutador MY\_SWITCH, se podrá acceder a la nueva unidad de cinta mediante MY\_SWITCH:5.3L2.

### Qué son los números de serie

Un número de serie (SN) es un identificador único para una unidad de cinta o un cambiador de medios. ONTAP genera alias basados en SN en lugar de WWN.

Dado que el SN es un identificador único para una unidad de cinta o un cambiador de medios, el alias permanece igual independientemente de las múltiples rutas de conexión a la unidad de cinta o al cambiador de medios. Esto ayuda a los sistemas de almacenamiento a realizar un seguimiento de la misma unidad de cinta o cambiador de medios en una configuración de biblioteca de cintas.

El número de serie de una unidad de cinta o un cambiador de medios no cambia aunque cambie el nombre del conmutador Fibre Channel al que está conectada la unidad de cinta o el cambiador de medios. Sin embargo, en una biblioteca de cintas si reemplaza una unidad de cinta existente con una nueva, ONTAP genera nuevos alias porque cambia el número de serie de la unidad de cinta. Además, si mueve una unidad de cinta existente a una nueva ranura de una biblioteca de cintas o reasigna el LUN de la unidad de cinta, ONTAP genera un nuevo alias para esa unidad de cinta.



Debe actualizar las aplicaciones de backup con los alias recién generados.

El número de serie de un dispositivo de cinta utiliza el siguiente formato: `SN[xxxxxxxxxx]L[X]`

x Es un carácter alfanumérico y Lx Es el LUN del dispositivo de cinta. Si el LUN es 0, la L.x no se muestra parte de la cadena.

Cada SN consta de hasta 32 caracteres; el formato para el SN no distingue entre mayúsculas y minúsculas.

**Consideraciones que tener en cuenta al configurar el acceso a cinta multivía**

Puede configurar dos rutas desde el sistema de almacenamiento para acceder a las unidades de cinta de una biblioteca de cintas. Si falla una ruta, el sistema de almacenamiento puede utilizar las otras rutas para acceder a las unidades de cinta sin tener que reparar inmediatamente la ruta con error. Esto garantiza que se puedan reiniciar las operaciones de cinta.

Al configurar el acceso a cinta multivía desde el sistema de almacenamiento, debe tener en cuenta lo siguiente:

- En bibliotecas de cintas que admiten la asignación de LUN, para acceder de varias rutas a un grupo LUN, la asignación de LUN debe ser simétrica en cada ruta.
- Las unidades de cinta e intercambiadores de medios se asignan a grupos de LUN (conjunto de LUN que comparten el mismo conjunto de rutas del iniciador) en una biblioteca de cintas. Todas las unidades de cinta de un grupo LUN deben estar disponibles para las operaciones de backup y restauración en todas las rutas múltiples.
- Se puede configurar un máximo de dos rutas desde el sistema de almacenamiento para acceder a las unidades de cinta de una biblioteca de cintas.
- El acceso a cinta multivía es compatible con el equilibrio de carga. El equilibrio de carga está deshabilitado de forma predeterminada.

En el ejemplo siguiente, el sistema de almacenamiento accede al grupo LUN 0 a través de dos rutas de iniciador: 0b y 0d. En estas dos rutas, el grupo de LUN tiene el mismo número de LUN, 0 y el número de LUN, 5. El sistema de almacenamiento accede al grupo LUN 1 a través de solo una ruta de iniciador, 3d.

```
STSW-3070-2_cluster::> storage tape library config show
```

| Node                   | LUN Group | LUN Count | Library Name  | Library |
|------------------------|-----------|-----------|---------------|---------|
| Target Port            | Initiator |           |               |         |
| STSW-3070-2_cluster-01 | 0         | 5         | IBM 3573-TL_1 |         |
| 510a09800000412d       | 0b        |           |               |         |
| 0d                     |           |           |               |         |
|                        | 1         | 2         | IBM 3573-TL_2 |         |
| 50050763124b4d6f       | 3d        |           |               |         |

3 entries were displayed

Para obtener más información, consulte las páginas de manual.

## Cómo se añaden unidades y bibliotecas de cinta a los sistemas de almacenamiento

Puede agregar bibliotecas y unidades de cinta al sistema de almacenamiento de forma dinámica (sin desconectar el sistema).

Al añadir un nuevo cambiador de medios, el sistema de almacenamiento detecta su presencia y la añade a la configuración. Si ya se hace referencia al cambiador de medios en la información del alias, no se crea ningún nombre lógico nuevo. Si no se hace referencia a la biblioteca, el sistema de almacenamiento crea un nuevo alias para el cambiador de medios.

En una configuración de biblioteca de cintas, debe configurar una unidad de cinta o un cambiador de medios en el LUN 0 de un puerto de destino para ONTAP para descubrir todos los cambiadores de medios y unidades de cinta en ese puerto de destino.

### Qué reservas de cinta son

Múltiples sistemas de almacenamiento pueden compartir el acceso a unidades de cinta, cambiadores de medio, puentes o bibliotecas de cintas. Las reservas de cintas garantizan que sólo un sistema de almacenamiento pueda acceder a un dispositivo en cualquier momento, ya sea habilitando el mecanismo de reserva/versión SCSI o las reservas persistentes SCSI para todas las unidades de cinta, cambiadores medianos, puentes y bibliotecas de cintas.



Todos los sistemas que comparten dispositivos en una biblioteca, incluidos o no conmutadores, deben utilizar el mismo método de reserva.

El mecanismo de reserva/liberación SCSI para reservar dispositivos funciona bien en condiciones normales. Sin embargo, durante los procedimientos de recuperación de errores de interfaz, se pueden perder las reservas. Si esto sucede, los iniciadores que no son el propietario reservado pueden acceder al dispositivo.

Las reservas realizadas con reservas persistentes SCSI no se ven afectadas por mecanismos de recuperación de errores, como el restablecimiento de bucle o el restablecimiento de objetivos; sin embargo, no todos los dispositivos implementan correctamente las reservas persistentes SCSI.

## Transferir datos mediante ndmpcopy

### Transfiera los datos utilizando la descripción general de ndmpcopy

La `ndmcopy` Nodelsinfierno Command transfiere datos entre sistemas de almacenamiento que admiten NDMP v4. Puede realizar transferencias de datos completas e incrementales. Puede transferir volúmenes completos o parciales, qtrees, directorios o archivos individuales.

### Acerca de esta tarea

Gracias al uso de ONTAP 8.x y versiones anteriores, las transferencias incrementales están limitadas a un máximo de dos niveles (uno completo y hasta dos backups incrementales).

A partir de ONTAP 9.0 y versiones posteriores, las transferencias incrementales están limitadas a un máximo de nueve niveles (uno completo y hasta nueve backups incrementales).


Puede ejecutar `ndmcopy` en la línea de comandos `nodesinfierno` de los sistemas de almacenamiento de

origen y destino, o un sistema de almacenamiento que no es el origen ni el destino de la transferencia de datos. También puede ejecutar `ndmpcopy` en un único sistema de almacenamiento que sea el origen y el destino de la transferencia de datos.

Las direcciones IPv4 o IPv6 de los sistemas de almacenamiento de origen y destino en el `ndmpcopy` comando. El formato de ruta es `/vserver_name/volume_name \[path\]`.


**Pasos**

1. Active el servicio NDMP en los sistemas de almacenamiento de origen y destino:

| Si realiza transferencia de datos en el origen o el destino en... | Usar el siguiente comando...                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Modo de NDMP con ámbito SVM                                       | <div><pre>vserver services ndmp on</pre></div> <div><div>Para la autenticación NDMP en la SVM de administrador, la cuenta de usuario es <code>admin</code> y el rol de usuario es <code>admin</code> o <code>backup</code>. En la SVM de datos, la cuenta de usuario es <code>vsadmin</code> y el rol de usuario es <code>vsadmin</code> o <code>vsadmin-backup</code> función.</div></div> |
| Modo de NDMP con ámbito del nodo                                  | <pre>system services ndmp on</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                           |

2. Transferir datos dentro de un sistema de almacenamiento o entre sistemas de almacenamiento mediante el `ndmpcopy` mando en el `nodesinfierno`:

```
::> system node run -node <node_name> < ndmpcopy [options]
source_IP:source_path destination_IP:destination_path [-mcs {inet|inet6}] [-mcd {inet|inet6}] [-md {inet|inet6}]
```



Los nombres DNS no son compatibles con `ndmpcopy`. Debe proporcionar la dirección IP del origen y del destino. La dirección de bucle invertido (127.0.0.1) no es compatible con la dirección IP de origen ni con la dirección IP de destino.

- La `ndmpcopy` command determina el modo de dirección para las conexiones de control de la siguiente manera:
  - El modo de dirección para la conexión de control corresponde a la dirección IP proporcionada.
  - Puede anular estas reglas mediante el `-mcs` y.. `-mcd` opciones.
- Si el origen o el destino son el sistema ONTAP, entonces según el modo NDMP (ámbito del nodo o ámbito de la SVM), utilice una dirección IP que permita el acceso al volumen de destino.
- `source_path` y.. `destination_path` son los nombres de ruta absolutos hasta el nivel granular de volumen, `qtree`, directorio o archivo.
- `-mcs` especifica el modo de direccionamiento preferido para la conexión de control al sistema de almacenamiento de origen.

`inet` Indica un modo de dirección IPv4 y `inet6` Indica un modo de dirección IPv6.

- `-mcd` especifica el modo de direccionamiento preferido para la conexión de control al sistema de almacenamiento de destino.

`inet` Indica un modo de dirección IPv4 y `inet6` Indica un modo de dirección IPv6.

- `-md` especifica el modo de direccionamiento preferido para transferencias de datos entre los sistemas de almacenamiento de origen y destino.

`inet` Indica un modo de dirección IPv4 y `inet6` Indica un modo de dirección IPv6.

Si no utiliza la `-md` en la `ndmcopy` comando, el modo de direccionamiento de la conexión de datos se determina de la siguiente manera:

- Si alguna de las direcciones especificadas para las conexiones de control es una dirección IPv6, el modo de dirección para la conexión de datos es IPv6.
- Si las dos direcciones especificadas para las conexiones de control son direcciones IPv4, el `ndmcopy` En primer lugar, Command intenta utilizar un modo de dirección IPv6 para la conexión de datos.

Si no es así, el comando utiliza un modo de dirección IPv4.



Una dirección IPv6, si se especifica, debe escribirse entre corchetes.

Este comando de ejemplo migra datos de una ruta de acceso de origen (`source_path`) a una ruta de destino (`destination_path`).

```
> ndmcopy -sa admin:<ndmp_password> -da admin:<ndmp_password>
 -st md5 -dt md5 192.0.2.129:/<src_svm>/<src_vol>
192.0.2.131:/<dst_svm>/<dst_vol>
```

+

Este comando de ejemplo establece explícitamente las conexiones de control y la conexión de datos para utilizar el modo de dirección IPv6:

```
> ndmcopy -sa admin:<ndmp_password> -da admin:<ndmp_password> -st md5
-dt md5 -mcs inet6 -mcd inet6 -md
 inet6 [2001:0db8:1:1:209:6bff:feae:6d67]:/<src_svm>/<src_vol>
[2001:0ec9:1:1:200:7cgg:gfd7:7e78]:/<dst_svm>/<dst_vol>
```

## Opciones para el comando `ndmcopy`

Debe comprender las opciones disponibles para el `ndmcopy nodeshell` comando para transferir datos con éxito.

En la siguiente tabla se enumeran las opciones disponibles. Para obtener más información, consulte

| Opción                                                                                                                                                                                                                                   | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -sa username:[password]                                                                                                                                                                                                                  | <p>Esta opción configura el nombre de usuario y la contraseña de autenticación de origen para conectarse con el sistema de almacenamiento de origen. Esta es una opción obligatoria.</p> <p>Para un usuario sin privilegios de administrador, debe especificar la contraseña específica de NDMP generada por el sistema del usuario. La contraseña que genera el sistema es obligatoria tanto para los usuarios administradores como para los que no son de administrador.</p> |
| -da username:[password]                                                                                                                                                                                                                  | <p>Esta opción establece el nombre de usuario y la contraseña de autenticación de destino para conectarse al sistema de almacenamiento de destino. Esta es una opción obligatoria.</p>                                                                                                                                                                                                                                                                                         |
| -st {md5                                                                                                                                                                                                                                 | text}                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Esta opción establece el tipo de autenticación de origen que se va a utilizar al conectarse al sistema de almacenamiento de origen. Esta es una opción obligatoria y, por lo tanto, el usuario debe proporcionar una text o. md5 opción. | -dt {md5                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| text}                                                                                                                                                                                                                                    | Esta opción establece el tipo de autenticación de destino que se utilizará al conectarse al sistema de almacenamiento de destino.                                                                                                                                                                                                                                                                                                                                              |
| -l                                                                                                                                                                                                                                       | Esta opción establece el nivel de volcado utilizado para la transferencia al valor especificado de level. Valid are 0, 1, a. 9, donde 0 indica una transferencia completa y. 1 para 9 especifica una transferencia incremental. El valor predeterminado es 0.                                                                                                                                                                                                                  |
| -d                                                                                                                                                                                                                                       | Esta opción permite la generación de mensajes de registro de depuración ndmpcopy. Los archivos de registro de depuración ndmpcopy se encuentran en la /mroot/etc/log volumen raíz. Los nombres de los archivos de registro de depuración ndmpcopy se encuentran en la ndmpcopy.yyyymmdd formato.                                                                                                                                                                               |
| -f                                                                                                                                                                                                                                       | Esta opción activa el modo forzado. Este modo permite que los archivos del sistema se sobrescriban en la /etc directorio en la raíz del volumen 7-Mode.                                                                                                                                                                                                                                                                                                                        |



| Opción   | Descripción                                                                                                                                                                                                                                                                                                                                                                     |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -h       | Esta opción imprime el mensaje de ayuda.                                                                                                                                                                                                                                                                                                                                        |
| -p       | <p>Esta opción le pide que introduzca la contraseña para la autorización de origen y destino. Esta contraseña anula la contraseña especificada para -sa y.. -da opciones.</p> <div>  <p>Esta opción solo se puede utilizar cuando el comando se ejecuta en una consola interactiva.</p> </div> |
| -exclude | Esta opción excluye los archivos o directorios especificados de la ruta de acceso especificada para la transferencia de datos. El valor puede ser una lista separada por comas de nombres de directorio o de archivo como <b>.pst</b> o <b>.txt</b> .                                                                                                                           |

## NDMP para volúmenes FlexVol

### Acerca de NDMP para volúmenes FlexVol

El protocolo de gestión de datos de red (NDMP) es un protocolo estandarizado para controlar el backup, la recuperación y otros tipos de transferencia de datos entre dispositivos de almacenamiento primarios y secundarios, como sistemas de almacenamiento y bibliotecas de cintas.

Al habilitar la compatibilidad con NDMP en un sistema de almacenamiento, permite que ese sistema de almacenamiento se comuniquen con aplicaciones de backup conectadas a la red compatibles con NDMP (también denominadas *Data Management Applications* o *DMAs*), servidores de datos y servidores de cinta que participan en operaciones de backup o recuperación. Todas las comunicaciones de red se producen a través de la red TCPIP o TCP/IPv6. NDMP también proporciona un control de bajo nivel de unidades de cinta e intercambiadores de tamaño medio.

Puede realizar operaciones de backup y restauración de cinta en el modo NDMP de ámbito del nodo o en el modo NDMP de la máquina virtual de almacenamiento (SVM) con ámbito.

Debe saber cuáles son las consideraciones que debe tener en cuenta a la hora de utilizar NDMP, la lista de variables de entorno y las topologías de backup en cinta de NDMP admitidas. También puede habilitar o deshabilitar la funcionalidad DAR mejorada. Los dos métodos de autenticación compatibles con ONTAP para autenticar el acceso NDMP a un sistema de almacenamiento son: Sin formato y sin reto.

### Información relacionada

[Variables de entorno compatibles con ONTAP](#)

### Acerca de los modos de funcionamiento de NDMP

Puede optar por realizar operaciones de backup y restauración a cinta, ya sea en el nivel de nodo o en el nivel de la máquina virtual de almacenamiento (SVM). Para ejecutar

estas operaciones correctamente en el nivel de SVM, el servicio NDMP debe estar habilitado en la SVM.

Si actualiza de Data ONTAP 8.2 a Data ONTAP 8.3, seguirá reteniendo el modo de funcionamiento NDMP usado en 8.2 después de la actualización de 8.2 a 8.3.

Si instala un clúster nuevo con Data ONTAP 8.2 o posterior, NDMP se encuentra en el modo NDMP de ámbito SVM de manera predeterminada. Para realizar operaciones de backup y restauración de cinta en el modo de NDMP de ámbito del nodo, debe habilitar explícitamente el modo de NDMP de ámbito del nodo.

#### **Información relacionada**

[Comandos para gestionar el modo NDMP de ámbito de nodo](#)

[Gestionar el modo NDMP de ámbito del nodo para volúmenes FlexVol](#)

[Gestionar el modo NDMP de ámbito SVM para volúmenes FlexVol](#)

#### **Lo que es el modo NDMP de ámbito del nodo**

En el modo NDMP de ámbito del nodo, puede realizar operaciones de backup y restauración a cinta en el nivel del nodo. Se seguirá reteniendo el modo de funcionamiento NDMP usado en Data ONTAP 8.2 después de la actualización de 8.2 a 8.3.

En el modo NDMP de ámbito del nodo, puede realizar operaciones de backup y restauración de cinta en un nodo que posea el volumen. Para realizar estas operaciones, debe establecer conexiones de control NDMP en una LIF alojada en el nodo propietario de los dispositivos de volumen o cinta.



Este modo quedó obsoleto y se quitará en un lanzamiento principal futuro.

#### **Información relacionada**

[Gestionar el modo NDMP de ámbito del nodo para volúmenes FlexVol](#)

#### **Qué es el modo NDMP con ámbito SVM**

Se pueden ejecutar operaciones de backup y restauración de cinta en el nivel de máquina virtual de almacenamiento (SVM) correctamente si el servicio NDMP está habilitado en la SVM. Puede realizar backups y restauraciones de todos los volúmenes alojados en diferentes nodos en la SVM de un clúster si la aplicación de backup admite la extensión CAB.

Se puede establecer una conexión de control NDMP en diferentes tipos de LIF. En el modo NDMP con ámbito SVM, estas LIF pertenecen a la SVM de datos o a la SVM de administrador. La conexión puede establecerse en un LIF solo si el servicio NDMP está habilitado en la SVM propietaria de este LIF.

Una LIF de datos pertenece a la SVM de datos y la LIF entre clústeres, la LIF de gestión de nodos y la LIF de gestión de clúster pertenecen a la SVM de administrador.

En el modo NDMP de ámbito SVM, la disponibilidad de volúmenes y dispositivos de cinta para operaciones de backup y restauración depende del tipo de LIF en el que se establezca la conexión de control NDMP y el estado de la extensión CAB. Si su aplicación de backup admite la extensión CAB y un volumen y el dispositivo de cinta comparten la misma afinidad, la aplicación de backup puede realizar una operación de backup o

restauración local, en lugar de una operación de backup o restauración triple.

## Información relacionada

[Gestionar el modo NDMP de ámbito SVM para volúmenes FlexVol](#)

## Consideraciones que tener en cuenta al utilizar NDMP

Debe tener en cuenta una serie de consideraciones que se deben tener en cuenta al iniciar el servicio NDMP en el sistema de almacenamiento.

- Cada nodo admite un máximo de 16 backups, restauraciones o combinación simultáneas de los dos mediante unidades de cinta conectadas.
- Los servicios NDMP pueden generar datos del historial de ficheros si así lo solicitan las aplicaciones de backup NDMP.

El historial de archivos se utiliza en las aplicaciones de copia de seguridad para permitir la recuperación optimizada de subconjuntos seleccionados de datos de una imagen de copia de seguridad. La generación y el procesamiento del historial de archivos pueden requerir mucho tiempo y requerir gran cantidad de CPU tanto en el sistema de almacenamiento como en la aplicación de backup.



SMTape no admite el historial de archivos.

Si la protección de datos está configurada para la recuperación ante desastres, donde se recuperará toda la imagen de copia de seguridad, puede deshabilitar la generación del historial de archivos para reducir el tiempo de copia de seguridad. Consulte la documentación de la aplicación de copia de seguridad para determinar si es posible desactivar la generación del historial de archivos NDMP.

- La política de firewall para NDMP está habilitada de forma predeterminada en todos los tipos de LIF.
- En el modo NDMP de ámbito del nodo, el backup de un volumen FlexVol requiere que utilice la aplicación de backup para iniciar un backup en un nodo propietario del volumen.

Sin embargo, no puede realizar backups de un volumen raíz de nodo.

- Puede realizar un backup NDMP desde cualquier LIF de la forma permitida por las políticas de firewall.

Si utiliza una LIF de datos, debe seleccionar una LIF que no esté configurada para la conmutación por error. Si una LIF de datos conmuta al nodo de respaldo durante una operación de NDMP, la operación de NDMP falla y debe volver a ejecutarse.

- En el modo NDMP de ámbito del nodo y la máquina virtual de almacenamiento (SVM) en modo NDMP sin soporte de extensión CAB, la conexión de datos NDMP usa la misma LIF que la conexión de control NDMP.
- Durante la migración de LIF, las operaciones de backup y restauración continuas se interrumpen.

Debe iniciar las operaciones de backup y restauración después de la migración de LIF.

- La ruta de backup NDMP tiene el formato `/vserver_name/volume_name/path_name`.

*path\_name* Es opcional y especifica la ruta del directorio, el archivo o la copia Snapshot.

- Cuando se realiza un backup de un destino de SnapMirror a cinta mediante el motor de volcado, solo se realiza un backup de los datos del volumen.

Sin embargo, si se realiza un backup de un destino de SnapMirror en cinta con SMTape, también se realiza el backup de los metadatos. Las relaciones de SnapMirror y los metadatos asociados no se realizan en un backup a cinta. Por lo tanto, durante la restauración, solo se restauran los datos de ese volumen, pero no se restauran las relaciones de SnapMirror asociadas.

## Información relacionada

[Qué hace la extensión Cluster Aware Backup](#)

["Conceptos de ONTAP"](#)

["Administración del sistema"](#)

## Variable de entorno

### Información general de las variables de entorno

Las variables de entorno se utilizan para comunicar información sobre una operación de backup o restauración entre una aplicación de backup habilitada para NDMP y un sistema de almacenamiento.

Por ejemplo, si un usuario especifica que una aplicación de backup debe realizar un backup `/vserver1/vol1/dir1`, La aplicación de copia de seguridad establece la variable de entorno `DEL SISTEMA de ARCHIVOS /vserver1/vol1/dir1`. Del mismo modo, si un usuario especifica que una copia de seguridad debe ser una copia de seguridad de nivel 1, la aplicación de copia de seguridad establece la variable DE entorno DE NIVEL en 1 (una).



La configuración y examen de las variables de entorno suelen ser transparentes para los administradores de backup, es decir, la aplicación de backup las establece automáticamente.

Un administrador de backup rara vez especifica variables de entorno; no obstante, se puede cambiar el valor de una variable de entorno de la cual establece la aplicación de backup para caracterizar o trabajar en torno a un problema funcional o de rendimiento. Por ejemplo, es posible que un administrador desee deshabilitar temporalmente la generación del historial de archivos para determinar si el procesamiento de la información del historial de archivos de la aplicación de copia de seguridad está contribuyendo a problemas de rendimiento o de funcionamiento.

Muchas aplicaciones de backup proporcionan un medio para anular o modificar variables de entorno o especificar variables de entorno adicionales. Para obtener información, consulte la documentación de la aplicación de copia de seguridad.

### Variables de entorno compatibles con ONTAP

Las variables de entorno se utilizan para comunicar información sobre una operación de backup o restauración entre una aplicación de backup habilitada para NDMP y un sistema de almacenamiento. ONTAP admite variables de entorno, con un valor predeterminado asociado. Sin embargo, puede modificar manualmente estos valores predeterminados.

Si modifica manualmente los valores establecidos por la aplicación de backup, la aplicación podría comportarse de forma impredecible. Esto se debe a que es posible que las operaciones de backup o restauración no hagan lo que la aplicación de backup esperaba que hicieran. Pero en algunos casos, una modificación juiciosa podría ayudar a identificar o a solucionar problemas.

En las tablas siguientes se enumeran las variables de entorno cuyo comportamiento es común para el volcado y SMTape y las variables que sólo se admiten para el volcado y SMTape. Estas tablas también contienen descripciones de cómo funcionan las variables de entorno compatibles con ONTAP si se utilizan:



En la mayoría de los casos, variables que tienen el valor, `Y` también aceptar `T` y.. `N` también aceptar `F`.

#### Variables de entorno compatibles para volcado y SMTape

| Variable de entorno | Valores válidos                 | Predeterminado    | Descripción                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------|---------------------------------|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DEPURAR             | <code>Y</code> o <code>N</code> | <code>N</code>    | Especifica que se imprime la información de depuración.                                                                                                                                                                                                                                                                                                                                                         |
| SISTEMA DE ARCHIVOS | <code>string</code>             | <code>none</code> | Especifica el nombre de la ruta de acceso de la raíz de los datos de los que se va a realizar una copia de seguridad.                                                                                                                                                                                                                                                                                           |
| VERSIÓN_NDMP        | <code>return_only</code>        | <code>none</code> | <p>No debe modificar la variable <code>NDMP_VERSION</code>. Creada por la operación de backup, la variable <code>NDMP_VERSION</code> devuelve la versión de NDMP.</p> <p>ONTAP establece la variable <code>NDMP_VERSION</code> durante un backup para uso interno y para pasar a una aplicación de backup con fines informativos. La versión NDMP de una sesión NDMP no está configurada con esta variable.</p> |

| Variable de entorno   | Valores válidos | Predeterminado | Descripción                                                                                                                                                                                                                                                                                                                  |
|-----------------------|-----------------|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SEPARADOR_NOMBRE_RUTA | return_value    | none           | <p>Especifica el carácter separador del nombre de ruta de acceso.</p> <p>Este carácter depende del sistema de archivos del que se va a realizar el backup. En el caso de ONTAP, el carácter «»/» se asignará a esta variable. El servidor NDMP configura esta variable antes de iniciar una operación de backup a cinta.</p> |
| TIPO                  | dump o. smtape  | dump           | Especifica el tipo de backup admitido para realizar operaciones de backup y restauración a cinta.                                                                                                                                                                                                                            |
| VERBOSE               | Y o. N          | N              | Aumenta los mensajes de registro mientras se realiza una operación de copia de seguridad o restauración de cinta.                                                                                                                                                                                                            |

#### Variables de entorno compatibles con el volcado

| Variable de entorno | Valores válidos | Predeterminado | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------|-----------------|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ACL_START           | return_only     | none           | <p>Creada por la operación de backup, la variable ACL_START es un valor de desplazamiento que utilizan una operación de restauración de acceso directo o de backup NDMP reinicializable.</p> <p>El valor de desplazamiento es el desplazamiento de bytes en el archivo de volcado donde comienzan los datos de ACL (pase V) y se devuelven al final de una copia de seguridad. Para que una operación de restauración de acceso directo restaure correctamente los datos de los que se ha realizado un backup, el valor de ACL_START debe pasarse a la operación de restauración cuando se inicia. Una operación de backup reinicializable de NDMP utiliza el valor ACL_START para comunicarse con la aplicación de backup donde comienza la parte no reinicializable del flujo de backup.</p> |

| Variable de entorno | Valores válidos              | Predeterminado | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------|------------------------------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FECHA_BASE          | 0, -1, o. DUMP_DATE<br>valor | -1             | <p>Especifica la fecha de inicio de las copias de seguridad incrementales.</p> <p>Cuando se establece en -1, El especificador incremental BASE_DATE está desactivado. Cuando se establece en 0 en un backup de nivel 0, se habilitan los backups incrementales. Después de la copia de seguridad inicial, el valor de la variable DUMP_DATE de la copia de seguridad incremental anterior se asigna a la variable BASE_DATE.</p> <p>Estas variables son una alternativa a las copias de seguridad incrementales basadas en NIVEL/ACTUALIZACIÓN.</p> |
| DIRECTO             | Y o. N                       | N              | <p>Especifica que una restauración se debe reenviar directamente a la ubicación de la cinta en la que residen los datos del archivo en lugar de analizar la cinta completa.</p> <p>Para que la recuperación de acceso directo funcione, la aplicación de backup debe proporcionar información de posicionamiento. Si esta variable está establecida en Y, la aplicación de copia de seguridad especifica los nombres de archivo o directorio y la información de posicionamiento.</p>                                                               |




| Variable de entorno | Valores válidos | Predeterminado | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------|-----------------|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NOMBRE_DMP          | string          | none           | <p>Especifica el nombre de una copia de seguridad de varios subárboles.</p> <p>Esta variable es obligatoria para varias copias de seguridad de subárbol.</p>                                                                                                                                                                                                                                                                                                              |
| FECHA_DE_VOLCADO    | return_value    | none           | <p>No se cambia esta variable directamente. Lo crea el backup si la variable BASE_DATE se establece en un valor distinto de -1.</p> <p>LA variable DUMP_DATE se deriva prependiente el valor de nivel de 32 bits a un valor de tiempo de 32 bits calculado por el software de volcado. El nivel se incrementa desde el valor del último nivel pasado a la variable BASE_DATE. El valor resultante se utiliza como valor BASE_DATE en un backup incremental posterior.</p> |


| Variable de entorno     | Valores válidos | Predeterminado | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------|-----------------|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MEJORADO_DAR_HABILITADO | Y o. N          | N              | <p>Especifica si la funcionalidad DAR mejorada está activada. La funcionalidad DAR mejorada es compatible con DAR de directorios y DAR de ficheros con secuencias NT. Proporciona mejoras de rendimiento.</p> <p>Las mejoras DE DAR durante la restauración solo son posibles si se cumplen las siguientes condiciones:</p> <ul style="list-style-type: none"> <li>• ONTAP admite DAR mejorado.</li> <li>• El historial de archivos está activado (HIST=y) durante la copia de seguridad.</li> <li>• La <code>ndmpd.offset_map.enable</code> opción establecida en on.</li> <li>• La variable <code>ENHANCED_DAR_ENABLED</code> se establece en Y durante la restauración.</li> </ul> |

| Variable de entorno | Valores válidos | Predeterminado | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------|-----------------|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EXCLUIR             | pattern_string  | none           | <p>Especifica los archivos o directorios que se excluyen al realizar una copia de seguridad de los datos.</p> <p>La lista de exclusión es una lista de nombres de archivos o directorios separados por comas. Si el nombre de un archivo o directorio coincide con uno de los nombres de la lista, se excluye de la copia de seguridad.</p> <p>Las siguientes reglas se aplican al especificar nombres en la lista excluir:</p> <ul style="list-style-type: none"> <li>• Debe utilizarse el nombre exacto del archivo o directorio.</li> <li>• El asterisco (*), un carácter comodín, debe ser el primer carácter o el último de la cadena.</li> </ul> <p>Cada cadena puede tener hasta dos asteriscos.</p> <ul style="list-style-type: none"> <li>• Una coma en un nombre de archivo o directorio debe ir precedida de una barra invertida.</li> <li>• La lista de exclusión puede contener hasta 32 nombres.</li> </ul> |
|                     |                 |                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| Variable de entorno | Valores válidos | Predeterminado | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------|-----------------|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EXTRAER             | Y, N, o. E      | N              | <p>Especifica que se van a restaurar los subárboles de un conjunto de datos de copia de seguridad.</p> <p>La aplicación de copia de seguridad especifica los nombres de los subárboles que se van a extraer. Si un archivo especificado coincide con un directorio cuyo contenido se hizo una copia de seguridad, el directorio se extrae recursivamente.</p> <p>Para cambiar el nombre de un archivo, directorio o qtree durante la restauración sin usar DAR, debe configurar la variable de entorno DE EXTRACCIÓN en E.</p> |
| EXTRAER_ACL         | Y o. N          | Y              | <p>Especifica que las ACL del archivo de copia de seguridad se restauran en una operación de restauración.</p> <p>El valor predeterminado es restaurar las ACL cuando se restauran los datos, excepto para DARS (DIRECT=y).</p>                                                                                                                                                                                                                                                                                                |

| Variable de entorno | Valores válidos | Predeterminado | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------|-----------------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FUERZA              | Y o. N          | N              | <p>Determina si la operación de restauración debe comprobar la disponibilidad de espacio de volumen y de nodos de información en el volumen de destino.</p> <p>Estableciendo esta variable en Y hace que la operación de restauración omita las comprobaciones del espacio del volumen y de la disponibilidad de nodos de información en la ruta de destino.</p> <p>Si no hay suficiente espacio o inodos en el volumen de destino, la operación de restauración recupera la cantidad de datos permitidos por el espacio del volumen de destino y la disponibilidad de nodos de información. La operación de restauración se detiene cuando el espacio del volumen o los inodos no están disponibles.</p> |

| Variable de entorno | Valores válidos | Predeterminado | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------|-----------------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HIST                | Y o. N          | N              | <p>Especifica que la información del historial de archivos se envía a la aplicación de copia de seguridad.</p> <p>La mayoría de las aplicaciones de copia de seguridad comerciales establecen la variable HIST como Y. Si desea aumentar la velocidad de una operación de copia de seguridad o desea solucionar un problema con la colección de historial de archivos, puede establecer esta variable en N.</p> <div>  <p>No debe establecer la variable HIST en Y si la aplicación de copia de seguridad no admite el historial de archivos.</p> </div> |


| Variable de entorno | Valores válidos | Predeterminado | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------|-----------------|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IGNORE_CTIME        | Y o. N          | N              | <p>Especifica que no se realiza una copia de seguridad incremental de un archivo si sólo ha cambiado su valor ctime desde la copia de seguridad incremental anterior.</p> <p>Algunas aplicaciones, como el software de análisis de virus, cambian el valor de ctime de un archivo dentro del inodo, aunque el archivo o sus atributos no hayan cambiado. Como resultado, una copia de seguridad incremental puede hacer una copia de seguridad de los archivos que no han cambiado. La IGNORE_CTIME la variable debe especificarse solo si los backups incrementales están tomando una cantidad de tiempo o espacio inaceptable debido a que se ha modificado el valor ctime.</p> <div><div></div><div><p>La NDMP dump conjuntos de comandos IGNORE_CTIME para false de forma predeterminada. Configuración en true puede provocar la siguiente pérdida de datos:</p><ol style="list-style-type: none"><li>Si IGNORE_CTIME se establece</li></ol></div></div> |
|                     |                 |                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

| Variable de entorno | Valores válidos | Predeterminado | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------|-----------------|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IGNORE_QTREES       | Y o. N          | N              | Especifica que la operación de restauración no restaura la información de qtree a partir de qtrees de los que se ha realizado un backup.                                                                                                                                                                                                                                                                                                                                                                                                        |
| NIVEL               | 0-31            | 0              | <p>Especifica el nivel de backup.</p> <p>El nivel 0 copia todo el conjunto de datos. Niveles de copia de seguridad incrementales, especificados por valores superiores a 0, copie todos los archivos (nuevos o modificados) desde la última copia de seguridad incremental. Por ejemplo, un nivel 1 realiza una copia de seguridad de los archivos nuevos o modificados desde la copia de seguridad de nivel 0, un nivel 2 realiza una copia de seguridad de los archivos nuevos o modificados desde la copia de seguridad de nivel 1, etc.</p> |
| LISTA               | Y o. N          | N              | Enumera los nombres de los archivos de backup y los números de nodos de información sin restaurar los datos realmente.                                                                                                                                                                                                                                                                                                                                                                                                                          |
| QTREES_DE_LISTAS    | Y o. N          | N              | Enumera los qtrees de los que se ha realizado backup sin restaurar realmente los datos.                                                                                                                                                                                                                                                                                                                                                                                                                                                         |


archivo  
s, que  
se  
mueve  
n entre  
qtrees  
de  
origen  
durante  
la  
restaur



| Variable de entorno    | Valores válidos | Predeterminado | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------|-----------------|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NOMBRES DE MULTIÁRBOL_ | string          | none           | <p>Especifica que la copia de seguridad es una copia de seguridad de varios subárboles.</p> <p>Se especifican varios subárboles en la cadena, que es una lista de nombres de subárboles separados por nuevas líneas y terminados en nulo. Los subárboles se especifican mediante nombres de ruta relativos a su directorio raíz común, que deben especificarse como último elemento de la lista.</p> <p>Si se usa esta variable, también se debe usar la variable DMP_NAME.</p> |
| NDMP_UNICODE_FH        | Y o. N          | N              | <p>Especifica que se incluye un nombre Unicode además del nombre NFS del archivo en la información del historial de archivos.</p> <p>Esta opción no la utilizan la mayoría de las aplicaciones de copia de seguridad y no debe establecerse a menos que la aplicación de copia de seguridad esté diseñada para recibir estos nombres de archivo adicionales. También se debe establecer la variable HIST.</p>                                                                   |
| NO_ACL                 | Y o. N          | N              | <p>Especifica que las ACL no se deben copiar al realizar copias de seguridad de datos.</p>                                                                                                                                                                                                                                                                                                                                                                                      |

| Variable de entorno | Valores válidos | Predeterminado | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------|-----------------|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ÁRBOL_NO_CUOTA      | Y o. N          | N              | <p>Especifica que los archivos y directorios en qtrees deben ignorarse al realizar una copia de seguridad de los datos.</p> <p>Cuando se establece en Y, No se realiza una copia de seguridad de los elementos de qtrees del conjunto de datos especificado por la variable DEL SISTEMA de ARCHIVOS. Esta variable solo tiene un efecto si la variable FILESYSTEM especifica un volumen completo. La variable NON_QUOTA_TREE sólo funciona en una copia de seguridad de nivel 0 y no funciona si se especifica la variable MULTI_SUBTREE_NAMES.</p> <div>  <p>Los archivos o directorios especificados para ser excluidos para la copia de seguridad no se excluyen si se establece NON_QUOTA_TREE en Y al mismo tiempo.</p> </div> |

| Variable de entorno | Valores válidos | Predeterminado | Descripción                                                                                                                                |
|---------------------|-----------------|----------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| NOWRITE             | Y o. N          | N              | <p>Especifica que la operación de restauración no debe escribir datos en el disco.</p> <p>Esta variable se utiliza para la depuración.</p> |

| Variable de entorno | Valores válidos | Predeterminado | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------|-----------------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RECURSIVA           | Y o. N          | Y              | <p>Especifica que se amplíen las entradas de directorio durante una restauración DE DAR.</p> <p>Deben habilitarse las variables de entorno DIRECT y ENHANCED_DAR_ENABLED (establecer en Y) también. Si la variable RECURSIVA está desactivada (establecida en N), sólo los permisos y las ACL de todos los directorios de la ruta de origen original se restauran desde cinta, no el contenido de los directorios. Si la variable RECURSIVA está establecida en N O BIEN, LA variable RECOVER_FULL_PATHS está establecida en Y, la ruta de recuperación debe terminar con la ruta original.</p> <div>  <p>Si la variable RECURSIVA está deshabilitada y hay más de una ruta de recuperación, todas las rutas de recuperación deben estar contenidas en el más largo de las rutas de recuperación. De lo contrario, se mostrará un mensaje de error.</p> </div> |

| Variable de entorno | Valores válidos | Predeterminado | Descripción                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------|-----------------|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RECUPERE_FULL_PATHS | Y o. N          | N              | <p>Especifica que la ruta de recuperación completa tendrá sus permisos y ACL restaurados después del DAR.</p> <p>DIRECT y ENHANCED_DAR_ENABLED deben estar habilitados (establecer en Y) también. Si RECOVER_FULL_PATHS está establecido en Y, la ruta de recuperación debe terminar con la ruta original. Si ya hay directorios en el volumen de destino, sus permisos y ACL no se restaurarán a partir de la cinta.</p> |
| ACTUALIZAR          | Y o. N          | Y              | <p>Actualiza la información de los metadatos para permitir la realización de backups incrementales basados EN NIVELES.</p>                                                                                                                                                                                                                                                                                                |

- /foo/dir2/myfile

#### Variables de entorno compatibles con SMTape

| Variable de entorno | Valores válidos | Predeterminado | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------|-----------------|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FECHA_BASE          | DUMP_DATE       | -1             | <p>Especifica la fecha de inicio de las copias de seguridad incrementales.</p> <div> <p><code>`BASE_DATE`</code> Es una representación de cadena de los identificadores de instantánea de referencia. Con el <code>`BASE_DATE`</code> String, SMTape localiza la copia Snapshot de referencia.</p> <p><code>`BASE_DATE`</code> no se requiere para backups básicos. Para un backup incremental, el valor de <code>`DUMP_DATE`</code> la variable de la base anterior o la copia de seguridad incremental se asigna a <code>`BASE_DATE`</code> variable.</p> <p>La aplicación de backup asigna el DUMP_DATE Valor de un backup incremental o base de SMTape anterior.</p> </div> |

| Variable de entorno  | Valores válidos | Predeterminado | Descripción                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------|-----------------|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FECHA_DE_VOLCADO     | return_value    | none           | <p>Al final de un backup de SMTape, DUMP_DATE contiene un identificador de cadena que identifica la copia Snapshot utilizada para ese backup. Esta copia Snapshot se puede utilizar como copia Snapshot de referencia para realizar un backup incremental posterior.</p> <p>El valor resultante de DUMP_DATE se utiliza como valor BASE_DATE para las copias de seguridad incrementales subsiguientes.</p> |
| SMTAPE_BACKUP_SET_ID | string          | none           | <p>Identifica la secuencia de backups incrementales asociados con el backup de referencia.</p> <p>El ID del conjunto de backup es un ID exclusivo de 128 bits que se genera durante una copia de seguridad de línea de base. La aplicación de copia de seguridad asigna este ID como entrada a SMTAPE_BACKUP_SET_ID variable durante una copia de seguridad incremental.</p>                               |

| Variable de entorno        | Valores válidos                                                         | Predeterminado | Descripción                                                                                                                                                                                                                                                                                                                                        |
|----------------------------|-------------------------------------------------------------------------|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SMTAPE_SNAPSHOT_N<br>AME   | Cualquier copia Snapshot<br>válida que esté disponible<br>en el volumen | Invalid        | <p>Cuando la variable SMTAPE_SNAPSHOT_N AME se establece en una copia de Snapshot, se realiza un backup de esa copia de Snapshot y de sus copias de Snapshot anteriores a cinta.</p> <p>Para backups incrementales, esta variable especifica la copia Snapshot incremental. La variable BASE_DATE proporciona la copia Snapshot de referencia.</p> |
| SMTAPE_DELETE_SNA<br>PSHOT | Y o. N                                                                  | N              | <p>Para una copia Snapshot creada automáticamente por SMTape, cuando la variable SMTAPE_DELETE_SNA PSHOT se establece en Y, Después de completar la operación de copia de seguridad, SMTape elimina esta copia snapshot. Sin embargo, no se eliminará una copia Snapshot creada por la aplicación de backup.</p>                                   |
| SMTAPE_BREAK_MIRR<br>OR    | Y o. N                                                                  | N              | <p>Cuando la variable SMTAPE_BREAK_MIRR OR se establece en Y, el volumen del tipo DP se cambia a a. RW volumen después de una restauración correcta.</p>                                                                                                                                                                                           |

### Topologías habituales de backup en cinta NDMP

NDMP admite una serie de topologías y configuraciones entre aplicaciones de backup y sistemas de almacenamiento u otros servidores NDMP que proporcionan datos (sistemas de archivos) y servicios de cinta.



## **Del sistema de almacenamiento a la cinta local**

En la configuración más simple, una aplicación de copia de seguridad realiza una copia de seguridad de los datos de un sistema de almacenamiento a un subsistema de cinta conectado al sistema de almacenamiento. La conexión de control NDMP existe en el límite de la red. La conexión de datos NDMP que existe dentro del sistema de almacenamiento entre los servicios de datos y cinta se denomina configuración local NDMP.

## **Sistema de almacenamiento a cinta conectado a otro sistema de almacenamiento**

Una aplicación de backup también puede realizar backups de datos de un sistema de almacenamiento en una librería de cintas (un cambiador medio con una o varias unidades de cinta) conectada a otro sistema de almacenamiento. En este caso, la conexión de datos NDMP entre los servicios de datos y la cinta se proporciona mediante una conexión de red TCP o TCP/IPv6. Esto se denomina configuración de sistema de almacenamiento triple NDMP.

## **Librería de cintas conectada a la red y del sistema de almacenamiento**

Las bibliotecas de cinta compatibles con NDMP proporcionan una variación de la configuración triple. En este caso, la biblioteca de cintas se conecta directamente a la red TCP/IP y se comunica con la aplicación de backup y el sistema de almacenamiento a través de un servidor NDMP interno.

## **Almacenamiento del sistema al servidor de datos, a cinta o servidor de datos al sistema de almacenamiento a cinta**

NDMP también admite configuraciones triples de sistemas de almacenamiento para servidores de datos y sistemas de datos-servidor-almacenamiento, aunque estas variantes se implementan menos en gran medida. El sistema de almacenamiento al servidor permite realizar backups de los datos del sistema de almacenamiento en una biblioteca de cintas conectada al host de aplicaciones de backup o a otro sistema servidor de datos. La configuración de servidor a sistema de almacenamiento permite realizar copias de seguridad de los datos del servidor en una biblioteca de cintas conectada al sistema de almacenamiento.

## **Métodos de autenticación NDMP compatibles**

Puede especificar un método de autenticación para permitir solicitudes de conexión NDMP. ONTAP es compatible con dos métodos para autenticar el acceso NDMP a un sistema de almacenamiento: Texto sin formato y el reto.

En el modo NDMP de ámbito nodo, tanto el reto como el texto sin formato están habilitados de forma predeterminada. Sin embargo, no puede desactivar el desafío. Puede activar y desactivar texto sin formato. En el método de autenticación de texto sin formato, la contraseña de inicio de sesión se transmite como texto sin cifrar.

En el modo NDMP de ámbito de la máquina virtual de almacenamiento (SVM), el método de autenticación es el reto de forma predeterminada. A diferencia del modo NDMP de ámbito de nodo, en este modo puede habilitar y deshabilitar los métodos de autenticación de texto sin formato y de desafío.

## **Información relacionada**

[Autenticación de usuario en un modo NDMP de ámbito de nodo](#)

[Autenticación de usuario en el modo NDMP con ámbito de SVM](#)

## **Extensiones NDMP compatibles con ONTAP**

NDMP v4 proporciona un mecanismo para crear extensiones de protocolo NDMP v4 sin tener que modificar el protocolo NDMP v4 de núcleo. Debe conocer las extensiones de

## NDMP v4 compatibles con ONTAP.

Las siguientes extensiones de NDMP v4 son compatibles con ONTAP:

- Respaldo para clúster (CAB)



Esta extensión solo es compatible con el modo NDMP con el ámbito de la SVM.

- Extensión de dirección de conexión (cae) para compatibilidad con IPv6
- Clase de extensión 0x2050

Esta extensión admite operaciones de backup reiniciables y extensiones de administración de Snapshot.



La NDMP\_SNAP\_RECOVER El mensaje, que forma parte de las extensiones de administración Snapshot, se utiliza para iniciar una operación de recuperación y transferir los datos recuperados de una copia Snapshot local a una ubicación del sistema de archivos local. En ONTAP, este mensaje solo permite la recuperación de volúmenes y archivos normales.

La NDMP\_SNAP\_DIR\_LIST Message le permite examinar a través de las copias Snapshot de un volumen. Si se realiza una operación no disruptiva mientras hay una operación de exploración en curso, la aplicación de backup debe volver a iniciar la operación de exploración.

### Extensión de backup reinicialable de NDMP para un volcado compatible con ONTAP

Puede utilizar la funcionalidad de extensión de backup reinicialable (RBE) de NDMP para reiniciar un backup desde un punto de control conocido en el flujo de datos antes del fallo.

### Qué es la funcionalidad DAR mejorada

Puede utilizar la funcionalidad DE recuperación DE acceso directo (DAR) mejorada para DAR de directorios y DAR de ficheros y secuencias NT. De forma predeterminada, la función DAR mejorada está activada.

Habilitar una funcionalidad DAR mejorada puede tener un impacto en el rendimiento de backup, ya que es necesario crear y escribir un mapa offset en cinta. Puede habilitar o deshabilitar EL DAR mejorado en los modos NDMP de ámbito de nodos y de máquinas virtuales de almacenamiento (SVM).

### Límites de escalabilidad para sesiones NDMP

Debe tener en cuenta el número máximo de sesiones NDMP que se pueden establecer de manera simultánea en sistemas de almacenamiento de diferentes capacidades de memoria del sistema. Este número máximo depende de la memoria del sistema de un sistema de almacenamiento.

Los límites mencionados en la siguiente tabla son para el servidor NDMP. Los límites mencionados en la sección "Límites de disponibilidad para sesiones de copia de seguridad y restauración de volcado" corresponden a la sesión de descarga y restauración.

| Memoria del sistema de un sistema de almacenamiento | Número máximo de sesiones NDMP |
|-----------------------------------------------------|--------------------------------|
| Menos de 16 GB                                      | 8                              |
| Mayor o igual que 16 GB pero menor que 24 GB        | 20                             |
| Mayor o igual que 24 GB                             | 36                             |

Puede obtener la memoria del sistema del sistema de almacenamiento mediante el `sysconfig -a` comando (disponible a través del nodeshell). Para obtener más información acerca de cómo utilizar este comando, consulte las páginas man.

## Acerca de NDMP para volúmenes FlexGroup

A partir de ONTAP 9.7, NDMP es compatible con los volúmenes FlexGroup.

A partir de ONTAP 9.7, se admite el comando `ndmpcopy` para la transferencia de datos entre volúmenes FlexVol y FlexGroup.

Si se revierte de ONTAP 9.7 a una versión anterior, la información de transferencia incremental de las transferencias anteriores no se conserva y, por lo tanto, se debe realizar una copia básica después de revertir.

A partir de ONTAP 9.8, las siguientes funciones NDMP son compatibles con los volúmenes FlexGroup:

- El mensaje `NDMP_SNAP_RECOVER` de la clase de extensión `0x2050` se puede utilizar para recuperar archivos individuales de un volumen FlexGroup.
- Se admite la extensión de backup NDMP restartable (RBE) para los volúmenes de FlexGroup.
- Las variables de entorno `EXCLUDE` y `MULTI_SUBTREE_NAMES` son compatibles con los volúmenes FlexGroup.

## Acerca de NDMP con volúmenes SnapLock

La creación de varias copias de datos regulados le proporciona escenarios de recuperación redundantes y, al utilizar el volcado y la restauración NDMP, es posible conservar las características DE escritura única y lectura múltiple (WORM) de los archivos de origen en un volumen SnapLock.

Los atributos WORM de los archivos de un volumen de SnapLock se conservan al realizar backups, restaurar y copiar datos; sin embargo, los atributos WORM solo se aplican al restaurar a un volumen de SnapLock. Si se restaura un backup de un volumen SnapLock en un volumen distinto a un volumen SnapLock, se conservan los atributos WORM, pero se ignoran y ONTAP no los aplica.

## Gestione el modo NDMP de ámbito del nodo para volúmenes FlexVol

### Gestione la información general del modo NDMP de ámbito del nodo para FlexVol Volumes

Puede administrar NDMP en el nivel de nodo mediante los comandos y las opciones de

NDMP. Las opciones de NDMP se pueden modificar mediante el `options` comando. Es necesario usar credenciales específicas de NDMP para acceder a un sistema de almacenamiento a fin de ejecutar operaciones de backup y restauración a cinta.

Para obtener más información acerca de `options` consulte las páginas de manual.

**Información relacionada**

[Comandos para gestionar el modo NDMP de ámbito de nodo](#)

[Lo que es el modo NDMP de ámbito del nodo](#)

**Comandos para gestionar el modo NDMP de ámbito de nodo**

Puede utilizar el `system services ndmp` Comandos para gestionar NDMP en el nivel de un nodo. Algunos de estos comandos quedan obsoletos y se quitarán en una versión principal futura.

Puede utilizar los siguientes comandos NDMP solamente en el nivel de privilegio avanzado:

- `system services ndmp service terminate`
- `system services ndmp service start`
- `system services ndmp service stop`
- `system services ndmp log start`
- `system services ndmp log stop`

| Si desea...                                                     | Se usa este comando...                           |
|-----------------------------------------------------------------|--------------------------------------------------|
| Active el servicio NDMP                                         | <code>system services ndmp on*</code>            |
| Desactive el servicio NDMP                                      | <code>system services ndmp off*</code>           |
| Mostrar la configuración de NDMP                                | <code>system services ndmp show*</code>          |
| Modifique la configuración de NDMP                              | <code>system services ndmp modify*</code>        |
| Muestra la versión predeterminada de NDMP                       | <code>system services ndmp version*</code>       |
| Mostrar la configuración del servicio NDMP                      | <code>system services ndmp service show</code>   |
| Modifique la configuración del servicio NDMP                    | <code>system services ndmp service modify</code> |
| Mostrar todas las sesiones de NDMP                              | <code>system services ndmp status</code>         |
| Mostrar información detallada acerca de todas las sesiones NDMP | <code>system services ndmp probe</code>          |

| Si desea...                                         | Se usa este comando...                                    |
|-----------------------------------------------------|-----------------------------------------------------------|
| Finalice la sesión NDMP especificada                | <code>system services ndmp kill</code>                    |
| Finalice todas las sesiones NDMP                    | <code>system services ndmp kill-all</code>                |
| Cambie la contraseña NDMP                           | <code>system services ndmp password*</code>               |
| Habilite el modo de NDMP de ámbito del nodo         | <code>system services ndmp node-scope-mode on*</code>     |
| Deshabilite el modo NDMP de ámbito del nodo         | <code>system services ndmp node-scope-mode off*</code>    |
| Muestra el estado del modo NDMP de ámbito del nodo  | <code>system services ndmp node-scope-mode status*</code> |
| Cierre todas las sesiones NDMP con fuerza           | <code>system services ndmp service terminate</code>       |
| Inicie el demonio del servicio NDMP                 | <code>system services ndmp service start</code>           |
| Detenga el demonio del servicio NDMP                | <code>system services ndmp service stop</code>            |
| Inicie el registro para la sesión NDMP especificada | <code>system services ndmp log start*</code>              |
| Detenga el registro de la sesión NDMP especificada  | <code>system services ndmp log stop*</code>               |

- Estos comandos quedaron obsoletos y se quitarán en una versión principal futura.

Para obtener más información sobre estos comandos, consulte las páginas de manual de `system services ndmp` comandos.

### Autenticación de usuario en un modo NDMP de ámbito de nodo

En el modo NDMP de ámbito del nodo, debe utilizar credenciales específicas de NDMP para acceder a un sistema de almacenamiento a fin de realizar operaciones de backup y restauración a cinta.

El ID de usuario predeterminado es "root". Antes de usar NDMP en un nodo, debe asegurarse de cambiar la contraseña de NDMP predeterminada asociada con el usuario NDMP. También es posible cambiar el ID de usuario predeterminado de NDMP.

### Información relacionada

[Comandos para gestionar el modo NDMP de ámbito de nodo](#)



| Si desea...                                                     | Se usa este comando...                                                                                                             |
|-----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Desactive el servicio NDMP                                      | <code>vserver services ndmp off</code>                                                                                             |
| Mostrar la configuración de NDMP                                | <code>vserver services ndmp show</code>                                                                                            |
| Modifique la configuración de NDMP                              | <code>vserver services ndmp modify</code>                                                                                          |
| Muestra la versión NDMP predeterminada                          | <code>vserver services ndmp version</code>                                                                                         |
| Mostrar todas las sesiones de NDMP                              | <code>vserver services ndmp status</code>                                                                                          |
| Mostrar información detallada acerca de todas las sesiones NDMP | <code>vserver services ndmp probe</code>                                                                                           |
| Terminar una sesión NDMP especificada                           | <code>vserver services ndmp kill</code>                                                                                            |
| Finalice todas las sesiones NDMP                                | <code>vserver services ndmp kill-all</code>                                                                                        |
| Genere la contraseña NDMP                                       | <code>vserver services ndmp generate-password</code>                                                                               |
| Mostrar el estado de la extensión NDMP                          | <code>vserver services ndmp extensions show</code><br><br>Este comando solo está disponible en el nivel de privilegios avanzado.   |
| Modifique el estado de la extensión NDMP (enable o disable)     | <code>vserver services ndmp extensions modify</code><br><br>Este comando solo está disponible en el nivel de privilegios avanzado. |
| Inicie el registro para la sesión NDMP especificada             | <code>vserver services ndmp log start</code><br><br>Este comando solo está disponible en el nivel de privilegios avanzado.         |
| Detenga el registro de la sesión NDMP especificada              | <code>vserver services ndmp log stop</code><br><br>Este comando solo está disponible en el nivel de privilegios avanzado.          |

Para obtener más información sobre estos comandos, consulte las páginas de manual de `vserver services ndmp` comandos.

## Qué hace la extensión Cluster Aware Backup

CAB (Backup para Cluster Aware) es una extensión del protocolo NDMP v4. Esta extensión permite que el servidor NDMP establezca una conexión de datos en un nodo propietario de un volumen. Esto también permite a la aplicación de backup determinar si hay volúmenes y dispositivos de cinta ubicados en el mismo nodo de un clúster.

Para permitir que el servidor NDMP identifique el nodo propietario de un volumen y establezca una conexión de datos en dicho nodo, la aplicación de backup debe admitir la extensión CAB. La extensión CAB requiere que la aplicación de copia de seguridad informe al servidor NDMP del volumen que se va a realizar una copia de seguridad o restaurar antes de establecer la conexión de datos. Esto permite que el servidor NDMP determine el nodo que aloja el volumen y establezca la conexión de datos correctamente.

Con la extensión CAB que admite la aplicación de backup, el servidor NDMP proporciona información de afinidad acerca de los volúmenes y los dispositivos de cinta. Con esta información de afinidad, la aplicación de backup puede realizar un backup local en lugar de un backup triple si un volumen y un dispositivo de cinta están ubicados en el mismo nodo de un clúster.

## Disponibilidad de volúmenes y dispositivos de cinta para realizar backups y restauraciones en diferentes tipos de LIF

Puede configurar una aplicación de backup para establecer una conexión de control NDMP en cualquiera de los tipos de LIF de un clúster. En el modo NDMP de la máquina virtual de almacenamiento (SVM), puede determinar la disponibilidad de volúmenes y dispositivos de cinta para las operaciones de backup y restauración, en función de estos tipos de LIF y el estado de la extensión CAB.

En las siguientes tablas, se muestra la disponibilidad de volúmenes y dispositivos de cinta para los tipos de LIF de conexión de control NDMP y el estado de la extensión CAB:

### La disponibilidad de volúmenes y dispositivos de cinta cuando la aplicación de backup no admite la extensión CAB

| Tipo de LIF de conexión de control NDMP | Volúmenes disponibles para backup o restauración                                         | Dispositivos de cinta disponibles para backup o restauración                                |
|-----------------------------------------|------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| LIF de gestión de nodos                 | Todos los volúmenes alojados por un nodo                                                 | Los dispositivos de cinta conectados al nodo que aloja el LIF de gestión del nodo           |
| LIF de datos                            | Solo los volúmenes que pertenecen a la SVM alojada por un nodo que aloja la LIF de datos | Ninguno                                                                                     |
| LIF de gestión de clústeres             | Todos los volúmenes alojados por un nodo que aloja el LIF de gestión de clústeres        | Ninguno                                                                                     |
| LIF entre clústeres                     | Todos los volúmenes alojados por un nodo que aloja la LIF de interconexión de clústeres  | Los dispositivos de cinta conectados al nodo que aloja la LIF de interconexión de clústeres |



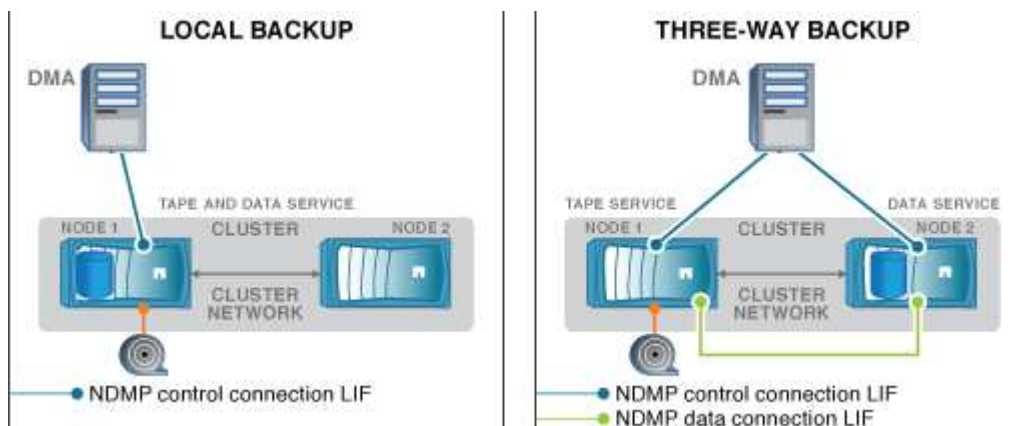
| Tipo de LIF de conexión de control NDMP | Volúmenes disponibles para backup o restauración                      | Dispositivos de cinta disponibles para backup o restauración                      |
|-----------------------------------------|-----------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| LIF de gestión de nodos                 | Todos los volúmenes alojados por un nodo                              | Los dispositivos de cinta conectados al nodo que aloja el LIF de gestión del nodo |
| LIF de datos                            | Todos los volúmenes que pertenecen a la SVM que aloja la LIF de datos | Ninguno                                                                           |
| LIF de gestión de clústeres             | Todos los volúmenes del clúster                                       | Todos los dispositivos de cinta del cluster                                       |
| LIF entre clústeres                     | Todos los volúmenes del clúster                                       | Todos los dispositivos de cinta del cluster                                       |

### Qué es la información de afinidad

Una vez que la aplicación de backup se detecta EN CABINA, el servidor NDMP proporciona información única sobre la ubicación de los volúmenes y los dispositivos de cinta. Mediante el uso de esta información de afinidad, la aplicación de backup puede realizar un backup local en lugar de un backup triple si un volumen y un dispositivo de cinta comparten la misma afinidad.

Si la conexión de control NDMP se establece en una LIF de gestión de nodos, LIF de gestión de clústeres, O mediante LIF de interconexión de clústeres, la aplicación de backup puede usar la información de afinidad para determinar si un volumen y un dispositivo de cinta están ubicados en el mismo nodo y, a continuación, realizar una operación de backup o restauración local o triple. Si la conexión del control NDMP se establece en una LIF de datos, la aplicación de backup siempre realiza un backup triple.

### Backup NDMP local y backup NDMP triple



Mediante la información de afinidad con los volúmenes y los dispositivos de cinta, DMA (aplicación de backup) realiza un backup NDMP local en el volumen y el dispositivo de cinta ubicados en el nodo 1 del clúster. Si el volumen se mueve del nodo 1 al nodo 2, cambia la información de afinidad sobre el volumen y el dispositivo

de cinta. Por lo tanto, para un backup posterior, DMA realiza una operación de backup NDMP triple. De este modo se garantiza la continuidad de la política de backup del volumen independientemente del nodo al que se traslade el volumen.

**Información relacionada**

[Qué hace la extensión Cluster Aware Backup](#)

**El servidor NDMP admite conexiones de control seguras en el modo SVM-scoped**

Se puede establecer una conexión de control segura entre la aplicación de administración de datos (DMA) y el servidor NDMP utilizando sockets seguros (SSL/TLS) como mecanismo de comunicación. Esta comunicación SSL se basa en los certificados del servidor. El servidor NDMP escucha en el puerto 30000 (asignado por IANA para el servicio "ndmps").

Tras establecer la conexión desde el cliente en este puerto, el protocolo de enlace SSL estándar se produce cuando el servidor presenta el certificado al cliente. Cuando el cliente acepta el certificado, se completa el apretón de manos SSL. Una vez completado este proceso, toda la comunicación entre el cliente y el servidor se cifra. El flujo de trabajo del protocolo NDMP sigue siendo exactamente igual que antes. La conexión NDMP segura sólo requiere autenticación de certificado del servidor. Un DMA puede optar por establecer una conexión mediante la conexión al servicio NDMP seguro o al servicio NDMP estándar.

De manera predeterminada, el servicio NDMP seguro está deshabilitado para una máquina virtual de almacenamiento (SVM). Puede habilitar o deshabilitar el servicio NDMP seguro en una SVM determinada mediante el `vserver services ndmp modify -vserver vserver -is-secure-control -connection-enabled [true|false]` comando.

**Tipos de conexión de datos NDMP**

En el modo NDMP de la máquina virtual de almacenamiento (SVM), los tipos de conexión de datos NDMP admitidos dependen del tipo de LIF de conexión de control NDMP y el estado de la extensión CAB. Este tipo de conexión de datos NDMP indica si se puede ejecutar una operación de backup o restauración NDMP local o triple.

Puede realizar un backup o una operación de restauración NDMP triple a través de una red TCP o TCP/IPv6. En las siguientes tablas, se muestran los tipos de conexión de datos NDMP según el tipo de LIF de conexión de control NDMP y el estado de la extensión CAB.

**Tipo de conexión de datos NDMP cuando la aplicación de backup admite una extensión CAB**

| Tipo de LIF de conexión de control NDMP | Tipo de conexión de datos NDMP |
|-----------------------------------------|--------------------------------|
| LIF de gestión de nodos                 | LOCAL, TCP Y TCP/IPV6          |
| LIF de datos                            | TCP/TCP                        |
| LIF de gestión de clústeres             | LOCAL, TCP Y TCP/IPV6          |
| LIF entre clústeres                     | LOCAL, TCP Y TCP/IPV6          |

## Tipo de conexión de datos NDMP cuando la aplicación de backup no admite la extensión CAB

| Tipo de LIF de conexión de control NDMP | Tipo de conexión de datos NDMP |
|-----------------------------------------|--------------------------------|
| LIF de gestión de nodos                 | LOCAL, TCP Y TCP/IPV6          |
| LIF de datos                            | TCP/TCP                        |
| LIF de gestión de clústeres             | TCP/TCP                        |
| LIF entre clústeres                     | LOCAL, TCP Y TCP/IPV6          |

### Información relacionada

[Qué hace la extensión Cluster Aware Backup](#)

["Gestión de redes"](#)

### Autenticación de usuario en el modo NDMP con ámbito de SVM

En el modo NDMP de la máquina virtual de almacenamiento (SVM), la autenticación de usuario NDMP está integrada con el control de acceso basado en roles. En el contexto de la SVM, el usuario NDMP debe tener el rol `"vsadmin"` o `"vsadmin-backup"`. En un contexto de cluster, el usuario NDMP debe tener el rol `«'admin'»` o `«'backup'»`.

Además de estas funciones predefinidas, una cuenta de usuario asociada a una función personalizada también puede utilizarse para la autenticación NDMP siempre y cuando la función personalizada tenga la carpeta `«'vserver Services ndmp'»` en su directorio de comandos y el nivel de acceso de la carpeta no sea `«'none'»`. En este modo, debe generar una contraseña NDMP para una cuenta de usuario determinada, que se crea mediante el control de acceso basado en roles. Los usuarios de clúster con un rol de administrador o backup pueden acceder a una LIF de gestión de nodos, una LIF de gestión de clústeres o una LIF de interconexión de clústeres. Los usuarios de un rol de vsadmin o de vsadmin pueden acceder solo a la LIF de datos para esa SVM. Por lo tanto, según la función de un usuario, la disponibilidad de volúmenes y dispositivos de cinta para las operaciones de backup y restauración varía.

Este modo también admite la autenticación de usuario para usuarios NIS y LDAP. Por lo tanto, los usuarios NIS y LDAP pueden acceder a varias SVM con un ID de usuario y una contraseña comunes. Sin embargo, la autenticación NDMP no admite usuarios de Active Directory.

En este modo, una cuenta de usuario debe estar asociada a la aplicación SSH y al método de autenticación `«'Contraseña de usuario'»`.

### Información relacionada

[Comandos para gestionar el modo NDMP con ámbito de la SVM](#)

["Administración del sistema"](#)

["Conceptos de ONTAP"](#)

### Genere una contraseña específica de NDMP para los usuarios de NDMP

En el modo NDMP de la máquina virtual de almacenamiento (SVM), debe generar una

contraseña para un ID de usuario específico. La contraseña generada se basa en la contraseña de inicio de sesión real para el usuario NDMP. Si cambia la contraseña de inicio de sesión real, deberá generar de nuevo la contraseña específica de NDMP.

### Pasos

1. Utilice la `vserver services ndmp generate-password` Para generar una contraseña específica de NDMP.

Puede utilizar esta contraseña en cualquier operación NDMP actual o futura que requiera la introducción de la contraseña.



Desde el contexto de la máquina virtual de almacenamiento (SVM, antes denominada Vserver), puede generar contraseñas de NDMP para usuarios que solo pertenecen a esa SVM.

El ejemplo siguiente muestra cómo generar una contraseña específica de NDMP para un ID de usuario usuario1:

```
cluster1::vserver services ndmp> generate-password -vserver vs1 -user
user1

Vserver: vs1
User: user1
Password: jWZiNt57huPOoD8d
```

2. Si cambia la contraseña a su cuenta de sistema de almacenamiento normal, repita este procedimiento para obtener su nueva contraseña específica de NDMP.

### **Cómo se ven afectadas las operaciones de backup y restauración de cinta durante la recuperación ante desastres en la configuración de MetroCluster**

Se pueden ejecutar operaciones de backup y restauración a cinta simultáneamente durante la recuperación ante desastres en una configuración de MetroCluster. Debe entender cómo se ven afectadas estas operaciones durante la recuperación de desastres.

Si las operaciones de backup y restauración de cinta se llevan a cabo en un volumen de anSVM en una relación de recuperación ante desastres, puede continuar con las operaciones de backup y restauración de cinta incrementales después de una conmutación de sitios y conmutación de estado.

### **Acerca del motor de volcado para volúmenes FlexVol**

#### **Acerca del motor de volcado para volúmenes FlexVol**

Dump es una solución de backup y recuperación basada en copias de Snapshot de ONTAP que ayuda a realizar backups de archivos y directorios desde una copia Snapshot a un dispositivo de cinta y restaura los datos del backup en un sistema de almacenamiento.

Puede realizar una copia de seguridad de los datos del sistema de archivos, como directorios, archivos y su configuración de seguridad asociada, en un dispositivo de cinta mediante la copia de seguridad de volcado. Puede realizar backup de un volumen completo, de un qtree completo o de un subárbol que no sea ni un volumen completo ni un qtree completo.

Puede realizar un backup o una restauración de volcado utilizando aplicaciones de backup compatibles con NDMP.

Cuando se realiza un backup de volcado, es posible especificar la copia Snapshot que se usará para un backup. Si no se especifica una copia Snapshot para el backup, el motor de volcado crea una copia Snapshot para el backup. Una vez completada la operación de copia de seguridad, el motor de volcado elimina esta copia snapshot.

Puede realizar copias de seguridad de nivel 0, incrementales o diferenciales en cinta utilizando el motor de descarga.



Después de revertir a una versión anterior a Data ONTAP 8.3, debe ejecutar una operación de backup base antes de realizar una operación de backup incremental.

### Información relacionada

["Actualización, reversión o degradación"](#)

### Cómo funciona un backup de volcado

Una copia de seguridad de volcado escribe los datos del sistema de archivos del disco a la cinta mediante un proceso predefinido. Puede realizar un backup de un volumen, un qtree o un subárbol que no sea ni un volumen completo ni un qtree completo.

En la siguiente tabla se describe el proceso que ONTAP utiliza para realizar un backup del objeto indicado por la ruta de volcado:

| Etapa | Acción                                                                                                                                                                                                                                                                                    |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1     | Para un volumen completo menor que los backups qtree o los backups completos de qtree, ONTAP atraviesa directorios para identificar los archivos en los que se va a realizar el backup. Si va a realizar el backup de un volumen o qtree completo, ONTAP combina esta fase con la fase 2. |
| 2     | Para un backup de volumen completo o de qtree completo, ONTAP identifica los directorios en los volúmenes o qtrees de los que se va a realizar un backup.                                                                                                                                 |
| 3     | ONTAP escribe los directorios en la cinta.                                                                                                                                                                                                                                                |
| 4     | ONTAP escribe los archivos en la cinta.                                                                                                                                                                                                                                                   |
| 5     | ONTAP escribe la información de ACL (si corresponde) en la cinta.                                                                                                                                                                                                                         |

El backup de volcado utiliza una copia Snapshot de los datos para el backup. Por lo tanto, no es necesario desconectar el volumen antes de iniciar el backup.

El backup de volcado asigna nombres a cada copia Snapshot que crea `snapshot_for_backup.n`, donde `n`

es un entero que comienza en 0. Cada vez que el backup volcado crea una copia Snapshot, incrementa el número entero en 1. El entero se restablece a 0 después de reiniciar el sistema de almacenamiento. Una vez completada la operación de copia de seguridad, el motor de volcado elimina esta copia snapshot.

Cuando ONTAP realiza varios backups de volcado de manera simultánea, el motor de volcado crea varias copias Snapshot. Por ejemplo, si ONTAP ejecuta dos backups de volcado de manera simultánea, puede encontrar las siguientes copias Snapshot en los volúmenes desde los cuales se realiza el backup de los datos: `snapshot_for_backup.0` y `snapshot_for_backup.1`.



Cuando se realiza un backup de una copia Snapshot, el motor de volcado no crea una copia Snapshot adicional.

### **Tipos de datos de los que el motor de descarga realiza una copia de seguridad**

El motor de volcado permite lanzar backups de los datos a cinta como protección ante desastres o interrupciones en la controladora. Además de realizar backups de objetos de datos como archivos, directorios, qtrees o volúmenes completos, el motor de volcado puede realizar backups de muchos tipos de información acerca de cada archivo.

Conocer los tipos de datos que el motor de volcado puede realizar y las restricciones que se deben tener en cuenta puede ayudarle a planificar su método de recuperación ante desastres.

Además de realizar una copia de seguridad de los datos de los archivos, el motor de volcado puede realizar una copia de seguridad de la siguiente información acerca de cada archivo, según corresponda:

- GID de UNIX, UID del propietario y permisos de archivo
- Acceso UNIX, creación y tiempo de modificación
- Tipo de archivo
- Tamaño de archivo
- Nombre dos, atributos dos y hora de creación
- Listas de control de acceso (ACL) con 1,024 entradas de control de acceso (ACE)
- Información de Qtree
- Rutas de unión

Las rutas de unión se copian como enlaces simbólicos.

- Clones LUN y LUN

Puede realizar backups de un objeto de LUN completo; sin embargo, no puede realizar backups de un único archivo dentro del objeto LUN. De igual modo, puede restaurar un objeto de LUN completo, pero no un solo archivo dentro de la LUN.



El motor de volcado realiza una copia de seguridad de los clones de LUN como LUN independientes.

- Archivos alineados con equipos virtuales

Las versiones anteriores a Data ONTAP 8.1.2 no admiten la copia de seguridad de archivos alineados con equipos virtuales.



Cuando se realiza la transición de un clon de LUN respaldado por snapshots de Data ONTAP operativo en 7-Mode a ONTAP, se convierte en una LUN inconsistente. El motor de volcado no realiza copias LUN incoherentes.

Cuando restaura datos en un volumen, las operaciones de I/O del cliente están restringidas en las LUN que se restauran. La restricción de LUN se elimina solo cuando se completa la operación de restauración de volcado. De forma similar, durante una operación de restauración de archivos o LUN únicos de SnapMirror, las I/O del cliente están restringidas a ambos archivos y LUN que se van a restaurar. Esta restricción se elimina solo cuando se completa la operación de restauración de archivos o LUN. Si se realiza un backup de volcado en un volumen en el que se está realizando una operación de restauración de volcado o restauración de archivo único de SnapMirror o LUN, los archivos o LUN que tienen restricción de I/O del cliente no se incluyen en el backup. Estos archivos o LUN se incluyen en una operación de copia de seguridad posterior si la restricción de I/O del cliente se elimina.



Una LUN que se ejecute en Data ONTAP 8.3 y que se realice un backup a cinta solo se podrá restaurar a las versiones 8.3 y posteriores, y no a una versión anterior. Si la LUN se restaura a una versión anterior, la LUN se restaura como un archivo.

Cuando se realiza un backup de un volumen secundario de SnapVault o de un destino de SnapMirror para volúmenes a cinta, solo se realiza un backup de los datos del volumen. No se realiza un backup de los metadatos asociados. Por lo tanto, cuando intenta restaurar el volumen, solo se restauran los datos de ese volumen. La información sobre las relaciones de SnapMirror para volúmenes no está disponible en el backup y, por lo tanto, no se restaura.

Si vuelca un archivo que sólo tiene permisos de Windows NT y lo restaura a un qtree o volumen de estilo UNIX, el archivo obtiene los permisos UNIX predeterminados para ese qtree o volumen.

Si vuelca un archivo que solo tiene permisos de UNIX y lo restaura a un qtree o volumen de estilo NTFS, el archivo obtiene los permisos de Windows predeterminados para ese qtree o volumen.

Otros volcados y restauraciones conservan los permisos.

Puede realizar un backup de los archivos alineados con las máquinas virtuales y del `vm-align-sector` opción. Para obtener más información sobre los archivos alineados con equipos virtuales, consulte ["Gestión de almacenamiento lógico"](#).

### Qué cadenas de incremento son

Una cadena de incremento es una serie de copias de seguridad incrementales de la misma ruta. Como puede especificar cualquier nivel de backup en cualquier momento, debe comprender las cadenas de incremento para poder realizar backups y restauraciones de manera efectiva. Es posible ejecutar 31 niveles de operaciones de backup incrementales.

Existen dos tipos de cadenas de incremento:

- Una cadena de incremento consecutiva, que es una secuencia de backups incrementales que comienza con el nivel 0 y se eleva por 1 en cada backup posterior.
- Una cadena de incremento no consecutiva, donde las copias de seguridad incrementales omiten niveles o tienen niveles que están fuera de secuencia, como 0, 2, 3, 1, 4 o más comúnmente 0, 1, 1, 1 o 0, 1, 2, 1, 2.

Los backups incrementales se basan en los backups más recientes de bajo nivel. Por ejemplo, la secuencia

de niveles de backup 0, 2, 3, 1, 4 proporciona dos cadenas de incremento: 0, 2, 3 y 0, 1, 4. La siguiente tabla explica las bases de los backups incrementales:

| Orden de copia de seguridad | Incrementar el nivel | Cadena de incremento | Base                                                                                                              | Archivos de copia de seguridad                                                                                                                                                     |
|-----------------------------|----------------------|----------------------|-------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1                           | 0                    | Ambas                | De los archivos del sistema de almacenamiento                                                                     | Todos los archivos de la ruta de copia de seguridad                                                                                                                                |
| 2                           | 2                    | 0, 2, 3              | Backup de nivel 0                                                                                                 | Archivos en la ruta de copia de seguridad creada desde la copia de seguridad de nivel 0                                                                                            |
| 3                           | 3                    | 0, 2, 3              | Backup de nivel 2                                                                                                 | Archivos en la ruta de copia de seguridad creada desde la copia de seguridad de nivel 2                                                                                            |
| 4                           | 1                    | 0, 1, 4              | Backup de nivel 0, porque es el nivel más reciente inferior al backup de nivel 1                                  | Archivos en la ruta de copia de seguridad creados desde la copia de seguridad de nivel 0, incluidos los archivos que se encuentran en las copias de seguridad de nivel 2 y nivel 3 |
| 5                           | 4                    | 0, 1, 4              | El backup de nivel 1, porque es un nivel inferior y es más reciente que los backups de nivel 0, nivel 2 o nivel 3 | Archivos creados desde la copia de seguridad de nivel 1                                                                                                                            |

### Qué es el factor de bloqueo

Un bloque de cinta es 1,024 bytes de datos. Durante un backup o una restauración de cinta, es posible especificar la cantidad de bloques de cinta que se transfieren en cada operación de lectura/escritura. Este número se llama el *factor de bloqueo*.

Puede utilizar un factor de bloqueo de 4 a 256. Si tiene previsto restaurar una copia de seguridad en un sistema distinto al del que hizo la copia de seguridad, el sistema de restauración debe admitir el factor de bloqueo que se utilizó para la copia de seguridad. Por ejemplo, si se utiliza un factor de bloqueo de 128, el sistema en el que se restaura ese backup debe admitir un factor de bloqueo de 128.



Durante una copia de seguridad NDMP, EL OBJETO `MOVER_RECORD_SIZE` determina el factor de bloqueo. ONTAP permite un valor máximo de 256 KB para `MOVER_RECORD_SIZE`.

### **Cuándo reiniciar una copia de seguridad de volcado**

En ocasiones, un backup de volcado no finaliza a causa de errores internos o externos, como errores de escritura en cinta, interrupciones del suministro eléctrico, interrupciones accidentales de los usuarios o incoherencias internas en el sistema de almacenamiento. Si falla el backup por uno de estos motivos, puede reiniciarlo.

Puede optar por interrumpir y reiniciar un backup para evitar periodos de gran tráfico en el sistema de almacenamiento o competir por otros recursos limitados del sistema de almacenamiento, como una unidad de cinta. Puede interrumpir una copia de seguridad larga y reiniciarla más tarde si una restauración (o copia de seguridad) más urgente requiere la misma unidad de cinta. Los backups reiniciables persisten durante los reinicios. Sólo puede reiniciar una copia de seguridad anulada en cinta si se cumplen las siguientes condiciones:

- La copia de seguridad anulada se encuentra en la fase IV
- Están disponibles todas las copias Snapshot asociadas que estaban bloqueadas por el comando `dump`.
- El historial de archivos debe estar activado.

Cuando se cancela una operación de volcado y se deja en un estado reiniciable, las copias Snapshot asociadas se bloquean. Estas copias Snapshot se liberan después de que se elimine el contexto de los backups. Puede ver la lista de contextos de copia de seguridad mediante la `vserver services ndmp restartable backup show` comando.

```

cluster::> vserver services ndmpd restartable-backup show
Vserver Context Identifier Is Cleanup Pending?

vserver1 330e6739-0179-11e6-a299-005056bb4bc9 false
vserver1 481025c1-0179-11e6-a299-005056bb4bc9 false
vserver2 5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::> vserver services ndmpd restartable-backup show -vserver
vserver1 -context-id 330e6739-0179-11e6-a299-005056bb4bc9

Vserver: vserver1
Context Identifier: 330e6739-0179-11e6-a299-005056bb4bc9
Volume Name: /vserver1/vol1
Is Cleanup Pending?: false
Backup Engine Type: dump
Is Snapshot Copy Auto-created?: true
Dump Path: /vol/vol1
Incremental Backup Level ID: 0
Dump Name: /vserver1/vol1
Context Last Updated Time: 1460624875
Has Offset Map?: true
Offset Verify: true
Is Context Restartable?: true
Is Context Busy?: false
Restart Pass: 4
Status of Backup: 2
Snapshot Copy Name: snapshot_for_backup.1
State of the Context: 7

cluster::>"

```

### Cómo funciona una restauración de volcado

Una restauración de volcado escribe los datos del sistema de archivos de una cinta a un disco mediante un proceso predefinido.

El proceso de la siguiente tabla muestra el funcionamiento de la restauración de volcado:

| Etapa | Acción                                                       |
|-------|--------------------------------------------------------------|
| 1     | ONTAP cataloga los archivos que deben extraerse de la cinta. |
| 2     | ONTAP crea directorios y archivos vacíos.                    |

| Etapa | Acción                                                                                                           |
|-------|------------------------------------------------------------------------------------------------------------------|
| 3     | ONTAP lee un archivo desde una cinta, lo escribe en el disco y establece los permisos (incluidas las ACL) en él. |
| 4     | ONTAP repite las fases 2 y 3 hasta que todos los archivos especificados se copien de la cinta.                   |

### Tipos de datos que restaura el motor de volcado

Cuando se produce un desastre o una interrupción de la controladora, el motor de volcado ofrece diversos métodos para recuperar todos los datos de los que se hizo backup, desde archivos individuales a atributos de archivo, a directorios completos. Conocer los tipos de datos que el motor de volcado puede restaurar y cuándo utilizar qué método de recuperación puede ayudar a minimizar el tiempo de inactividad.

Puede restaurar datos a una LUN asignada en línea. Sin embargo, las aplicaciones host no pueden acceder a esta LUN hasta que se complete la operación de restauración. Una vez finalizada la operación de restauración, la caché del host de los datos de LUN se debe vaciar para ofrecer coherencia con los datos restaurados.

El motor de descarga puede recuperar los siguientes datos:

- Contenido de los archivos y directorios
- Permisos de archivos UNIX
- ACL

Si restaura un archivo que solo tiene permisos de archivo UNIX a un qtree o volumen NTFS, el archivo no tiene ACL de Windows NT. El sistema de almacenamiento utiliza sólo los permisos de archivo UNIX en este archivo hasta que se crea una ACL de Windows NT en él.



Si restaura ACL respaldados de sistemas de almacenamiento que ejecutan Data ONTAP 8.2 a sistemas de almacenamiento que ejecutan Data ONTAP 8.1.x y versiones anteriores que tienen un límite de ACE inferior a 1,024, se restaura una ACL predeterminada.

- Información de Qtree

La información de qtree se utiliza solo si un qtree se restaura en la raíz de un volumen. La información de qtree no se utiliza si un qtree se restaura a un directorio inferior, como /vs1/vol1/subdir/lowerdir, y deja de ser un qtree.

- Todos los demás atributos de archivo y directorio
- Secuencias de Windows NT
- LUN
  - Es necesario restaurar una LUN a nivel de volumen o un nivel de qtree para que permanezca como una LUN.

Si se restaura a un directorio, se restaura como un archivo porque no contiene metadatos válidos.

- Un LUN de 7-Mode se restaura como LUN en un volumen ONTAP.
- Un volumen de 7-Mode se puede restaurar en un volumen de ONTAP.
- Los archivos alineados con máquinas virtuales restaurados en un volumen de destino heredan las propiedades de alineación de máquinas virtuales del volumen de destino.
- El volumen de destino de una operación de restauración puede tener archivos con bloqueos obligatorios o de asesoramiento.

Mientras se realiza una operación de restauración en dicho volumen de destino, el motor de volcado ignora estos bloqueos.

### Consideraciones que tener en cuenta antes de restaurar datos

Puede restaurar los datos de los que se ha realizado una copia de seguridad en su ruta original o en otro destino. Si va a restaurar datos con un backup en otro destino, debe preparar el destino para la operación de restauración.

Antes de restaurar datos en su ruta original o en un destino diferente, debe disponer de la siguiente información y cumplir los requisitos siguientes:

- El nivel de la restauración
- La ruta a la que se van a restaurar los datos
- El factor de bloqueo utilizado durante el backup
- Si realiza una restauración incremental, todas las cintas deben estar en la cadena de backup
- Una unidad de cinta disponible y compatible con la cinta a restaurar

Antes de restaurar los datos en otro destino, debe ejecutar las operaciones siguientes:

- Si va a restaurar un volumen, debe crear un volumen nuevo.
- Si va a restaurar un qtree o un directorio, debe cambiar el nombre de los archivos que probablemente tengan los mismos nombres que los archivos que va a restaurar.



En ONTAP 9, los nombres de qtree admiten el formato Unicode. Las versiones anteriores de ONTAP no admiten este formato. Si un qtree con nombres Unicode en ONTAP 9 se copia en una versión anterior de ONTAP mediante `ndmcopy` O mediante la restauración desde una imagen de copia de seguridad en una cinta, el qtree se restaura como un directorio normal y no como un qtree con formato Unicode.



Si un archivo restaurado tiene el mismo nombre que un archivo existente, el archivo existente se sobrescribe con el archivo restaurado. Sin embargo, los directorios no se sobrescriben.

Para cambiar el nombre de un archivo, directorio o qtree durante la restauración sin usar DAR, debe configurar la variable de entorno DE EXTRACCIÓN en E.

### Espacio requerido en el sistema de almacenamiento de destino

Necesita aproximadamente 100 MB de espacio en el sistema de almacenamiento de destino que la cantidad de datos que se van a restaurar.



La operación de restauración comprueba la disponibilidad de espacio de los volúmenes y de nodos de información en el volumen de destino cuando se inicia la operación de restauración. Establecer la variable de entorno FORCE a. Y hace que la operación de restauración omita las comprobaciones del espacio del volumen y de la disponibilidad de nodos de información en la ruta de destino. Si no hay suficiente espacio o inodos disponibles en el volumen de destino, la operación de restauración recupera la cantidad de datos permitidos por el espacio del volumen de destino y la disponibilidad del inodo. La operación de restauración se detiene cuando no queda más espacio del volumen o inodos.

## Límites de escalabilidad para sesiones de backup y restauración de volcado

Es necesario conocer la cantidad máxima de sesiones de backup y restauración de volcado que se pueden ejecutar simultáneamente en sistemas de almacenamiento de diferentes capacidades de memoria del sistema. Este número máximo depende de la memoria del sistema de un sistema de almacenamiento.

Los límites mencionados en la tabla siguiente son para el motor de descarga o restauración. Los límites mencionados en los límites de escalabilidad para las sesiones NDMP son para el servidor NDMP, que son más altos que los límites del motor.

| Memoria del sistema de un sistema de almacenamiento | Cantidad total de sesiones de backup y restauración de volcado |
|-----------------------------------------------------|----------------------------------------------------------------|
| Menos de 16 GB                                      | 4                                                              |
| Mayor o igual que 16 GB pero menor que 24 GB        | 16                                                             |
| Mayor o igual que 24 GB                             | 32                                                             |



Si utiliza `ndmptcopy` Comando para copiar datos dentro de los sistemas de almacenamiento, se establecen dos sesiones NDMP, una para backup de volcado y la otra para restauración de volcado.

Puede obtener la memoria del sistema del sistema de almacenamiento mediante el `sysconfig -a` comando (disponible a través del nodeshell). Para obtener más información acerca de cómo utilizar este comando, consulte las páginas man.

## Información relacionada

[Límites de escalabilidad para sesiones NDMP](#)

## Compatibilidad con backup y restauración a cinta entre Data ONTAP operando en 7-Mode y ONTAP

Es posible restaurar datos de los que se ha realizado un backup desde un sistema de almacenamiento operativo en 7-Mode o donde se ejecuta ONTAP en un sistema de almacenamiento que funciona en 7-Mode o en ONTAP.

Las siguientes operaciones de backup y restauración de cinta son compatibles entre Data ONTAP en 7-Mode y ONTAP:

- Realizar un backup de un volumen de 7-Mode a una unidad de cinta conectada a un sistema de almacenamiento que ejecuta ONTAP
- Realizar backups de un volumen de ONTAP en una unidad de cinta conectada a un sistema 7-Mode
- Restaurar los datos con backup de un volumen de 7-Mode a partir de una unidad de cinta conectada a un sistema de almacenamiento que ejecuta ONTAP
- Restaurar datos con backup de un volumen ONTAP a partir de una unidad de cinta conectada a un sistema 7-Mode
- Restaurar un volumen de 7-Mode en un volumen de ONTAP



- A 7-Mode LUN is restored as a LUN on an ONTAP volume.
- You should retain the ONTAP LUN identifiers when restoring a 7-Mode LUN to an existing ONTAP LUN.

- Restaurar un volumen ONTAP en un volumen de 7-Mode



Un LUN de ONTAP se restaura como un archivo normal en un volumen de 7-Mode.

## Eliminar contextos reiniciables

Si desea iniciar un backup en lugar de reiniciar un contexto, puede eliminar el contexto.

### Acerca de esta tarea

Puede eliminar un contexto reinicializable mediante el `vserver services ndmp restartable-backup delete` Para proporcionar el nombre de SVM y el ID de contexto.

### Pasos

1. Eliminar un contexto reinicializable:

```
vserver services ndmp restartable-backup delete -vserver vserver-name -context -id context_identifier.
```

```

cluster::> vserver services ndmpd restartable-backup show
Vserver Context Identifier Is Cleanup Pending?

vserver1 330e6739-0179-11e6-a299-005056bb4bc9 false
vserver1 481025c1-0179-11e6-a299-005056bb4bc9 false
vserver2 5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::>
cluster::> vserver services ndmp restartable-backup delete -vserver
vserver1 -context-id 481025c1-0179-11e6-a299-005056bb4bc9

cluster::> vserver services ndmpd restartable-backup show
Vserver Context Identifier Is Cleanup Pending?

vserver1 330e6739-0179-11e6-a299-005056bb4bc9 false
vserver2 5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::>"

```

## Cómo funciona el volcado en un volumen secundario de SnapVault

Es posible realizar operaciones de backup a cinta en datos que estén reflejados en el volumen secundario de SnapVault. Puede realizar un backup únicamente de los datos que se reflejan en el volumen secundario de SnapVault a cinta, y no los metadatos de la relación de SnapVault.

Cuando se rompe la relación de reflejo de protección de datos (`snapmirror break`) O cuando se produce una resincronización de SnapMirror, siempre es necesario ejecutar un backup básico.

## Cómo funciona el volcado con la recuperación tras fallos del almacenamiento y las operaciones ARL

Antes de ejecutar operaciones de backup de volcado o restauración, debe comprender cómo funcionan estas operaciones con las operaciones de conmutación por error (toma de control y devolución) de almacenamiento o reubicación de agregados (ARL). La `-override-vetoes` Option determina el comportamiento de un motor de volcado durante una operación de ARL o una conmutación por error del almacenamiento.

Cuando se ejecuta una operación de volcado de backup o restauración, y la `-override-vetoes` opción establecida en `false`, Se detiene una operación ARL o una recuperación tras fallos de almacenamiento iniciada por el usuario. Sin embargo, si la `-override-vetoes` opción establecida en `true`, La operación de recuperación tras fallos de almacenamiento o ARL continúa y se cancela la operación de copia de seguridad o restauración de volcado. Cuando el sistema de almacenamiento inicia automáticamente una conmutación por error o una operación de ARL del almacenamiento, siempre se cancela una operación de backup o restauración de volcado activa. No es posible reiniciar las operaciones de volcado de backup y restauración

incluso después de la conmutación por error de almacenamiento o de la finalización de las operaciones de ARL.

**Operaciones de descarga cuando se admite la extensión DE LA CABINA**

Si la aplicación de backup admite la extensión CAB, puede seguir realizando operaciones de backup de volcado y restauración incrementales sin tener que volver a configurar las políticas de backup tras una conmutación por error del almacenamiento o una operación ARL.

**Operaciones de volcado cuando la extensión DE LA CABINA no es compatible**

Si la aplicación de backup no admite la extensión CAB, puede seguir realizando operaciones de backup y restauración de volcado incrementales si migra la LIF configurada en la política de backup al nodo que aloja el agregado de destino. De lo contrario, una vez realizada la conmutación por error del almacenamiento y la operación ARL, debe realizar un backup básico antes de realizar la operación de backup incremental.



Para las operaciones de recuperación tras fallos de almacenamiento, el LIF configurado en la política de backup se debe migrar al nodo compañero.

**Información relacionada**

["Conceptos de ONTAP"](#)

["Alta disponibilidad"](#)

**Cómo funciona el volcado con el movimiento de volúmenes**

El sistema de almacenamiento puede ejecutar en paralelo las operaciones de backup y restauración de cinta y el movimiento de volúmenes hasta que el sistema de almacenamiento intente la fase final de transposición. Una vez completada esta fase, no se permiten nuevas operaciones de backup y restauración en cinta en el volumen que se mueve. No obstante, las operaciones actuales siguen en ejecución hasta que se complete.

En la siguiente tabla se describe el comportamiento de las operaciones de backup a cinta y restauración después de la operación de movimiento de volúmenes:

| Si realiza operaciones de backup y restauración en cinta en...                                                  | Realice lo siguiente...                                                                                                                                                                 |
|-----------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| La aplicación de backup admite la extensión CAB del modo NDMP de las máquinas virtuales de almacenamiento (SVM) | Puede seguir realizando operaciones incrementales de backup a cinta y restauración en volúmenes de lectura/escritura y solo lectura sin tener que reconfigurar las políticas de backup. |



| Si realiza operaciones de backup y restauración en cinta en...                        | Realice lo siguiente...                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| El modo NDMP con ámbito SVM cuando la aplicación de backup no admite la extensión CAB | Puede seguir realizando operaciones incrementales de backup a cinta y restauración en volúmenes de lectura/escritura y solo lectura si migra la LIF configurada en la política de backup al nodo que aloja el agregado de destino. De lo contrario, después del movimiento de volumen, debe ejecutar un backup básico antes de ejecutar la operación de backup incremental. |



Cuando se produce un movimiento de volúmenes, si el volumen que pertenece a una SVM diferente del nodo de destino tiene el mismo nombre que el del volumen movido, no se pueden ejecutar operaciones de backup incrementales del volumen movido.

#### Información relacionada

["Conceptos de ONTAP"](#)

#### Cómo funciona el volcado cuando un volumen FlexVol está lleno

Antes de realizar una operación de backup de volcado incremental, debe asegurarse de que haya suficiente espacio libre en el volumen FlexVol.

Si se produce un error en la operación, debe aumentar el espacio libre en el volumen FlexVol aumentando su tamaño o eliminando las copias de Snapshot. A continuación, vuelva a realizar la operación de copia de seguridad incremental.

#### Cómo funciona el volcado cuando cambia el tipo de acceso de volúmenes

Cuando un volumen de destino de SnapMirror o un volumen secundario de SnapVault cambian el estado de lectura/escritura a solo lectura o de solo lectura a lectura/escritura, se debe ejecutar una operación de backup o restauración de cinta de referencia.

Los volúmenes secundarios de destino de SnapMirror y SnapVault son volúmenes de solo lectura. Si realiza operaciones de backup y restauración de cinta en dichos volúmenes, se debe ejecutar una operación de backup o restauración de línea base siempre que el volumen cambie el estado de solo lectura a lectura/escritura o de lectura/escritura a solo lectura.

#### Información relacionada

["Conceptos de ONTAP"](#)

#### Cómo funciona el volcado con la restauración de archivos únicos o LUN de SnapMirror

Antes de realizar operaciones de volcado de backup o restauración en un volumen en el que se restaura un solo archivo o LUN mediante la tecnología SnapMirror, debe entender cómo funcionan las operaciones de volcado con una sola operación de restauración de archivos o LUN.

Durante una operación de restauración de un único archivo o LUN de SnapMirror, las I/O del cliente están

restringidas en el archivo o LUN que se van a restaurar. Cuando la operación de restauración de archivos o LUN individuales finaliza, se elimina la restricción de I/O del archivo o LUN. Si se realiza un backup de volcado en un volumen para el que se restaura un solo archivo o LUN, el archivo o el LUN que tiene restricción de I/O del cliente no se incluye en el backup de volcado. En una operación de copia de seguridad posterior, se realiza una copia de seguridad de este archivo o LUN en cinta después de eliminar la restricción de E/S.

No se puede realizar una restauración de volcado y una operación de restauración de archivos o LUN de SnapMirror simultáneamente en el mismo volumen.

### **Cómo las operaciones de volcado de backup y restauración se ven afectadas por las configuraciones de MetroCluster**

Antes de llevar a cabo operaciones de backup de volcado y restauración en una configuración de MetroCluster, debe comprender cómo se ven afectadas las operaciones de volcado cuando se produzca una operación de conmutación de sitios o conmutación de estado.

#### **Operación de copia de seguridad o restauración de volcado seguida de la conmutación**

Considere dos clústeres: El clúster 1 y el clúster 2. Durante una operación de backup de volcado o restauración en el clúster 1, si se inicia una conmutación por error desde el clúster 1 al clúster 2, se produce lo siguiente:

- Si el valor de `override-vetoes` la opción es `false`, a continuación, se cancela la operación de switchover y continúa la operación de copia de seguridad o restauración.
- Si el valor de la opción es `true`, la operación de copia de seguridad de volcado o restauración se cancela y la operación de switchover continúa.

#### **Operación de copia de seguridad o restauración de volcado seguida de una conmutación de estado**

Una conmutación de sitios se realiza desde el clúster 1 al clúster 2 y se inicia una operación de backup de volcado o restauración en el clúster 2. La operación de volcado realiza un backup o restaura un volumen ubicado en el clúster 2. En este punto, si se inicia una conmutación de estado del clúster 2 al clúster 1, sucede lo siguiente:

- Si el valor de `override-vetoes` la opción es `false`, a continuación, la conmutación de regreso se cancela y la operación de copia de seguridad o restauración continúa.
- Si el valor de la opción es `true`, a continuación, la operación de copia de seguridad o restauración se cancela y la conmutación de regreso continúa.

#### **La operación de backup o restauración de volcado se inició durante una conmutación de sitios o una conmutación de estado**

Durante una conmutación de sitios del clúster 1 al clúster 2, si se inicia una operación de backup de volcado o restauración en el clúster 1, las operaciones de backup o restauración fallan y la conmutación continúa.

Durante una conmutación de estado del clúster 2 al clúster 1, si se inicia una operación de backup o restauración de volcado desde el clúster 2, la operación de backup o restauración dará error y esta continuará.

### **Acerca del motor SMTape para volúmenes de FlexVol**

## Acerca del motor SMTape para volúmenes de FlexVol

SMTape es una solución de recuperación ante desastres de ONTAP que realiza backup de bloques de datos a cinta. Puede usar SMTape para realizar backups de volúmenes a las cintas. Sin embargo, no puede realizar un backup en el nivel qtree o subárbol. SMTape admite copias de seguridad de línea base, diferenciales e incrementales. SMTape no requiere una licencia.

Puede realizar una operación de backup y restauración de SMTape mediante una aplicación de backup compatible con NDMP. Puede elegir SMTape para realizar operaciones de backup y restauración solo en el modo de NDMP de las máquinas virtuales de almacenamiento (SVM) con ámbito.



No se admite el proceso de reversión cuando hay una sesión de copia de seguridad o restauración de SMTape en curso. Debe esperar hasta que finalice la sesión o debe anular la sesión NDMP.

Con SMTape, puede realizar backups de 255 copias Snapshot. Para obtener backups completos, incrementales o diferenciales posteriores, debe eliminar las copias Snapshot con backup más antiguas.

Antes de ejecutar una restauración básica, debe ser del tipo el volumen al que se van a restaurar los datos DP y este volumen debe estar en estado restringido. Después de una restauración correcta, este volumen está en línea automáticamente. Se pueden realizar restauraciones posteriores incrementales o diferenciales en este volumen en el orden en que se ejecutaron los backups.

## Use las copias Snapshot durante el backup de SMTape

Debe comprender cómo se utilizan las copias Snapshot durante un backup básico de SMTape y un backup incremental. También hay que tener en cuenta al realizar un backup con SMTape.

### Backup de línea de base

Al realizar un backup de referencia, es posible especificar el nombre de la copia Snapshot de la que se realizará un backup en cinta. Si no se especifica ninguna copia Snapshot, según el tipo de acceso del volumen (lectura/escritura o solo lectura), se crea automáticamente una copia Snapshot o se utilizan copias Snapshot existentes. Cuando especifica una copia Snapshot para el backup, también se realiza un backup en cinta de todas las copias Snapshot más antiguas de la copia Snapshot especificada.

Si no se especifica una copia Snapshot para el backup, ocurre lo siguiente:

- En el caso de un volumen de lectura/escritura, se crea automáticamente una copia Snapshot.

La copia Snapshot recién creada y se realiza un backup en cinta de todas las copias Snapshot más antiguas.

- Para un volumen de solo lectura, todas las copias Snapshot, incluida la última copia de Snapshot, se copian en cinta.

No se realiza un backup de ninguna copia Snapshot nueva creada después de comenzar el backup.

## Backup incremental

Para las operaciones de backup incremental o diferencial de SMTape, las aplicaciones de backup compatibles con NDMP crean y gestionan las copias Snapshot.

Siempre debe especificar una copia de Snapshot mientras realiza una operación de backup incremental. Para que la operación de backup incremental se realice correctamente, la copia de Snapshot de la que se realizó un backup durante la operación de backup anterior (de referencia o incremental) debe estar en el volumen a partir del cual se ejecutó el backup. Para garantizar que usa esta copia Snapshot con backup, debe tener en cuenta la política de Snapshot asignada en este volumen al configurar la política de backup.

## Consideraciones sobre backups de SMTape en destinos de SnapMirror

- Una relación de mirroring de protección de datos crea copias Snapshot temporales en el volumen de destino para la replicación.

No debe usar estas copias Snapshot para backup de SMTape.

- Si se produce una actualización de SnapMirror en un volumen de destino en una relación de reflejo de protección de datos durante una operación de backup de SMTape en el mismo volumen, la copia de Snapshot de la que SMTape se realiza el backup no debe eliminarse en el volumen de origen.

Durante la operación de backup, SMTape bloquea la copia Snapshot en el volumen de destino y si se elimina la copia de Snapshot correspondiente en el volumen de origen, se producirá un error en la operación de actualización de SnapMirror posterior.

- No debe utilizar estas copias Snapshot durante un backup incremental.

## Capacidades SMTape

Las funcionalidades de SMTape como el backup de copias Snapshot, backups incrementales y diferenciales, la conservación de las funciones de deduplicación y compresión en volúmenes restaurados y de propagación en cinta ayudan a optimizar las operaciones de backup y restauración en cinta.

SMTape ofrece las siguientes capacidades:

- Ofrece una solución de recuperación tras siniestros
- Permite backups incrementales y diferenciales
- Realiza un backup de copias Snapshot
- Permite realizar backups y restauraciones de volúmenes deduplicados y mantiene la deduplicación en los volúmenes restaurados
- Realiza backups de volúmenes comprimidos y mantiene la compresión en los volúmenes restaurados
- Permite siembra de cintas

SMTape admite el factor de bloqueo en múltiplos de 4 KB, dentro del intervalo de 4 KB a 256 KB.



Es posible restaurar datos en volúmenes creados solo en dos versiones principales consecutivas de ONTAP.

## Funciones no admitidas en SMTape

SMTape no admite backups reiniciables ni la verificación de archivos con backup.

## Límites de escalabilidad para las sesiones de backup y restauración de SMTape

Al ejecutar operaciones de backup y restauración de SMTape mediante NDMP o interfaz de línea de comandos (propagación de cintas), debe tener en cuenta la cantidad máxima de sesiones de backup y restauración de SMTape que pueden realizarse de manera simultánea en sistemas de almacenamiento con diferentes capacidades de memoria del sistema. Este número máximo depende de la memoria del sistema de un sistema de almacenamiento.



Los límites de escalabilidad de las sesiones de backup y restauración de SMTape son diferentes de los límites de sesiones de NDMP y los límites de sesiones de volcado.

| Memoria del sistema de almacenamiento        | Cantidad total de sesiones de backup y restauración de SMTape |
|----------------------------------------------|---------------------------------------------------------------|
| Menos de 16 GB                               | 6                                                             |
| Mayor o igual que 16 GB pero menor que 24 GB | 16                                                            |
| Mayor o igual que 24 GB                      | 32                                                            |

Puede obtener la memoria del sistema del sistema de almacenamiento mediante el `sysconfig -a` comando (disponible a través del nodeshell). Para obtener más información acerca de cómo utilizar este comando, consulte las páginas man.

### Información relacionada

[Límites de escalabilidad para sesiones NDMP](#)

[Límites de escalabilidad para sesiones de backup y restauración de volcado](#)

## Qué es la siembra de cintas

La propagación de cintas es una funcionalidad SMTape que ayuda a inicializar un volumen de FlexVol de destino en una relación de mirroring de protección de datos.

La propagación de cintas permite establecer una relación de mirroring para la protección de datos entre un sistema de origen y un sistema de destino a través de una conexión de ancho de banda bajo.

El mirroring incremental de las copias Snapshot del origen al destino es factible gracias a una conexión de ancho de banda bajo. Sin embargo, un mirroring inicial de la copia Snapshot base demora mucho tiempo en una conexión de ancho de banda bajo. En estos casos, se puede realizar un backup de SMTape del volumen de origen a una cinta y usar la cinta para transferir la copia Snapshot básica inicial al destino. A continuación, puede configurar las actualizaciones incrementales de SnapMirror en el sistema de destino mediante la conexión con un ancho de banda bajo.

### Información relacionada

## **Funcionamiento de SMTape con la recuperación tras fallos de almacenamiento y las operaciones de ARL**

Antes de ejecutar operaciones de backup o restauración de SMTape, debe comprender cómo funcionan estas operaciones con la operación de conmutación al nodo de respaldo (toma de control y retorno al nodo primario) de almacenamiento o la operación de reubicación de agregados (ARL). La `-override-vetoes` Option determina el comportamiento del motor de SMTape durante una recuperación tras fallos de almacenamiento o una operación de ARL.

Cuando se ejecuta una operación de backup o restauración de SMTape y la `-override-vetoes` opción establecida en `false`, Se detiene una operación de ARL o una conmutación por error del almacenamiento iniciada por el usuario y se completa la operación de copia de seguridad o restauración. Si la aplicación de backup admite la extensión CAB, puede seguir realizando operaciones incrementales de backup y restauración de datos SMTape sin tener que reconfigurar las políticas de backup. Sin embargo, si la `-override-vetoes` opción establecida en `true`, La operación de recuperación tras fallos de almacenamiento o ARL continúa y se anula la operación de copia de seguridad o restauración de SMTape.

### **Información relacionada**

["Gestión de redes"](#)

["Alta disponibilidad"](#)

## **Funcionamiento de SMTape con el movimiento de volúmenes**

Las operaciones de backup de SMTape y las operaciones de movimiento de volúmenes se pueden ejecutar en paralelo hasta que el sistema de almacenamiento intente la fase final de la transición. Una vez pasada esta fase, no se pueden ejecutar nuevas operaciones de backup de SMTape en el volumen que se va a mover. No obstante, las operaciones actuales siguen en ejecución hasta que se complete.

Antes de iniciar la fase de transición de un volumen, la operación de movimiento de volúmenes comprueba las operaciones de backup de SMTape activas en el mismo volumen. Si hay operaciones de backup de SMTape activas, la operación de movimiento de volúmenes pasa al estado de transposición diferida y permite que se completen las operaciones de backup de SMTape. Una vez completadas estas operaciones de backup, debe reiniciar manualmente la operación de movimiento de volúmenes.

Si la aplicación de backup admite la extensión CAB, puede seguir realizando operaciones incrementales de backup y restauración de cinta en volúmenes de lectura/escritura y solo lectura sin tener que reconfigurar las políticas de backup.

No se pueden ejecutar las operaciones de restauración básica y movimiento de volúmenes de forma simultánea; sin embargo, la restauración incremental puede ejecutarse en paralelo con las operaciones de movimiento de volúmenes, con un comportamiento similar al de las operaciones de backup de SMTape durante las operaciones de movimiento de volúmenes.

### **Información relacionada**

["Conceptos de ONTAP"](#)

## Cómo funciona SMTape con las operaciones de realojamiento de volúmenes

No se pueden iniciar las operaciones de SMTape cuando hay una operación de realojamiento de volumen en curso en un volumen. Cuando un volumen está implicado en una operación de realojamiento de volúmenes, no debe iniciarse la sesión de SMTape en ese volumen.

Si hay alguna operación de rehost de volumen en curso, se produce un error en el backup o la restauración de SMTape. Si hay un backup o una restauración de SMTape en curso, se producirá un error en las operaciones de rehost de volúmenes con el mensaje de error correspondiente. Esta condición se aplica tanto a las operaciones de backup o restauración basadas en NDMP como a las basadas en CLI.

## Cómo se ve afectada la política de backup NDMP durante el Bad

Cuando se habilita el equilibrador automático de datos (ADB), el equilibrador analiza las estadísticas de uso de agregados para identificar el agregado que ha superado el porcentaje de uso de umbral alto configurado.

Tras identificar el agregado que ha superado el umbral, el equilibrador identifica un volumen que se puede mover a agregados que residen en otro nodo del clúster e intenta mover dicho volumen. Esta situación afecta a la política de backup configurada para este volumen porque si la aplicación de gestión de datos (DMA) no tiene en CUENTA LA CABINA, el usuario debe volver a configurar la política de backup y ejecutar la operación de backup de referencia.



Si el DMA es compatible CON CAB y la política de respaldo se ha configurado utilizando una interfaz específica, el ADB no se ve afectado.

## Cómo se ven afectadas las operaciones de backup y restauración de SMTape en las configuraciones de MetroCluster

Antes de ejecutar operaciones de backup y restauración de SMTape en una configuración de MetroCluster, debe comprender cómo se ven afectadas las operaciones de SMTape cuando se produce una operación de conmutación de sitios o conmutación de estado.

### Operación de backup o restauración de SMTape seguida de una conmutación

Considere dos clústeres: El clúster 1 y el clúster 2. Durante una operación de backup o restauración de SMTape en el clúster 1, si se inicia una conmutación entre el clúster 1 y el clúster 2, se produce lo siguiente:

- Si el valor de `-override-vetoes` la opción es `false`, a continuación, el proceso de switchover se cancela y la operación de copia de seguridad o restauración continúa.
- Si el valor de la opción es `true`, La operación de copia de seguridad o restauración de SMTape se cancela y el proceso de cambio continúa.

### Operación de copia de seguridad o restauración de SMTape seguida de una conmutación de estado

Se realiza una conmutación de sitios desde el clúster 1 al clúster 2 y se inicia una operación de backup o restauración de SMTape en el clúster 2. La operación SMTape realiza backups o restaura un volumen ubicado en el clúster 2. En este punto, si se inicia una conmutación de estado del clúster 2 al clúster 1, sucede lo siguiente:

- Si el valor de `-override-vetoes` la opción es `false`, a continuación, el proceso de regreso se cancela y la operación de copia de seguridad o restauración continúa.
- Si el valor de la opción es `true`, la operación de copia de seguridad o restauración se cancela y el proceso de regreso continúa.

**La operación de backup o restauración de SMTape se inició durante una conmutación de sitios o conmutación de estado**

Durante un proceso de conmutación de sitios del clúster 1 al clúster 2, si se inicia una operación de backup o restauración de SMTape en el clúster 1, la operación de backup o restauración falla y la conmutación continúa.

Durante un proceso de conmutación de estado del clúster 2 al clúster 1, si se inicia una operación de backup o restauración SMTape desde el clúster 2, la operación de backup o restauración falla y la conmutación de estado continúa.

## **Supervisar las operaciones de backup y restauración a cinta para volúmenes de FlexVol**

**Supervisar la información general sobre las operaciones de backup y restauración a cinta para volúmenes de FlexVol**

Es posible ver los archivos de registro de eventos para supervisar las operaciones de backup a cinta y restauración. ONTAP registra automáticamente los eventos de backup y restauración importantes, así como el momento en que se producen en un archivo de registro denominado `backup` en las controladoras `/etc/log/` directorio. De forma predeterminada, el registro de eventos está establecido en `on`.

Es posible que desee ver los archivos de registro de eventos por los siguientes motivos:

- Comprobar si un backup nocturno se ha realizado correctamente
- Recopilación de estadísticas sobre operaciones de backup
- Para usar la información de los archivos de registro de eventos anteriores con el fin de ayudar a diagnosticar problemas con las operaciones de backup y restauración

Una vez cada semana, los archivos de registro de eventos se rotan. La `/etc/log/backup` se cambia el nombre del archivo a `/etc/log/backup.0`, la `/etc/log/backup.0` se cambia el nombre del archivo a `/etc/log/backup.1`, y así sucesivamente. El sistema guarda los archivos de registro durante un máximo de seis semanas; por lo tanto, puede tener hasta siete archivos de mensaje (`/etc/log/backup.[0-5]` y la corriente `/etc/log/backup` archivo).

### **Acceda a los archivos de registro de eventos**

Es posible acceder a los archivos de registro de eventos para las operaciones de backup a cinta y restauración en la `/etc/log/` mediante el directorio `rdfile` orden en el `nodesinfierno`. Es posible ver estos archivos de registro de eventos para supervisar las operaciones de backup a cinta y restauración.

### **Acerca de esta tarea**

Con configuraciones adicionales, como una función de control de acceso con acceso al `spi` servicio web o una cuenta de usuario configurada con `http` método de acceso, también puede utilizar un explorador web



para acceder a estos archivos de registro.

**Pasos**

- 1. Para acceder a nodeshell, introduzca el siguiente comando:

```
node run -node node_name
```

node\_name es el nombre del nodo.

- 2. Para acceder a los archivos del registro de eventos para las operaciones de backup a cinta y restauración, escriba el siguiente comando:

```
rdfile /etc/log/backup
```

**Información relacionada**

["Administración del sistema"](#)

["Conceptos de ONTAP"](#)

**Qué es el formato de mensaje de volcado y restauración del registro de eventos**

**Información general sobre el formato del mensaje de registro de eventos de volcado y restauración**

Para cada evento de volcado y restauración, se escribe un mensaje en el archivo de registro de copia de seguridad.

El formato del mensaje de volcado y restauración del registro de eventos es el siguiente:

```
type timestamp identifier event (event_info)
```

En la lista siguiente se describen los campos en el formato de mensaje del registro de eventos:

- Cada mensaje de registro comienza con uno de los indicadores de tipo descritos en la siguiente tabla:

| Tipo     | Descripción            |
|----------|------------------------|
| registro | Evento de registro     |
| dmp      | Evento de volcado      |
| rst      | Evento de restauración |

- timestamp muestra la fecha y la hora del evento.
- La identifier El campo de un evento de volcado incluye la ruta de volcado y el ID exclusivo del volcado. La identifier el campo de un evento de restauración solo utiliza el nombre de ruta de destino de restauración como identificador único. Los mensajes de eventos relacionados con el registro no incluyen un identifier campo.

## Qué son los eventos de registro

El campo de evento de un mensaje que comienza con un registro especifica el comienzo de un registro o el final de un registro.

Contiene uno de los eventos que se muestran en la siguiente tabla:

| Evento          | Descripción                                                                                            |
|-----------------|--------------------------------------------------------------------------------------------------------|
| Inicio_registro | Indica el comienzo del registro o que el registro se ha vuelto a activar después de estar desactivado. |
| Stop_Logging    | Indica que se ha desactivado el registro.                                                              |

## ¿Qué eventos de volcado son

El campo de evento de un evento de volcado contiene un tipo de evento seguido de información específica del evento entre paréntesis.

En la siguiente tabla se describen los eventos, sus descripciones y la información de eventos relacionada que puede registrarse para una operación de volcado:

| Evento         | Descripción                                                 | Información del evento                                                  |
|----------------|-------------------------------------------------------------|-------------------------------------------------------------------------|
| Comenzar       | Se ha iniciado el volcado NDMP                              | Nivel de descarga y tipo de volcado                                     |
| Fin            | Volcados completados correctamente                          | Cantidad de datos procesados                                            |
| Anular         | Se cancela la operación                                     | Cantidad de datos procesados                                            |
| Opciones       | Se muestran las opciones especificadas                      | Todas las opciones y sus valores asociados, incluidas las opciones NDMP |
| Tape_open      | La cinta está abierta para lectura y escritura              | Nombre del nuevo dispositivo de cinta                                   |
| Tape_close     | La cinta se cierra para lectura/escritura                   | El nombre del dispositivo de cinta                                      |
| Cambio de fase | Un volcado está entrando en una nueva fase de procesamiento | El nombre de la nueva fase                                              |
| Error          | Un volcado ha encontrado un evento inesperado               | Mensaje de error                                                        |
| Snapshot       | Se crea o se encuentra una copia Snapshot                   | El nombre y la hora de la copia Snapshot                                |

| Evento       | Descripción                                                           | Información del evento                                                 |
|--------------|-----------------------------------------------------------------------|------------------------------------------------------------------------|
| Volcado_base | Se ha localizado una entrada de volcado base en el metarchivo interno | El nivel y la hora del volcado base (sólo para volcados incrementales) |

#### Qué eventos de restauración son

El campo de evento de restauración contiene un tipo de evento seguido de información específica del evento entre paréntesis.

En la siguiente tabla, se proporciona información sobre los eventos, sus descripciones y la información de eventos relacionada que se puede registrar para una operación de restauración:

| Evento         | Descripción                                              | Información del evento                                                  |
|----------------|----------------------------------------------------------|-------------------------------------------------------------------------|
| Comenzar       | Se ha iniciado la restauración NDMP                      | Nivel de restauración y tipo de restauración                            |
| Fin            | Las restauraciones se completaron correctamente          | Número de archivos y cantidad de datos procesados                       |
| Anular         | Se cancela la operación                                  | Número de archivos y cantidad de datos procesados                       |
| Opciones       | Se muestran las opciones especificadas                   | Todas las opciones y sus valores asociados, incluidas las opciones NDMP |
| Tape_open      | La cinta está abierta para lectura y escritura           | Nombre del nuevo dispositivo de cinta                                   |
| Tape_close     | La cinta se cierra para lectura/escritura                | El nombre del dispositivo de cinta                                      |
| Cambio de fase | Restore está entrando en una nueva fase de procesamiento | El nombre de la nueva fase                                              |
| Error          | La restauración encuentra un evento inesperado           | Mensaje de error                                                        |

#### Habilitar o deshabilitar el registro de eventos

Puede activar o desactivar el registro de eventos.

#### Pasos

1. Para habilitar o deshabilitar el registro de eventos, introduzca el siguiente comando en el clustershell:

```
options -option_name backup.log.enable -option-value {on | off}
```

on activa el inicio de sesión de eventos.

off desactiva la sesión de eventos.



El registro de eventos está activado de forma predeterminada.

## Mensajes de error para backup y restauración a cinta de volúmenes de FlexVol

### Mensajes de error de copia de seguridad y restauración

#### Limitación de recursos: No hay ningún subproceso disponible

- **Mensaje**

Resource limitation: no available thread

- **Causa**

El número máximo de subprocesos de E/S de cinta local activos está actualmente en uso. Puede tener un máximo de 16 unidades de cinta locales activas.

- **Acción Correctiva**

Espere a que finalicen algunos trabajos de cinta antes de iniciar una nueva tarea de copia de seguridad o restauración.

#### Reserva de cintas prehecha

- **Mensaje**

Tape reservation preempted

- **Causa**

La unidad de cinta está en uso por otra operación o la cinta se ha cerrado prematuramente.

- **Acción Correctiva**

Asegúrese de que la unidad de cinta no esté en uso en otra operación y de que la aplicación DMA no haya cancelado el trabajo y vuelva a intentarlo.

#### No se pudo inicializar el medio

- **Mensaje**

Could not initialize media

- **Causa**

Puede obtener este error por uno de los siguientes motivos:

- La unidad de cinta utilizada para la copia de seguridad está dañada o dañada.

- La cinta no contiene la copia de seguridad completa o está dañada.
- El número máximo de subprocesos de E/S de cinta local activos está actualmente en uso.

Puede tener un máximo de 16 unidades de cinta locales activas.

- **Acción Correctiva**

- Si la unidad de cinta está dañada o dañada, vuelva a intentar la operación con una unidad de cinta válida.
- Si la cinta no contiene la copia de seguridad completa o está dañada, no podrá realizar la operación de restauración.
- Si no hay recursos de cinta disponibles, espere a que finalicen algunos de los trabajos de backup o restauración y vuelva a intentar la operación.

#### Número máximo de volcados o restauraciones permitidos (límite máximo de sesión) en curso

- **Mensaje**

Maximum number of allowed dumps or restores (*maximum session limit*) in progress

- **Causa**

Ya se está ejecutando la cantidad máxima de trabajos de backup o restauración.

- **Acción Correctiva**

Vuelva a intentar la operación después de que finalicen algunos de los trabajos en ejecución actualmente.

#### Error de soporte al escribir la cinta

- **Mensaje**

Media error on tape write

- **Causa**

La cinta utilizada para la copia de seguridad está dañada.

- **Acción Correctiva**

Sustituya la cinta y vuelva a intentar la tarea de copia de seguridad.

#### Error al escribir en la cinta

- **Mensaje**

Tape write failed

- **Causa**

La cinta utilizada para la copia de seguridad está dañada.

- **Acción Correctiva**

Sustituya la cinta y vuelva a intentar la tarea de copia de seguridad.

#### **Error al escribir la cinta: La nueva cinta encontró un error de soporte**

- **Mensaje**

Tape write failed - new tape encountered media error

- **Causa**

La cinta utilizada para la copia de seguridad está dañada.

- **Acción Correctiva**

Sustituir la cinta y volver a intentar la copia de seguridad.

#### **Error al escribir en la cinta: La nueva cinta está rota o está protegida contra escritura**

- **Mensaje**

Tape write failed - new tape is broken or write protected

- **Causa**

La cinta utilizada para el backup está dañada o protegida contra escritura.

- **Acción Correctiva**

Sustituir la cinta y volver a intentar la copia de seguridad.

#### **Error al escribir en cinta: La nueva cinta ya está al final del soporte**

- **Mensaje**

Tape write failed - new tape is already at the end of media

- **Causa**

No hay suficiente espacio en la cinta para completar la copia de seguridad.

- **Acción Correctiva**

Sustituir la cinta y volver a intentar la copia de seguridad.

#### **Error de escritura de cinta**

- **Mensaje**

Tape write error - The previous tape had less than the required minimum capacity, size MB, for this tape operation, The operation should be restarted from the beginning

- **Causa**

La capacidad de la cinta no es suficiente para contener los datos de copia de seguridad.

- **Acción Correctiva**

Utilice cintas con mayor capacidad y vuelva a intentar realizar la tarea de backup.

#### Error de soporte en la cinta de lectura

- **Mensaje**

Media error on tape read

- **Causa**

La cinta de la que se van a restaurar los datos está dañada y puede que no contenga los datos de copia de seguridad completos.

- **Acción Correctiva**

Si está seguro de que la cinta tiene la copia de seguridad completa, vuelva a intentar la operación de restauración. Si la cinta no contiene la copia de seguridad completa, no se puede ejecutar la operación de restauración.

#### Error de lectura de cinta

- **Mensaje**

Tape read error

- **Causa**

La unidad de cinta está dañada o la cinta no contiene la copia de seguridad completa.

- **Acción Correctiva**

Si la unidad de cinta está dañada, utilice otra unidad de cinta. Si la cinta no contiene la copia de seguridad completa, no podrá restaurar los datos.

#### Ya al final de la cinta

- **Mensaje**

Already at the end of tape

- **Causa**

La cinta no contiene datos o debe rebobinarse.

- **Acción Correctiva**

Si la cinta no contiene datos, utilice la cinta que contiene la copia de seguridad y vuelva a intentar la tarea de restauración. De lo contrario, rebobine la cinta y vuelva a intentar el trabajo de restauración.

El tamaño del registro de cinta es demasiado pequeño. Pruebe con un tamaño mayor.

- **Mensaje**

`Tape record size is too small. Try a larger size.`

- **Causa**

El factor de bloqueo especificado para la operación de restauración es menor que el factor de bloqueo que se utilizó durante el backup.

- **Acción Correctiva**

Utilice el mismo factor de bloqueo que se especificó durante la copia de seguridad.

El tamaño del registro de cinta debe ser `block_Siz1` y no `Block_Size2`

- **Mensaje**

`Tape record size should be block_size1 and not block_size2`

- **Causa**

El factor de bloqueo especificado para la restauración local es incorrecto.

- **Acción Correctiva**

Vuelva a intentar la tarea de restauración con `block_size1` como factor de bloqueo.

El tamaño del registro de la cinta debe estar comprendido entre 4 KB y 256 KB

- **Mensaje**

`Tape record size must be in the range between 4KB and 256KB`

- **Causa**

El factor de bloqueo especificado para la operación de backup o restauración no se encuentra dentro del rango permitido.

- **Acción Correctiva**

Especifique un factor de bloqueo entre 4 KB y 256 KB.

## Mensajes de error de NDMP

### Error de comunicación de red

- **Mensaje**

`Network communication error`

- **Causa**



Se produjo un error en la comunicación a una cinta remota en una conexión triple NDMP.

- **Acción Correctiva**

Compruebe la conexión de red al mando a distancia.

#### **Mensaje de Read Socket: Error\_string**

- **Mensaje**

Message from Read Socket: error\_string

- **Causa**

Restaurar la comunicación desde la cinta remota en la conexión NDMP 3-way tiene errores.

- **Acción Correctiva**

Compruebe la conexión de red al mando a distancia.

#### **Mensaje de Write Dirnet: Error\_string**

- **Mensaje**

Message from Write Dirnet: error\_string

- **Causa**

Se produjo un error en la comunicación de backup a una cinta remota en una conexión triple NDMP.

- **Acción Correctiva**

Compruebe la conexión de red al mando a distancia.

#### **Leer el conector hembra EOF recibido**

- **Mensaje**

Read Socket received EOF

- **Causa**

El intento de comunicarse con una cinta remota en una conexión triple NDMP ha alcanzado el fin de la Marca de archivo. Es posible que se intente realizar una restauración triple desde una imagen de backup con un tamaño de bloque mayor.

- **Acción Correctiva**

Especifique el tamaño de bloque correcto y vuelva a intentar la operación de restauración.

#### **ndmpd número de versión no válido: version\_number "**

- **Mensaje**

```
ndmpd invalid version number: version_number
```

- **Causa**

La versión NDMP especificada no es compatible con el sistema de almacenamiento.

- **Acción Correctiva**

Especifique la versión 4 de NDMP.

#### **Ndmpd session\_ID no activo**

- **Mensaje**

```
ndmpd session session_ID not active
```

- **Causa**

Es posible que la sesión NDMP no exista.

- **Acción Correctiva**

Utilice la `ndmpd status` Comando para ver las sesiones NDMP activas.

#### **No se puede obtener la referencia de volumen para Volume\_name**

- **Mensaje**

```
Could not obtain vol ref for Volume vol_name
```

- **Causa**

No se pudo obtener la referencia del volumen debido a que este puede estar en uso por parte de otras operaciones.

- **Acción Correctiva**

Volver a intentar la operación más tarde.

#### **El tipo de conexión de datos ["NDMP4\_ADDR\_TCP"|"NDMP4\_ADDR\_TCP\_IPv6"] no es compatible con las conexiones de control ["IPv6"|"IPv4"]**

- **Mensaje**

```
Data connection type ["NDMP4_ADDR_TCP"|"NDMP4_ADDR_TCP_IPv6"] not supported
for ["IPv6"|"IPv4"] control connections
```

- **Causa**

En el modo NDMP de ámbito de nodo, la conexión de datos NDMP establecida debe ser del mismo tipo de dirección de red (IPv4 o IPv6) que la conexión de control NDMP.

- **Acción Correctiva**

Póngase en contacto con el proveedor de sus aplicaciones de backup.

#### **ESCUCHA DE DATOS: Error de condición de preparación de la conexión DE datos DE LA CABINA**

- **Mensaje**

DATA LISTEN: CAB data connection prepare precondition error

- **Causa**

Se produce un error en la escucha de datos NDMP cuando la aplicación de backup ha negociado la extensión CAB con el servidor NDMP y el tipo de dirección de conexión de datos NDMP especificado no coincide entre los mensajes NDMP\_CAB\_DATA\_CONN\_PREPARE y NDMP\_DATA\_LISTEN.

- **Acción Correctiva**

Póngase en contacto con el proveedor de sus aplicaciones de backup.

#### **CONEXIÓN DE DATOS: Error de condición de preparación de la conexión DE datos DE LA CABINA**

- **Mensaje**

DATA CONNECT: CAB data connection prepare precondition error

- **Causa**

Se produce un error en la conexión de datos NDMP cuando la aplicación de backup ha negociado la extensión CAB con el servidor NDMP y el tipo de dirección de conexión de datos NDMP especificado no coincide entre los mensajes NDMP\_CAB\_DATA\_CONN\_PREPARE y NDMP\_DATA\_CONNECT.

- **Acción Correctiva**

Póngase en contacto con el proveedor de sus aplicaciones de backup.

#### **Error:error al mostrar: No se puede obtener la contraseña del usuario '<username>'**

- **Mensaje**

Error: show failed: Cannot get password for user '<username>'

- **Causa**

Configuración de cuenta de usuario incompleta para NDMP

- **Acción Correctiva**

Asegúrese de que la cuenta de usuario esté asociada con el método de acceso SSH y que el método de autenticación sea la contraseña de usuario.

#### **Mensajes de error de volcado**

#### El volumen de destino es de solo lectura

- **Mensaje**

`Destination volume is read-only`

- **Causa**

La ruta a la que se intenta realizar la operación de restauración es de solo lectura.

- **Acción Correctiva**

Intente restaurar los datos en una ubicación diferente.

#### El qtree de destino es de solo lectura

- **Mensaje**

`Destination qtree is read-only`

- **Causa**

El qtree al que se intenta restaurar es de solo lectura.

- **Acción Correctiva**

Intente restaurar los datos en una ubicación diferente.

#### Vuelca temporalmente desactivado en el volumen, vuelva a intentarlo

- **Mensaje**

`Dumps temporarily disabled on volume, try again`

- **Causa**

Se intenta realizar un backup de volcado NDMP en un volumen de destino de SnapMirror que forma parte de cualquiera de los dos `snapmirror break` o a `snapmirror resync` funcionamiento.

- **Acción Correctiva**

Espere a que el `snapmirror break` o `snapmirror resync` operación para finalizar y después realizar la operación de volcado.



Siempre que el estado de un volumen de destino de SnapMirror cambie de lectura/escritura a solo lectura o de solo lectura a lectura/escritura, debe ejecutar un backup de referencia.

#### Etiquetas de NFS no reconocidas

- **Mensaje**

`Error: Aborting: dump encountered NFS security labels in the file system`

- **Causa**

Las etiquetas de seguridad NFS son compatibles a partir de ONTAP 9.9.1 cuando NFSv4.2 está habilitado. Sin embargo, el motor de volcado no reconoce actualmente las etiquetas de seguridad NFS. Si encuentra alguna etiqueta de seguridad NFS en los archivos, directorios o cualquier archivo especial en cualquier formato de volcado, el volcado falla.

- **Acción Correctiva**

Compruebe que ningún archivo o directorio tiene etiquetas de seguridad NFS.

#### No se crearon archivos

- **Mensaje**

```
No files were created
```

- **Causa**

Se intentó un DAR de directorio sin permitir la funcionalidad DAR mejorada.

- **Acción Correctiva**

Active la funcionalidad DAR mejorada y vuelva a intentar DAR.

#### Error en la restauración del <file name> de archivo

- **Mensaje**

```
Restore of the file file name failed
```

- **Causa**

Cuando SE realiza UN DAR (recuperación de acceso directo) de un archivo cuyo nombre de archivo es el mismo que el de un LUN del volumen de destino, se produce un error EN EL DAR.

- **Acción Correctiva**

Vuelva a intentar DAR del archivo.

#### Error de truncamiento para el inode <inode number> src...

- **Mensaje**

```
Truncation failed for src inode <inode number>. Error <error number>. Skipping inode.
```

- **Causa**

El inodo de un archivo se elimina cuando se restaura el archivo.

- **Acción Correctiva**

Espere a que se complete la operación de restauración en un volumen antes de usar ese volumen.

#### No se puede bloquear una snapshot necesaria mediante el volcado

- **Mensaje**

Unable to lock a snapshot needed by dump

- **Causa**

La copia Snapshot especificada para el backup no está disponible.

- **Acción Correctiva**

Vuelva a intentar el backup con una copia Snapshot diferente.

Utilice la `snap list` Comando para ver la lista de copias Snapshot disponibles.

#### No se pueden localizar los archivos de mapa de bits

- **Mensaje**

Unable to locate bitmap files

- **Causa**

Es posible que se hayan eliminado los archivos de mapa de bits necesarios para la operación de copia de seguridad. En este caso, no se puede reiniciar el backup.

- **Acción Correctiva**

Vuelva a ejecutar la copia de seguridad.

#### El volumen se encuentra temporalmente en estado transitorio

- **Mensaje**

Volume is temporarily in a transitional state

- **Causa**

El volumen del que se realiza el backup se encuentra temporalmente en el estado desmontado.

- **Acción Correctiva**

Espere algún tiempo y vuelva a realizar la copia de seguridad.

#### Mensajes de error de SMTape

##### Trozos fuera de servicio

- **Mensaje**

Chunks out of order

- **Causa**

Las cintas de copia de seguridad no se restauran en el orden correcto.

- **Acción Correctiva**

Vuelva a intentar la operación de restauración y cargue las cintas en la secuencia correcta.

#### **Formato de fragmento no compatible**

- **Mensaje**

Chunk format not supported

- **Causa**

La imagen de copia de seguridad no es de SMTape.

- **Acción Correctiva**

Si la imagen de copia de seguridad no es de SMTape, vuelva a intentar la operación con una cinta que tenga la copia de seguridad de SMTape.

#### **Error al asignar memoria**

- **Mensaje**

Failed to allocate memory

- **Causa**

El sistema se ha quedado sin memoria.

- **Acción Correctiva**

Vuelva a intentar el trabajo más tarde cuando el sistema no esté demasiado ocupado.

#### **Error al obtener el búfer de datos**

- **Mensaje**

Failed to get data buffer

- **Causa**

El sistema de almacenamiento se agotó de los búferes.

- **Acción Correctiva**

Espere a que algunas operaciones del sistema de almacenamiento finalicen y luego vuelva a intentar la tarea.

#### **Error al encontrar la snapshot**

- **Mensaje**

Failed to find snapshot

- **Causa**

La copia Snapshot especificada para el backup no está disponible.

- **Acción Correctiva**

Compruebe si la copia Snapshot especificada está disponible. En caso contrario, vuelva a intentarlo con la copia de Snapshot correcta.

#### No se puede crear la snapshot

- **Mensaje**

Failed to create snapshot

- **Causa**

El volumen ya contiene el número máximo de copias snapshot.

- **Acción Correctiva**

Elimine algunas copias de Snapshot y vuelva a intentar la operación de backup.

#### Error al bloquear la snapshot

- **Mensaje**

Failed to lock snapshot

- **Causa**

La copia Snapshot está en uso o se ha eliminado.

- **Acción Correctiva**

Si otra operación utiliza la copia de Snapshot, espere a que finalice y vuelva a intentar el backup. Si la copia Snapshot se ha eliminado, no puede realizar el backup.

#### Error al eliminar la snapshot

- **Mensaje**

Failed to delete snapshot

- **Causa**

No se pudo eliminar la copia automática de Snapshot porque está en uso en otras operaciones.

- **Acción Correctiva**

Utilice la `snap` Comando para determinar el estado de la copia Snapshot. Si no es necesaria la copia Snapshot, elimínela manualmente.



#### Error al obtener la snapshot más reciente

- **Mensaje**

Failed to get latest snapshot

- **Causa**

Es posible que la copia Snapshot más reciente no exista porque SnapMirror inicializa el volumen.

- **Acción Correctiva**

Vuelva a intentarlo una vez completada la inicialización.

#### No se pudo cargar la nueva cinta

- **Mensaje**

Failed to load new tape

- **Causa**

Error en unidad de cinta o soporte.

- **Acción Correctiva**

Sustituya la cinta y vuelva a intentar la operación.

#### Error al inicializar la cinta

- **Mensaje**

Failed to initialize tape

- **Causa**

Puede obtener este mensaje de error por uno de los siguientes motivos:

- La imagen de copia de seguridad no es de SMTape.
- El factor de bloqueo de cinta especificado es incorrecto.
- La cinta está dañada o dañada.
- Se ha cargado una cinta incorrecta para la restauración.

- **Acción Correctiva**

- Si la imagen de copia de seguridad no es de SMTape, vuelva a intentar la operación con una cinta que tiene una copia de seguridad de SMTape.
- Si el factor de bloqueo es incorrecto, especifique el factor de bloqueo correcto y vuelva a intentar la operación.
- Si la cinta está dañada, no podrá realizar la operación de restauración.
- Si se carga la cinta incorrecta, vuelva a intentar la operación con la cinta correcta.

## Error al inicializar el flujo de restauración

### • Mensaje

```
Failed to initialize restore stream
```

### • Causa

Puede obtener este mensaje de error por uno de los siguientes motivos:

- La imagen de copia de seguridad no es de SMTape.
- El factor de bloqueo de cinta especificado es incorrecto.
- La cinta está dañada o dañada.
- Se ha cargado una cinta incorrecta para la restauración.

### • Acción Correctiva

- Si la imagen de copia de seguridad no es de SMTape, vuelva a intentar la operación con una cinta que tenga la copia de seguridad de SMTape.
- Si el factor de bloqueo es incorrecto, especifique el factor de bloqueo correcto y vuelva a intentar la operación.
- Si la cinta está dañada, no podrá realizar la operación de restauración.
- Si se carga la cinta incorrecta, vuelva a intentar la operación con la cinta correcta.

## Error al leer la imagen de la copia de seguridad

### • Mensaje

```
Failed to read backup image
```

### • Causa

La cinta está dañada.

### • Acción Correctiva

Si la cinta está dañada, no podrá realizar la operación de restauración.

## Falta el encabezado de la imagen o está dañado

### • Mensaje

```
Image header missing or corrupted
```

### • Causa

La cinta no contiene una copia de seguridad de SMTape válida.

### • Acción Correctiva

Vuelva a intentarlo con una cinta que contenga un backup válido.

#### **Afirmación interna**

- **Mensaje**

Internal assertion

- **Causa**

Hay un error interno de SMTape.

- **Acción Correctiva**

Informe del error y envíe el `etc/log/backup` archivar para soporte técnico.

#### **Número mágico de imagen de copia de seguridad no válido**

- **Mensaje**

Invalid backup image magic number

- **Causa**

La imagen de copia de seguridad no es de SMTape.

- **Acción Correctiva**

Si la imagen de copia de seguridad no es de SMTape, vuelva a intentar la operación con una cinta que tenga la copia de seguridad de SMTape.

#### **Suma de comprobación de imagen de backup no válida**

- **Mensaje**

Invalid backup image checksum

- **Causa**

La cinta está dañada.

- **Acción Correctiva**

Si la cinta está dañada, no podrá realizar la operación de restauración.

#### **Cinta de entrada no válida**

- **Mensaje**

Invalid input tape

- **Causa**

La firma de la imagen de copia de seguridad no es válida en el encabezado de la cinta. La cinta tiene datos dañados o no contiene una imagen de copia de seguridad válida.

- **Acción Correctiva**

Vuelva a intentar el trabajo de restauración con una imagen de backup válida.

#### La ruta de volumen no es válida

- **Mensaje**

```
Invalid volume path
```

- **Causa**

No se encuentra el volumen especificado para la operación de backup o restauración.

- **Acción Correctiva**

Vuelva a intentar el trabajo con una ruta de volumen y un nombre de volumen válidos.

#### El ID del conjunto de copia de seguridad no coincide

- **Mensaje**

```
Mismatch in backup set ID
```

- **Causa**

La cinta cargada durante un cambio de cinta no forma parte del conjunto de copia de seguridad.

- **Acción Correctiva**

Cargue la cinta correcta y vuelva a intentar el trabajo.

#### No coincide con la Marca de tiempo de backup

- **Mensaje**

```
Mismatch in backup time stamp
```

- **Causa**

La cinta cargada durante un cambio de cinta no forma parte del conjunto de copia de seguridad.

- **Acción Correctiva**

Utilice la `smtape restore -h` comando para verificar la información de encabezado de una cinta.

#### Trabajo anulado debido a cierre

- **Mensaje**

```
Job aborted due to shutdown
```

- **Causa**

El sistema de almacenamiento se está reiniciando.

- **Acción Correctiva**

Vuelva a intentar el trabajo después de que se reinicie el sistema de almacenamiento.

#### **Trabajo anulado debido a la eliminación automática de snapshot**

- **Mensaje**

Job aborted due to Snapshot autodelete

- **Causa**

El volumen no tiene suficiente espacio y ha activado la eliminación automática de copias Snapshot.

- **Acción Correctiva**

Libere espacio en el volumen y vuelva a intentar el trabajo.

#### **En la actualidad, la cinta se está utilizando en otras operaciones**

- **Mensaje**

Tape is currently in use by other operations

- **Causa**

La unidad de cinta está en uso por otro trabajo.

- **Acción Correctiva**

Se debe reintentar la copia de seguridad una vez finalizado el trabajo actualmente activo.

#### **Las cintas están fuera de servicio**

- **Mensaje**

Tapes out of order

- **Causa**

La primera cinta de la secuencia de cinta para la operación de restauración no tiene el encabezado de la imagen.

- **Acción Correctiva**

Cargue la cinta con el encabezado de la imagen y vuelva a intentar el trabajo.

#### **Error de transferencia (se canceló debido a una operación de MetroCluster)**

- **Mensaje**

Transfer failed (Aborted due to MetroCluster operation)

- **Causa**

La operación SMTape se cancela debido a una operación de conmutación de sitios o conmutación de estado.

- **Acción Correctiva**

Lleve a cabo la operación SMTape después de que finalice la operación de conmutación o conmutación de regreso.

#### **Error en la transferencia (ARL Initiated abort)**

- **Mensaje**

`Transfer failed (ARL initiated abort)`

- **Causa**

Mientras se está realizando una operación SMTape si se inicia una reubicación de agregado, se cancela la operación SMTape.

- **Acción Correctiva**

Realice la operación SMTape después de que finalice la operación de reubicación de agregados.

#### **Error en la transferencia (interrupción iniciada por el CFO)**

- **Mensaje**

`Transfer failed (CFO initiated abort)`

- **Causa**

La operación SMTape se cancela debido a una operación de recuperación tras fallos (toma de control y retorno al nodo primario) del almacenamiento de un agregado CFO.

- **Acción Correctiva**

Ejecutar la operación de SMTape tras la recuperación tras la recuperación tras fallos del agregado CFO de almacenamiento.

#### **Error en la transferencia (interrupción iniciada por SFO)**

- **Mensaje**

`Transfer failed (SFO initiated abort)`

- **Causa**

La operación SMTape se cancela debido a una operación de conmutación al nodo de respaldo (toma de control y retorno al nodo primario) del almacenamiento.

- **Acción Correctiva**

Realice la operación SMTape después de que termine la operación de recuperación tras fallos (toma de control y devolución) del almacenamiento.

#### Agregado subyacente durante la migración

- **Mensaje**

Underlying aggregate under migration

- **Causa**

Si se inicia una operación SMTape en un agregado que se está realizando la migración (conmutación por error del almacenamiento o reubicación de agregados), la operación SMTape falla.

- **Acción Correctiva**

Realice la operación SMTape una vez finalizada la migración de agregado.

#### El volumen se encuentra actualmente en proceso de migración

- **Mensaje**

Volume is currently under migration

- **Causa**

La migración de volúmenes y el backup de SMTape no se pueden ejecutar simultáneamente.

- **Acción Correctiva**

Vuelva a intentar el trabajo de backup después de completar la migración del volumen.

#### Volumen sin conexión

- **Mensaje**

Volume offline

- **Causa**

El volumen del cual se realiza el backup está sin conexión.

- **Acción Correctiva**

Coloque el volumen en línea y vuelva a intentar el backup.

#### Volumen no restringido

- **Mensaje**

Volume not restricted

- **Causa**

No está restringido el volumen de destino al que se restauran los datos.

- **Acción Correctiva**

Restrinja el volumen y vuelva a intentar la operación de restauración.

## Configuración de NDMP

### Información general de la configuración de NDMP

Puede configurar rápidamente un clúster ONTAP 9 para utilizar el protocolo de gestión de datos de red (NDMP) con el fin de realizar backups de los datos directamente en cinta mediante una aplicación de backup de terceros.

Si la aplicación de backup admite Cluster Aware Backup (CAB), puede configurar NDMP como *SVM-scoped* o *node-scoped*:

- Con el ámbito de SVM en el nivel del clúster (SVM de administrador), puede realizar backup de todos los volúmenes alojados en diferentes nodos del clúster. Siempre que sea posible, se recomienda utilizar NDMP con ámbito SVM.
- NDMP de ámbito de nodo le permite realizar backup de todos los volúmenes alojados en ese nodo.

Si la aplicación de backup no admite CAB, debe utilizar NDMP de ámbito de nodo.

El protocolo NDMP de ámbito SVM y el de ámbito de nodo son mutuamente exclusivos; no se pueden configurar en el mismo clúster.



NDMP de ámbito del nodo está obsoleto en ONTAP 9.

Más información acerca de "[Respaldo para clúster \(CAB\)](#)".

Antes de configurar NDMP, compruebe lo siguiente:

- Tiene una aplicación de copia de seguridad de terceros (también llamada aplicación de administración de datos o DMA).
- Es un administrador de clúster.
- Se instalan dispositivos de cinta y un servidor multimedia opcional.
- Los dispositivos de cinta están conectados al clúster a través de un switch Fibre Channel (FC) y no están conectados directamente.
- Al menos un dispositivo de cinta tiene un número de unidad lógica (LUN) de 0.

### Flujo de trabajo de configuración de NDMP

La configuración del backup en cinta mediante NDMP implica preparar la configuración NDMP, verificar las conexiones del dispositivo de cinta, habilitar las reservas en cinta, configurar NDMP en el nivel de SVM o nodo, habilitar NDMP en el clúster, configurar un usuario de backup, configurar LIF y configurar la aplicación de backup.





## Prepárese para la configuración de NDMP

Antes de configurar el acceso al backup a cinta mediante el protocolo de gestión de datos de red (NDMP), debe comprobar que la configuración planificada es compatible y comprobar que las unidades de cinta aparecen como unidades adecuadas en cada nodo, verificar que todos los nodos tienen LIF de interconexión de clústeres. E identifique si la aplicación de backup es compatible con la extensión Cluster Aware Backup (CAB).

### Pasos

1. Consulte la matriz de compatibilidad del proveedor de aplicaciones de backup para obtener información sobre la compatibilidad con ONTAP (NetApp no reúne los requisitos de aplicaciones de backup de terceros con ONTAP o NDMP).

Debe verificar que los siguientes componentes de NetApp sean compatibles:

- La versión de ONTAP 9 que se ejecuta en el clúster.
- El proveedor de aplicaciones de backup y la versión: Por ejemplo, Veritas NetBackup 8.2 o

CommVault.

- Los detalles de los dispositivos de cinta, como el fabricante, el modelo y la interfaz de las unidades de cinta: Por ejemplo, IBM Ultrium 8 o HPE StoreEver Ultrium 30750 LTO-8.
- Las plataformas de los nodos del clúster: Por ejemplo, FAS8700 o A400.



Puede encontrar matrices de compatibilidad con ONTAP heredadas para aplicaciones de backup en la ["Herramienta de matriz de interoperabilidad de NetApp"](#).

2. Compruebe que las unidades de cinta aparecen como unidades cualificadas en el archivo de configuración de cinta incorporado de cada nodo:

- a. En la interfaz de línea de comandos, consulte el archivo de configuración de cinta incorporado mediante la `storage tape show-supported-status` comando.

```
cluster1::> storage tape show-supported-status

Node: cluster1-1

Tape Drives Is
----- -
Certance Ultrium 2 true Dynamically Qualified
Certance Ultrium 3 true Dynamically Qualified
Digital DLT2000 true Qualified
```

- b. Compare las unidades de cinta con la lista de unidades cualificadas de la salida.



Los nombres de los dispositivos de cinta de la salida pueden variar ligeramente con respecto a los nombres de la etiqueta del dispositivo o de la matriz de interoperabilidad. Por ejemplo, Digital DLT2000 también se conoce como DLT2k. Puede ignorar estas pequeñas diferencias de nomenclatura.

- c. Si un dispositivo no aparece como cualificado en el resultado a pesar de que el dispositivo está cualificado según la matriz de interoperabilidad, descargue e instale un archivo de configuración actualizado para el dispositivo con las instrucciones en el sitio de soporte de NetApp.

["Descargas de NetApp: Archivos de configuración de dispositivo de cinta"](#)

Es posible que un dispositivo cualificado no aparezca en el archivo de configuración de cinta integrado si el dispositivo de cinta fue cualificado después de enviar el nodo.

3. Compruebe que todos los nodos del clúster tienen una LIF de interconexión de clústeres:

- a. Consulte las LIF de interconexión de clústeres de los nodos mediante el `network interface show -role intercluster` comando.

```
cluster1::> network interface show -role intercluster
```

|            | Logical   | Status     | Network       | Current    |
|------------|-----------|------------|---------------|------------|
| Current Is |           |            |               |            |
| Vserver    | Interface | Admin/Oper | Address/Mask  | Node       |
| Port       | Home      |            |               |            |
| -----      | -----     | -----      | -----         | -----      |
| -----      | -----     | -----      | -----         | -----      |
| cluster1   | IC1       | up/up      | 192.0.2.65/24 | cluster1-1 |
| e0a        | true      |            |               |            |

- b. Si no hay ninguna LIF de interconexión de clústeres en ningún nodo, cree una LIF de interconexión de clústeres mediante la `network interface create` comando.

```
cluster1::> network interface create -vserver cluster1 -lif IC2 -role
intercluster
-home-node cluster1-2 -home-port e0b -address 192.0.2.68 -netmask
255.255.255.0
-status-admin up -failover-policy local-only -firewall-policy
intercluster
```

```
cluster1::> network interface show -role intercluster
```

|            | Logical   | Status     | Network       | Current    |
|------------|-----------|------------|---------------|------------|
| Current Is |           |            |               |            |
| Vserver    | Interface | Admin/Oper | Address/Mask  | Node       |
| Port       | Home      |            |               |            |
| -----      | -----     | -----      | -----         | -----      |
| -----      | -----     | -----      | -----         | -----      |
| cluster1   | IC1       | up/up      | 192.0.2.65/24 | cluster1-1 |
| e0a        | true      |            |               |            |
| cluster1   | IC2       | up/up      | 192.0.2.68/24 | cluster1-2 |
| e0b        | true      |            |               |            |

### "Gestión de redes"

4. Identifique si la aplicación de backup es compatible con Cluster Aware Backup (CAB) mediante la documentación proporcionada con la aplicación de backup.

El soporte CAB es un factor clave a la hora de determinar el tipo de backup que se puede realizar.

## Compruebe las conexiones del dispositivo de cinta

Debe asegurarse de que todas las unidades e intercambiadores de medios sean visibles en ONTAP como dispositivos.

**Pasos**

- 1. Ver información acerca de todas las unidades e intercambiadores de medios utilizando `storage tape show` comando.

```
cluster1::> storage tape show

Node: cluster1-01
Device ID Device Type Description
Status

sw4:10.11 tape drive HP LTO-3
normal
0b.125L1 media changer HP MSL G3 Series
normal
0d.4 tape drive IBM LTO 5 ULT3580
normal
0d.4L1 media changer IBM 3573-TL
normal
...
```

- 2. Si no se muestra una unidad de cinta, solucione el problema.
- 3. Si no se muestra un cambiador de materiales, consulte la información sobre los intercambiadores de material utilizando `storage tape show-media-changer` y, a continuación, solucione el problema.

```
cluster1::> storage tape show-media-changer

Media Changer: sw4:10.11L1
Description: PX70-TL
 WWNN: 2:00a:000e11:10b919
 WWPN: 2:00b:000e11:10b919
Serial Number: 00FRU7800000_LL1

Errors: -

Paths:
Node Initiator Alias Device State
Status

cluster1-01 2b mc0 in-use
normal
...
```

## Activar reservas de cinta

Debe asegurarse de que las unidades de cinta estén reservadas para que las aplicaciones de backup las operaciones de backup de NDMP.

### Acerca de esta tarea

La configuración de las reservas varía en diferentes aplicaciones de backup, y esta configuración debe coincidir con la aplicación de backup y los nodos o servidores que utilizan las mismas unidades. Consulte la documentación del proveedor de la aplicación de backup para obtener los ajustes de reserva correctos.

### Pasos

1. Habilite las reservas mediante el `options -option-name tape.reservations -option-value persistent` comando.

El siguiente comando habilita las reservas con `persistent` valor:

```
cluster1::> options -option-name tape.reservations -option-value
persistent
2 entries were modified.
```

2. Compruebe que las reservas estén habilitadas en todos los nodos mediante el `options tape.reservations` y, a continuación, revise el resultado.

```
cluster1::> options tape.reservations

cluster1-1
 tape.reservations persistent

cluster1-2
 tape.reservations persistent
2 entries were displayed.
```

## Configure NDMP con ámbito SVM

### Habilite NDMP con ámbito de SVM en el clúster

Si el DMA admite la extensión Cluster Aware Backup (CAB), puede realizar un backup de todos los volúmenes alojados en diferentes nodos de un clúster mediante la habilitación de NDMP de ámbito SVM, la habilitación del servicio NDMP en el clúster (SVM de administrador) y la configuración de LIF para la conexión de datos y control.

### Lo que necesitará

La extensión DE LA CABINA debe ser compatible con el DMA.

### Acerca de esta tarea

Al desactivar el modo de NDMP con ámbito del nodo, es posible habilitar el modo NDMP con ámbito SVM en

el clúster.

## Pasos

1. Habilitar modo NDMP en ámbito de SVM:

```
cluster1::> system services ndmp node-scope-mode off
```

El modo NDMP en el ámbito de SVM está habilitado.

2. Habilite el servicio NDMP en la SVM de administrador:

```
cluster1::> vserver services ndmp on -vserver cluster1
```

El tipo de autenticación se establece en `challenge` de forma predeterminada, la autenticación de texto sin formato está deshabilitada.



Para una comunicación segura, debe mantener la autenticación de texto sin formato deshabilitada.

3. Compruebe que el servicio NDMP está activado:

```
cluster1::> vserver services ndmp show
```

| Vserver  | Enabled | Authentication type |
|----------|---------|---------------------|
| -----    | -----   | -----               |
| cluster1 | true    | challenge           |
| vs1      | false   | challenge           |

## Habilitar un usuario de backup para la autenticación NDMP

Para autenticar NDMP de ámbito SVM desde la aplicación de backup, debe haber un usuario administrativo con suficientes privilegios y una contraseña NDMP.

### Acerca de esta tarea

Debe generar una contraseña de NDMP para los usuarios administradores de backup. Puede habilitar los usuarios administradores de backup en el nivel del clúster o la SVM; si fuera necesario, puede crear un usuario nuevo. De forma predeterminada, los usuarios con los siguientes roles pueden autenticar para el backup NDMP:

- En todo el clúster: `admin` o `backup`
- SVM individuales: `vsadmin` o `vsadmin-backup`

Si utiliza un usuario NIS o LDAP, el usuario debe existir en el servidor correspondiente. No puede utilizar un usuario de Active Directory.

## Pasos

1. Mostrar los usuarios y permisos de administrador actuales:

```
security login show
```

2. Si es necesario, cree un nuevo usuario de backup NDMP con el `security login create` Y el rol apropiado para privilegios de SVM individuales o en todo el clúster.

Puede especificar un nombre de usuario de backup local o un nombre de usuario NIS o LDAP para el `-user-or-group-name` parámetro.

El siguiente comando crea el usuario de backup `backup_admin1` con la `backup` rol para todo el clúster:

```
cluster1::> security login create -user-or-group-name backup_admin1
-application ssh -authmethod password -role backup
```

El siguiente comando crea el usuario de backup `vsbackup_admin1` con la `vsadmin-backup` Rol para una SVM individual:

```
cluster1::> security login create -user-or-group-name vsbackup_admin1
-application ssh -authmethod password -role vsadmin-backup
```

Introduzca una contraseña para el nuevo usuario y confirme.

3. Genere una contraseña para la SVM de administrador con el `vserver services ndmp generate password` comando.

La contraseña generada debe utilizarse para autenticar la conexión NDMP por parte de la aplicación de copia de seguridad.

```
cluster1::> vserver services ndmp generate-password -vserver cluster1
-user backup_admin1

Vserver: cluster1
User: backup_admin1
Password: qG5CqQHYxw7tE57g
```

## Configure las LIF

Debe identificar las LIF que se usarán para establecer una conexión de datos entre los recursos de cinta y los de datos, y para controlar la conexión entre la SVM de administrador y la aplicación de backup. Tras identificar las LIF, debe verificar que las políticas de conmutación por error y firewall están establecidas para las LIF y especificar el rol de interfaz preferido.

A partir de ONTAP 9.10.1, las políticas de firewall están obsoletas y sustituidas por completo por políticas de servicios LIF. Para obtener más información, consulte ["LIF y políticas de servicio en ONTAP 9.6 y posteriores"](#).

## Pasos

1. Identifique los LIF de interconexión de clústeres, gestión de clústeres y gestión de nodos mediante el `network interface show` con el `-role` parámetro.

El siguiente comando muestra las LIF de interconexión de clústeres:

```
cluster1::> network interface show -role intercluster
```

|            | Logical   | Status     | Network       | Current    |
|------------|-----------|------------|---------------|------------|
| Current Is |           |            |               |            |
| Vserver    | Interface | Admin/Oper | Address/Mask  | Node       |
| Port       | Home      |            |               |            |
| -----      | -----     | -----      | -----         |            |
| -----      | -----     |            |               |            |
| cluster1   | IC1       | up/up      | 192.0.2.65/24 | cluster1-1 |
| e0a        | true      |            |               |            |
| cluster1   | IC2       | up/up      | 192.0.2.68/24 | cluster1-2 |
| e0b        | true      |            |               |            |

El siguiente comando muestra la LIF de gestión del clúster:

```
cluster1::> network interface show -role cluster-mgmt
```

|            | Logical      | Status     | Network       | Current    |
|------------|--------------|------------|---------------|------------|
| Current Is |              |            |               |            |
| Vserver    | Interface    | Admin/Oper | Address/Mask  | Node       |
| Port       | Home         |            |               |            |
| -----      | -----        | -----      | -----         |            |
| -----      | -----        |            |               |            |
| cluster1   | cluster_mgmt | up/up      | 192.0.2.60/24 | cluster1-2 |
| e0M        | true         |            |               |            |

El siguiente comando muestra las LIF de gestión de nodos:



```
cluster1::> network interface show -role node-mgmt
```

|            |      | Logical          | Status     | Network       | Current    |
|------------|------|------------------|------------|---------------|------------|
| Current Is |      |                  |            |               |            |
| Vserver    |      | Interface        | Admin/Oper | Address/Mask  | Node       |
| Port       | Home |                  |            |               |            |
| -----      |      |                  |            |               |            |
| -----      |      |                  |            |               |            |
| cluster1   |      | cluster1-1_mgmt1 | up/up      | 192.0.2.69/24 | cluster1-1 |
| e0M        | true |                  |            |               |            |
|            |      | cluster1-2_mgmt1 | up/up      | 192.0.2.70/24 | cluster1-2 |
| e0M        | true |                  |            |               |            |

2. Compruebe que la política de firewall está habilitada para NDMP en las LIF de interconexión de clústeres, gestión de clústeres (gestión de clústeres) y gestión de nodos (gestión de nodos):

- Compruebe que la directiva de firewall está activada para NDMP mediante el `system services firewall policy show` comando.

El siguiente comando muestra la política de firewall para la LIF de administración de clústeres:

```
cluster1::> system services firewall policy show -policy cluster
```

| Vserver | Policy  | Service | Allowed     |
|---------|---------|---------|-------------|
| -----   |         |         |             |
| cluster | cluster | dns     | 0.0.0.0/0   |
|         |         | http    | 0.0.0.0/0   |
|         |         | https   | 0.0.0.0/0   |
|         |         | ** ndmp | 0.0.0.0/0** |
|         |         | ndmps   | 0.0.0.0/0   |
|         |         | ntp     | 0.0.0.0/0   |
|         |         | rsh     | 0.0.0.0/0   |
|         |         | snmp    | 0.0.0.0/0   |
|         |         | ssh     | 0.0.0.0/0   |
|         |         | telnet  | 0.0.0.0/0   |

10 entries were displayed.

El siguiente comando muestra la política de firewall para la LIF de interconexión de clústeres:

```
cluster1::> system services firewall policy show -policy intercluster
```

| Vserver  | Policy       | Service | Allowed           |
|----------|--------------|---------|-------------------|
| cluster1 | intercluster | dns     | -                 |
|          |              | http    | -                 |
|          |              | https   | -                 |
|          |              | **ndmp  | 0.0.0.0/0, ::/0** |
|          |              | ndmps   | -                 |
|          |              | ntp     | -                 |
|          |              | rsh     | -                 |
|          |              | ssh     | -                 |
|          |              | telnet  | -                 |

9 entries were displayed.

El siguiente comando muestra la política de firewall de la LIF de gestión de nodos:

```
cluster1::> system services firewall policy show -policy mgmt
```

| Vserver    | Policy | Service | Allowed           |
|------------|--------|---------|-------------------|
| cluster1-1 | mgmt   | dns     | 0.0.0.0/0, ::/0   |
|            |        | http    | 0.0.0.0/0, ::/0   |
|            |        | https   | 0.0.0.0/0, ::/0   |
|            |        | **ndmp  | 0.0.0.0/0, ::/0** |
|            |        | ndmps   | 0.0.0.0/0, ::/0   |
|            |        | ntp     | 0.0.0.0/0, ::/0   |
|            |        | rsh     | -                 |
|            |        | snmp    | 0.0.0.0/0, ::/0   |
|            |        | ssh     | 0.0.0.0/0, ::/0   |
|            |        | telnet  | -                 |

10 entries were displayed.

- b. Si la directiva de firewall no está activada, active la directiva de firewall mediante el `system services firewall policy modify` con el `-service` parámetro.

El siguiente comando habilita la política de firewall para la LIF de interconexión de clústeres:

```
cluster1::> system services firewall policy modify -vserver cluster1
-policy intercluster -service ndmp 0.0.0.0/0
```

3. Asegurarse de que la política de conmutación por error esté establecida de forma adecuada para todos los LIF:

- a. Compruebe que la política de conmutación por error para la LIF de administración del clúster está establecida en `broadcast-domain-wide`Y` la directiva para las LIF de interconexión de clústeres y de gestión de nodos se establece en ``local-only` mediante el uso de `network interface show -failover` comando.

El siguiente comando muestra la política de conmutación por error para las LIF de gestión de clústeres, interconexión de clústeres y nodos:

```
cluster1::> network interface show -failover
```

| Failover Vserver Group     | Logical Interface | Home Node:Port | Failover Policy       |
|----------------------------|-------------------|----------------|-----------------------|
| cluster cluster            | cluster1_clus1    | cluster1-1:e0a | local-only            |
| Failover Targets:<br>..... |                   |                |                       |
| **cluster1 Default**       | cluster_mgmt      | cluster1-1:e0m | broadcast-domain-wide |
| Failover Targets:<br>..... |                   |                |                       |
| Default**                  | **IC1             | cluster1-1:e0a | local-only            |
| Failover Targets:<br>..... |                   |                |                       |
| Default**                  | **IC2             | cluster1-1:e0b | local-only            |
| Failover Targets:<br>..... |                   |                |                       |
| **cluster1-1 Default**     | cluster1-1_mgmt1  | cluster1-1:e0m | local-only            |
| Failover Targets:<br>..... |                   |                |                       |
| **cluster1-2 Default**     | cluster1-2_mgmt1  | cluster1-2:e0m | local-only            |
| Failover Targets:<br>..... |                   |                |                       |

- a. Si las políticas de conmutación por error no están definidas de forma adecuada, modifique la política de conmutación por error mediante el `network interface modify` con el `-failover-policy` parámetro.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

4. Especifique las LIF necesarias para la conexión de datos mediante el `vserver services ndmp modify` con el `preferred-interface-role` parámetro.

```
cluster1::> vserver services ndmp modify -vserver cluster1 -preferred
-interface-role intercluster,cluster-mgmt,node-mgmt
```

5. Compruebe que el rol de interfaz preferida esté establecido para el clúster mediante el `vserver services ndmp show` comando.

```
cluster1::> vserver services ndmp show -vserver cluster1

Vserver: cluster1
NDMP Version: 4
.....
.....
Preferred Interface Role: intercluster, cluster-mgmt, node-
mgmt
```

## Configure el NDMP de ámbito del nodo

### Habilite NDMP de ámbito del nodo en el clúster

Puede realizar backups de volúmenes alojados en un único nodo. Para ello, active el NDMP de ámbito del nodo, lo que habilita el servicio NDMP y configura una LIF para la conexión de datos y control. Esto puede hacerse para todos los nodos del clúster.



NDMP de ámbito del nodo está obsoleto en ONTAP 9.

### Acerca de esta tarea

Cuando se utiliza NDMP en el modo de alcance del nodo, la autenticación debe configurarse por nodo. Para obtener más información, consulte ["El artículo de la base de conocimientos "Cómo configurar la autenticación NDMP en el modo de alcance de nodo"](#).

### Pasos

1. Habilitar modo NDMP de ámbito de nodo:

```
cluster1::> system services ndmp node-scope-mode on
```

NDMP node-scope-mode está activado.

## 2. Habilite el servicio NDMP en todos los nodos del clúster:

Si utiliza el comodín "\*", se habilita el servicio NDMP en todos los nodos al mismo tiempo.

Debe especificar una contraseña para la autenticación de la conexión NDMP mediante la aplicación de backup.

```
cluster1::> system services ndmp on -node *
```

```
Please enter password:
Confirm password:
2 entries were modified.
```

## 3. Deshabilite el -clear-text Opción de comunicación segura de la contraseña NDMP:

Usando el comodín "\*" disables the -clear-text opción en todos los nodos al mismo tiempo.

```
cluster1::> system services ndmp modify -node * -clear-text false
```

## 4. Compruebe que el servicio NDMP esté habilitado y el -clear-text la opción está desactivada:

```
cluster1::> system services ndmp show
```

| Node       | Enabled | Clear text | User Id |
|------------|---------|------------|---------|
| cluster1-1 | true    | false      | root    |
| cluster1-2 | true    | false      | root    |

2 entries were displayed.

## Configure una LIF

Debe identificar una LIF que se utilizará para establecer una conexión de datos y controlar la conexión entre el nodo y la aplicación de backup. Tras identificar la LIF, debe verificar que las políticas de firewall y recuperación tras fallos están establecidas para la LIF.



A partir de ONTAP 9.10.1, las políticas de firewall están obsoletas y sustituidas por completo por políticas de servicios LIF. Para obtener más información, consulte ["Configurar políticas de firewall para LIF"](#).

## Pasos

1. Identifique la LIF de interconexión de clústeres alojada en los nodos mediante el `network interface`

show con el `-role` parámetro.

```
cluster1::> network interface show -role intercluster
```

| Current Is | Logical   | Status     | Network       | Current    |      |
|------------|-----------|------------|---------------|------------|------|
| Vserver    | Interface | Admin/Oper | Address/Mask  | Node       | Port |
| Home       |           |            |               |            |      |
| -----      | -----     | -----      | -----         | -----      |      |
| -----      | -----     |            |               |            |      |
| cluster1   | IC1       | up/up      | 192.0.2.65/24 | cluster1-1 | e0a  |
| true       |           |            |               |            |      |
| cluster1   | IC2       | up/up      | 192.0.2.68/24 | cluster1-2 | e0b  |
| true       |           |            |               |            |      |

2. Compruebe que la política de firewall está activada para NDMP en las LIF de interconexión de clústeres:

- Compruebe que la directiva de firewall está activada para NDMP mediante el `system services firewall policy show` comando.

El siguiente comando muestra la política de firewall para la LIF de interconexión de clústeres:

```
cluster1::> system services firewall policy show -policy intercluster
```

| Vserver  | Policy       | Service | Allowed           |
|----------|--------------|---------|-------------------|
| -----    | -----        | -----   | -----             |
| cluster1 | intercluster | dns     | -                 |
|          |              | http    | -                 |
|          |              | https   | -                 |
|          |              | **ndmp  | 0.0.0.0/0, ::/0** |
|          |              | ndmps   | -                 |
|          |              | ntp     | -                 |
|          |              | rsh     | -                 |
|          |              | ssh     | -                 |
|          |              | telnet  | -                 |

9 entries were displayed.

- Si la directiva de firewall no está activada, active la directiva de firewall mediante el `system services firewall policy modify` con el `-service` parámetro.

El siguiente comando habilita la política de firewall para la LIF de interconexión de clústeres:

```
cluster1::> system services firewall policy modify -vserver cluster1
-policy intercluster -service ndmp 0.0.0.0/0
```

3. Asegúrese de que la normativa de recuperación tras fallos esté establecida de forma adecuada para las LIF de interconexión de clústeres:
  - a. Compruebe que la política de recuperación tras fallos de las LIF de interconexión de clústeres está establecida en local-only mediante el uso de network interface show -failover comando.

```
cluster1::> network interface show -failover
```

| Vserver    | Logical Interface | Home Node:Port | Failover Policy | Failover Group    |
|------------|-------------------|----------------|-----------------|-------------------|
| cluster1   | **IC1             | cluster1-1:e0a | local-only      |                   |
| Default**  |                   |                |                 |                   |
|            |                   |                |                 | Failover Targets: |
|            |                   |                |                 | .....             |
|            | **IC2             | cluster1-2:e0b | local-only      |                   |
| Default**  |                   |                |                 |                   |
|            |                   |                |                 | Failover Targets: |
|            |                   |                |                 | .....             |
| cluster1-1 | cluster1-1_mgmt1  | cluster1-1:e0m | local-only      | Default           |
|            |                   |                |                 | Failover Targets: |
|            |                   |                |                 | .....             |

- b. Si la política de conmutación por error no está definida de forma adecuada, modifique la política de conmutación por error mediante el network interface modify con el -failover-policy parámetro.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

### Configure la aplicación de backup

Una vez que se configura el clúster para el acceso NDMP, debe recopilar información de la configuración del clúster y, a continuación, configurar el resto del proceso de backup en la aplicación de backup.

#### Pasos

1. Recopile la siguiente información configurada anteriormente en ONTAP:
  - El nombre de usuario y la contraseña que la aplicación de backup necesita para crear la conexión NDMP
  - Las direcciones IP de las LIF de interconexión de clústeres que necesita la aplicación de backup para conectarse al clúster
2. En ONTAP, muestre los alias que ONTAP asignó a cada dispositivo utilizando storage tape alias show comando.

Los alias suelen ser útiles para configurar la aplicación de copia de seguridad.

```
cluster1::> storage tape show -alias
```

```
Device ID: 2a.0
Device Type: tape drive
Description: Hewlett-Packard LTO-5
```

| Node               | Alias | Mapping        |
|--------------------|-------|----------------|
| -----              | ----- | -----          |
| stsw-3220-4a-4b-02 | st2   | SN[HU19497WVR] |
| ...                |       |                |

3. En la aplicación de copia de seguridad, configure el resto del proceso de copia de seguridad utilizando la documentación de la aplicación de copia de seguridad.

### Después de terminar

Si se produce un evento de movilidad de datos, como un movimiento de volúmenes o una migración LIF, debe estar preparado para reiniciar todas las operaciones de backup interrumpidas.

## Replicación entre software de NetApp Element y ONTAP

### Replicación entre software de NetApp Element y información general de ONTAP

Puede garantizar la continuidad empresarial en un sistema Element mediante SnapMirror para replicar copias de Snapshot de un volumen de Element en un destino de ONTAP. En caso de desastre en el sitio de Element, podrá seguir prestando servicio a los clientes desde el sistema ONTAP y, a continuación, reactivar el sistema Element cuando el servicio se restaure.

A partir de ONTAP 9.4, puede replicar copias Snapshot de una LUN creada en un nodo ONTAP de nuevo en un sistema Element. Puede haber creado una LUN durante una interrupción del servicio en el sitio de Element, o bien podría utilizar una LUN para migrar datos desde ONTAP al software Element.

Debe trabajar con Element en el backup de ONTAP si se aplica lo siguiente:

- Quiere utilizar las prácticas recomendadas, no explorar todas las opciones disponibles.
- Desea usar la interfaz de línea de comandos (CLI) de ONTAP, no System Manager ni una herramienta de secuencias de comandos automatizada.
- Usted utiliza iSCSI para servir datos a los clientes.

Si se necesita información conceptual o de configuración adicional, consulte la siguiente documentación:

- Configuración de Element

["Documentación sobre el software NetApp Element"](#)

- Conceptos y configuración de SnapMirror

["Información general sobre la protección de datos"](#)



## Acerca de la replicación entre Element y ONTAP

A partir de ONTAP 9.3, se puede usar SnapMirror para replicar copias de Snapshot de un volumen de Element en un destino de ONTAP. En caso de desastre en el sitio de Element, puede seguir prestando servicio a los clientes desde el sistema ONTAP y, a continuación, reactivar el volumen de origen de Element cuando el servicio se restaure.

A partir de ONTAP 9.4, puede replicar copias Snapshot de una LUN creada en un nodo ONTAP de nuevo en un sistema Element. Puede haber creado una LUN durante una interrupción del servicio en el sitio de Element, o bien podría utilizar una LUN para migrar datos desde ONTAP al software Element.

### Los tipos de relaciones de protección de datos

SnapMirror ofrece dos tipos de relación de protección de datos. Para cada tipo, SnapMirror crea una copia Snapshot del volumen de origen de Element antes de inicializar o actualizar la relación:

- En una relación de protección de datos *recuperación ante desastres (DR)*, el volumen de destino solo contiene la copia Snapshot creada por SnapMirror, desde la cual puede continuar sirviendo datos en el caso de una catástrofe en el sitio principal.
- En una relación de protección de datos *de retención a largo plazo*, el volumen de destino contiene copias Snapshot puntuales creadas por el software Element, así como la copia de Snapshot creada por SnapMirror. Podría querer conservar copias Snapshot mensuales creadas en un plazo de 20 años, por ejemplo.

### Políticas predeterminadas

La primera vez que se invoca SnapMirror, se realiza una transferencia *baseline* del volumen de origen al volumen de destino. La *política de SnapMirror* define el contenido de la línea de base y cualquier actualización.

Se puede usar una política predeterminada o personalizada al crear una relación de protección de datos. El *policy type* determina qué copias Snapshot se incluirán y cuántas copias se retendrán.

La siguiente tabla muestra las directivas predeterminadas. Utilice la `MirrorLatest` Política para crear una relación de recuperación ante desastres tradicional. Utilice la `MirrorAndVault` o `Unified7year` Política para crear una relación de replicación unificada, en la que la recuperación ante desastres y la retención a largo plazo se configuran en el mismo volumen de destino.

| Política            | Tipo de directiva | Comportamiento de actualización                                                                                                                                                                                          |
|---------------------|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MirrorÚltimas       | reflejo asíncrono | Transfiere la copia snapshot creada por SnapMirror.                                                                                                                                                                      |
| Reflejo de AndVault | mirror-vault      | Transferir la copia snapshot creada por SnapMirror y cualquier otra copia snapshot menos reciente realizada desde la última actualización, siempre y cuando tengan etiquetas de SnapMirror «día» o «semanal».            |
| Unified7 año        | mirror-vault      | Transferir la copia snapshot creada por SnapMirror y cualquier otra copia snapshot menos reciente realizada desde la última actualización, siempre y cuando tengan etiquetas de SnapMirror «día», «semanal» o «mensual». |



Para obtener información de referencia completa sobre las políticas de SnapMirror, incluidas las directrices sobre qué política usar, consulte ["Protección de datos"](#).

### Etiquetas de SnapMirror

Todas las normas que tengan el tipo de política «espejo» deben tener una regla que especifique las copias snapshot que desea replicar. La regla «diaria», por ejemplo, indica que solo deben replicarse las copias Snapshot asignadas a la etiqueta «diaria» de SnapMirror. La etiqueta de SnapMirror se asigna al configurar copias de Snapshot de Element.

### Replicación desde un clúster de origen de Element a un clúster de destino de ONTAP

SnapMirror se puede usar para replicar copias de Snapshot de un volumen de Element en un sistema de destino de ONTAP. En caso de desastre en el sitio de Element, puede seguir prestando servicio a los clientes desde el sistema ONTAP y, a continuación, reactivar el volumen de origen de Element cuando el servicio se restaure.

Un volumen de Element es aproximadamente equivalente a una LUN de ONTAP. SnapMirror crea un LUN con el nombre del volumen de Element cuando se inicializa una relación de protección de datos entre el software Element y ONTAP. SnapMirror replica datos a una LUN existente si la LUN cumple con los requisitos para la replicación de Element en ONTAP.

Las reglas de replicación son las siguientes:

- Un volumen de ONTAP puede contener datos solo de un volumen de Element.
- No es posible replicar datos desde un volumen de ONTAP en varios volúmenes de Element.

### Replicación desde un clúster de origen de ONTAP a un clúster de destino de Element

A partir de ONTAP 9.4, puede replicar copias Snapshot de una LUN creada en un sistema ONTAP de vuelta a un volumen de Element:

- Si ya existe una relación de SnapMirror entre un origen de elemento y un destino de ONTAP, una LUN creada mientras ofrece datos desde el destino se replica automáticamente cuando el origen se vuelve a activar.
- De lo contrario, debe crear e inicializar una relación de SnapMirror entre el clúster de origen de ONTAP y el clúster de destino de Element.

Las reglas de replicación son las siguientes:

- La relación de replicación debe tener una política de tipo «"duplicación asíncrona"».

No se admiten las políticas de tipo «espejo».

- Solo se admiten LUN iSCSI.
- No es posible replicar más de un LUN desde un volumen de ONTAP a un volumen de Element.
- No es posible replicar un LUN desde un volumen de ONTAP a varios volúmenes de Element.

### Requisitos previos

Debe haber completado las siguientes tareas antes de configurar una relación de protección de datos entre Element y ONTAP:

- El clúster de Element debe ejecutar la versión 10.1 o posterior del software NetApp Element.
- El clúster de ONTAP debe ejecutar ONTAP 9.3 o una versión posterior.
- Debe haber obtenido la licencia de SnapMirror en el clúster de ONTAP.
- Debe haber configurado volúmenes en los clústeres de Element y ONTAP que sean lo suficientemente grandes como para manejar las transferencias de datos anticipadas.
- Si utiliza el tipo de política «mirror-vault», debe haber configurado una etiqueta de SnapMirror para que se repliquen las copias Snapshot de Element.



Es posible realizar esta tarea únicamente en la interfaz de usuario web del software Element. Para obtener más información, consulte "[Documentación sobre el software NetApp Element](#)"

- Debe haberse asegurado de que el puerto 5010 está disponible.
- Si prevé que podría necesitar mover un volumen de destino, debe asegurarse de que existe una conectividad de malla completa entre el origen y el destino. Cada nodo del clúster de origen de Element debe poder comunicarse con cada nodo del clúster de destino de ONTAP.

#### Detalles de soporte

En la siguiente tabla se muestran detalles de compatibilidad de elemento en un backup de ONTAP.

| Recurso o característica | Detalles de soporte                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SnapMirror               | <ul style="list-style-type: none"> <li>• No se admite la función SnapMirror restore.</li> <li>• La <code>MirrorAllSnapshots</code> y <code>XDPDefault</code> no se admiten políticas.</li> <li>• No se admite el tipo de política «'vault'».</li> <li>• No se admite la regla definida por el sistema <code>"all_source_snapshots"</code>.</li> <li>• El tipo de política «mirror-vault» solo se admite para la replicación del software Element a ONTAP. Utilice «duplicación asíncrona» para la replicación de ONTAP al software Element.</li> <li>• La <code>-schedule</code> y <code>-prefix</code> opciones para <code>snapmirror policy add-rule</code> no son compatibles.</li> <li>• La <code>-preserve</code> y <code>-quick-resync</code> opciones para <code>snapmirror resync</code> no son compatibles.</li> <li>• No se mantiene la eficiencia del almacenamiento.</li> <li>• No se admiten las puestas en marcha de protección de datos en cascada ni en distribución ramificada.</li> </ul> |
| ONTAP                    | <ul style="list-style-type: none"> <li>• ONTAP Select es compatible a partir de ONTAP 9.4 y Element 10.3.</li> <li>• Cloud Volumes ONTAP es compatible a partir de ONTAP 9.5 y Element 11.0.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

|              |                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Elemento     | <ul style="list-style-type: none"> <li>• El límite de tamaño del volumen es de 8 TIB.</li> <li>• El tamaño de bloque del volumen debe ser 512 bytes. No se admite un tamaño de bloque de 4 KB.</li> <li>• El tamaño del volumen debe ser múltiplo de 1 MIB.</li> <li>• Los atributos del volumen no se conservan.</li> <li>• El número máximo de copias de Snapshot que se deben replicar es 30.</li> </ul> |
| Red          | <ul style="list-style-type: none"> <li>• Se permite una sola conexión TCP por transferencia.</li> <li>• El nodo de Element se debe especificar como dirección IP. No se admite la búsqueda de nombre de host DNS.</li> <li>• No se admiten los espacios IP.</li> </ul>                                                                                                                                      |
| SnapLock     | No se admiten los volúmenes de SnapLock.                                                                                                                                                                                                                                                                                                                                                                    |
| FlexGroup    | No se admiten los volúmenes de FlexGroup.                                                                                                                                                                                                                                                                                                                                                                   |
| DR DE SVM    | No se admiten los volúmenes de ONTAP en una configuración de recuperación ante desastres de SVM.                                                                                                                                                                                                                                                                                                            |
| MetroCluster | No se admiten los volúmenes de ONTAP en una configuración de MetroCluster.                                                                                                                                                                                                                                                                                                                                  |

## Flujo de trabajo de replicación entre Element y ONTAP

Si va a replicar datos de Element en ONTAP o de ONTAP a Element, debe configurar una programación de trabajo, especificar una política y crear e inicializar la relación. Puede usar una directiva predeterminada o personalizada.

En el flujo de trabajo se supone que ha completado las tareas de requisitos previos que se enumeran en [Requisitos previos](#). Para obtener información de referencia completa sobre las políticas de SnapMirror, incluidas las directrices sobre qué política usar, consulte ["Protección de datos"](#).



## Habilite SnapMirror en el software Element

### Habilite SnapMirror en el clúster de Element

Es necesario habilitar SnapMirror en el clúster de Element para poder crear una relación

de replicación. Es posible realizar esta tarea únicamente en la interfaz de usuario web del software Element.

#### Antes de empezar

- El clúster de Element debe ejecutar la versión 10.1 o posterior del software NetApp Element.
- Solo se puede habilitar SnapMirror en clústeres de Element que se usan con los volúmenes de ONTAP de NetApp.

#### Acerca de esta tarea

El sistema Element viene con SnapMirror deshabilitado de forma predeterminada. SnapMirror no se habilita automáticamente como parte de una nueva instalación o actualización.



Una vez que está habilitada, SnapMirror no se puede deshabilitar. Solo puede deshabilitar la función SnapMirror y restaurar la configuración predeterminada si devuelve el clúster a la imagen de fábrica.

#### Pasos

1. Haga clic en **Clusters > Configuración**.
2. Busque la configuración específica del clúster para SnapMirror.
3. Haga clic en **Activar SnapMirror**.

#### Habilite SnapMirror en el volumen de origen de Element

Es necesario habilitar SnapMirror en el volumen de origen de Element para poder crear una relación de replicación. Es posible realizar esta tarea únicamente en la interfaz de usuario web del software Element.


#### Antes de empezar

- Debe haber habilitado SnapMirror en el clúster de Element.
- El tamaño de bloque del volumen debe ser 512 bytes.
- El volumen no debe participar en la replicación remota de Element.
- El tipo de acceso al volumen no debe ser «'destino de replicación'».

#### Acerca de esta tarea

En el siguiente procedimiento se asume que el volumen ya existe. SnapMirror también es posible habilitar cuando se crea o se clona un volumen.

#### Pasos

1. Seleccione **Gestión > volúmenes**.
2. Seleccione la  botón para el volumen.
3. En el menú desplegable, seleccione **Editar**.
4. En el cuadro de diálogo **Editar volumen**, seleccione **Activar SnapMirror**.
5. Seleccione **Guardar cambios**.

#### Cree un extremo de SnapMirror

Debe crear un extremo de SnapMirror para poder crear una relación de replicación. Es

posible realizar esta tarea únicamente en la interfaz de usuario web del software Element.

### Antes de empezar

Debe haber habilitado SnapMirror en el clúster de Element.

### Pasos

1. Haga clic en **Protección de datos > terminales de SnapMirror**.
2. Haga clic en **Crear extremo**.
3. En el cuadro de diálogo **Crear un nuevo extremo**, introduzca la dirección IP de administración del clúster ONTAP.
4. Introduzca el ID de usuario y la contraseña del administrador del clúster de ONTAP.
5. Haga clic en **Crear extremo**.

## Configurar una relación de replicación

### Cree una programación de trabajo de replicación

Si va a replicar datos de Element en ONTAP o de ONTAP a Element, debe configurar una programación de trabajo, especificar una política y crear e inicializar la relación. Puede usar una directiva predeterminada o personalizada.

Puede utilizar el `job schedule cron create` comando para crear una programación de trabajo de replicación. La programación de tareas determina el momento en que SnapMirror actualiza automáticamente la relación de protección de datos a la que se asigna la programación.

### Acerca de esta tarea

Debe asignar una programación de tareas cuando crea una relación de protección de datos. Si no asigna una programación de trabajo, debe actualizar la relación manualmente.

### Paso

1. Crear un programa de trabajo:

```
job schedule cron create -name job_name -month month -dayofweek day_of_week
-day day_of_month -hour hour -minute minute
```

Para `-month`, `-dayofweek`, y `-hour`, puede especificar `all` para ejecutar el trabajo cada mes, día de la semana y hora, respectivamente.

A partir de ONTAP 9.10.1, puede incluir Vserver para su programación de trabajo:

```
job schedule cron create -name job_name -vserver Vserver_name -month month
-dayofweek day_of_week -day day_of_month -hour hour -minute minute
```

En el ejemplo siguiente se crea una programación de trabajo denominada `my_weekly`. Es decir, los sábados a las 3:00 horas:

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

## Personalizar una política de replicación

### Cree una política de replicación personalizada

Puede usar una directiva predeterminada o personalizada al crear una relación de replicación. Para una política de replicación unificada personalizada, debe definir una o más *rules* que determinen las copias snapshot que se transfieren durante la inicialización y actualización.

Puede crear una directiva de replicación personalizada si la directiva predeterminada para una relación no es adecuada. Puede que desee comprimir datos en una transferencia de red, por ejemplo, o modificar el número de intentos que realiza SnapMirror para transferir copias Snapshot.

### Acerca de esta tarea

El *policy type* de la directiva de replicación determina el tipo de relación que admite. En la siguiente tabla se muestran los tipos de directivas disponibles.

| Tipo de política  | Tipo de relación                          |
|-------------------|-------------------------------------------|
| reflejo asíncrono | Recuperación ante desastres de SnapMirror |
| mirror-vault      | Replicación unificada                     |

### Paso

1. Cree una política de replicación personalizada:

```
snapmirror policy create -vserver SVM -policy policy -type async-
mirror|mirror-vault -comment comment -tries transfer_tries -transfer-priority
low|normal -is-network-compression-enabled true|false
```

Para obtener una sintaxis de comando completa, consulte la página [man](#).

A partir de ONTAP 9.5, puede especificar la programación para crear una programación de copia Snapshot común para relaciones de SnapMirror síncrono mediante la `-common-snapshot-schedule` parámetro. De forma predeterminada, la programación común de copias de Snapshot para relaciones de SnapMirror síncrono es una hora. Puede especificar un valor de 30 minutos a dos horas para la programación de la copia de Snapshot para las relaciones de SnapMirror Synchronous.

En el ejemplo siguiente se crea una política de replicación personalizada para la recuperación ante desastres de SnapMirror que permite la compresión de red para las transferencias de datos:

```
cluster_dst::> snapmirror policy create -vserver svml -policy
DR_compressed -type async-mirror -comment "DR with network compression
enabled" -is-network-compression-enabled true
```



En el ejemplo siguiente se crea una política de replicación personalizada para la replicación unificada:

```
cluster_dst::> snapmirror policy create -vserver svml -policy my_unified
-type mirror-vault
```

### Después de terminar

En el caso de los tipos de políticas «mirror-vault», debe definir las reglas que determinen las copias snapshot que se transfieren durante la inicialización y la actualización.

Utilice la `snapmirror policy show` Comando para comprobar que la política de SnapMirror se ha creado. Para obtener una sintaxis de comando completa, consulte la página man.

### Defina una regla para una política

En el caso de las directivas personalizadas con el tipo de política «mirror-vault», debe definir al menos una regla que determine las copias snapshot que se transfieren durante la inicialización y la actualización. También puede definir reglas para las políticas predeterminadas con el tipo de política «mirror-vault».

### Acerca de esta tarea

Todas las normas que tengan el tipo de política «espejo» deben tener una regla que especifique las copias snapshot que desea replicar. La regla «'bimensual'», por ejemplo, indica que sólo deben replicarse las copias snapshot asignadas a la etiqueta «'bimensual'» de SnapMirror. La etiqueta de SnapMirror se asigna al configurar copias de Snapshot de Element.

Cada tipo de política está asociado a una o más reglas definidas por el sistema. Estas reglas se asignan automáticamente a una directiva cuando se especifica su tipo de directiva. La siguiente tabla muestra las reglas definidas por el sistema.

| Regla definida por el sistema | Se utiliza en tipos de políticas        | Resultado                                                                                                                           |
|-------------------------------|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| sm_creado                     | reflejo asíncrono, reflejo de almacenes | Una copia Snapshot creada por SnapMirror se transfiere tras la inicialización y la actualización.                                   |
| todos los días                | mirror-vault                            | Las nuevas copias snapshot del origen con la etiqueta de SnapMirror «día» se transfieren durante la inicialización y actualización. |
| semanal                       | mirror-vault                            | Al inicializar y actualizar, se transfieren las nuevas copias snapshot del origen con la etiqueta de SnapMirror «'Weekly'».         |

|         |              |                                                                                                                                           |
|---------|--------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| mensual | mirror-vault | Las nuevas copias snapshot en el origen con la etiqueta de SnapMirror «mensual» se transfieren durante la inicialización y actualización. |
|---------|--------------|-------------------------------------------------------------------------------------------------------------------------------------------|

Puede especificar reglas adicionales según sea necesario, para directivas predeterminadas o personalizadas. Por ejemplo:

- Para el valor predeterminado `MirrorAndVault` Política puede crear una regla llamada «bimensual» para hacer coincidir las copias Snapshot de la fuente con la etiqueta «bimensual» de SnapMirror.
- En el caso de una política personalizada con el tipo de política «mercado de productos vault», puede crear una regla llamada «bisemanal» para hacer coincidir las copias Snapshot del origen con la etiqueta de SnapMirror «bisemanales».

## Paso

1. Definir una regla para una directiva:

```
snapmirror policy add-rule -vserver SVM -policy policy_for_rule -snapmirror
-label snapmirror-label -keep retention_count
```

Para obtener una sintaxis de comando completa, consulte la página man.

En el siguiente ejemplo, se añade una regla con la etiqueta de SnapMirror `bi-monthly` al valor predeterminado `MirrorAndVault` política:

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
MirrorAndVault -snapmirror-label bi-monthly -keep 6
```

En el siguiente ejemplo, se añade una regla con la etiqueta de SnapMirror `bi-weekly` al personalizado `my_snapvault` política:

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
my_snapvault -snapmirror-label bi-weekly -keep 26
```

En el siguiente ejemplo, se añade una regla con la etiqueta de SnapMirror `app_consistent` al personalizado `Sync` política:

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy Sync
-snapmirror-label app_consistent -keep 1
```

Luego, puede replicar las copias Snapshot del clúster de origen que coincidan con esta etiqueta de SnapMirror:

```
cluster_src::> snapshot create -vserver vs1 -volume voll -snapshot
snapshot1 -snapmirror-label app_consistent
```

## Cree una relación de replicación

### Crear una relación desde un origen de elemento a un destino de ONTAP

La relación entre el volumen de origen del almacenamiento primario y el volumen de destino del almacenamiento secundario se denomina *relación de protección de datos*. Puede utilizar el `snapmirror create` Comando para crear una relación de protección de datos desde un origen de elemento a un destino de ONTAP, o desde un origen de ONTAP a un destino de Element.

SnapMirror se puede usar para replicar copias de Snapshot de un volumen de Element en un sistema de destino de ONTAP. En caso de desastre en el sitio de Element, puede seguir prestando servicio a los clientes desde el sistema ONTAP y, a continuación, reactivar el volumen de origen de Element cuando el servicio se restaure.

#### Antes de empezar

- ONTAP debe haber accesible desde el nodo Element que contiene el volumen que se va a replicar.
- El volumen de Element debe estar habilitado para la replicación de SnapMirror.
- Si utiliza el tipo de política «mirror-vault», debe haber configurado una etiqueta de SnapMirror para que se repliquen las copias Snapshot de Element.



Es posible realizar esta tarea únicamente en la interfaz de usuario web del software Element. Para obtener más información, consulte ["Documentación de Element"](#).

#### Acerca de esta tarea

Debe especificar la ruta de origen del elemento en el formulario `hostip:/lun/name`, donde «lun» es la cadena real «lun» y. name Es el nombre del volumen de Element.

Un volumen de Element es aproximadamente equivalente a una LUN de ONTAP. SnapMirror crea un LUN con el nombre del volumen de Element cuando se inicializa una relación de protección de datos entre el software Element y ONTAP. SnapMirror replica datos a una LUN existente si la LUN cumple con los requisitos para replicar del software Element en ONTAP.

Las reglas de replicación son las siguientes:

- Un volumen de ONTAP puede contener datos solo de un volumen de Element.
- No es posible replicar datos desde un volumen de ONTAP en varios volúmenes de Element.

En ONTAP 9.3 y versiones anteriores, los volúmenes de destino pueden contener hasta 251 copias Snapshot. A partir de la versión 9.4 de ONTAP, un volumen de destino puede contener hasta 1019 copias snapshot.

#### Paso

1. A partir del clúster de destino, cree una relación de replicación desde un origen de Element en un destino de ONTAP:

```
snapmirror create -source-path hostip:/lun/name -destination-path SVM:volume
|cluster://SVM/volume -type XDP -schedule schedule -policy policy
```

Para obtener una sintaxis de comando completa, consulte la página *man*.

En el siguiente ejemplo se crea una relación de recuperación ante desastres de SnapMirror con los valores predeterminados `MirrorLatest` política:

```
cluster_dst:> snapmirror create -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily
-policy MirrorLatest
```

En el ejemplo siguiente se crea una relación de replicación unificada con la opción predeterminada `MirrorAndVault` política:

```
cluster_dst:> snapmirror create -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily
-policy MirrorAndVault
```

En el siguiente ejemplo se crea una relación de replicación unificada mediante `Unified7year` política:

```
cluster_dst:> snapmirror create -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily
-policy Unified7year
```

En el siguiente ejemplo se crea una relación de replicación unificada mediante el método personalizado `my_unified` política:

```
cluster_dst:> snapmirror create -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily
-policy my_unified
```

## Después de terminar

Utilice la `snapmirror show` Comando para verificar que la relación de SnapMirror se ha creado. Para obtener una sintaxis de comando completa, consulte la página *man*.

## Cree una relación desde un origen de ONTAP a un destino de elemento

A partir de ONTAP 9.4, puede usar SnapMirror para replicar copias Snapshot de una LUN creada en un origen de ONTAP de nuevo en un destino de Element. Es posible que utilice la LUN para migrar datos desde ONTAP al software Element.

## Antes de empezar

- ONTAP debe haber accesible el nodo de destino de Element.

- El volumen de Element debe estar habilitado para la replicación de SnapMirror.

### Acerca de esta tarea

Debe especificar la ruta de destino del elemento en el formulario `hostip:/lun/name`, donde «'lun'» es la cadena real «'lun'» y. name Es el nombre del volumen de Element.

Las reglas de replicación son las siguientes:

- La relación de replicación debe tener una política de tipo «"duplicación asíncrona"».

Puede usar una directiva predeterminada o personalizada.

- Solo se admiten LUN iSCSI.
- No es posible replicar más de un LUN desde un volumen de ONTAP a un volumen de Element.
- No es posible replicar un LUN desde un volumen de ONTAP a varios volúmenes de Element.

### Paso

1. Cree una relación de replicación desde un origen de ONTAP a un destino de Element:

```
snapmirror create -source-path SVM:volume|cluster://SVM/volume -destination
-path hostip:/lun/name -type XDP -schedule schedule -policy policy
```

Para obtener una sintaxis de comando completa, consulte la página man.

En el siguiente ejemplo se crea una relación de recuperación ante desastres de SnapMirror con los valores predeterminados `MirrorLatest` política:

```
cluster_dst:> snapmirror create -source-path svm_1:volA_dst
-destination-path 10.0.0.11:/lun/0005 -type XDP -schedule my_daily
-policy MirrorLatest
```

En el siguiente ejemplo se crea una relación de recuperación ante desastres de SnapMirror mediante el método personalizado `my_mirror` política:

```
cluster_dst:> snapmirror create -source-path svm_1:volA_dst
-destination-path 10.0.0.11:/lun/0005 -type XDP -schedule my_daily
-policy my_mirror
```

### Después de terminar

Utilice la `snapmirror show` Comando para verificar que la relación de SnapMirror se ha creado. Para obtener una sintaxis de comando completa, consulte la página man.

### Inicializar una relación de replicación

Para todos los tipos de relaciones, la inicialización realiza una *transferencia\_de base*: Realiza una copia Snapshot del volumen de origen y, a continuación, transfiere esa copia y todos los bloques de datos a los que hace referencia al volumen de destino.

## Antes de empezar

- ONTAP debe haber accesible desde el nodo Element que contiene el volumen que se va a replicar.
- El volumen de Element debe estar habilitado para la replicación de SnapMirror.
- Si utiliza el tipo de política «mirror-vault», debe haber configurado una etiqueta de SnapMirror para que se repliquen las copias Snapshot de Element.

## Acerca de esta tarea

Debe especificar la ruta de origen del elemento en el formulario `hostip:/lun/name`, donde «'lun'» es la cadena real «'lun'» y. `name` Es el nombre del volumen de Element.

La inicialización puede requerir mucho tiempo. Puede ser conveniente ejecutar la transferencia básica en horas de menor actividad.

Si la inicialización de una relación desde un origen de ONTAP a un destino de Element genera errores por cualquier motivo, seguirá presentando errores incluso después de haber corregido el problema (un nombre de LUN no válido, por ejemplo). La solución es la siguiente:



1. Eliminar la relación.
2. Elimine el volumen de destino de Element.
3. Cree un nuevo volumen de destino de Element.
4. Cree e inicialice una nueva relación desde el origen de ONTAP hasta el volumen de destino de Element.

## Paso

1. Inicializar una relación de replicación:

```
snapmirror initialize -source-path hostip:/lun/name -destination-path
SVM:volume|cluster://SVM/volume
```

Para obtener una sintaxis de comando completa, consulte la página man.

En el siguiente ejemplo, se inicializa la relación entre el volumen de origen 0005 En la dirección IP 10.0.0.11 y el volumen de destino volA\_dst encendido svm\_backup:

```
cluster_dst:> snapmirror initialize -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst
```

## Proporcione datos desde un volumen de destino de recuperación ante desastres de SnapMirror

### Haga que el volumen de destino sea modificable

Cuando el desastre deshabilita el sitio principal para una relación de recuperación ante desastres de SnapMirror, puede proporcionar datos del volumen de destino con una interrupción mínima. Se puede reactivar el volumen de origen cuando el servicio se restaura en el sitio primario.

Debe hacer que el volumen de destino sea editable, para poder proporcionar datos del volumen a los clientes. Puede utilizar el `snapmirror quiesce` comando para detener las transferencias programadas al destino, el `snapmirror abort` comando para detener las transferencias continuas y el `snapmirror break` comando para hacer que el destino sea editable.

### Acerca de esta tarea

Debe especificar la ruta de origen del elemento en el formulario `hostip:/lun/name`, donde «lun» es la cadena real «lun» y. name Es el nombre del volumen de Element.

### Pasos

1. Detenga las transferencias programadas al destino:

```
snapmirror quiesce -source-path hostip:/lun/name -destination-path SVM:volume
|cluster://SVM/volume
```

Para obtener una sintaxis de comando completa, consulte la página man.

El siguiente ejemplo detiene las transferencias programadas entre el volumen de origen 0005 En la dirección IP 10.0.0.11 y el volumen de destino volA\_dst encendido svm\_backup:

```
cluster_dst:> snapmirror quiesce -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst
```

2. Detenga las transferencias continuas al destino:

```
snapmirror abort -source-path hostip:/lun/name -destination-path SVM:volume
|cluster://SVM/volume
```

Para obtener una sintaxis de comando completa, consulte la página man.

El siguiente ejemplo detiene las transferencias continuas entre el volumen de origen 0005 En la dirección IP 10.0.0.11 y el volumen de destino volA\_dst encendido svm\_backup:

```
cluster_dst:> snapmirror abort -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst
```

3. Rompa la relación de recuperación ante desastres de SnapMirror:

```
snapmirror break -source-path hostip:/lun/name -destination-path SVM:volume
|cluster://SVM/volume
```

Para obtener una sintaxis de comando completa, consulte la página man.

En el siguiente ejemplo, se rompe la relación entre el volumen de origen 0005 En la dirección IP 10.0.0.11 y el volumen de destino volA\_dst encendido svm\_backup y el volumen de destino volA\_dst encendido svm\_backup:

```
cluster_dst::> snapmirror break -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst
```

### Configure el volumen de destino para acceder a los datos

Tras hacer que el volumen de destino sea editable, debe configurar el volumen para el acceso a los datos. Los hosts SAN pueden acceder a los datos desde el volumen de destino hasta que se reactive el volumen de origen.

1. Asigne la LUN de Element al iGroup correspondiente.
2. Crear sesiones iSCSI desde los iniciadores de host SAN a los LIF DE SAN.
3. En el cliente SAN, realice una nueva exploración del almacenamiento para detectar la LUN conectada.

### Vuelva a activar el volumen de origen original

Puede restablecer la relación de protección de datos original entre los volúmenes de origen y destino cuando ya no necesite servir datos desde el destino.

#### Acerca de esta tarea

En el siguiente procedimiento se asume que la línea base del volumen de origen original está intacta. Si la base de referencia no está intacta, debe crear e inicializar la relación entre el volumen desde el que se sirven datos y el volumen de origen original antes de realizar el procedimiento.

Debe especificar la ruta de origen del elemento en el formulario *hostip:/lun/name*, donde «lun'» es la cadena real «lun'» y. name Es el nombre del volumen de Element.

A partir de ONTAP 9.4, las copias Snapshot de una LUN creada mientras ofrece datos del destino de ONTAP se replican automáticamente cuando la fuente de Element se reactiva.

Las reglas de replicación son las siguientes:

- Solo se admiten LUN iSCSI.
- No es posible replicar más de un LUN desde un volumen de ONTAP a un volumen de Element.
- No es posible replicar un LUN desde un volumen de ONTAP a varios volúmenes de Element.

### Pasos

1. Elimine la relación de protección de datos original:

```
snapmirror delete -source-path SVM:volume|cluster://SVM/volume -destination
-path hostip:/lun/name -policy policy
```

Para obtener una sintaxis de comando completa, consulte la página man.

En el siguiente ejemplo, se elimina la relación entre el volumen de origen original, 0005 En la dirección IP 10.0.0.11 y el volumen desde el que se proporcionan datos, volA\_dst encendido svm\_backup:



```
cluster_dst:> snapmirror delete -source-path 10.0.0.11:/lun/0005
-policy MirrorLatest -destination-path svm_backup:volA_dst
```

## 2. Invierta la relación de protección de datos original:

```
snapmirror resync -source-path SVM:volume|cluster://SVM/volume -destination
-path hostip:/lun/name -policy policy
```

Para obtener una sintaxis de comando completa, consulte la página man.

Aunque la resincronización no requiere una transferencia básica, puede requerir mucho tiempo. Puede que desee ejecutar la resincronización en horas de menor actividad.

En el siguiente ejemplo, se revierte la relación entre el volumen de origen original, 0005 En la dirección IP 10.0.0.11 y el volumen desde el que se proporcionan datos, volA\_dst encendido svm\_backup:

```
cluster_dst:> snapmirror resync -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005 -policy MirrorLatest
```

## 3. Actualice la relación de inversión:

```
snapmirror update -source-path SVM:volume|cluster://SVM/volume -destination
-path hostip:/lun/name
```

Para obtener una sintaxis de comando completa, consulte la página man.



El comando genera errores si no existe una copia Snapshot común en el origen y el destino. Uso `snapmirror initialize` para volver a inicializar la relación.

En el siguiente ejemplo, se actualiza la relación entre el volumen desde el que se proporcionan datos, volA\_dst encendido svm\_backup, y el volumen de origen original, 0005 En la dirección IP 10.0.0.11:

```
cluster_dst:> snapmirror update -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005
```

## 4. Detenga las transferencias programadas para la relación de inversión:

```
snapmirror quiesce -source-path SVM:volume|cluster://SVM/volume -destination
-path hostip:/lun/name
```

Para obtener una sintaxis de comando completa, consulte la página man.

En el siguiente ejemplo, se detienen las transferencias programadas entre el volumen desde el que se proporcionan datos: volA\_dst encendido svm\_backup, y el volumen de origen original, 0005 En la dirección IP 10.0.0.11:

```
cluster_dst:> snapmirror quiesce -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005
```

5. Detenga las transferencias continuas para la relación de inversión:

```
snapmirror abort -source-path SVM:volume|cluster://SVM/volume -destination
-path hostip:/lun/name
```

Para obtener una sintaxis de comando completa, consulte la página man.

El ejemplo siguiente detiene las transferencias continuas entre el volumen desde el que ofrece datos, volA\_dst encendido svm\_backup, y el volumen de origen original, 0005 En la dirección IP 10.0.0.11:

```
cluster_dst:> snapmirror abort -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005
```

6. Rompa la relación inversa:

```
snapmirror break -source-path SVM:volume|cluster://SVM/volume -destination
-path hostip:/lun/name
```

Para obtener una sintaxis de comando completa, consulte la página man.

En el siguiente ejemplo, se rompe la relación entre el volumen desde el que se proporcionan datos, volA\_dst encendido svm\_backup, y el volumen de origen original, 0005 En la dirección IP 10.0.0.11:

```
cluster_dst:> snapmirror break -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005
```

7. Elimine las relaciones de protección de datos revertidas:

```
snapmirror delete -source-path SVM:volume|cluster://SVM/volume -destination
-path hostip:/lun/name -policy policy
```

Para obtener una sintaxis de comando completa, consulte la página man.

En el siguiente ejemplo, se elimina la relación inversa entre el volumen de origen original, 0005 En la dirección IP 10.0.0.11 y el volumen desde el que se proporcionan datos, volA\_dst encendido svm\_backup:

```
cluster_src:> snapmirror delete -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005 -policy MirrorLatest
```

8. Restablezca la relación de protección de datos original:

```
snapmirror resync -source-path hostip:/lun/name -destination-path
```

```
SVM:volume|cluster://SVM/volume
```

Para obtener una sintaxis de comando completa, consulte la página man.

En el siguiente ejemplo, se restablece la relación entre el volumen de origen original, 0005 En la dirección IP 10.0.0.11, y el volumen de destino original, volA\_dst encendido svm\_backup:

```
cluster_dst:> snapmirror resync -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst
```

### Después de terminar

Utilice la `snapmirror show` Comando para verificar que la relación de SnapMirror se ha creado. Para obtener una sintaxis de comando completa, consulte la página man.

## Actualice manualmente una relación de replicación

Es posible que deba actualizar una relación de replicación manualmente si falla una actualización debido a un error de red.

### Acerca de esta tarea

Debe especificar la ruta de origen del elemento en el formulario `hostip:/lun/name`, donde «lun» es la cadena real «lun» y. name Es el nombre del volumen de Element.

### Pasos

1. Actualice manualmente una relación de replicación:

```
snapmirror update -source-path hostip:/lun/name -destination-path SVM:volume
|cluster://SVM/volume
```

Para obtener una sintaxis de comando completa, consulte la página man.



El comando genera errores si no existe una copia Snapshot común en el origen y el destino. Uso `snapmirror initialize` para volver a inicializar la relación.

En el ejemplo siguiente se actualiza la relación entre el volumen de origen 0005 En la dirección IP 10.0.0.11 y el volumen de destino volA\_dst encendido svm\_backup:

```
cluster_src:> snapmirror update -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst
```

## Resincronice una relación de replicación

Es necesario volver a sincronizar una relación de replicación después de hacer que un volumen de destino sea modificable, después de un error en la actualización porque no existe una copia Snapshot común en los volúmenes de origen y destino o si desea cambiar la política de replicación de la relación.

## Acerca de esta tarea

Aunque la resincronización no requiere una transferencia básica, puede requerir mucho tiempo. Puede que desee ejecutar la resincronización en horas de menor actividad.

Debe especificar la ruta de origen del elemento en el formulario `hostip:/lun/name`, donde «lun'» es la cadena real «lun'» y. name Es el nombre del volumen de Element.

## Paso

1. Resincronización de los volúmenes de origen y destino:

```
snapmirror resync -source-path hostip:/lun/name -destination-path SVM:volume
|cluster://SVM/volume -type XDP -policy policy
```

Para obtener una sintaxis de comando completa, consulte la página `man`.

En el siguiente ejemplo, vuelva a establecer la relación entre el volumen de origen 0005 En la dirección IP 10.0.0.11 y el volumen de destino `volA_dst` encendido `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path 10.0.0.11:/lun/0005
-policy MirrorLatest -destination-path svm_backup:volA_dst
```

# Supervisión de eventos, rendimiento y estado

## Supervise el rendimiento del clúster con System Manager

### Supervise el rendimiento del clúster mediante System Manager

Los temas de esta sección muestran cómo gestionar el estado y el rendimiento de los clústeres con System Manager en ONTAP 9.7 y versiones posteriores.

Para supervisar el rendimiento del clúster, consulte información sobre el sistema en la consola de System Manager. La consola muestra información sobre alertas y notificaciones importantes, la eficiencia y capacidad de los niveles de almacenamiento y volúmenes, los nodos disponibles en un clúster, el estado de los nodos de un par de alta disponibilidad, las aplicaciones y objetos más activos, y las métricas de rendimiento de un clúster o un nodo.

El panel permite determinar la siguiente información:

- **Salud:** ¿Qué tan saludable es el clúster?
- **Capacidad:** ¿Qué capacidad está disponible en el cluster?
- **Rendimiento:** ¿Hasta qué punto está funcionando el clúster en función de la latencia, IOPS y rendimiento?
- **Red:** ¿Cómo se configura la red con hosts y objetos de almacenamiento, como puertos, interfaces y equipos virtuales de almacenamiento?

En la información general de estado y capacidad, puede hacer clic en [→](#) para ver información adicional y realizar tareas.

En la información general sobre rendimiento, puede ver las métricas en función de la hora, el día, la semana, el mes o el año.

En la información general sobre la red, se muestra el número de cada objeto de la red (por ejemplo, "8 puertos NVMe/FC"). Puede hacer clic en los números para ver los detalles de cada objeto de red.

### Vea el rendimiento en la consola de clústeres

Utilice la consola para tomar decisiones informadas sobre las cargas de trabajo que puede añadir o mover. También puede observar los tiempos de uso máximos para planificar posibles cambios.

Los valores de rendimiento se actualizan cada 3 segundos y el gráfico de rendimiento se actualiza cada 15 segundos.

#### Pasos

1. Haga clic en **Panel**.
2. En **rendimiento**, seleccione el intervalo.

### Identifique volúmenes activos y otros objetos

Acelere el rendimiento de su clúster identificando los volúmenes a los que se accede con

frecuencia (volúmenes activos) y los datos (objetos activos).



A partir de ONTAP 9.10.1, puede usar la función Seguimiento de actividades de Análisis del sistema de archivos para supervisar los objetos activos de un volumen.


#### Pasos

1. Haga clic en **almacenamiento > volúmenes**.
2. Filtre las columnas IOPS, latencia y rendimiento para ver los volúmenes y los datos a los que se accede con frecuencia.

## Modifique la calidad de servicio

A partir de ONTAP 9,8, cuando aprovisiona almacenamiento, [Calidad de servicio \(QoS\)](#) está activado de forma predeterminada. Puede deshabilitar la calidad de servicio o elegir una política de calidad de servicio personalizada durante el proceso de aprovisionamiento. También puede modificar la calidad de servicio después de aprovisionar el almacenamiento.

#### Pasos

1. En System Manager, seleccione **Almacenamiento** y luego **Volúmenes**.
2. Junto al volumen para el que desea modificar la calidad de servicio, seleccione  Luego **Editar**.

## Control de riesgos

A partir de ONTAP 9.10.0, puede usar System Manager para supervisar los riesgos notificados por el asesor digital de Active IQ. A partir de ONTAP 9.10.1, puede usar System Manager para reconocer también los riesgos.

El asesor digital de Active IQ de NetApp informa sobre las oportunidades de reducir el riesgo y mejorar el rendimiento y la eficiencia de su entorno de almacenamiento. System Manager le permite obtener información sobre los riesgos registrados por Active IQ y recibir información procesable que le ayuda a administrar el almacenamiento y lograr una mayor disponibilidad, una seguridad mejorada y un mejor rendimiento del almacenamiento.

### Enlace a su cuenta de Active IQ

Para recibir información sobre riesgos de Active IQ, primero debe enlazar con la cuenta de Active IQ de System Manager.

#### Pasos

1. En System Manager, haga clic en **clúster > Configuración**.
2. En **Registro de Active IQ**, haga clic en **Registro**.
3. Introduzca sus credenciales para Active IQ.
4. Una vez autenticadas las credenciales, haga clic en **Confirmar para vincular Active IQ con System Manager**.

## Ver el número de riesgos

A partir de ONTAP 9.10.0, puede ver desde la consola de System Manager la cantidad de riesgos notificados por Active IQ.

### Antes de empezar

Debe establecer una conexión desde System Manager con la cuenta de Active IQ. Consulte [Enlace a su cuenta de Active IQ](#).

### Pasos

1. En System Manager, haga clic en **Panel**.
2. En la sección **Salud**, vea el número de riesgos reportados.



Puede ver información más detallada sobre cada riesgo haciendo clic en el mensaje que muestra el número de riesgos. Consulte [Consulte detalles de riesgos](#).

## Consulte detalles de riesgos

A partir de ONTAP 9.10.0, puede ver desde System Manager cómo se clasifican los riesgos notificados por Active IQ en las áreas de impacto. También puede ver información detallada sobre cada riesgo notificado, su impacto potencial en el sistema y las acciones correctivas que puede tomar.

### Antes de empezar

Debe establecer una conexión desde System Manager con la cuenta de Active IQ. Consulte [Enlace a su cuenta de Active IQ](#).

### Pasos


1. Haga clic en **Eventos > todos los eventos**.
2. En la sección **Descripción general**, en **Sugerencias** de Active IQ, vea el número de riesgos en cada categoría de área de impacto. Las categorías de riesgo incluyen:
  - Rendimiento y eficiencia
  - Disponibilidad y protección
  - Capacidad
  - Configuración
  - Seguridad
3. Haga clic en la ficha **Sugerencias** de Active IQ para ver información sobre cada riesgo, incluidos los siguientes:
  - Nivel de impacto en el sistema
  - Categoría del riesgo
  - Nodos afectados
  - Tipo de mitigación necesaria
  - Acciones correctivas que puede tomar

## Reconocer riesgos

A partir de ONTAP 9.10.1, puede usar System Manager para reconocer cualquiera de los riesgos abiertos.

**Pasos**

- 1. En System Manager, muestre la lista de riesgos siguiendo el procedimiento en [Consulte detalles de riesgos](#).
- 2. Haga clic en el nombre de riesgo de un riesgo abierto que desee reconocer.
- 3. Introduzca información en los siguientes campos:
  - Recordatorio (fecha)
  - Justificación
  - Comentarios
- 4. Haga clic en **acuse de recibo**.




Tras reconocer un riesgo, el cambio tarda unos minutos en reflejarse en la lista de sugerencias de Active IQ.

**No reconocer riesgos**

A partir de ONTAP 9.10.1, puede usar System Manager para anular el reconocimiento de cualquier riesgo que anteriormente se hubiera reconocido.

**Pasos**


- 1. En System Manager, muestre la lista de riesgos siguiendo el procedimiento en [Consulte detalles de riesgos](#).
- 2. Haga clic en el nombre de riesgo de un riesgo reconocido que desea no reconocer.
- 3. Introduzca información en los siguientes campos:
  - Justificación
  - Comentarios
- 4. Haga clic en **no confirmar**.



Tras reconocer un riesgo, el cambio tarda unos minutos en reflejarse en la lista de sugerencias de Active IQ.

**Información de System Manager**

A partir de ONTAP 9.11.1, System Manager muestra *insights* que le ayudan a optimizar el rendimiento y la seguridad de su sistema.



Para ver, personalizar y responder a los datos, consulte "[Obtenga información interna para ayudarlo a optimizar su sistema](#)"

**Información de la capacidad**

System Manager puede mostrar la siguiente información en respuesta a las condiciones de capacidad de su sistema:

| Insight | Gravedad | Condición | Soluciones |
|---------|----------|-----------|------------|
|---------|----------|-----------|------------|



|                                                    |                             |                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A los niveles locales les falta espacio            | Solucione los riesgos       | Uno o más niveles locales están llenos al 95% y crecen rápidamente. Es posible que las cargas de trabajo existentes no puedan crecer o, en casos extremos, las cargas de trabajo existentes pueden quedarse sin espacio y fallar.                                       | <p><b>Revisión recomendada:</b> Realice una de las siguientes opciones.</p> <ul style="list-style-type: none"> <li>• Borre la cola de recuperación del volumen.</li> <li>• Habilite thin provisioning en volúmenes de thick provisioning para liberar el almacenamiento atrapado.</li> <li>• Mueva volúmenes a otro nivel local.</li> <li>• Elimine las copias Snapshot no necesarias.</li> <li>• Elimine los directorios o los archivos que no sean necesarios en los volúmenes.</li> <li>• Habilite Fabric Pool para organizar los datos en niveles en el cloud.</li> </ul> |
| Las aplicaciones carecen de espacio                | Necesita atención           | Uno o más volúmenes están llenos a más del 95 %, pero no tienen habilitado el crecimiento automático.                                                                                                                                                                   | <p><b>Recomendado:</b> Habilita el crecimiento automático hasta el 150% de la capacidad actual.</p> <p><b>Otras opciones:</b></p> <ul style="list-style-type: none"> <li>• Reclame espacio eliminando copias Snapshot.</li> <li>• Cambie el tamaño de los volúmenes.</li> <li>• Elimine directorios o archivos.</li> </ul>                                                                                                                                                                                                                                                    |
| La capacidad del volumen FlexGroup se desequilibra | Optimizar el almacenamiento | El tamaño de los volúmenes constituyentes de uno o más volúmenes FlexGroup creció de forma desigual con el tiempo, lo que conduce a un desequilibrio en el uso de la capacidad. Si los volúmenes constituyentes se completan, se podrían producir errores de escritura. | <p><b>Recomendado:</b> Reequilibra los volúmenes de FlexGroup.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

|                                                                           |                             |                                                                                                                                                                                                                                              |                                                                                                      |
|---------------------------------------------------------------------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| Los equipos virtuales de almacenamiento o se están quedando sin capacidad | Optimizar el almacenamiento | Una o varias máquinas virtuales de almacenamiento se encuentran cerca de su capacidad máxima. No podrá aprovisionar más espacio para volúmenes nuevos o existentes si las máquinas virtuales de almacenamiento alcanzan la capacidad máxima. | <b>Recomendado:</b> Si es posible, aumente el límite de capacidad máxima de la VM de almacenamiento. |
|---------------------------------------------------------------------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|

## Información sobre seguridad

System Manager puede mostrar la siguiente información en respuesta a condiciones que podrían poner en peligro la seguridad de sus datos o del sistema.

| Insight                                                                      | Gravedad          | Condición                                                                                | Soluciones                                                                                                                                                                            |
|------------------------------------------------------------------------------|-------------------|------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Los volúmenes siguen en modo de aprendizaje anti-ransomware                  | Necesita atención | Uno o más volúmenes han estado en el modo de aprendizaje antiransomware durante 90 días. | <b>Recomendado:</b> Habilita el modo activo anti-ransomware para esos volúmenes.                                                                                                      |
| La eliminación automática de copias de Snapshot se habilita en los volúmenes | Necesita atención | La eliminación automática de Snapshot se habilita en uno o más volúmenes.                | <b>Recomendado:</b> Desactiva la eliminación automática de copias snapshot. De lo contrario, podría no ser posible llevar a cabo la recuperación de datos de estos volúmenes.         |
| Los volúmenes no tienen políticas de Snapshot                                | Necesita atención | Uno o más volúmenes no tienen una política de Snapshot adecuada anexada a ellos.         | <b>Recomendado:</b> Adjunte una política de Snapshot a volúmenes que no tengan uno. De lo contrario, podría no ser posible llevar a cabo la recuperación de datos de estos volúmenes. |

|                                                             |                |                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------------------------------|----------------|---------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FPolicy nativo no configurado                               | Mejor práctica | La política nativa de FPolicy no está configurada en una o más máquinas virtuales de almacenamiento NAS.                        | <b>Recomendado: IMPORTANTE:</b> Bloquear extensiones puede dar lugar a resultados inesperados. A partir de 9.11.1, podrá habilitar FPolicy nativo para máquinas virtuales de almacenamiento, que bloquea más de 3000 extensiones de archivos que se sabe que se utilizan para ataques de ransomware. " <a href="#">Configurar FPolicy nativa</a> " En equipos virtuales de almacenamiento NAS para controlar las extensiones de archivos que permiten o no escribirse en volúmenes del entorno. |
| Telnet está activado                                        | Mejor práctica | Se debe utilizar Secure Shell (SSH) para un acceso remoto seguro.                                                               | <b>Recomendado:</b> Desactiva Telnet y usa SSH para un acceso remoto seguro.                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Hay muy pocos servidores NTP configurados                   | Mejor práctica | El número de servidores configurados para NTP es inferior a 3.                                                                  | <b>Recomendado:</b> Asocie al menos tres servidores NTP con el cluster. De lo contrario, se pueden producir problemas con la sincronización de la hora del clúster.                                                                                                                                                                                                                                                                                                                             |
| Shell remoto (RSH) está activado                            | Mejor práctica | Se debe utilizar Secure Shell (SSH) para un acceso remoto seguro.                                                               | <b>Recomendado:</b> Desactiva RSH y usa SSH para un acceso remoto seguro.                                                                                                                                                                                                                                                                                                                                                                                                                       |
| El banner de inicio de sesión no está configurado           | Mejor práctica | Los mensajes de inicio de sesión no están configurados para el clúster, para la máquina virtual de almacenamiento o para ambos. | <b>Recomendado:</b> Configure los banners de inicio de sesión para el clúster y la VM de almacenamiento y habilite su uso.                                                                                                                                                                                                                                                                                                                                                                      |
| AutoSupport está utilizando un protocolo no seguro          | Mejor práctica | AutoSupport no está configurado para comunicarse a través de HTTPS.                                                             | <b>Recomendado:</b> Se recomienda encarecidamente utilizar HTTPS como protocolo de transporte predeterminado para enviar mensajes AutoSupport al soporte técnico.                                                                                                                                                                                                                                                                                                                               |
| El usuario administrador predeterminado o no está bloqueado | Mejor práctica | Nadie ha iniciado sesión con una cuenta administrativa predeterminada (admin o diag), y estas cuentas no están bloqueadas.      | <b>Recomendado:</b> Bloquea las cuentas administrativas predeterminadas cuando no se estén utilizando.                                                                                                                                                                                                                                                                                                                                                                                          |

|                                                                                     |                   |                                                                                                                  |                                                                                                                                                                                                                                                              |
|-------------------------------------------------------------------------------------|-------------------|------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Secure Shell (SSH) utiliza cifrados no seguros                                      | Mejor práctica    | La configuración actual utiliza cifrados de CBC no seguros.                                                      | <b>Recomendado:</b> Solo debe permitir cifrados seguros en su servidor web para proteger la comunicación segura con sus visitantes. Elimine los cifrados que tengan nombres que contengan “cbc”, como “ais128-cbc”, “AES192-cbc”, “AES256-cbc” y “3DES-cbc”. |
| El cumplimiento de la normativa global FIPS 140-2 está desactivado                  | Mejor práctica    | El cumplimiento de la normativa global FIPS 140-2 está deshabilitado en el clúster.                              | <b>Recomendado:</b> Por razones de seguridad, debe habilitar la criptografía conforme a FIPS 140-2 global para garantizar que ONTAP pueda comunicarse de forma segura con clientes externos o clientes de servidor.                                          |
| No se supervisan los volúmenes de ataques de ransomware                             | Necesita atención | El anti-ransomware está deshabilitado en uno o más volúmenes.                                                    | <b>Recomendado:</b> Habilitar anti-ransomware en los volúmenes. De lo contrario, es posible que no note cuándo los volúmenes se están amenazando o bajo ataque.                                                                                              |
| Las máquinas virtuales de almacenamiento o no están configuradas para el ransomware | Mejor práctica    | Una o varias máquinas virtuales de almacenamiento no están configuradas para la protección contra el ransomware. | <b>Recomendado:</b> Habilitar anti-ransomware en las VM de almacenamiento. De lo contrario, es posible que no se dé cuenta de cuándo las máquinas virtuales de almacenamiento se ven amenazadas o sufren un ataque.                                          |

## Información de configuración

System Manager puede mostrar la siguiente información en respuesta a las dudas acerca de la configuración del sistema.

| Insight                                            | Gravedad       | Condición                                                                                                                                                   | Soluciones                                                     |
|----------------------------------------------------|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|
| El clúster no está configurado para notificaciones | Mejor práctica | Correo electrónico, WebHooks o un host de capturas de SNMP no están configurados para permitirle recibir notificaciones acerca de problemas con el clúster. | <b>Recomendado:</b> Configurar notificaciones para el cluster. |

|                                                                      |                |                                                                                                                                                                                                                                          |                                                      |
|----------------------------------------------------------------------|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|
| El clúster no está configurado para las actualizaciones automáticas. | Mejor práctica | El clúster no se ha configurado para recibir actualizaciones automáticas del paquete de cualificación de disco más reciente, el firmware de disco, el firmware de la bandeja y los archivos de firmware SP/BMC cuando estén disponibles. | <b>Recomendado:</b> Habilita esta función.           |
| El firmware del clúster no está actualizado                          | Mejor práctica | Su sistema no dispone de la última actualización del firmware, lo que podría tener mejoras, parches de seguridad o nuevas funciones que ayuden a proteger el clúster para lograr un mejor rendimiento.                                   | <b>Recomendado:</b> Actualizar el firmware de ONTAP. |

## Obtenga información interna para ayudarle a optimizar su sistema

Con System Manager, puede ver información que le ayudará a optimizar su sistema.

### Acerca de esta tarea

A partir de ONTAP 9.11.0, puede ver información de System Manager que le ayuda a optimizar el cumplimiento de normativas de seguridad y capacidad de su sistema.

A partir de ONTAP 9.11.1, puede ver información adicional que le ayuda a optimizar la capacidad, el cumplimiento de normativas de seguridad y la configuración del sistema.



**Las extensiones de bloqueo pueden dar lugar a resultados inesperados.** A partir de ONTAP 9.11.1, puedes habilitar FPolicy nativa para VM de almacenamiento usando System Manager. Puede recibir un mensaje de System Manager Insight que le recomienda "[Configurar FPolicy nativa](#)" Para una máquina virtual de almacenamiento.

Con el modo nativo de FPolicy, puede permitir o rechazar extensiones de archivo específicas. System Manager recomienda más de 3000 extensiones de archivos no permitidas que se hayan usado en ataques anteriores de ransomware. Algunas de estas extensiones pueden ser utilizadas por archivos legítimos en su entorno y bloquearlas puede dar lugar a problemas inesperados.

Por lo tanto, se recomienda encarecidamente que modifique la lista de extensiones para satisfacer las necesidades de su entorno. Consulte "[Cómo quitar una extensión de archivo de una configuración nativa de FPolicy creada por System Manager con System Manager para volver a crear la política](#)".

Para obtener más información sobre las FPolicy nativas, consulte "[Tipos de configuración de FPolicy](#)".

Basándose en las prácticas recomendadas, esta información se muestra en una página desde la cual puede iniciar acciones inmediatas para optimizar su sistema. Para obtener más información sobre cada detalle, consulte "[Información de System Manager](#)".

## Vea información sobre optimización





### Pasos

1. En System Manager, haga clic en **Insights** en la columna de navegación de la izquierda.

La página **Insights** muestra grupos de perspectivas. Cada grupo de perspectivas puede contener una o más información. Se muestran los siguientes grupos:

- Necesita su atención
- Solucione los riesgos
- Optimice su almacenamiento

2. (Opcional) filtre las estadísticas que se muestran haciendo clic en estos botones en la esquina superior derecha de la página:

-  Muestra información relacionada con la seguridad.
-  Muestra la información relacionada con la capacidad.
-  Muestra la información relacionada con la configuración.
-  Muestra todas las estadísticas.

## Responda a la información para optimizar su sistema

En System Manager, puede responder a información descontada, explorando distintas formas de solucionar los problemas o iniciando el proceso para solucionarlos.

## Pasos

1. En System Manager, haga clic en **Insights** en la columna de navegación de la izquierda.
2. Pase el ratón sobre una información para mostrar los botones que se utilizan para llevar a cabo las siguientes acciones:
  - **Descartar**: Quita la visión de la vista. Para «desconocer» la información, consulte [\[customize-settings-insights\]](#).
  - **Explore**: Descubra varias formas de solucionar el problema mencionado en la visión. Este botón sólo aparece si hay más de un método de corrección.
  - **Fix**: Iniciar el proceso de solucionar el problema mencionado en la perspectiva. Se le pedirá que confirme si desea realizar la acción necesaria para aplicar la corrección.




Algunas de estas acciones se pueden iniciar desde otras páginas en System Manager, pero la página **Insights** le ayuda a optimizar sus tareas diarias al permitirle iniciar esta acción desde esta página única.

## Personalice la configuración para obtener información

Puede personalizar las conclusiones sobre las que se le notificará en System Manager.


### Pasos

1. En System Manager, haga clic en **Insights** en la columna de navegación de la izquierda.
2. En la esquina superior derecha de la página, haga clic en , Luego seleccione **Configuración**.
3. En la página **Configuración**, asegúrese de que hay una Marca en las casillas de verificación situadas junto a las estadísticas sobre las que desea recibir notificación. Si ha rechazado previamente una información, puede descartarla asegurándose de que la casilla de verificación está en su lugar.
4. Haga clic en **Guardar**.

## Exporte las estadísticas como un archivo PDF

Puede exportar todos los datos aplicables como un archivo PDF.

### Pasos

1. En System Manager, haga clic en **Insights** en la columna de navegación de la izquierda.
2. En la esquina superior derecha de la página, haga clic en , Luego seleccione **Exportar**.

## Configurar FPolicy nativa

A partir de ONTAP 9.11.1, cuando recibe un informe del administrador del sistema que sugiere implementar FPolicy nativa, puede configurarla en sus máquinas virtuales y volúmenes de almacenamiento.

### Antes de empezar

Al acceder a System Manager Insights, en **Aplicar prácticas recomendadas**, es posible que reciba un mensaje que indique que FPolicy nativo no está configurado.

Para obtener más información sobre los tipos de configuración FPolicy, consulte ["Tipos de configuración de FPolicy"](#).

### Pasos

1. En System Manager, haga clic en **Insights** en la columna de navegación de la izquierda.
2. En **Aplicar las mejores prácticas**, localice **La FPolicy nativa no está configurada**.
3. Lea el siguiente mensaje antes de tomar medidas:



**Las extensiones de bloqueo pueden dar lugar a resultados inesperados.** A partir de ONTAP 9.11.1, puedes habilitar FPolicy nativa para VM de almacenamiento usando System Manager.

Con el modo nativo de FPolicy, puede permitir o rechazar extensiones de archivo específicas. System Manager recomienda más de 3000 extensiones de archivos no permitidas que se hayan usado en ataques anteriores de ransomware. Algunas de estas extensiones pueden ser utilizadas por archivos legítimos en su entorno y bloquearlas puede dar lugar a problemas inesperados.

Por lo tanto, se recomienda encarecidamente que modifique la lista de extensiones para satisfacer las necesidades de su entorno. Consulte ["Cómo quitar una extensión de archivo de una configuración nativa de FPolicy creada por System Manager con System Manager para volver a crear la política"](#).

4. Haga clic en **Fix**.
5. Seleccione las máquinas virtuales de almacenamiento a las que desea aplicar la FPolicy nativa.
6. Para cada máquina virtual de almacenamiento, seleccione los volúmenes que recibirán la FPolicy nativa.
7. Haga clic en **Configurar**.

## Supervise y gestione el rendimiento de los clústeres mediante la CLI

### Información general sobre la gestión y el control del rendimiento

Puede configurar tareas básicas de supervisión y gestión del rendimiento, e identificar y resolver problemas comunes de rendimiento.

Puede utilizar estos procedimientos para supervisar y gestionar el rendimiento del clúster si se aplican las siguientes suposiciones a su situación:

- Quiere utilizar las prácticas recomendadas, no explorar todas las opciones disponibles.
- Si desea mostrar el estado y las alertas del sistema, supervisar el rendimiento del clúster y realizar análisis de las causas subyacentes utilizando Active IQ Unified Manager (antes Unified Manager de OnCommand), además de la interfaz de línea de comandos de ONTAP.
- Se utiliza la interfaz de línea de comandos de ONTAP para configurar la calidad de servicio (QoS) de almacenamiento.

La calidad de servicio también está disponible en System Manager, NSLM, WFA, VSC (complemento de VMware) y API.

- Desea instalar Unified Manager mediante un dispositivo virtual, en lugar de una instalación basada en Linux o Windows.
- Está dispuesto a utilizar una configuración estática en lugar de DHCP para instalar el software.
- Puede acceder a los comandos de ONTAP en el nivel de privilegios avanzados.



- Es un administrador de clústeres con el rol "admin".

### Información relacionada

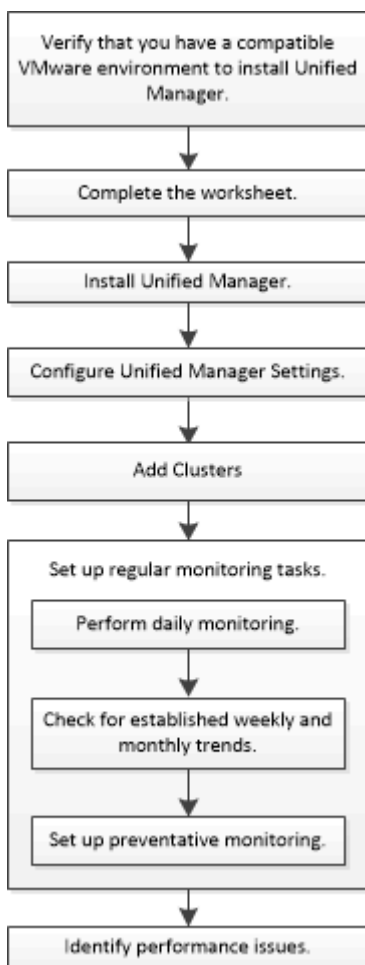
Si estas suposiciones no son correctas para su situación, debería consultar los recursos siguientes:

- ["Instalación de Active IQ Unified Manager 9.8"](#)
- ["Administración del sistema"](#)

## Supervisión del rendimiento

### Información general sobre el flujo de trabajo de supervisión y mantenimiento del rendimiento

La supervisión y el mantenimiento del rendimiento de los clústeres implica instalar el software Active IQ Unified Manager, configurar tareas de supervisión básicas, identificar problemas de rendimiento y realizar ajustes según sea necesario.



### Comprobar que su entorno VMware es compatible

Para instalar Active IQ Unified Manager correctamente, debe comprobar que el entorno de VMware cumple con los requisitos necesarios.

### Pasos

1. Compruebe que su infraestructura VMware cumple los requisitos de tamaño para la instalación de Unified

Manager.

2. Vaya a la ["Matriz de interoperabilidad"](#) para verificar que tiene una combinación compatible de los siguientes componentes:

- Versión de ONTAP
- Versión del sistema operativo ESXi
- La versión de VMware vCenter Server
- Versión de VMware Tools
- Tipo y versión del navegador



La ["Matriz de interoperabilidad"](#) Enumera las configuraciones admitidas para Unified Manager.

3. Haga clic en el nombre de la configuración seleccionada.

Los detalles de esa configuración se muestran en la ventana Detalles de configuración.

4. Revise la información en las siguientes pestañas:

- Notas

Enumera las alertas e información importantes que son específicas de su configuración.

- Políticas y directrices

Proporciona directrices generales para todas las configuraciones.

## Hoja de cálculo de Active IQ Unified Manager

Antes de instalar, configurar y conectar Active IQ Unified Manager, debe tener disponible información específica acerca de su entorno. Puede registrar la información en la hoja de cálculo.

### Información de instalación de Unified Manager

|                                                              |          |
|--------------------------------------------------------------|----------|
| Máquina virtual en la que se ha puesto en marcha el software | Su valor |
| Dirección IP del servidor ESXi                               |          |
| Nombre de dominio completo del host                          |          |
| Dirección IP del host                                        |          |
| Máscara de red                                               |          |
| Dirección IP de la pasarela                                  |          |
| Dirección DNS principal                                      |          |


|                                        |  |
|----------------------------------------|--|
| Dirección DNS secundaria               |  |
| Buscar dominios                        |  |
| Nombre de usuario de mantenimiento     |  |
| Contraseña de usuario de mantenimiento |  |

#### Información de configuración de Unified Manager

| Ajuste                                                              | Su valor                  |
|---------------------------------------------------------------------|---------------------------|
| Dirección de correo electrónico del usuario de mantenimiento        |                           |
| Servidor NTP                                                        |                           |
| Nombre de host o dirección IP del servidor SMTP                     |                           |
| Nombre de usuario SMTP                                              |                           |
| Contraseña SMTP                                                     |                           |
| Puerto predeterminado SMTP                                          | 25 (valor predeterminado) |
| Correo electrónico desde el cual se envían notificaciones de alerta |                           |
| Nombre distintivo de enlace LDAP                                    |                           |
| Contraseña de enlace LDAP                                           |                           |
| Nombre del administrador de Active Directory                        |                           |
| Contraseña de Active Directory                                      |                           |
| Nombre distintivo de la base del servidor de autenticación          |                           |
| Nombre de host o dirección IP del servidor de autenticación         |                           |

#### Información del clúster

Capture la siguiente información para cada clúster en Unified Manager.

| Clúster 1 de N                                                                                                                                                              | Su valor |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| El nombre de host o la dirección IP de administración del clúster                                                                                                           |          |
| Nombre de usuario del administrador ONTAP<br> Debe haber asignado el rol de administrador. |          |
| Contraseña del administrador de ONTAP                                                                                                                                       |          |
| Protocolo (HTTP o HTTPS)                                                                                                                                                    |          |

## Información relacionada

["Autenticación de administrador y RBAC"](#)

## Instale Active IQ Unified Manager

### Descargue e implemente Active IQ Unified Manager

Para instalar el software, debe descargar el archivo de instalación de dispositivos virtuales (va) y, a continuación, usar un cliente de VMware vSphere para implementar el archivo en un servidor ESXi de VMware. El va está disponible en un archivo OVA.

### Pasos

1. Vaya a la página **Descarga de software del sitio de soporte de NetApp** y localice Active IQ Unified Manager.  
  
<https://mysupport.netapp.com/products/index.html>
2. Seleccione **VMware vSphere** en el menú desplegable **Select Platform** y haga clic en **Go!**
3. Guarde el archivo «'OVA» en una ubicación local o de red a la que pueda acceder VMware vSphere Client.
4. En VMware vSphere Client, haga clic en **Archivo > implementar plantilla OVF**.
5. Localice el archivo «'OVA'» y utilice el asistente para implementar el dispositivo virtual en el servidor ESXi.

Puede utilizar la ficha **Propiedades** del asistente para introducir la información de configuración estática.

6. Encienda la máquina virtual.
7. Haga clic en la ficha **Consola** para ver el proceso de inicio inicial.
8. Siga el prompt para instalar VMware Tools en la VM.
9. Configure la zona horaria.
10. Introduzca un nombre de usuario y una contraseña de mantenimiento.
11. Vaya a la URL que muestra la consola de VM.

## Configure los ajustes iniciales de Active IQ Unified Manager

El cuadro de diálogo Active IQ Unified Manager Initial Setup aparece cuando se accede por primera vez a la interfaz de usuario web, que permite configurar algunos ajustes iniciales y añadir clústeres.

### Pasos

1. Acepte la configuración predeterminada de AutoSupport habilitada.
2. Introduzca los detalles del servidor NTP, la dirección de correo electrónico del usuario de mantenimiento, el nombre de host del servidor SMTP y las opciones SMTP adicionales y, a continuación, haga clic en **Guardar**.

### Después de terminar

Una vez finalizada la configuración inicial, se muestra la página Cluster Data Sources, donde puede agregar los detalles del clúster.

### Especifique los clústeres que se van a supervisar

Debe añadir un clúster a un servidor Active IQ Unified Manager para supervisar el clúster, ver el estado de detección del clúster y supervisar su rendimiento.

### Lo que necesitará

- Debe tener la siguiente información:
  - El nombre de host o la dirección IP de administración del clúster

El nombre de host es el nombre de dominio completo (FQDN) o el nombre corto que Unified Manager utiliza para conectarse con el clúster. Este nombre de host debe resolver a la dirección IP de administración del clúster.

La dirección IP de administración del clúster debe ser el LIF de gestión del clúster de la máquina virtual de almacenamiento (SVM) administrativa. Si utiliza un LIF de gestión de nodos, la operación da error.

- Nombre de usuario y contraseña del administrador de ONTAP
- Tipo de protocolo (HTTP o HTTPS) que se puede configurar en el clúster y el número de puerto del clúster
- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- El administrador de ONTAP debe tener los roles de administrador ONAPI y SSH.
- El FQDN de Unified Manager debe poder hacer ping ONTAP.

Puede verificarlo con el comando ONTAP `ping -node node_name -destination Unified_Manager_FQDN`.

### Acerca de esta tarea

Para una configuración de MetroCluster, debe añadir los clústeres local y remoto, y los clústeres deben configurarse correctamente.

### Pasos

1. Haga clic en **Configuración > fuentes de datos de clúster**.

2. En la página Clusters, haga clic en **Add**.
3. En el cuadro de diálogo **Agregar clúster**, especifique los valores necesarios, como el nombre de host o la dirección IP (IPv4 o IPv6) del clúster, el nombre de usuario, la contraseña, el protocolo para la comunicación y el número de puerto.

De manera predeterminada, se selecciona el protocolo HTTPS.

Es posible cambiar la dirección IP de gestión del clúster de IPv6 a IPv4 o de IPv4 a IPv6. La nueva dirección IP se refleja en la cuadrícula del clúster y en la página de configuración del clúster una vez que finaliza el próximo ciclo de supervisión.

4. Haga clic en **Agregar**.
5. Si selecciona HTTPS, realice los siguientes pasos:
  - a. En el cuadro de diálogo **autorizar host**, haga clic en **Ver certificado** para ver la información del certificado sobre el clúster.
  - b. Haga clic en **Sí**.

Unified Manager comprueba el certificado solo cuando se añade el clúster inicialmente, pero no lo comprueba para cada llamada API a ONTAP.

Si el certificado ha caducado, no puede añadir el clúster. Debe renovar el certificado SSL y, a continuación, añadir el clúster.

6. **Opcional:** Ver el estado de detección del clúster:
    - a. Revise el estado de detección del clúster desde la página **Configuración del clúster**.
- El clúster se añade a la base de datos de Unified Manager después del intervalo de supervisión predeterminado de aproximadamente 15 minutos.

## Configurar tareas básicas de supervisión

### Realizar una supervisión diaria

Puede realizar una supervisión diaria para garantizar que no tenga ningún problema de rendimiento inmediato que requiera atención.

#### Pasos

1. Desde la interfaz de usuario de Active IQ Unified Manager, vaya a la página **Inventario de eventos** para ver todos los eventos actuales y obsoletos.
2. En la opción **Ver**, seleccione `Active Performance Events` y determinar qué acción se requiere.

### Utilice tendencias de rendimiento semanales y mensuales para identificar problemas de rendimiento

La identificación de las tendencias de rendimiento puede ayudarle a identificar si el clúster se está utilizando en exceso o está infrautilizado mediante el análisis de latencia de volumen. Puede seguir pasos similares para identificar cuellos de botella en la CPU, la red u otros sistemas.

#### Pasos

1. Localice el volumen que sospecha está infrautilizado o en exceso.
2. En la ficha **Detalles de volumen**, haga clic en **30 d** para mostrar los datos históricos.
3. En el menú desplegable "Break down data by", seleccione **latencia** y, a continuación, haga clic en **Enviar**.
4. Anule la selección de **agregado** en el gráfico de comparación de componentes del clúster y, a continuación, compare la latencia del clúster con el gráfico de latencia del volumen.
5. Seleccione **agregado** y anule la selección de todos los demás componentes del gráfico de comparación de componentes del clúster y, a continuación, compare la latencia de agregado con el gráfico de latencia de volumen.
6. Compare el gráfico de latencia de lecturas/escrituras con el gráfico de latencia de volúmenes.
7. Determine si las cargas de aplicaciones cliente han causado una contención de carga de trabajo y reequilibrio de cargas de trabajo según sea necesario.
8. Determine si el agregado está sobrecargado y causa contención y reequilibre las cargas de trabajo según sea necesario.

#### Utilice umbrales de rendimiento para generar notificaciones de eventos

Los eventos son notificaciones que el Active IQ Unified Manager genera automáticamente cuando se produce una condición predefinida o cuando un valor de contador de rendimiento cruza un umbral. Los eventos le ayudan a identificar problemas de rendimiento en los clústeres que se supervisan. Es posible configurar alertas para que envíen notificaciones por correo electrónico automáticamente cuando se produzcan eventos de ciertos tipos de gravedad.

#### Definir umbrales de rendimiento

Se pueden establecer umbrales de rendimiento para supervisar problemas de rendimiento críticos. Los umbrales definidos por el usuario activan una notificación de sucesos críticos o de advertencia cuando el sistema se acerca o supera el umbral definido.

#### Pasos

1. Cree los umbrales de sucesos críticos y de advertencia:
  - a. Seleccione **Configuración > umbrales de rendimiento**.
  - b. Haga clic en **Crear**.
  - c. Seleccione el tipo de objeto y especifique un nombre y una descripción de la política.
  - d. Seleccione la condición del contador de objetos y especifique los valores de límite que definen los eventos de advertencia y críticos.
  - e. Seleccione la duración del tiempo durante el que deben incumplir los valores límite para que se envíe un evento y, a continuación, haga clic en **Guardar**.
2. Asigne la política de umbral al objeto de almacenamiento.
  - a. Vaya a la página Inventory para el mismo tipo de objeto de clúster que seleccionó anteriormente y seleccione **Performance** en la opción View.
  - b. Seleccione el objeto al que desea asignar la directiva de umbral y, a continuación, haga clic en **asignar directiva de umbral**.

c. Seleccione la directiva que creó anteriormente y, a continuación, haga clic en **asignar directiva**.

### Ejemplo

Puede establecer umbrales definidos por el usuario para aprender acerca de problemas de rendimiento críticos. Por ejemplo, si tiene un servidor Microsoft Exchange Server y sabe que falla si la latencia del volumen supera los 20 milisegundos, puede establecer un umbral de advertencia de 12 milisegundos y un umbral crítico de 15 milisegundos. Con este ajuste de umbral, se pueden recibir notificaciones cuando la latencia del volumen supere el límite.



Object Counter Condition\*    Average Latency ms/op     Warning    12    ms/op     Critical    15    ms/op

### Añadir alertas

Puede configurar alertas para que le notifiquen un evento determinado. Es posible configurar alertas para un solo recurso, para un grupo de recursos o para eventos de un tipo de gravedad determinado. Puede especificar la frecuencia con la que desea que se le notifique y asociar un script a la alerta.

### Lo que necesitará

- Debe haber configurado los ajustes de notificación, como la dirección de correo electrónico de usuario, el servidor SMTP y el host de captura SNMP, con el fin de permitir que el servidor Active IQ Unified Manager utilice estos ajustes para enviar notificaciones a los usuarios cuando se genera un evento.
- Debe conocer los recursos y los eventos sobre los que desea activar la alerta, así como los nombres de usuario o las direcciones de correo electrónico de los usuarios a los que desea notificar.
- Si desea que un script se ejecute según el evento, debe haber añadido el script a Unified Manager mediante la página Scripts.
- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

### Acerca de esta tarea

Puede crear una alerta directamente desde la página de detalles Event después de recibir un evento además de crear una alerta desde la página Alert Setup, tal y como se describe aquí.

### Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento > Configuración de alertas**.
2. En la página **Configuración de alertas**, haga clic en **Agregar**.
3. En el cuadro de diálogo **Agregar alerta**, haga clic en **Nombre** e introduzca un nombre y una descripción para la alerta.
4. Haga clic en **Recursos** y seleccione los recursos que se incluirán o excluirán de la alerta.

Puede establecer un filtro especificando una cadena de texto en el campo **Nombre contiene** para seleccionar un grupo de recursos. Según la cadena de texto que especifique, la lista de recursos disponibles solo muestra los recursos que coinciden con la regla de filtro. La cadena de texto que especifique distingue mayúsculas y minúsculas.

Si un recurso cumple las reglas de inclusión y exclusión especificadas, la regla de exclusión tiene prioridad sobre la regla de inclusión y no se genera la alerta para los eventos relacionados con el recurso excluido.



5. Haga clic en **Eventos** y seleccione los eventos según el nombre del evento o el tipo de gravedad del evento para el que desea activar una alerta.



Para seleccionar más de un evento, pulse la tecla Ctrl mientras realiza las selecciones.

6. Haga clic en **acciones** y seleccione los usuarios a los que desea notificar, elija la frecuencia de notificación, elija si se enviará una captura SNMP al receptor de capturas y asigne una secuencia de comandos para que se ejecute cuando se genere una alerta.



Si modifica la dirección de correo electrónico especificada para el usuario y vuelve a abrir la alerta para su edición, el campo Nombre aparecerá en blanco porque la dirección de correo electrónico modificada ya no está asignada al usuario que se seleccionó previamente. Además, si modificó la dirección de correo electrónico del usuario seleccionado desde la página usuarios, la dirección de correo electrónico modificada no se actualizará para el usuario seleccionado.

También puede optar por notificar a los usuarios a través de las capturas SNMP.

7. Haga clic en **Guardar**.

### Ejemplo de añadir una alerta

Este ejemplo muestra cómo crear una alerta que cumpla con los siguientes requisitos:

- Nombre de alerta: HealthTest
- Recursos: Incluye todos los volúmenes cuyo nombre contiene "abc" y excluye todos los volúmenes cuyo nombre contiene "xyz".
- Eventos: Incluye todos los eventos críticos de salud
- Acciones: Incluye "[sample@domain.com](mailto:sample@domain.com)", una secuencia de comandos "Test" y el usuario debe ser notificado cada 15 minutos

Realice los siguientes pasos en el cuadro de diálogo Agregar alerta:

1. Haga clic en **Nombre** e introduzca HealthTest En el campo **Nombre de alerta**.
2. Haga clic en **Recursos** y, en la ficha incluir, seleccione **volúmenes** en la lista desplegable.
  - a. Introduzca abc En el campo **Nombre contiene** para mostrar los volúmenes cuyo nombre contiene "abc".
  - b. Seleccione **<<All Volumes whose name contains 'abc'>>** en el área Recursos disponibles y muévelos al área Recursos seleccionados.
  - c. Haga clic en **excluir** e introduzca xyz En el campo **Nombre contiene** y, a continuación, haga clic en **Agregar**.
3. Haga clic en **Eventos** y seleccione **críticos** en el campo gravedad del evento.
4. Seleccione **todos los eventos críticos** en el área Eventos coincidentes y muévelos al área Eventos seleccionados.
5. Haga clic en **acciones** e introduzca [sample@domain.com](mailto:sample@domain.com) En el campo Alerta a estos usuarios.
6. Seleccione **Recordar cada 15 minutos** para notificar al usuario cada 15 minutos.

Puede configurar una alerta para que envíe repetidamente notificaciones a los destinatarios durante un período de tiempo específico. Debe determinar la hora desde la cual está activa la notificación de eventos

para la alerta.

7. En el menú **Select Script to Execute**, seleccione **Test** script.
8. Haga clic en **Guardar**.

### Configure los ajustes de alerta

Es posible especificar qué eventos de Active IQ Unified Manager desencadenan las alertas, los destinatarios de correo electrónico para esas alertas y la frecuencia de las alertas.

### Lo que necesitará

Debe tener la función Administrador de aplicaciones.

### Acerca de esta tarea

Puede configurar ajustes de alerta únicos para los siguientes tipos de eventos de rendimiento:

- Eventos críticos desencadenados por infracciones de umbrales definidos por el usuario
- Eventos de advertencia provocados por infracciones de umbrales definidos por el usuario, umbrales definidos por el sistema o umbrales dinámicos

De manera predeterminada, las alertas por correo electrónico se envían a los usuarios administradores de Unified Manager para todos los eventos nuevos. Es posible que se envíen alertas por correo electrónico a otros usuarios con la adición de las direcciones de correo electrónico de esos usuarios.



Para deshabilitar el envío de alertas para determinados tipos de eventos, debe desactivar todas las casillas de comprobación de una categoría de eventos. Esta acción no detiene que los eventos aparezcan en la interfaz de usuario.

### Pasos

1. En el panel de navegación izquierdo, seleccione **Administración de almacenamiento > Configuración de alertas**.

Aparecerá la página Configuración de alertas.

2. Haga clic en **Agregar** y configure los valores adecuados para cada uno de los tipos de evento.

Para que se envíen alertas de correo electrónico a varios usuarios, introduzca una coma entre cada dirección de correo electrónico.

3. Haga clic en **Guardar**.

### Identifique problemas de rendimiento en Active IQ Unified Manager

Si se produce un evento de rendimiento, puede localizar el origen del problema en Active IQ Unified Manager y utilizar otras herramientas para solucionarlo. Es posible que reciba una notificación por correo electrónico sobre un evento o que se lo notifique durante su supervisión diaria.

### Pasos

1. Haga clic en el enlace de la notificación por correo electrónico, que le llevará directamente al objeto de

almacenamiento que tiene un evento de rendimiento.

| Si...                                                        | Realice lo siguiente...                                                         |
|--------------------------------------------------------------|---------------------------------------------------------------------------------|
| Recibir una notificación por correo electrónico de un evento | Haga clic en el enlace para ir directamente a la página de detalles del evento. |
| Observe el evento mientras analiza la página Event Inventory | Seleccione el evento para ir directamente a la página de detalles del evento.   |

2. Si el evento ha superado un umbral definido por el sistema, siga las acciones sugeridas en la interfaz de usuario para solucionar el problema.
3. Si el evento ha superado un umbral definido por el usuario, analice el evento para determinar si necesita realizar alguna acción.
4. Si el problema persiste, compruebe los siguientes ajustes:
  - Configuración de protocolo en el sistema de almacenamiento
  - Ajustes de red en cualquier switch Ethernet o estructural
  - Ajustes de red en el sistema de almacenamiento
  - Distribución de discos y métricas agregadas en el sistema de almacenamiento
5. Si el problema persiste, póngase en contacto con el soporte técnico para obtener ayuda.

## Utilice el asesor digital de Active IQ para ver el rendimiento del sistema

En cualquier sistema ONTAP que envíe telemetría AutoSupport a NetApp, puede ver una gran cantidad de datos sobre rendimiento y capacidad. Active IQ muestra el rendimiento del sistema durante un período más largo de lo que se puede ver en System Manager.

Puede ver gráficos de la utilización de CPU, latencia, IOPS, IOPS por protocolo y rendimiento de la red. También puede descargar estos datos en formato .csv para analizarlos en otras herramientas.

Además de estos datos de rendimiento, Active IQ puede mostrarle eficiencia de almacenamiento por carga de trabajo y comparar esa eficiencia con la eficiencia esperada para ese tipo de carga de trabajo. Puede ver las tendencias de capacidad y calcular una estimación de la cantidad de almacenamiento adicional que puede necesitar añadir en un periodo de tiempo determinado.



- La eficiencia del almacenamiento está disponible a nivel del cliente, clúster y nodo en el lado izquierdo del panel principal.
- El rendimiento está disponible en el nivel del clúster y del nodo en el lado izquierdo del panel principal.

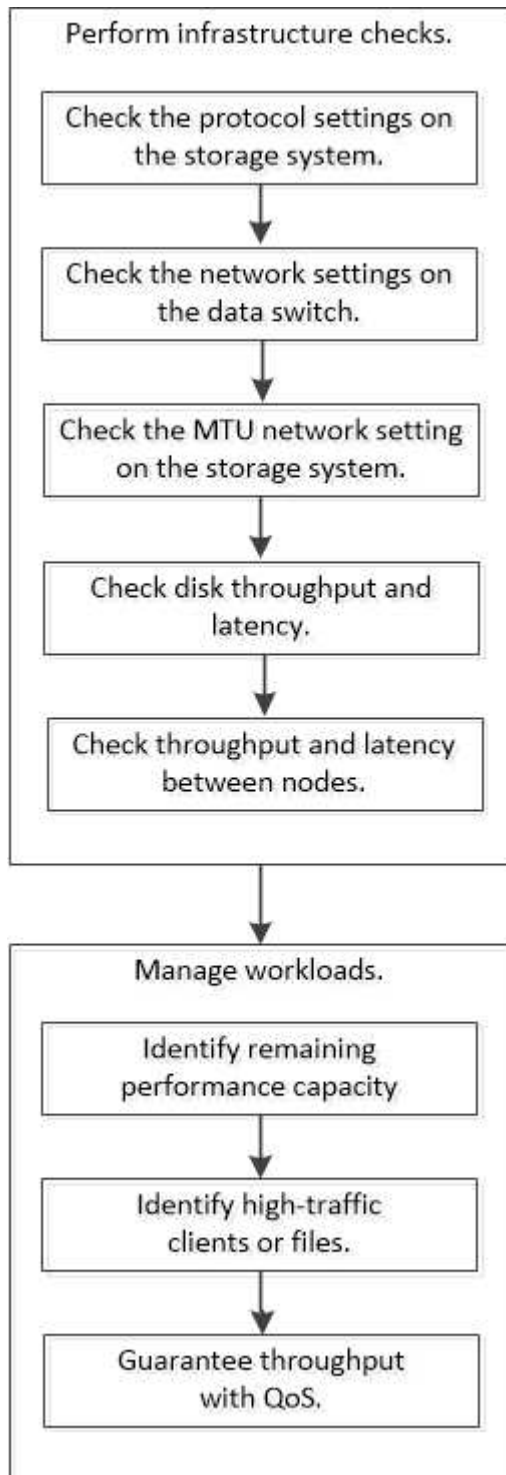
### Información relacionada

- ["Documentación del asesor digital de Active IQ"](#)
- ["Lista de reproducción de vídeo del asesor digital Active IQ"](#)
- ["Portal web de Active IQ"](#)

## Gestione los problemas de rendimiento

### Flujo de trabajo de gestión del rendimiento

Una vez identificado un problema de rendimiento, puede llevar a cabo algunas comprobaciones de diagnóstico básicas de la infraestructura para descartar errores evidentes de configuración. Si esas personas no identifican el problema, puede empezar a examinar problemas de gestión de la carga de trabajo.



## Realizar comprobaciones básicas de la infraestructura

Compruebe la configuración del protocolo en el sistema de almacenamiento

### Compruebe el tamaño máximo de transferencia de TCP de NFS

Para NFS, puede comprobar si el tamaño máximo de transferencia TCP para lecturas y escrituras puede estar provocando un problema de rendimiento. Si cree que el tamaño ralentiza el rendimiento, puede aumentarlo.

#### Lo que necesitará

- Para realizar esta tarea, debe tener privilegios de administrador de clúster.
- Para esta tarea, debe utilizar comandos de nivel de privilegio avanzado.

#### Pasos

1. Cambie al nivel de privilegio avanzado:

```
set -privilege advanced
```

2. Compruebe el tamaño máximo de transferencia TCP:

```
vserver nfs show -vserver vserver_name -instance
```

3. Si el tamaño máximo de transferencia del TCP es demasiado pequeño, aumente el tamaño:

```
vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer
```

4. Volver al nivel de privilegio administrativo:

```
set -privilege admin
```

#### Ejemplo

En el ejemplo siguiente se cambia el tamaño máximo de transferencia TCP de SVM1 a 1048576:

```
cluster1::*> vserver nfs modify -vserver SVM1 -tcp-max-xfer-size 1048576
```

### Compruebe el tamaño de lectura/escritura del TCP de iSCSI

Para iSCSI, es posible comprobar el tamaño de lectura/escritura de TCP para determinar si la configuración de tamaño está creando un problema de rendimiento. Si el tamaño es el origen de un problema, puede corregirlo.

#### Lo que necesitará

Para esta tarea, se requieren comandos de nivel de privilegio avanzado.

#### Pasos

1. Cambie al nivel de privilegio avanzado:

```
set -privilege advanced
```

## 2. Compruebe la configuración del tamaño de la ventana TCP:

```
vserver iscsi show -vserver,er vserver_name -instance
```

## 3. Modifique la configuración del tamaño de la ventana TCP:

```
vserver iscsi modify -vserver vserver_name -tcp-window-size integer
```

## 4. Devolver al privilegio administrativo:

```
set -privilege admin
```

### Ejemplo

En el ejemplo siguiente se cambia el tamaño de la ventana TCP de SVM1 a 131,400 bytes:

```
cluster1::*> vserver iscsi modify -vserver vs1 -tcp-window-size 131400
```

### Controlar los valores multiplexados CIFS

Si el rendimiento lento de la red CIFS provoca un problema de rendimiento, puede modificar los ajustes multiplexados para mejorarlos y corregirlos.

#### Pasos

##### 1. Controlar el reglaje multiplexado CIFS:

```
vserver cifs options show -vserver -vserver_name -instance
```

##### 2. Modificar el reglaje multiplexado CIFS:

```
vserver cifs options modify -vserver -vserver_name -max-mpx integer
```

### Ejemplo

En el ejemplo siguiente se modifica el recuento máximo de los multiplexados SVM1 a 255:

```
cluster1::> vserver cifs options modify -vserver SVM1 -max-mpx 255
```

### Compruebe la velocidad del puerto del adaptador de FC

La velocidad del puerto de destino del adaptador debe coincidir con la velocidad del dispositivo al que se conecta, para optimizar el rendimiento. Si el puerto está definido en autonegociación, puede tardar más en reconectar después de una toma de control y devolución u otra interrupción.

#### Lo que necesitará

Todos los LIF que utilizan este adaptador como puerto de inicio deben estar desconectados.

#### Pasos

1. Desconectar el adaptador:

```
network fcp adapter modify -node nodename -adapter adapter -state down
```

2. Compruebe la velocidad máxima del adaptador de puerto:

```
fcp adapter show -instance
```

3. Cambie la velocidad del puerto, si es necesario:

```
network fcp adapter modify -node nodename -adapter adapter -speed
{1|2|4|8|10|16|auto}
```

4. Conectar el adaptador:

```
network fcp adapter modify -node nodename -adapter adapter -state up
```

5. Conectar todas las LIF del adaptador:

```
network interface modify -vserver * -lif * { -home-node node1 -home-port e0c }
-status-admin up
```

### Ejemplo

En el ejemplo siguiente se cambia la velocidad del puerto del adaptador 0d encendido *node1* Hasta 2 Gbps:

```
cluster1::> network fcp adapter modify -node node1 -adapter 0d -speed 2
```

### Compruebe la configuración de red en los switches de datos

Aunque debe mantener la misma configuración MTU en los clientes, los servidores y los sistemas de almacenamiento (es decir, los extremos de red), los dispositivos de red intermedios como las NIC y los switches deben configurarse con sus valores máximos de MTU para garantizar que el rendimiento no se vea afectado.

Para obtener el mejor rendimiento, todos los componentes de la red deben ser capaces de reenviar tramas gigantes (IP de 9000 bytes, 9022 bytes incluyendo Ethernet). Los switches de datos deben establecerse en al menos 9022 bytes, pero es posible un valor típico de 9216 en la mayoría de los switches.

### Procedimiento

En el caso de los switches de datos, compruebe que el tamaño de MTU esté establecido en 9022 o superior.

Para obtener más información, consulte la documentación del proveedor de switches.

### Compruebe la configuración de red MTU en el sistema de almacenamiento

Puede cambiar la configuración de red en el sistema de almacenamiento si no son los mismos que en el cliente o en otros extremos de red. Mientras que la configuración de MTU de red de gestión se establece en 1500, el tamaño de MTU de red de datos debe ser de 9000.

## Acerca de esta tarea

Todos los puertos dentro de un dominio de retransmisión tienen el mismo tamaño de MTU, a excepción del puerto e0M que gestiona el tráfico de gestión. Si el puerto forma parte de un dominio de retransmisión, use el `broadcast-domain modify` Comando para cambiar la MTU de todos los puertos dentro del dominio de retransmisión modificado.

Tenga en cuenta que los dispositivos de red intermedios, como NIC y switches de datos, se pueden establecer con tamaños de MTU superiores a los extremos de red. Para obtener más información, consulte ["Compruebe la configuración de red en los switches de datos"](#).

## Pasos

1. Compruebe la configuración de puerto MTU en el sistema de almacenamiento:

```
network port show -instance
```

2. Cambie la MTU en el dominio de retransmisión que utilizan los puertos:

```
network port broadcast-domain modify -ipspace ipspace -broadcast-domain
broadcast_domain -mtu new_mtu
```

## Ejemplo

En el ejemplo siguiente se cambia la configuración de puerto MTU a 9000:

```
network port broadcast-domain modify -ipspace Cluster -broadcast-domain
Cluster -mtu 9000
```

## Comprobar el rendimiento del disco y la latencia

Puede comprobar las métricas de rendimiento de disco y latencia para los nodos del clúster para ayudarle a resolver problemas.

## Acerca de esta tarea

Para esta tarea, se requieren comandos de nivel de privilegio avanzado.

## Pasos

1. Cambie al nivel de privilegio avanzado:

```
set -privilege advanced
```

2. Compruebe las métricas de rendimiento y latencia del disco:

```
statistics disk show -sort-key latency
```

## Ejemplo

En el siguiente ejemplo se muestran los totales de cada operación de lectura o escritura de usuario para `node2` encendido `cluster1`:



```
::*> statistics disk show -sort-key latency
cluster1 : 8/24/2015 12:44:15
```

| Disk    | Node  | Busy (%) | Total Ops | Read Ops | Write Ops | Read (Bps) | Write (Bps) | *Latency (us) |
|---------|-------|----------|-----------|----------|-----------|------------|-------------|---------------|
| 1.10.20 | node2 | 4        | 5         | 3        | 2         | 95232      | 367616      | 23806         |
| 1.10.8  | node2 | 4        | 5         | 3        | 2         | 138240     | 386048      | 22113         |
| 1.10.6  | node2 | 3        | 4         | 2        | 2         | 48128      | 371712      | 19113         |
| 1.10.19 | node2 | 4        | 6         | 3        | 2         | 102400     | 443392      | 19106         |
| 1.10.11 | node2 | 4        | 4         | 2        | 2         | 122880     | 408576      | 17713         |

### Compruebe el rendimiento y la latencia entre los nodos

Puede utilizar el `network test-path` comando para identificar cuellos de botella de red o para precalificar las rutas de red entre los nodos. Se puede ejecutar el comando entre nodos de interconexión de clústeres o nodos dentro del clúster.

#### Lo que necesitará

- Para realizar esta tarea, debe ser un administrador de clústeres.
- Para esta tarea, se requieren comandos de nivel de privilegio avanzado.
- En el caso de una ruta de interconexión de clústeres, los clústeres de origen y destino deben tener una relación entre iguales.

#### Acerca de esta tarea

En ocasiones, es posible que el rendimiento de red entre nodos no cumpla las expectativas de la configuración de la ruta. Por ejemplo, una tasa de transmisión de 1 Gbps para el tipo de transferencias de datos grandes que se ven en operaciones de replicación de SnapMirror no sería coherente con un enlace de 10 GbE entre los clústeres de origen y destino.

Puede utilizar el `network test-path` comando para medir el rendimiento y la latencia entre nodos. Se puede ejecutar el comando entre nodos de interconexión de clústeres o nodos dentro del clúster.



La prueba satura la ruta de red con los datos, de modo que debe ejecutar el comando cuando el sistema no está ocupado y cuando el tráfico de red entre nodos no es excesivo. El tiempo de prueba se agota al cabo de diez segundos. El comando se puede ejecutar solo entre nodos de ONTAP 9.

La `session-type` Option identifica el tipo de operación que se ejecuta en la ruta de red, por ejemplo, "AsyncMirrorRemote" para la replicación de SnapMirror en un destino remoto. El tipo determina la cantidad de datos utilizados en la prueba. En la siguiente tabla se definen los tipos de sesión:

| Tipo de sesión | Descripción |
|----------------|-------------|
|----------------|-------------|

|                    |                                                                                                                                                                                                              |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AsyncMirrorLocal   | Configuración que utiliza SnapMirror entre nodos del mismo clúster                                                                                                                                           |
| AsyncMirrorRemote  | Configuración que utiliza SnapMirror entre nodos de diferentes clústeres (tipo predeterminado)                                                                                                               |
| RemoteDataTransfer | La configuración que utiliza ONTAP para acceder de forma remota a datos entre nodos del mismo clúster (por ejemplo, una solicitud NFS a un nodo de un archivo almacenado en un volumen en un nodo diferente) |

## Pasos

1. Cambie al nivel de privilegio avanzado:

```
set -privilege advanced
```

2. Mida el rendimiento y la latencia entre nodos:

```
network test-path -source-node source_nodename |local -destination-cluster
destination_clustername -destination-node destination_nodename -session-type
Default|AsyncMirrorLocal|AsyncMirrorRemote|SyncMirrorRemote|RemoteDataTransfer
```

El nodo de origen debe estar en el clúster local. El nodo de destino puede estar en el clúster local o en un clúster con una relación entre iguales. Valor "local" para `-source-node` especifica el nodo en el que está ejecutando el comando.

El siguiente comando mide el rendimiento y la latencia de las operaciones de replicación del tipo SnapMirror entre `node1` en el clúster local y `node3` encendido `cluster2`:

```
cluster1::> network test-path -source-node node1 -destination-cluster
cluster2 -destination-node node3 -session-type AsyncMirrorRemote
Test Duration: 10.88 secs
Send Throughput: 18.23 MB/sec
Receive Throughput: 18.23 MB/sec
MB sent: 198.31
MB received: 198.31
Avg latency in ms: 2301.47
Min latency in ms: 61.14
Max latency in ms: 3056.86
```

3. Devolver al privilegio administrativo:

```
set -privilege admin
```

## Después de terminar

Si el rendimiento no cumple las expectativas de configuración de la ruta, debe comprobar las estadísticas de rendimiento del nodo, utilizar las herramientas disponibles para aislar el problema en la red, comprobar la

configuración del switch, etc.

## Gestionar cargas de trabajo

### Identifique la capacidad de rendimiento restante

La capacidad de rendimiento, o *margen adicional*, mide la cantidad de trabajo que se puede realizar en un nodo o en un agregado antes de que el rendimiento de las cargas de trabajo del recurso comience a verse afectado por la latencia. Saber que la capacidad de rendimiento disponible en el clúster le ayuda a aprovisionar y equilibrar las cargas de trabajo.

### Lo que necesitará

Para esta tarea, se requieren comandos de nivel de privilegio avanzado.

### Acerca de esta tarea

Puede usar los siguientes valores para el `-object` opción de recopilar y mostrar estadísticas de margen adicional:

- Para CPU, `resource_headroom_cpu`.
- Para agregados, `resource_headroom_aggr`.

También puede completar esta tarea mediante System Manager y Active IQ Unified Manager.

### Pasos

1. Cambie al nivel de privilegio avanzado:

```
set -privilege advanced
```

2. Inicie la recopilación de estadísticas de margen en tiempo real:

```
statistics start -object resource_headroom_cpu|aggr
```

Para obtener una sintaxis de comando completa, consulte la página [man](#).

3. Mostrar información de estadísticas de margen adicional en tiempo real:

```
statistics show -object resource_headroom_cpu|aggr
```

Para obtener una sintaxis de comando completa, consulte la página [man](#).

4. Devolver al privilegio administrativo:

```
set -privilege admin
```

### Ejemplo

En el siguiente ejemplo, se muestran las estadísticas de margen adicional medio por hora para los nodos del clúster.

Puede calcular la capacidad de rendimiento disponible para un nodo restando el `current_utilization` en el contador de `optimal_point_utilization` contador. En este ejemplo, la capacidad de utilización para

CPU\_sti2520-213 Es de -14% (72%-86%), lo que sugiere que la CPU ha sido sobreutilizada de media durante la última hora.

Podría haber especificado ewma\_daily, ewma\_weekly, o ewma\_monthly obtener la misma información promediada en periodos de tiempo más largos.

```
sti2520-2131454963690::*> statistics show -object resource_headroom_cpu
-raw -counter ewma_hourly
(statistics show)

Object: resource_headroom_cpu
Instance: CPU_sti2520-213
Start-time: 2/9/2016 16:06:27
End-time: 2/9/2016 16:06:27
Scope: sti2520-213
```

| Counter                         | Value |
|---------------------------------|-------|
| ewma_hourly                     | -     |
| current_ops                     | 4376  |
| current_latency                 | 37719 |
| current_utilization             | 86    |
| optimal_point_ops               | 2573  |
| optimal_point_latency           | 3589  |
| optimal_point_utilization       | 72    |
| optimal_point_confidence_factor | 1     |

```
Object: resource_headroom_cpu
Instance: CPU_sti2520-214
Start-time: 2/9/2016 16:06:27
End-time: 2/9/2016 16:06:27
Scope: sti2520-214
```

| Counter                         | Value |
|---------------------------------|-------|
| ewma_hourly                     | -     |
| current_ops                     | 0     |
| current_latency                 | 0     |
| current_utilization             | 0     |
| optimal_point_ops               | 0     |
| optimal_point_latency           | 0     |
| optimal_point_utilization       | 71    |
| optimal_point_confidence_factor | 1     |

```
2 entries were displayed.
```

**Identifique los ficheros o clientes de alto tráfico**

Puede utilizar la tecnología ONTAP Active Objects para identificar clientes o archivos que son responsables de una cantidad desproporcionadamente grande del tráfico del clúster. Cuando haya identificado estos archivos o clientes «principales», podrá reequilibrar las cargas de trabajo del clúster o realizar otros pasos para resolver el problema.

**Lo que necesitará**

Para realizar esta tarea, debe ser un administrador de clústeres.

**Pasos**

- 1. Vea los principales clientes que acceden al clúster:

```
statistics top client show -node node_name -sort-key sort_column -interval
seconds_between_updates -iterations iterations -max number_of_instances
```

Para obtener una sintaxis de comando completa, consulte la página man.

El siguiente comando muestra los principales clientes que acceden cluster1:

```
cluster1::> statistics top client show

cluster1 : 3/23/2016 17:59:10
```

| Client         | Vserver | Node         | Protocol | *Total<br>Ops |
|----------------|---------|--------------|----------|---------------|
| 172.17.180.170 | vs4     | siderop1-vs4 | nfs      | 668           |
| 172.17.180.169 | vs3     | siderop1-vs3 | nfs      | 337           |
| 172.17.180.171 | vs3     | siderop1-vs3 | nfs      | 142           |
| 172.17.180.170 | vs3     | siderop1-vs3 | nfs      | 137           |
| 172.17.180.123 | vs3     | siderop1-vs3 | nfs      | 137           |
| 172.17.180.171 | vs4     | siderop1-vs4 | nfs      | 95            |
| 172.17.180.169 | vs4     | siderop1-vs4 | nfs      | 92            |
| 172.17.180.123 | vs4     | siderop1-vs4 | nfs      | 92            |
| 172.17.180.153 | vs3     | siderop1-vs3 | nfs      | 0             |

- 2. Vea los archivos principales a los que se accede en el clúster:

```
statistics top file show -node node_name -sort-key sort_column -interval
seconds_between_updates -iterations iterations -max number_of_instances
```

Para obtener una sintaxis de comando completa, consulte la página man.

El siguiente comando muestra los principales archivos en los que se puede acceder cluster1:

```
cluster1::> statistics top file show
```

```
cluster1 : 3/23/2016 17:59:10
```

|                          |       |        | *Total         |       |       |
|--------------------------|-------|--------|----------------|-------|-------|
|                          | File  | Volume | Vserver        | Node  | Ops   |
| -----                    | ----- | -----  | -----          | ----- | ----- |
| /vol/vol1/vm170-read.dat | vol1  | vs4    | siderop1-vsim4 | 22    |       |
| /vol/vol1/vm69-write.dat | vol1  | vs3    | siderop1-vsim3 | 6     |       |
| /vol/vol2/vm171.dat      | vol2  | vs3    | siderop1-vsim3 | 2     |       |
| /vol/vol2/vm169.dat      | vol2  | vs3    | siderop1-vsim3 | 2     |       |
| /vol/vol2/p123.dat       | vol2  | vs4    | siderop1-vsim4 | 2     |       |
| /vol/vol2/p123.dat       | vol2  | vs3    | siderop1-vsim3 | 2     |       |
| /vol/vol1/vm171.dat      | vol1  | vs4    | siderop1-vsim4 | 2     |       |
| /vol/vol1/vm169.dat      | vol1  | vs4    | siderop1-vsim4 | 2     |       |
| /vol/vol1/vm169.dat      | vol1  | vs4    | siderop1-vsim3 | 2     |       |
| /vol/vol1/p123.dat       | vol1  | vs4    | siderop1-vsim4 | 2     |       |

#### Garantice el rendimiento con calidad de servicio

#### Garantice el rendimiento con información general de calidad de servicio

Puede utilizar calidad de servicio del almacenamiento para garantizar que el rendimiento de las cargas de trabajo críticas no se vea degradado por cargas de trabajo de la competencia. Puede establecer un rendimiento *plaft* en una carga de trabajo en competencia para limitar su impacto en los recursos del sistema o establecer un rendimiento *floor* para una carga de trabajo crítica, garantizando que cumple los objetivos de rendimiento mínimos, sin importar la demanda de otras cargas de trabajo de la competencia. Puede incluso fijar un techo y un suelo para la misma carga de trabajo.

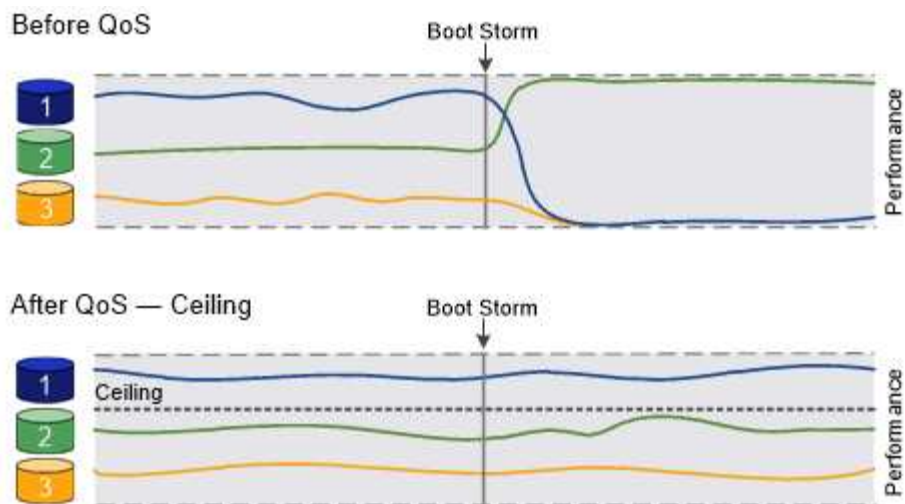
#### Acerca de los techos de rendimiento (QoS máx.)

Un techo de rendimiento limita el rendimiento de una carga de trabajo a un número máximo de IOPS o Mbps, o IOPS y Mbps. En la siguiente figura, el máximo rendimiento de la carga de trabajo 2 garantiza que no "intimida" las cargas de trabajo 1 y 3.

Un *policy group* define el techo de rendimiento de una o más cargas de trabajo. Una carga de trabajo representa las operaciones de I/O para un objeto *Storage*: un volumen, un archivo, un qtree o una LUN o todos los volúmenes, archivos, qtrees o LUN de una SVM. Puede especificar el techo al crear el grupo de políticas, o bien se puede esperar hasta después de supervisar las cargas de trabajo para especificarlo.



El rendimiento en las cargas de trabajo puede superar el límite máximo especificado hasta en un 10 %, especialmente si una carga de trabajo experimenta cambios rápidos en el rendimiento. El techo podría ser superado en hasta un 50% para manejar las ráfagas. Las ráfagas se producen en nodos únicos cuando los tokens se acumulan hasta un 150 %



### Acerca de los pisos de rendimiento (calidad de servicio mínima)

Un nivel de rendimiento garantiza que el rendimiento de una carga de trabajo no caiga por debajo del número mínimo de IOPS o MBps, ni de IOPS y MBps. En la siguiente figura, los pisos de rendimiento de la carga de trabajo 1 y la carga de trabajo 3 garantizan que cumplen los objetivos de rendimiento mínimos, sin importar la demanda por carga de trabajo 2.



Tal y como sugieren los ejemplos, un límite máximo de rendimiento limita el rendimiento directamente. Un entorno de rendimiento limita el rendimiento de forma indirecta, al dar prioridad a las cargas de trabajo para las que se ha establecido un piso.

Puede especificar la planta al crear el grupo de políticas, o bien esperar hasta que supervise las cargas de trabajo para especificarlas.

A partir de ONTAP 9.13.1, se pueden establecer pisos de rendimiento en el ámbito de SVM con [\[adaptive-qos-templates\]](#). En versiones de ONTAP anteriores a 9.13.1, no puede aplicarse a una SVM un grupo de políticas que define un piso de rendimiento.



En las versiones anteriores a ONTAP 9.7, se garantizan pisos de rendimiento cuando hay suficiente capacidad de rendimiento disponible.

En ONTAP 9.7 y versiones posteriores, se puede garantizar el uso de suelos de rendimiento incluso cuando la capacidad de rendimiento no sea suficiente. Este nuevo comportamiento del suelo se llama pisos v2. Para cumplir las garantías, el segundo plano puede generar una mayor latencia en las cargas de trabajo sin tener que pasar por una planta de rendimiento o en el trabajo que supere la configuración inicial. Floors v2 se aplica tanto a QoS como a QoS adaptativo.

La opción de habilitar/deshabilitar el nuevo comportamiento de los pisos v2 está disponible en ONTAP 9.7P6 y posteriores. Una carga de trabajo puede quedar por debajo del piso especificado durante operaciones cruciales como `volume move trigger-cutover`. Incluso cuando haya suficiente capacidad disponible y no se realicen operaciones críticas, el rendimiento de una carga de trabajo puede quedar por debajo del nivel especificado hasta un 5 %. Si se sobreaprovisiona la tasa de suelos y no hay capacidad de rendimiento, es posible que algunas cargas de trabajo se encuentren por debajo de la superficie especificada.



### Acerca de los grupos de políticas de calidad de servicio compartidos y no compartidos

A partir de ONTAP 9.4, puede usar un grupo de políticas *no compartido* QoS para especificar que el techo o el piso de rendimiento definidos se apliquen a la carga de trabajo de cada miembro de manera individual. El comportamiento de los grupos de directivas *shared* depende del tipo de directiva:

- Para los techos de rendimiento, el rendimiento total de las cargas de trabajo asignadas al grupo de políticas compartidas no puede exceder el techo especificado.
- En los pisos de rendimiento, el grupo de políticas compartidas puede aplicarse únicamente a una única carga de trabajo.

### Acerca de la calidad de servicio adaptativa

Por lo general, el valor del grupo de políticas que asigna a un objeto de almacenamiento es fijo. Es necesario cambiar el valor de forma manual cuando cambia el tamaño del objeto de almacenamiento. Por ejemplo, un aumento de la cantidad de espacio utilizado en un volumen requiere, por lo general, un aumento correspondiente en el techo de rendimiento especificado para el volumen.

*Adaptive QoS* escala automáticamente el valor del grupo de políticas al tamaño de la carga de trabajo, y mantiene la ratio de IOPS en TB|GB a medida que cambia el tamaño de la carga de trabajo. Esto es una ventaja importante si gestiona cientos o miles de cargas de trabajo en una puesta en marcha grande.

Normalmente, la calidad de servicio adaptativa se puede utilizar para ajustar los techos de rendimiento, pero también para gestionar el uso de pisos de rendimiento (cuando aumenta el tamaño de la carga de trabajo). El tamaño de la carga de trabajo se expresa como el espacio asignado para el objeto de almacenamiento o el espacio utilizado por el objeto de almacenamiento.



El espacio usado está disponible para pisos de rendimiento en ONTAP 9.5 y versiones posteriores. No se admite para pisos de rendimiento en ONTAP 9.4 y versiones anteriores.

- Una política de *espacio* mantiene la ratio de IOPS/TB|GB según el tamaño nominal del objeto de almacenamiento. Si la relación es de 100 IOPS/GB, un volumen de 150 GB tendrá un techo de rendimiento de 15,000 IOPS mientras el volumen siga siendo de ese tamaño. Si el tamaño del volumen cambia a 300 GB, la calidad de servicio adaptativa ajusta el techo de rendimiento a 30,000 IOPS.
- Una política de *space* utilizada (predeterminada) mantiene la relación IOPS/TB|GB según la cantidad de datos reales almacenados antes de las eficiencias de almacenamiento. Si la relación es de 100 IOPS/GB, un volumen de 150 GB que tiene 100 GB de datos almacenados tendría un límite máximo de rendimiento de 10,000 IOPS. A medida que cambia la cantidad de espacio usado, la calidad de servicio adaptativa



ajusta el techo de rendimiento en función de la ratio.

A partir de ONTAP 9.5, es posible especificar un tamaño de bloque de I/O para su aplicación que permite expresar un límite de rendimiento tanto en IOPS como en Mbps. El límite de Mbps se calcula a partir del tamaño de bloque multiplicado por el límite de IOPS. Por ejemplo, un tamaño de bloque de I/O de 32 KB para un límite de IOPS de 6144 IOPS/TB proporciona un límite de Mbps de 192 MBps.

Puede esperar el siguiente comportamiento tanto para techos de rendimiento como para pisos:

- Cuando una carga de trabajo se asigna a un grupo de políticas de calidad de servicio adaptativa, el techo o el piso se actualizan de inmediato.
- Cuando se cambia el tamaño de una carga de trabajo de un grupo de políticas de calidad de servicio adaptativa, el techo o el piso se actualizan en aproximadamente cinco minutos.

El rendimiento debe aumentar al menos en 10 000 IOPS antes de que se produzca la actualización.

Los grupos de políticas de calidad de servicio adaptativos siempre no son compartidos: El techo o el piso de rendimiento definidos se aplican a la carga de trabajo de cada miembro de forma individual.

A partir de ONTAP 9,6, los pisos de rendimiento son compatibles con ONTAP Select Premium con SSD.

### Plantilla de grupo de políticas adaptativas

A partir de ONTAP 9.13.1, puede establecer una plantilla de calidad de servicio adaptativa en una SVM. Las plantillas de grupos de políticas adaptativas permiten establecer pisos y techos de rendimiento para todos los volúmenes de una SVM.

Las plantillas de grupos de políticas adaptativas solo pueden establecerse después de crear la SVM. Utilice la `vserver modify` con el `-qos-adaptive-policy-group-template` parámetro para establecer la política.

Cuando establece una plantilla de grupo de políticas adaptativas, los volúmenes creados o migrados después de configurar la política heredan automáticamente la política. Los volúmenes que existan en la SVM no se ven afectados al asignar la plantilla de políticas. Si deshabilita la política en la SVM, todos los volúmenes posteriores migrados o creados en la SVM no recibirán la política. La desactivación de la plantilla de grupo de políticas adaptativas no afecta a los volúmenes que han heredado la plantilla de políticas, ya que conservan la plantilla de políticas.

Para obtener más información, consulte [Defina una plantilla de grupo de políticas adaptativas](#).

### Apoyo general

En la siguiente tabla se muestran las diferencias en compatibilidad con los techos de rendimiento, pisos de rendimiento y calidad de servicio adaptativa.

| Recurso o característica | Techo de rendimiento | Piso de rendimiento | Piso de salida v2 | Calidad de servicio adaptativa |
|--------------------------|----------------------|---------------------|-------------------|--------------------------------|
| Versión de ONTAP 9       | Todo                 | 9,2 y posterior     | 9,7 y posterior   | 9,3 y posterior                |

| Recurso o característica | Techo de rendimiento | Piso de rendimiento                                                                                                 | Piso de salida v2                                                                                               | Calidad de servicio adaptativa |
|--------------------------|----------------------|---------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|--------------------------------|
| Plataformas              | Todo                 | <ul style="list-style-type: none"> <li>• AFF</li> <li>• C190 *</li> <li>• ONTAP Select premium con SSD *</li> </ul> | <ul style="list-style-type: none"> <li>• AFF</li> <li>• C190</li> <li>• ONTAP Select premium con SSD</li> </ul> | Todo                           |
| Protocolos               | Todo                 | Todo                                                                                                                | Todo                                                                                                            | Todo                           |
| FabricPool               | Sí                   | Sí, si la política de organización en niveles está establecida en "ninguna" y no hay bloques en el cloud.           | Sí, si la política de organización en niveles está establecida en "ninguna" y no hay bloques en el cloud.       | No                             |
| SnapMirror síncrono      | Sí                   | No                                                                                                                  | No                                                                                                              | Sí                             |

La compatibilidad con C190 y ONTAP Select comenzó con la versión 9,6 de ONTAP.

### Cargas de trabajo compatibles con techos de rendimiento

En la siguiente tabla se muestra compatibilidad con cargas de trabajo para techos de rendimiento con la versión ONTAP 9. No se admiten los volúmenes raíz, los reflejos con uso compartido de carga y los reflejos de protección de datos.

| Soporte de carga de trabajo: Techo | ONTAP 9,0 | ONTAP 9,1 | ONTAP 9,2 | ONTAP 9,3 | ONTAP 9,4 - 9,7 | ONTAP 9,8 y versiones posteriores |
|------------------------------------|-----------|-----------|-----------|-----------|-----------------|-----------------------------------|
| Volumen                            | sí        | sí        | sí        | sí        | sí              | sí                                |
| Archivo                            | sí        | sí        | sí        | sí        | sí              | sí                                |
| LUN                                | sí        | sí        | sí        | sí        | sí              | sí                                |
| SVM                                | sí        | sí        | sí        | sí        | sí              | sí                                |
| Volumen FlexGroup                  | no        | no        | no        | sí        | sí              | sí                                |
| qtrees*                            | no        | no        | no        | no        | no              | sí                                |

| <b>Soporte de carga de trabajo: Techo</b>       | <b>ONTAP 9,0</b> | <b>ONTAP 9,1</b> | <b>ONTAP 9,2</b> | <b>ONTAP 9,3</b> | <b>ONTAP 9,4 - 9,7</b> | <b>ONTAP 9,8 y versiones posteriores</b> |
|-------------------------------------------------|------------------|------------------|------------------|------------------|------------------------|------------------------------------------|
| Varias cargas de trabajo por grupo de políticas | sí               | sí               | sí               | sí               | sí                     | sí                                       |
| Grupos de políticas no compartidos              | no               | no               | no               | no               | sí                     | sí                                       |

A partir de ONTAP 9,8, el acceso NFS es compatible con qtrees en volúmenes FlexVol y FlexGroup con NFS habilitado. A partir de ONTAP 9.9.1, también se admite el acceso SMB en qtrees de volúmenes FlexVol y FlexGroup con SMB habilitado.

### **Cargas de trabajo admitidas para el nivel de rendimiento**

En la siguiente tabla se muestra la compatibilidad con cargas de trabajo para pisos de rendimiento en la versión de ONTAP 9. No se admiten los volúmenes raíz, los reflejos con uso compartido de carga y los reflejos de protección de datos.

| <b>Soporte de cargas de trabajo: Suelo</b>      | <b>ONTAP 9,2</b> | <b>ONTAP 9,3</b> | <b>ONTAP 9,4 - 9,7</b> | <b>ONTAP 9,8 - 9.13.0</b> | <b>ONTAP 9.13.1 y versiones posteriores</b> |
|-------------------------------------------------|------------------|------------------|------------------------|---------------------------|---------------------------------------------|
| Volumen                                         | sí               | sí               | sí                     | sí                        | sí                                          |
| Archivo                                         | no               | sí               | sí                     | sí                        | sí                                          |
| LUN                                             | sí               | sí               | sí                     | sí                        | sí                                          |
| SVM                                             | no               | no               | no                     | no                        | sí                                          |
| Volumen FlexGroup                               | no               | no               | sí                     | sí                        | sí                                          |
| qtrees *                                        | no               | no               | no                     | sí                        | sí                                          |
| Varias cargas de trabajo por grupo de políticas | no               | no               | sí                     | sí                        | sí                                          |
| Grupos de políticas no compartidos              | no               | no               | sí                     | sí                        | sí                                          |

\\*A partir de ONTAP 9,8, el acceso NFS es compatible con qtrees en volúmenes FlexVol y FlexGroup con NFS habilitado. A partir de ONTAP 9.9.1, también se admite el acceso SMB en qtrees de volúmenes FlexVol y FlexGroup con SMB habilitado.

## Cargas de trabajo compatibles para calidad de servicio adaptable

En la siguiente tabla se muestra la compatibilidad con las cargas de trabajo para la calidad de servicio adaptativa según la versión de ONTAP 9. No se admiten los volúmenes raíz, los reflejos con uso compartido de carga y los reflejos de protección de datos.

| Compatibilidad con cargas de trabajo: Calidad de servicio adaptable | ONTAP 9,3 | ONTAP 9,4 - 9.13.0 | ONTAP 9.13.1 y versiones posteriores |
|---------------------------------------------------------------------|-----------|--------------------|--------------------------------------|
| Volumen                                                             | sí        | sí                 | sí                                   |
| Archivo                                                             | no        | sí                 | sí                                   |
| LUN                                                                 | no        | sí                 | sí                                   |
| SVM                                                                 | no        | no                 | sí                                   |
| Volumen FlexGroup                                                   | no        | sí                 | sí                                   |
| Varias cargas de trabajo por grupo de políticas                     | sí        | sí                 | sí                                   |
| Grupos de políticas no compartidos                                  | sí        | sí                 | sí                                   |

## El número máximo de cargas de trabajo y grupos de políticas

En la siguiente tabla se muestra el número máximo de cargas de trabajo y grupos de políticas en la versión de ONTAP 9.

| Compatibilidad con cargas de trabajo        | ONTAP 9,3 y anteriores | ONTAP 9,4 y versiones posteriores |
|---------------------------------------------|------------------------|-----------------------------------|
| Cargas de trabajo máximas por clúster       | 12.000                 | 40.000                            |
| Número máximo de cargas de trabajo por nodo | 12.000                 | 40.000                            |
| Número máximo de grupos de políticas        | 12.000                 | 12.000                            |

## Habilite o deshabilite pisos de salida v2

Puede habilitar o deshabilitar las plantas de procesamiento v2 en AFF. El valor predeterminado es Enabled. Con el suelo v2 habilitado, se pueden cumplir los pisos de rendimiento cuando se utilizan en gran medida las controladoras a expensas de una mayor latencia en otras cargas de trabajo. Floors v2 se aplica tanto a QoS como a Adaptive QoS.

### Pasos

1. Cambie al nivel de privilegio avanzado:

```
set -privilege advanced
```

2. Escriba uno de los siguientes comandos:

| Si desea...         | Utilizar este comando:                                       |
|---------------------|--------------------------------------------------------------|
| Desactivar pisos v2 | <code>qos settings throughput-floors-v2 -enable false</code> |
| Habilitar pisos v2  | <code>qos settings throughput-floors-v2 -enable true</code>  |



Para deshabilitar los pisos de procesamiento v2 en un clúster de MetroCluster, debe ejecutar la

```
qos settings throughput-floors-v2 -enable false
```

comando en los clústeres de origen y destino.

```
cluster1::*> qos settings throughput-floors-v2 -enable false
```

## Flujo de trabajo de calidad de servicio del almacenamiento

Si ya conoce los requisitos de rendimiento de las cargas de trabajo que desea gestionar con calidad de servicio, puede especificar el límite de rendimiento al crear el grupo de políticas. De lo contrario, puede esperar hasta que supervise las cargas de trabajo para especificar el límite.

### Establezca el límite máximo de rendimiento con calidad de servicio

Puede utilizar el `max-throughput` Campo para un grupo de políticas a fin de definir un techo de rendimiento para las cargas de trabajo de objetos de almacenamiento (QoS máx.). Puede aplicar el grupo de políticas cuando crea o modifica el objeto de almacenamiento.

#### Lo que necesitará

- Para crear un grupo de políticas, debe ser un administrador de clústeres.
- Para aplicar un grupo de políticas a una SVM, debe ser un administrador de clústeres.

#### Acerca de esta tarea

- A partir de ONTAP 9.4, puede usar un grupo de políticas *no compartido* QoS para especificar que el techo de rendimiento definido se aplique a la carga de trabajo de cada miembro de forma individual. De lo contrario, el grupo de políticas es *shared*: el rendimiento total de las cargas de trabajo asignadas al grupo de políticas no puede superar el límite máximo especificado.

Configurado `-is-shared=false` para la `qos policy-group create` comando para especificar un

grupo de políticas no compartido.

- Puede especificar el límite de rendimiento para el límite máximo en IOPS, MB/s o IOPS, MB/s. Si especifica tanto IOPS como MB/s, se aplicará el límite alcanzado primero.



Si establece un techo y un piso para la misma carga de trabajo, puede especificar el límite de rendimiento para el techo solo en IOPS.

- Un objeto de almacenamiento sujeto a un límite de calidad de servicio debe ser contenido por la SVM a la que pertenece el grupo de políticas. Pueden pertenecer varios grupos de políticas a la misma SVM.
- No puede asignar un objeto de almacenamiento a un grupo de políticas si su objeto que contiene o sus objetos secundarios pertenecen al grupo de políticas.
- Es una práctica recomendada de la calidad de servicio aplicar un grupo de políticas al mismo tipo de objetos de almacenamiento.

## Pasos

1. Cree un grupo de políticas:

```
qos policy-group create -policy-group policy_group -vserver SVM -max-throughput number_of_iops|Mb/S|iops,Mb/S -is-shared true|false
```

Para obtener una sintaxis de comando completa, consulte la página man. Puede utilizar el `qos policy-group modify` comando para ajustar los techos de rendimiento.

El siguiente comando crea el grupo de políticas compartidas `pg-vs1` Con un rendimiento máximo de 5,000 IOPS:

```
cluster1::> qos policy-group create -policy-group pg-vs1 -vserver vs1 -max-throughput 5000iops -is-shared true
```

El siguiente comando crea el grupo de políticas no compartido `pg-vs3` Con un rendimiento máximo de 100 000 IOPS y 400 Kb/s:

```
cluster1::> qos policy-group create -policy-group pg-vs3 -vserver vs3 -max-throughput 100iops,400KB/s -is-shared false
```

El siguiente comando crea el grupo de políticas no compartido `pg-vs4` sin límite de rendimiento:

```
cluster1::> qos policy-group create -policy-group pg-vs4 -vserver vs4 -is-shared false
```

2. Aplique un grupo de políticas a una SVM, un archivo, un volumen o una LUN:

```
storage_object create -vserver SVM -qos-policy-group policy_group
```

Para obtener una sintaxis de comando completa, consulte las páginas man. Puede utilizar el `storage_object modify` comando para aplicar un grupo de políticas diferente al objeto de

almacenamiento.

El siguiente comando aplica un grupo de políticas `pg-vs1` A SVM `vs1`:

```
cluster1::> vserver create -vserver vs1 -qos-policy-group pg-vs1
```

Los siguientes comandos aplican grupo de políticas `pg-app` a los volúmenes `app1` y.. `app2`:

```
cluster1::> volume create -vserver vs2 -volume app1 -aggregate aggr1
-qos-policy-group pg-app
```

```
cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr1
-qos-policy-group pg-app
```

### 3. Supervise el rendimiento del grupo de políticas:

```
qos statistics performance show
```

Para obtener una sintaxis de comando completa, consulte la página [man](#).



Supervise el rendimiento desde el clúster. No utilice una herramienta en el host para supervisar el rendimiento.

El siguiente comando muestra el rendimiento del grupo de políticas:

```
cluster1::> qos statistics performance show
```

| Policy Group        | IOPS  | Throughput | Latency   |
|---------------------|-------|------------|-----------|
| -total-             | 12316 | 47.76MB/s  | 1264.00us |
| pg_vs1              | 5008  | 19.56MB/s  | 2.45ms    |
| _System-Best-Effort | 62    | 13.36KB/s  | 4.13ms    |
| _System-Background  | 30    | 0KB/s      | 0ms       |

### 4. Supervisar el rendimiento de la carga de trabajo:

```
qos statistics workload performance show
```

Para obtener una sintaxis de comando completa, consulte la página [man](#).



Supervise el rendimiento desde el clúster. No utilice una herramienta en el host para supervisar el rendimiento.

El siguiente comando muestra el rendimiento de la carga de trabajo:

```
cluster1::> qos statistics workload performance show
```

| Workload        | ID    | IOPS  | Throughput | Latency   |
|-----------------|-------|-------|------------|-----------|
| -total-         | -     | 12320 | 47.84MB/s  | 1215.00us |
| app1-wid7967    | 7967  | 7219  | 28.20MB/s  | 319.00us  |
| vs1-wid12279    | 12279 | 5026  | 19.63MB/s  | 2.52ms    |
| _USERSPACE_APPS | 14    | 55    | 10.92KB/s  | 236.00us  |
| _Scan_Backgro.. | 5688  | 20    | 0KB/s      | 0ms       |



Puede utilizar el `qos statistics workload latency show` Comando para ver estadísticas detalladas de latencia de las cargas de trabajo de calidad de servicio.

## Fije un piso de rendimiento con calidad de servicio

Puede utilizar el `min-throughput` Campo para un grupo de políticas a fin de definir un piso de rendimiento para las cargas de trabajo de objetos de almacenamiento (QoS mín.). Puede aplicar el grupo de políticas cuando crea o modifica el objeto de almacenamiento. A partir de ONTAP 9.8, puede especificar el nivel mínimo de rendimiento en IOPS o Mbps, o IOPS y Mbps.

### Antes de empezar

- Debe ejecutar ONTAP 9.2 o una versión posterior. Los pisos de alto rendimiento están disponibles a partir de ONTAP 9.2.
- Para crear un grupo de políticas, debe ser un administrador de clústeres.
- A partir de ONTAP 9.13.1, puede aplicar pisos de rendimiento a nivel de la SVM mediante un [plantilla de grupo de políticas adaptativas](#). No puede establecer una plantilla de grupo de políticas adaptativas en una SVM con un grupo de políticas de calidad de servicio.

### Acerca de esta tarea

- A partir de ONTAP 9.4, puede usar un grupo de políticas *no compartido* QoS para especificar que la planta de rendimiento definida se aplique a cada carga de trabajo miembro de forma individual. Esta es la única condición en la que un grupo de políticas para una planta de rendimiento se puede aplicar a varias cargas de trabajo.

Configurado `-is-shared=false` para la `qos policy-group create` comando para especificar un grupo de políticas no compartido.

- El rendimiento de una carga de trabajo puede caer por debajo de la superficie especificada si no hay suficiente capacidad de rendimiento (margen adicional) en el nodo o el agregado.
- Un objeto de almacenamiento sujeto a un límite de calidad de servicio debe ser contenido por la SVM a la que pertenece el grupo de políticas. Pueden pertenecer varios grupos de políticas a la misma SVM.
- Es una práctica recomendada de la calidad de servicio aplicar un grupo de políticas al mismo tipo de objetos de almacenamiento.
- Un grupo de políticas que define un piso de rendimiento no se puede aplicar a una SVM.

## Pasos



1. Compruebe que la capacidad de rendimiento sea adecuada en el nodo o el agregado, como se describe en "[Identificar la capacidad de rendimiento restante](#)".
2. Cree un grupo de políticas:

```
qos policy-group create -policy group policy_group -vserver SVM -min
-throughput qos_target -is-shared true|false
```

Para obtener una sintaxis de comando completa, consulte la página man de la versión ONTAP. Puede utilizar el `qos policy-group modify` comando para ajustar los pisos de rendimiento.

El siguiente comando crea el grupo de políticas compartidas `pg-vs2` Con un rendimiento mínimo de 1,000 IOPS:

```
cluster1::> qos policy-group create -policy group pg-vs2 -vserver vs2
-min-throughput 1000iops -is-shared true
```

El siguiente comando crea el grupo de políticas no compartido `pg-vs4` sin límite de rendimiento:

```
cluster1::> qos policy-group create -policy group pg-vs4 -vserver vs4
-is-shared false
```

3. Aplique un grupo de políticas a un volumen o una LUN:

```
storage_object create -vserver SVM -qos-policy-group policy_group
```

Para obtener una sintaxis de comando completa, consulte las páginas man. Puede utilizar el `_storage_object_modify` comando para aplicar un grupo de políticas diferente al objeto de almacenamiento.

El siguiente comando aplica un grupo de políticas `pg-app2` al volumen `app2`:

```
cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr1
-qos-policy-group pg-app2
```

4. Supervise el rendimiento del grupo de políticas:

```
qos statistics performance show
```

Para obtener una sintaxis de comando completa, consulte la página man.



Supervise el rendimiento desde el clúster. No utilice una herramienta en el host para supervisar el rendimiento.

El siguiente comando muestra el rendimiento del grupo de políticas:

```
cluster1::> qos statistics performance show
```

| Policy Group        | IOPS  | Throughput | Latency   |
|---------------------|-------|------------|-----------|
| -total-             | 12316 | 47.76MB/s  | 1264.00us |
| pg_app2             | 7216  | 28.19MB/s  | 420.00us  |
| _System-Best-Effort | 62    | 13.36KB/s  | 4.13ms    |
| _System-Background  | 30    | 0KB/s      | 0ms       |

## 5. Supervisar el rendimiento de la carga de trabajo:

```
qos statistics workload performance show
```

Para obtener una sintaxis de comando completa, consulte la página man.



Supervise el rendimiento desde el clúster. No utilice una herramienta en el host para supervisar el rendimiento.

El siguiente comando muestra el rendimiento de la carga de trabajo:

```
cluster1::> qos statistics workload performance show
```

| Workload        | ID    | IOPS  | Throughput | Latency   |
|-----------------|-------|-------|------------|-----------|
| -total-         | -     | 12320 | 47.84MB/s  | 1215.00us |
| app2-wid7967    | 7967  | 7219  | 28.20MB/s  | 319.00us  |
| vs1-wid12279    | 12279 | 5026  | 19.63MB/s  | 2.52ms    |
| _USERSPACE_APPS | 14    | 55    | 10.92KB/s  | 236.00us  |
| _Scan_Backgro.. | 5688  | 20    | 0KB/s      | 0ms       |



Puede utilizar el `qos statistics workload latency show` Comando para ver estadísticas detalladas de latencia de las cargas de trabajo de calidad de servicio.

## Utilice grupos de políticas de calidad de servicio adaptativos

Puede usar un grupo de políticas *Adaptive QoS* para escalar automáticamente un techo o un tamaño de piso a volumen y mantener la ratio de IOPS en TB|GB a medida que cambie el tamaño del volumen. Esto es una ventaja importante si gestiona cientos o miles de cargas de trabajo en una puesta en marcha grande.

### Antes de empezar

- Debe ejecutar ONTAP 9.3 o una versión posterior. Los grupos de políticas de calidad de servicio adaptativa están disponibles a partir de ONTAP 9.3.
- Para crear un grupo de políticas, debe ser un administrador de clústeres.

### Acerca de esta tarea

Un objeto de almacenamiento puede ser miembro de un grupo de políticas adaptables o de un grupo de

políticas no adaptativas, pero no ambos. La SVM del objeto de almacenamiento y la política deben ser iguales. El objeto de almacenamiento debe estar en línea.

Los grupos de políticas de calidad de servicio adaptativos siempre no son compartidos: El techo o el piso de rendimiento definidos se aplican a la carga de trabajo de cada miembro de forma individual.

La relación de límites de rendimiento con el tamaño de objeto de almacenamiento se determina por la interacción de los siguientes campos:

- `expected-iops` Es el mínimo esperado de IOPS por TB|GB asignado.



``expected-iops`` Sólo se garantiza en plataformas AFF.  
``expected-iops`` FabricPool solo tiene garantía si la política de organización en niveles está establecida en "none" y no hay bloques en el cloud. ``expected-iops`` Está garantizado para volúmenes que no estén en una relación de SnapMirror síncrono.

- `peak-iops` Es la cantidad máxima de IOPS posible por TB|GB asignado o usada.
- `expected-iops-allocation` especifica si el espacio asignado (predeterminado) o el espacio utilizado se usa para el iops esperado.



`expected-iops-allocation` Está disponible en ONTAP 9.5 y versiones posteriores. No es compatible con ONTAP 9.4 y versiones anteriores.

- `peak-iops-allocation` especifica si se utiliza el espacio asignado o el espacio utilizado (el valor predeterminado) para `peak-iops`.
- `absolute-min-iops` Es el número mínimo absoluto de IOPS. Puede utilizar este campo con objetos de almacenamiento muy pequeños. Anula ambos `peak-iops` y/o. `expected-iops` cuando `absolute-min-iops` es mayor que el calculado `expected-iops`.

Por ejemplo, si ha establecido `expected-iops` Para 1,000 IOPS/TB, y el tamaño del volumen es inferior a 1 GB, calculado `expected-iops` Será un IOP fraccionario. El calculado `peak-iops` será una fracción aún menor. Puede evitar esto mediante la configuración `absolute-min-iops` a un valor realista.

- `block-size` Especifica el tamaño de bloque de I/O de la aplicación. El valor predeterminado es 32K. Los valores válidos son 8K, 16K, 32K, 64K, CUALQUIERA. CUALQUIER significa que no se aplica el tamaño de los bloques.

Existen tres grupos de políticas de calidad de servicio adaptativas predeterminados disponibles, como se muestra en la siguiente tabla. Puede aplicar estos grupos de políticas directamente a un volumen.

| Grupo de políticas predeterminado | Tasa prevista de IOPS/TB | Pico de IOPS/TB | IOPS mín. Absoluto |
|-----------------------------------|--------------------------|-----------------|--------------------|
| extreme                           | 6.144                    | 12.288          | 1000               |

|             |       |       |     |
|-------------|-------|-------|-----|
| performance | 2.048 | 4.096 | 500 |
| value       | 128   | 512   | 75  |

No puede asignar un objeto de almacenamiento a un grupo de políticas si su objeto que contiene o sus objetos secundarios pertenecen a un grupo de políticas. En la siguiente tabla se enumeran las restricciones.

| Si asigna...                        | No puede asignar...                                                               |
|-------------------------------------|-----------------------------------------------------------------------------------|
| SVM a un grupo de políticas         | Todos los objetos de almacenamiento que contiene la SVM a un grupo de políticas   |
| Del volumen a un grupo de políticas | El volumen que contiene la SVM o cualquier LUN secundario a un grupo de políticas |
| LUN a un grupo de políticas         | El volumen o la SVM que contiene el LUN a un grupo de políticas                   |
| Archivo a un grupo de políticas     | El volumen o la SVM del archivo a un grupo de políticas                           |

## Pasos

1. Cree un grupo de políticas de calidad de servicio adaptativo:

```
qos adaptive-policy-group create -policy group policy_group -vserver SVM
-expected-iops number_of_iops/TB|GB -peak-iops number_of_iops/TB|GB -expected
-iops-allocation-space|used-space -peak-iops-allocation allocated-space|used-
space -absolute-min-iops number_of_iops -block-size 8K|16K|32K|64K|ANY
```

Para obtener una sintaxis de comando completa, consulte la página [man](#).



-expected-iops-allocation y.. -block-size Está disponible en ONTAP 9.5 y versiones posteriores. Estas opciones no son compatibles con ONTAP 9.4 y versiones anteriores.

El siguiente comando crea un grupo de políticas de calidad de servicio adaptativo `adpg-app1` con `-expected-iops` Establecido en 300 IOPS/TB, `-peak-iops` Establecido en 1,000 IOPS/TB, `-peak-iops-allocation` establezca en `used-space`, y. `-absolute-min-iops` Establecido en 50 IOPS:

```
cluster1::> qos adaptive-policy-group create -policy group adpg-app1
-vserver vs2 -expected-iops 300iops/tb -peak-iops 1000iops/TB -peak-iops
-allocation used-space -absolute-min-iops 50iops
```

2. Aplique un grupo de políticas de calidad de servicio adaptable a un volumen:

```
volume create -vserver SVM -volume volume -aggregate aggregate -size number_of
TB|GB -qos-adaptive-policy-group policy_group
```

Para obtener una sintaxis de comando completa, consulte las páginas man.

El siguiente comando aplica el grupo de políticas de calidad de servicio adaptativa `adpg-app1` al volumen `app1`:

```
cluster1::> volume create -vserver vs1 -volume app1 -aggregate aggr1
-size 2TB -qos-adaptive-policy-group adpg-app1
```

Los siguientes comandos aplican el grupo de políticas de calidad de servicio adaptativo predeterminado `extreme` al nuevo volumen `app4` y al volumen existente `app5`. El techo de rendimiento definido para el grupo de políticas se aplica a los volúmenes `app4` y `app5` individualmente:

```
cluster1::> volume create -vserver vs4 -volume app4 -aggregate aggr4
-size 2TB -qos-adaptive-policy-group extreme
```

```
cluster1::> volume modify -vserver vs5 -volume app5 -qos-adaptive-policy
-group extreme
```

## Defina una plantilla de grupo de políticas adaptativas

A partir de ONTAP 9.13.1, puede aplicar pisos y techos de rendimiento en el nivel de SVM mediante una plantilla de grupo de políticas adaptativas.

### Acerca de esta tarea

- La plantilla de grupo de políticas adaptativas es una política predeterminada `apg1`. La política se puede modificar en cualquier momento. Solo se puede establecer con la interfaz de línea de comandos o la API DE REST DE ONTAP y solo se puede aplicar a las SVM existentes.
- La plantilla de grupo de políticas adaptativas solo afecta a los volúmenes creados en la SVM o migrados a ella después de establecer la política. Los volúmenes existentes en la SVM conservan su estado existente.

Si deshabilita la plantilla de grupo de políticas adaptativas, los volúmenes de la SVM conservarán las políticas existentes. Solo los volúmenes que se creen posteriormente en la SVM o se migren a ella se verán afectados por la desactivación.

- No puede establecer una plantilla de grupo de políticas adaptativas en una SVM con un grupo de políticas de calidad de servicio.
- Las plantillas de grupos de políticas adaptativas están diseñadas para las plataformas AFF. Se puede definir una plantilla de grupo de políticas adaptativas en otras plataformas, pero es posible que la política no aplique un rendimiento mínimo. Del mismo modo, puede añadir una plantilla de grupo de políticas adaptable a una SVM en un agregado de FabricPool o en un agregado que no admita un rendimiento mínimo, pero el nivel de rendimiento no se aplicará.
- Si la SVM está en una configuración de MetroCluster o una relación de SnapMirror, la plantilla de grupo de políticas adaptativas se aplicará en la SVM reflejada.

## Pasos

1. Modifique la SVM para aplicar la plantilla de grupo de políticas adaptativas:

```
vserver modify -qos-adaptive-policy-group-template apg1
```

2. Confirme que se ha establecido la política:

```
vserver show -fields qos-adaptive-policy-group
```

## Supervise el rendimiento del clúster con Unified Manager

Con Active IQ Unified Manager, puede maximizar la disponibilidad y mantener el control de su infraestructura de almacenamiento AFF y FAS de NetApp para disfrutar de una mayor escalabilidad, compatibilidad, rendimiento y seguridad.

Active IQ Unified Manager supervisa de forma continua el estado del sistema y envía alertas, para que su organización pueda liberar recursos del personal DE TECNOLOGÍA. Puede ver al instante el estado de su almacenamiento desde un único panel y abordar rápidamente problemas mediante acciones recomendadas.

La gestión de datos se simplifica porque puede detectar, supervisar y recibir notificaciones para gestionar el almacenamiento de forma proactiva y resolver los problemas con rapidez. La eficiencia de administración ha mejorado porque puede supervisar petabytes de datos desde una única consola y gestionar sus datos a escala.

Con Active IQ Unified Manager, puede mantener el ritmo de las fluctuaciones en las demandas del negocio y optimizar el rendimiento mediante datos del rendimiento y análisis avanzados. Las funciones de generación de informes permiten acceder a informes estándar o crear informes operativos personalizados que satisfagan las necesidades específicas de su empresa.

Enlaces relacionados:

- ["Obtenga más información acerca de Active IQ Unified Manager"](#)
- ["Comienza a usar Active IQ Unified Manager para VMware"](#)
- ["Comience con Active IQ Unified Manager para Linux"](#)
- ["Comience a usar Active IQ Unified Manager para Windows"](#)

## Supervise el rendimiento del clúster con Cloud Insights

Cloud Insights de NetApp es una herramienta de supervisión que le ofrece visibilidad de toda su infraestructura. Con Cloud Insights, puede supervisar, solucionar problemas y optimizar todos los recursos, incluidos los clouds públicos y los centros de datos privados.

### Cloud Insights se presenta en dos ediciones

La edición básica de Cloud Insights está diseñada específicamente para supervisar y optimizar sus activos de Data Fabric de NetApp. Proporciona análisis avanzados para las conexiones entre todos los recursos de NetApp, incluidos HCI y All Flash FAS (AFF) en el entorno de forma gratuita.

Cloud Insights Standard Edition no solo se centra en componentes de infraestructura habilitados para Data Fabric de NetApp, sino también en entornos de varios proveedores y clouds. Con sus capacidades enriquecidas, usted puede acceder al apoyo para más de 100 servicios y recursos.

En el mundo actual, donde los recursos están en juego desde los centros de datos locales hasta varios clouds públicos, es fundamental tener una imagen completa desde la propia aplicación hasta el disco de back-end de la cabina de almacenamiento. El soporte adicional para la supervisión de aplicaciones (como Kafka, MongoDB y Nginx) le proporciona la información y el conocimiento que necesita para operar al nivel óptimo de utilización, así como con el búfer de riesgo perfecto.

Ambas ediciones (Basic y Standard) pueden integrarse con Active IQ Unified Manager de NetApp. Los clientes que usan Active IQ Unified Manager pueden ver la información de unión dentro de la interfaz de usuario de Cloud Insights. Las notificaciones publicadas en Active IQ Unified Manager no se pasan por alto y pueden correlacionarse con eventos en Cloud Insights. En otras palabras, obtienes lo mejor de ambos mundos.

## **Supervisión, solución de problemas y optimización de todos los recursos**

Cloud Insights le ayuda a reducir significativamente el tiempo necesario para resolver problemas y evitar que afecten a los usuarios finales. También le ayuda a reducir los costes de infraestructura del cloud. Su exposición a las amenazas internas se reduce al proteger sus datos con una inteligencia práctica.

Cloud Insights le ofrece visibilidad de toda su infraestructura híbrida en un mismo lugar, desde el cloud público hasta su centro de datos. Puede crear instantáneamente paneles relevantes que se puedan personalizar según sus necesidades específicas. También puedes crear alertas específicas y condicionales que sean específicas y relevantes para las necesidades de tu organización.

La detección avanzada de anomalías le ayuda a corregir problemas de forma proactiva antes de que surjan. Puede ver automáticamente la contención y degradación de los recursos para restaurar rápidamente las cargas de trabajo afectadas. La solución de problemas va más rápido con la jerarquía automatizada de relaciones entre los distintos componentes de la pila.

Puede identificar los recursos no utilizados o abandonados en todo su entorno, lo que le ayudará a descubrir oportunidades para dimensionar adecuadamente la infraestructura y optimizar el gasto completo.

Cloud Insights visualiza la topología de su sistema para entender su arquitectura de Kubernetes. Puede supervisar el estado de los clústeres de Kubernetes, incluidos qué nodos tienen problemas y ampliar cuando observe un problema.

Cloud Insights le ayuda a proteger los datos de la organización frente a un uso inadecuado por parte de usuarios malintencionados o en riesgo mediante el aprendizaje automático avanzado y la detección de anomalías que le proporciona inteligencia procesable sobre amenazas internas.

Cloud Insights le ayuda a visualizar métricas de Kubernetes para que pueda comprender por completo las relaciones entre los pods, los nodos y los clústeres. Podrá evaluar el estado de un clúster o un módulo de trabajo, así como la carga que está procesando actualmente, lo que le permite tomar el control del clúster K8S y controlar tanto el estado como el coste de la implementación.

### **Enlaces relacionados**

- ["Obtenga más información acerca de Cloud Insights"](#)
- ["Comience a usar Cloud Insights"](#)

## **Registro de auditoría**

### **Cómo implementa ONTAP el registro de auditoría**

Las actividades de gestión registradas en el registro de auditoría se incluyen en los

informes estándar de AutoSupport y determinadas actividades de registro se incluyen en los mensajes de EMS. También puede reenviar el registro de auditoría a los destinos que especifique y mostrar los archivos de registro de auditoría mediante la CLI o un explorador web.

A partir de ONTAP 9.11.1, es posible mostrar contenido del registro de auditoría mediante System Manager.

A partir de ONTAP 9.12.1, ONTAP proporciona alertas de manipulación para los registros de auditoría. ONTAP ejecuta un trabajo diario en segundo plano para comprobar si hay manipulación de archivos `audit.log` y envía una alerta de EMS si encuentra algún archivo de registro que se haya modificado o alterado.

ONTAP registra las actividades de gestión que se realizan en el clúster; por ejemplo, qué solicitud se emitió, el usuario que activó la solicitud, el método de acceso del usuario y la hora de la solicitud.

Las actividades de gestión pueden ser uno de los siguientes tipos:

- SET Requests, que suelen aplicarse a comandos o operaciones que no son de visualización
  - Estas solicitudes se emiten cuando se ejecuta un `create`, `modify`, o `delete` por ejemplo.
  - Las solicitudes SET se registran de forma predeterminada.
- OBTENGA solicitudes, que recuperan información y la muestran en la interfaz de gestión
  - Estas solicitudes se emiten cuando se ejecuta un `show` por ejemplo.
  - LAS solicitudes GET no se registran de forma predeterminada, pero puede controlar si GET Requests enviadas desde la CLI de ONTAP (`-cliget`), de la API de ONTAP (`-ontapiget`), o desde la API DE REST (`-httpget`) se registran en el archivo.

ONTAP actividades de gestión de registros en el `/mroot/etc/log/mlog/audit.log` archivo de un nodo. Los comandos de los tres shell para los comandos de la CLI -el clustershell, el nodeshell y el shell del sistema no interactivo (los comandos de shell del sistema interactivos no se registran)- así como los comandos de la API se registran aquí. Los registros de auditoría incluyen marcas de tiempo para mostrar si todos los nodos de un clúster están sincronizados con la hora.

La `audit.log` El archivo es enviado por la herramienta AutoSupport a los destinatarios especificados. También es posible reenviar el contenido de manera segura a destinos externos que especifique; por ejemplo, un servidor de Splunk o syslog.

La `audit.log` el archivo se gira diariamente. La rotación también ocurre cuando alcanza los 100 MB de tamaño y se conservan las 48 copias anteriores (con un máximo de 49 archivos). Cuando el archivo de auditoría realiza su rotación diaria, no se genera ningún mensaje EMS. Si el archivo de auditoría gira porque se supera el límite de tamaño de archivo, se genera un mensaje EMS.

## Cambios en el registro de auditoría en ONTAP 9

A partir de ONTAP 9, el `command-history.log` el archivo se sustituye por `audit.log`, y la `mgwd.log` el archivo ya no contiene información de auditoría. Si actualiza a ONTAP 9, debe revisar cualquier script o herramienta que haga referencia a los archivos heredados y su contenido.

Después de actualizar a ONTAP 9, existente `command-history.log` los archivos se conservan. Se rotan (eliminan) como nuevas `audit.log` los archivos se giran en (crean).



Herramientas y scripts que comprueban `command-history.log` es posible que el archivo continúe funcionando, porque un vínculo de `software de command-history.log` para `audit.log` se crea al actualizar. Sin embargo, herramientas y scripts que comprueban `mgwd.log` el archivo fallará porque ese archivo ya no contiene información de auditoría.

Además, los registros de auditoría de ONTAP 9 y versiones posteriores ya no incluyen las siguientes entradas porque no se consideran útiles y provocan una actividad de registro innecesaria:

- Comandos internos ejecutados por ONTAP (es decir, donde `username=root`)
- Alias de comandos (por separado del comando al que apuntan)

A partir de ONTAP 9, puede transmitir los registros de auditoría de manera segura a destinos externos mediante los protocolos TCP y TLS.

## Mostrar el contenido del registro de auditoría

Puede mostrar el contenido del clúster `/mroot/etc/log/mlog/audit.log` Archivos mediante la interfaz de línea de comandos de ONTAP, System Manager o un explorador web.

Las entradas del archivo de registro del clúster incluyen lo siguiente:

### Tiempo

Marca de hora de entrada del registro.

### Cliente más

La aplicación utilizada para conectarse al clúster. Ejemplos de valores posibles son `internal`, `console`, `ssh`, `http`, `ontapi`, `snmp`, `rsh`, `telnet`, y `service-processor`.

### Usuario

El nombre de usuario del usuario remoto.

### Estado

El estado actual de la solicitud de auditoría, que podría ser `success`, `pending`, o `error`.

### Mensaje

Un campo opcional que puede contener errores o información adicional acerca del estado de un comando.

### ID de sesión

El ID de sesión en el que se recibe la solicitud. A cada SSH *Session* se le asigna un ID de sesión, mientras que a cada HTTP, ONAPI o SNMP *Request* se le asigna un ID de sesión único.

### Máquina virtual de almacenamiento

La SVM a través de la cual se conectó el usuario.

### Ámbito

Pantallas `svm` Cuando la solicitud se encuentra en una máquina virtual de almacenamiento de datos; de lo contrario, se muestra `cluster`.

## ID del comando

El ID de cada comando recibido en una sesión de CLI. Esto permite correlacionar una solicitud y una respuesta. LAS solicitudes ZAPI, HTTP y SNMP no tienen ID de comandos.

Puede mostrar las entradas del registro del clúster desde la interfaz de línea de comandos de ONTAP, desde un explorador web y a partir de ONTAP 9.11.1, desde System Manager.

### System Manager

- Para visualizar el inventario, seleccione **Eventos y trabajos > registros de auditoría**. Cada columna tiene controles para filtrar, ordenar, buscar, mostrar y categorías de inventario. Los detalles del inventario se pueden descargar como un libro de Excel.
- Para establecer filtros, haga clic en el botón **Filtro** en la parte superior derecha y, a continuación, seleccione los campos deseados. También puede ver todos los comandos ejecutados en la sesión en la que se produjo un fallo haciendo clic en el enlace Identificador de Sesión.

### CLI

Para mostrar las entradas de auditoría combinadas de varios nodos en el clúster, introduzca:

```
security audit log show [parameters]
```

Puede utilizar el `security audit log show` comando para mostrar las entradas de auditoría de nodos individuales o fusionadas desde varios nodos en el clúster. También puede mostrar el contenido de `/mroot/etc/log/mlog` directorio en un solo nodo mediante un navegador web.

Consulte la página man para obtener más información.

### Navegador Web


Puede mostrar el contenido de `/mroot/etc/log/mlog` directorio en un solo nodo mediante un navegador web. ["Obtenga información acerca de cómo acceder a los archivos log, de volcado principal y MIB de un nodo mediante un explorador web"](#).

## Gestione la configuración DE SOLICITUDES DE RECEPCIÓN de auditoría

Mientras QUE LAS solicitudes SET se registran de forma predeterminada, LAS solicitudes GET no lo son. Sin embargo, puede controlar si SE envían solicitudes desde HTML de ONTAP (`-httpget`), la CLI de ONTAP (`-cliget`), o desde las API de ONTAP (`-ontapiget`) se registran en el archivo.

Es posible modificar la configuración de registro de auditoría desde la interfaz de línea de comandos de ONTAP, y a partir de ONTAP 9.11.1, desde System Manager.

## System Manager

1. Seleccione **Eventos y trabajos > registros de auditoría**.
2. Haga clic en  en la esquina superior derecha, elija las solicitudes que desea agregar o quitar.

## CLI

- Para especificar que las solicitudes GET de la CLI o las API de ONTAP se deben registrar en el registro de auditoría (el archivo audit.log), además de las solicitudes predeterminadas, introduzca:  
`security audit modify [-cliget {on|off}][--httpget {on|off}][--ontapiget {on|off}]`
- Para mostrar los ajustes actuales, introduzca:  
`security audit show`

Consulte las páginas de manual para obtener más información.

## Permite gestionar destinos de registro de auditoría

Es posible reenviar el registro de auditoría a un máximo de 10 destinos. Por ejemplo, es posible reenviar el registro a un servidor de Splunk o syslog para que realice tareas de supervisión, análisis o backup.

### Acerca de esta tarea

Para configurar el reenvío, debe proporcionar la dirección IP del host de syslog o Splunk, su número de puerto, un protocolo de transmisión y la facilidad de syslog que se usarán para los registros reenviados. ["Obtenga información sobre las instalaciones de syslog"](#).

Puede seleccionar uno de los siguientes valores de transmisión:

### UDP no cifrado

Protocolo de datagramas de usuario sin seguridad (predeterminado)

### TCP sin cifrar

Protocolo de control de la transmisión sin seguridad




### Cifrado TCP

Protocolo de control de transmisión con seguridad de la capa de transporte (TLS)

Una opción **Verificar servidor** está disponible cuando se selecciona el protocolo cifrado TCP.

Es posible reenviar registros de auditoría desde la interfaz de línea de comandos de ONTAP y a partir de ONTAP 9.11.1, desde System Manager.

## System Manager

- Para visualizar los destinos de registro de auditoría, seleccione **clúster > Configuración**. Se muestra un recuento de destinos de registro en el mosaico **Gestión de notificaciones**. Haga clic en  para mostrar los detalles.
- Para agregar, modificar o eliminar destinos de registro de auditoría, seleccione **Eventos y trabajos > registros de auditoría** y, a continuación, haga clic en **Administrar destinos de auditoría** en la parte superior derecha de la pantalla. Haga clic en  **Add** o haga clic en  En la columna **Dirección de host** para editar o eliminar entradas.

## CLI

1. Para cada destino al que se desea reenviar el registro de auditoría, especifique la dirección IP o el nombre de host de destino y todas las opciones de seguridad.

```
cluster1::> cluster log-forwarding create -destination
192.168.123.96
-port 514 -facility user

cluster1::> cluster log-forwarding create -destination
192.168.123.98
-port 514 -protocol tcp-encrypted -facility user
```

- Si la `cluster log-forwarding create` el comando no puede hacer ping al host de destino para verificar la conectividad; se produce un error en el comando. Aunque no se recomienda, utilice la `-force` parámetro con el comando omite la verificación de conectividad.
  - Al ajustar la `-verify-server` parámetro a `true`, la identidad del destino de reenvío de registros se verifica mediante la validación de su certificado. Puede establecer el valor en `true` sólo cuando seleccione la `tcp-encrypted` valor en la `-protocol` campo.
2. Compruebe que los registros de destino son correctos mediante el `cluster log-forwarding show` comando.

```
cluster1::> cluster log-forwarding show
```

| Destination Host | Port | Protocol        | Verify Server | Syslog Facility |
|------------------|------|-----------------|---------------|-----------------|
| 192.168.123.96   | 514  | udp-unencrypted | false         | user            |
| 192.168.123.98   | 514  | tcp-encrypted   | true          | user            |

2 entries were displayed.

Consulte las páginas de manual para obtener más información.

# AutoSupport

## Gestione la configuración de AutoSupport con System Manager

Puede usar System Manager para gestionar la configuración de su cuenta de AutoSupport.

Puede realizar los siguientes procedimientos:

### Ver la configuración de AutoSupport

Puede usar System Manager para ver la configuración de su cuenta de AutoSupport.

#### Pasos

1. En System Manager, haga clic en **clúster > Configuración**.

En la sección **AutoSupport**, se muestra la siguiente información:

- Estado
- Protocolo de transporte
- Servidor proxy
- Dirección de correo electrónico del remitente


2. En la sección **AutoSupport**, selecciona , A continuación, seleccione **Más opciones**.

Se muestra información adicional acerca de la configuración de la conexión AutoSupport y del correo electrónico. Además, se muestra el historial de transferencia de mensajes.

### Generar y enviar datos de AutoSupport

En System Manager, puede iniciar la generación de mensajes de AutoSupport y elegir el nodo o los nodos del clúster que se recopilan los datos.


#### Pasos

1. En System Manager, seleccione **Cluster > Settings**.
2. En la sección **AutoSupport**, selecciona , A continuación, seleccione **Generar y Enviar**.
3. Introduzca un asunto.
4. Seleccione la casilla de verificación en **Recopilar datos de** para especificar los nodos de los cuales recopilar los datos.

### Pruebe la conexión a AutoSupport

En System Manager, es posible enviar un mensaje de prueba para verificar la conexión a AutoSupport.

#### Pasos

1. En System Manager, haga clic en **clúster > Configuración**.
2. En la sección **AutoSupport**, selecciona , A continuación, seleccione **Test Connectivity**.
3. Introduzca un asunto para el mensaje.

## Habilite o deshabilite AutoSupport



AutoSupport ofrece ventajas empresariales demostradas a los clientes de NetApp, incluida la identificación proactiva de posibles problemas de configuración y la resolución acelerada de los casos de soporte. AutoSupport está activado de forma predeterminada en los sistemas nuevos. Si es necesario, puede usar System Manager para deshabilitar la capacidad de AutoSupport de supervisar el estado del sistema de almacenamiento y enviar mensajes de notificación. Es posible habilitar AutoSupport de nuevo después de que se haya deshabilitado.

### Acerca de esta tarea

Antes de deshabilitar AutoSupport, tiene que tener en cuenta que está desactivando el sistema de llamada a casa de NetApp y perderá los siguientes beneficios:

- **Monitoreo de salud:** AutoSupport supervisa el estado de su sistema de almacenamiento y envía notificaciones al soporte técnico y a su organización de soporte interno.
- **Automatización:** AutoSupport automatiza la presentación de informes de casos de soporte. La mayoría de los casos de soporte se abren automáticamente antes de que los clientes se den cuenta de que hay un problema.
- **Resolución más rápida:** Los sistemas que envían datos AutoSupport tienen sus casos de soporte resueltos en la mitad del tiempo en comparación con los casos de los sistemas que no envían datos AutoSupport.
- **\* Actualizaciones más rápidas \*:** AutoSupport impulsa los flujos de trabajo de autoservicio de los clientes, como actualizaciones de versiones, complementos, renovaciones y automatización de actualizaciones de firmware en System Manager.
- **Más funciones:** Ciertas funciones de otras herramientas solo funcionan cuando AutoSupport está habilitado, por ejemplo, algunos flujos de trabajo en BlueXP.

### Pasos

1. Seleccione **Cluster > Settings**.
2. En la sección **AutoSupport**, seleccione , A continuación, seleccione **Desactivar**.
3. Si desea volver a activar AutoSupport, en la sección **AutoSupport**, seleccione , A continuación, seleccione **Activar**.

## Suprimir la generación de casos de soporte


A partir de ONTAP 9.10.1, se puede utilizar System Manager para enviar una solicitud a AutoSupport con el fin de suprimir la generación de casos de soporte.

### Acerca de esta tarea

Para suprimir la generación de casos de soporte, especifique los nodos y el número de horas para las que desea que se produzca la supresión.

La supresión de casos de soporte puede ser especialmente útil si no desea que AutoSupport cree casos automatizados mientras realiza el mantenimiento en los sistemas.

### Pasos


1. Seleccione **Cluster > Settings**.
2. En la sección **AutoSupport**, seleccione , A continuación, seleccione **Suprimir Soporte Case Generation**.
3. Introduzca el número de horas que desea que se produzca la supresión.

4. Seleccione los nodos para los que desea que se produzca la supresión.

## Reanudar la generación de casos de soporte

A partir de ONTAP 9.10.1, es posible usar System Manager para reanudar la generación de casos de soporte desde AutoSupport si se ha suprimido.



### Pasos

1. Seleccione **Cluster > Settings**.
2. En la sección **AutoSupport**, seleccione , A continuación, seleccione **Reanudar Support Case Generation**.
3. Seleccione los nodos para los que desea que se reanude la generación.

## Editar configuración de AutoSupport

Puede usar System Manager para modificar la configuración de conexión y correo electrónico de la cuenta de AutoSupport.

### Pasos

1. Seleccione **Cluster > Settings**.
2. En la sección **AutoSupport**, seleccione , A continuación, seleccione **Más opciones**.
3. En la sección **Conexiones** o en la sección **Correo electrónico**, seleccione  **Edit** para modificar la configuración de cualquiera de las secciones.

## Gestione AutoSupport con la interfaz de línea de comandos

### Información general sobre Manage AutoSupport

AutoSupport es un mecanismo que supervisa de forma proactiva el estado del sistema y envía automáticamente mensajes al soporte técnico de NetApp, su organización de soporte interno y un partner de soporte. Aunque los mensajes de AutoSupport al soporte técnico se habilitan de forma predeterminada, debe establecer las opciones correctas y disponer de un host de correo válido para que se envíen mensajes a la organización de soporte interna.

Solo el administrador de clúster puede realizar la gestión de AutoSupport. El administrador de máquinas virtuales de almacenamiento (SVM) no tiene acceso a AutoSupport.

De forma predeterminada, AutoSupport se habilita al configurar el sistema de almacenamiento por primera vez. AutoSupport comienza a enviar mensajes al soporte técnico 24 horas después de habilitar AutoSupport. Se puede reducir el período de 24 horas mediante la actualización o la reversión del sistema, la modificación de la configuración de AutoSupport o el cambio de la hora del sistema para que sea algo distinto de un período de 24 horas.



Es posible deshabilitar AutoSupport en cualquier momento, pero debe dejarla habilitada. Habilitar AutoSupport puede ayudar significativamente a acelerar la detección y resolución de problemas cuando se producen fallos en el sistema de almacenamiento. De forma predeterminada, el sistema recopila información de AutoSupport y la almacena localmente, incluso si deshabilita AutoSupport.

Para obtener más información sobre AutoSupport, consulte el sitio de soporte de NetApp.

#### Información relacionada

- ["Soporte de NetApp"](#)
- ["Obtenga más información acerca de los comandos de la AutoSupport en la CLI de ONTAP"](#)

#### Utilice el asesor digital AutoSupport y Active IQ

El componente AutoSupport de ONTAP recopila telemetría y la envía para su análisis. El asesor digital de Active IQ analiza los datos de AutoSupport y ofrece optimización y atención proactivas. Utilizando la inteligencia artificial, Active IQ puede identificar problemas potenciales y ayudarle a resolverlos antes de que afecten a su negocio.

Active IQ le permite optimizar su infraestructura de datos en el cloud híbrido global mediante la entrega de análisis predictivos aplicables y soporte proactivo a través de un portal basado en cloud y una aplicación para dispositivos móviles. En Active IQ, todos los clientes de NetApp con un contrato activo de SupportEdge disponen de información y recomendaciones basadas en los datos (las funciones varían según el producto y el nivel de soporte).

Estas son algunas cosas que puede hacer con Active IQ:

- Planificación de actualizaciones. Active IQ identifica los problemas en su entorno que se pueden resolver actualizando a una versión más reciente de ONTAP y el componente Upgrade Advisor le ayuda a planificar una actualización correcta.
- Ver el bienestar del sistema. Su consola de Active IQ informa de cualquier problema con el bienestar y le ayuda a corregir estos problemas. Supervise la capacidad del sistema para asegurarse de que nunca se queda sin espacio de almacenamiento. Vea los casos de soporte de su sistema.
- Gestión del rendimiento. Active IQ muestra el rendimiento del sistema durante un período más largo de lo que se puede ver en System Manager. Identifique problemas de configuración y del sistema que afectan a su rendimiento.
- Optimice la eficiencia. Consulte los criterios de medición de la eficiencia del almacenamiento e identifique formas de almacenar más datos en menos espacio.
- Ver el inventario y la configuración. Active IQ muestra información completa sobre la configuración de inventario y software y hardware. Vea cuándo caducan los contratos de servicio y renueve su soporte para asegurarse de que sigue siendo compatible.

#### Información relacionada

["Documentación de NetApp: Asesor digital de Active IQ"](#)

["Inicie Active IQ"](#)

["Servicios de SupportEdge"](#)

#### Cuándo y dónde se envían los mensajes de AutoSupport

AutoSupport envía mensajes a diferentes destinatarios, en función del tipo de mensaje. Saber cuándo y dónde envía AutoSupport los mensajes puede ayudarle a comprender los mensajes que recibe por correo electrónico o visualizarlos en el sitio web de Active IQ (antes conocido como My AutoSupport).



A menos que se especifique lo contrario, la configuración de las tablas siguientes son parámetros de `system node autosupport modify` comando.

### Mensajes activados por eventos

Cuando se producen eventos en el sistema que requieren una acción correctiva, AutoSupport envía automáticamente un mensaje activado por el evento.

| Cuando se envía el mensaje                             | Dónde se envía el mensaje                                                                                                                                                                                                                                                                         |
|--------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AutoSupport responde a un evento desencadenante en EMS | Direcciones especificadas en <code>-to</code> y.. <code>-noteto</code> . (Solo se envían los eventos críticos que afectan al servicio).<br><br>Direcciones especificadas en <code>-partner-address</code><br><br>El soporte técnico, si <code>-support</code> se establece en <code>enable</code> |

### Mensajes programados

AutoSupport envía automáticamente varios mensajes con una programación normal.

| Cuando se envía el mensaje                                                                                                                                                        | Dónde se envía el mensaje                                                                                                                           |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| Daily (de forma predeterminada, enviado entre las 12:00 a.m. y la 1:00 a.m. como mensaje de registro)                                                                             | Direcciones especificadas en <code>-partner-address</code><br><br>El soporte técnico, si <code>-support</code> se establece en <code>enable</code>  |
| Daily (de forma predeterminada, enviado entre las 12:00 a.m. y la 1:00 a.m. como mensaje de rendimiento), si el <code>-perf</code> el parámetro se establece en <code>true</code> | Direcciones especificadas en <code>-Partner-address'</code><br><br>El soporte técnico, si <code>-support</code> se establece en <code>enable</code> |
| Semanal (de forma predeterminada, enviado el domingo entre las 12:00 a.m. y la 1:00 a. m.)                                                                                        | Direcciones especificadas en <code>-partner-address</code><br><br>El soporte técnico, si <code>-support</code> se establece en <code>enable</code>  |

### Mensajes activados manualmente

Puede iniciar o reenviar manualmente un mensaje de AutoSupport.

| Cuando se envía el mensaje                                                                                                      | Dónde se envía el mensaje                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Puede iniciar manualmente un mensaje mediante el <code>system node autosupport invoke</code> comando</p>                     | <p>Si se especifica un URI mediante el <code>-uri</code> en la <code>system node autosupport invoke</code> Comando, el mensaje se envía a ese URI.</p> <p>Si <code>-uri</code> se omite, el mensaje se envía a las direcciones especificadas en <code>-to</code> y.. <code>-partner-address</code>. El mensaje también se envía al soporte técnico si <code>-support</code> se establece en <code>enable</code>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <p>Puede iniciar manualmente un mensaje mediante el <code>system node autosupport invoke-core-upload</code> comando</p>         | <p>Si se especifica un URI mediante el <code>-uri</code> en la <code>system node autosupport invoke-core-upload</code> Comando, el mensaje se envía a ese URI y el archivo de volcado principal se carga en el URI.</p> <p>Si <code>-uri</code> se omite en la <code>system node autosupport invoke-core-upload</code> comando, el mensaje se envía al soporte técnico y el archivo de volcado principal se carga en el sitio de soporte técnico.</p> <p>Ambos escenarios lo requieren <code>-support</code> se establece en <code>enable</code> y.. <code>-transport</code> se establece en <code>https</code> o. <code>http</code>.</p> <p>Debido al gran tamaño de los archivos de volcado principales, el mensaje no se envía a las direcciones especificadas en la <code>-to</code> y.. <code>-partner-addresses</code> parámetros.</p>             |
| <p>Puede iniciar manualmente un mensaje mediante el <code>system node autosupport invoke-performance-archive</code> comando</p> | <p>Si se especifica un URI mediante el <code>-uri</code> en la <code>system node autosupport invoke-performance-archive</code> Comando, el mensaje se envía a ese URI y el archivo de archivado de rendimiento se carga en el URI.</p> <p>Si <code>-uri</code> se omite en la <code>system node autosupport invoke-performance-archive</code>, el mensaje se envía al soporte técnico y el archivo de rendimiento se carga en el sitio de soporte técnico.</p> <p>Ambos escenarios lo requieren <code>-support</code> se establece en <code>enable</code> y.. <code>-transport</code> se establece en <code>https</code> o. <code>http</code>.</p> <p>Debido al gran tamaño de los archivos de archivo de rendimiento, el mensaje no se envía a las direcciones especificadas en la <code>-to</code> y.. <code>-partner-addresses</code> parámetros.</p> |

| Cuando se envía el mensaje                                                                                          | Dónde se envía el mensaje                                                                                                               |
|---------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Reenvíe manualmente un mensaje anterior mediante el <code>system node autosupport history retransmit</code> comando | Únicamente del URI que especifique en la <code>-uri</code> parámetro de <code>system node autosupport history retransmit</code> comando |

### Mensajes activados por el soporte técnico

El soporte técnico puede solicitar mensajes de AutoSupport con la función AutoSupport OnDemand.

| Cuando se envía el mensaje                                                                                                                                             | Dónde se envía el mensaje                                                                                                                                                                                                                                 |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cuando AutoSupport obtiene instrucciones de entrega para generar nuevos mensajes de AutoSupport                                                                        | Direcciones especificadas en <code>-partner-address</code><br><br>El soporte técnico, si <code>-support</code> se establece en <code>enable</code> y.. <code>-transport</code> se establece en <code>https</code>                                         |
| Cuando AutoSupport obtiene instrucciones de entrega para reenviar mensajes anteriores de AutoSupport                                                                   | El soporte técnico, si <code>-support</code> se establece en <code>enable</code> y.. <code>-transport</code> se establece en <code>https</code>                                                                                                           |
| Cuando AutoSupport obtiene instrucciones de entrega para generar nuevos mensajes de AutoSupport que cargan archivos de volcado principales o de archivo de rendimiento | El soporte técnico, si <code>-support</code> se establece en <code>enable</code> y.. <code>-transport</code> se establece en <code>https</code> . El volcado principal o el archivo de archivado de rendimiento se cargan en el sitio de soporte técnico. |

### Cómo crea AutoSupport y envía los mensajes activados por un evento

AutoSupport crea mensajes de AutoSupport activados por un evento cuando EMS procesa un evento de activación. Un mensaje AutoSupport activado para el evento alerta a los destinatarios sobre problemas que requieren acción correctiva y solo contiene información relevante para el problema. Puede personalizar el contenido que desea incluir y quién recibe los mensajes.

AutoSupport utiliza el siguiente proceso para crear y enviar mensajes de AutoSupport activados por un evento:

1. Cuando EMS procesa un evento de activación, EMS envía una solicitud a AutoSupport.

Un evento trigger es un evento de EMS con un destino de AutoSupport y un nombre que comienza por `callhome.` prefijo.

2. AutoSupport crea un mensaje de AutoSupport activado por eventos.

AutoSupport recopila información básica y de solución de problemas de subsistemas asociados con el desencadenador para crear un mensaje que incluya únicamente información relevante para el evento desencadenador.

Un conjunto predeterminado de subsistemas está asociado con cada desencadenador. Sin embargo, puede optar por asociar subsistemas adicionales a un desencadenador mediante el `system node`

`autosupport trigger modify` comando.

3. AutoSupport envía el mensaje AutoSupport activado por el evento a los destinatarios definidos por el `system node autosupport modify` con el `-to`, `-noteto`, `-partner-address`, y. `-support` parámetros.

Puede habilitar y deshabilitar la entrega de mensajes de AutoSupport para activadores específicos mediante el `system node autosupport trigger modify` con el `-to` y. `-noteto` parámetros.

### Ejemplo de datos enviados para un evento específico

La `storage shelf PSU failed` El evento EMS activa un mensaje que contiene datos básicos de la obligatoria, Archivos de registro, almacenamiento, RAID, ha, Los subsistemas de plataforma y red y los datos de solución de problemas de los subsistemas de almacenamiento, Archivos de registro y obligatorios.

Decide que desea incluir datos sobre NFS en cualquier mensaje de AutoSupport que se envíe como respuesta a un futuro `storage shelf PSU failed` evento. Introduzca el siguiente comando para habilitar los datos a nivel de solución de problemas para NFS en el `callhome.shlf.ps.fault` evento:

```
cluster1::\>
system node autosupport trigger modify -node nodel -autosupport
-message shlf.ps.fault -troubleshooting-additional nfs
```

Observe que el `callhome.` el prefijo se descarta de `callhome.shlf.ps.fault` evento cuando utilice `system node autosupport trigger` Comandos o cuando los eventos de AutoSupport y EMS se hagan referencia en la CLI.

### Tipos de mensajes de AutoSupport y su contenido

Los mensajes AutoSupport contienen información de estado acerca de los subsistemas compatibles. Saber qué contienen los mensajes de AutoSupport puede ayudarle a interpretar o a responder a los mensajes que reciba por correo electrónico o que aparecen en el sitio Web de Active IQ (anteriormente denominado My AutoSupport).

| Tipo de mensaje     | Tipo de datos que contiene el mensaje                                                                   |
|---------------------|---------------------------------------------------------------------------------------------------------|
| Activado por evento | Archivos que contienen datos contextuales sobre el subsistema específico en el que se produjo el evento |
| Todos los días      | Archivos de registro                                                                                    |
| Rendimiento         | Datos de rendimiento muestreados durante las 24 horas anteriores                                        |
| Semanal             | Datos de configuración y estado                                                                         |

| Tipo de mensaje                                                                         | Tipo de datos que contiene el mensaje                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Activado por la <code>system node autosupport invoke</code> comando                     | <p>Depende del valor especificado en la <code>-type</code> parámetro:</p> <ul style="list-style-type: none"> <li>• <code>test</code> envía un mensaje activado por el usuario con algunos datos básicos.</li> </ul> <p>Este mensaje también activa una respuesta de correo electrónico automática del soporte técnico a cualquier dirección de correo electrónico especificada mediante el <code>-to</code>. Para confirmar que se están recibiendo mensajes de AutoSupport.</p> <ul style="list-style-type: none"> <li>• <code>performance</code> envía datos de rendimiento.</li> <li>• <code>all</code> envía un mensaje activado por el usuario con un conjunto completo de datos similar al mensaje semanal, incluidos los datos de resolución de problemas de cada subsistema.</li> </ul> <p>El soporte técnico normalmente solicita este mensaje.</p> |
| Activado por la <code>system node autosupport invoke-core-upload</code> comando         | Archivos de volcado principales para un nodo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Activado por la <code>system node autosupport invoke-performance-archive</code> comando | Archivos de archivado de rendimiento durante un periodo de tiempo específico                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Activado por AutoSupport OnDemand                                                       | <p>AutoSupport OnDemand puede solicitar mensajes nuevos o pasados:</p> <ul style="list-style-type: none"> <li>• Los mensajes nuevos, dependiendo del tipo de colección AutoSupport, pueden ser <code>test</code>, <code>all</code>, o <code>performance</code>.</li> <li>• Los mensajes anteriores dependen del tipo de mensaje que se vuelva a enviar.</li> </ul> <p>AutoSupport OnDemand puede solicitar nuevos mensajes que cargan los siguientes archivos en el sitio de soporte de NetApp en <a href="https://mysupport.netapp.com">"mysupport.netapp.com"</a>:</p> <ul style="list-style-type: none"> <li>• Volcado de memoria</li> <li>• Archivado del rendimiento</li> </ul>                                                                                                                                                                         |

## Qué son los subsistemas AutoSupport

Cada subsistema proporciona información básica y de solución de problemas que

AutoSupport utiliza para sus mensajes. Cada subsistema también está asociado con eventos desencadenadores que permiten a AutoSupport recopilar de subsistemas únicamente información relevante para el evento desencadenante.

AutoSupport recopila contenido sensible al contexto. Puede ver información acerca de los subsistemas y los eventos desencadenadores mediante el `system node autosupport trigger show` comando.

### **Tamaño y tiempo de AutoSupport**

AutoSupport recopila información organizada por subsistemas y aplica un presupuesto de tamaño y tiempo sobre el contenido de cada subsistema. A medida que crecen los sistemas de almacenamiento, los presupuestos de AutoSupport proporcionan control sobre la carga útil de AutoSupport, que, a su vez, proporciona una entrega escalable de datos de AutoSupport.

AutoSupport deja de recopilar información y acorta el contenido de AutoSupport si el contenido del subsistema supera su tamaño o presupuesto para tiempo. Si el contenido no se puede truncar fácilmente (por ejemplo, archivos binarios), AutoSupport omite el contenido.

Solo debe modificar el tamaño y el presupuesto de tiempo predeterminados si el soporte de NetApp le solicita que lo haga. También puede revisar el tamaño predeterminado y los presupuestos de tiempo de los subsistemas mediante el `autosupport manifest show` comando.

### **Archivos enviados en mensajes AutoSupport activados por eventos**

Los mensajes AutoSupport activados por eventos sólo contienen información básica y de solución de problemas de subsistemas asociados al evento que provocó que AutoSupport genere el mensaje. Los datos específicos ayudan a los partners de soporte y soporte de NetApp a solucionar el problema.

AutoSupport utiliza los siguientes criterios para controlar el contenido de los mensajes de AutoSupport activados por un evento:

- Qué subsistemas están incluidos

Los datos se agrupan en subsistemas, incluidos subsistemas comunes, como los archivos de registro y subsistemas específicos, como RAID. Cada evento activa un mensaje que sólo contiene los datos de subsistemas específicos.

- El nivel de detalle de cada subsistema incluido

Los datos de cada subsistema incluido se proporcionan a nivel básico o de resolución de problemas.

Puede ver todos los eventos posibles y determinar qué subsistemas se incluyen en los mensajes acerca de cada evento mediante el `system node autosupport trigger show` con el `-instance` parámetro.

Además de los subsistemas incluidos de forma predeterminada para cada evento, puede agregar subsistemas adicionales en un nivel básico o de solución de problemas mediante el `system node autosupport trigger modify` comando.

## Archivos de registro enviados en mensajes de AutoSupport

Los mensajes de AutoSupport pueden contener varios archivos de registro clave que permiten al personal de soporte técnico revisar la actividad reciente del sistema.

Todos los tipos de mensajes de AutoSupport pueden incluir los siguientes archivos de registro cuando el subsistema de archivos de registro está habilitado:

| Archivo de registro                                                                                                                                                                                                                          | Cantidad de datos incluidos del archivo                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>Archivos de registro de /mroot/etc/log/mlog/ directorio</li><li>El archivo de registro DE MENSAJES</li></ul>                                                                                           | <p>Solo se han añadido líneas nuevas a los registros desde el último mensaje de AutoSupport hasta un máximo especificado. Esto garantiza que los mensajes AutoSupport tengan datos únicos, relevantes, no superpuestos.</p> <p>(Los archivos de registro de los partners son la excepción; para los partners, se incluyen los datos máximos permitidos).</p> |
| <ul style="list-style-type: none"><li>Archivos de registro de /mroot/etc/log/shelflog/ directorio</li><li>Archivos de registro de /mroot/etc/log/acp/ directorio</li><li>Datos de registro del sistema de gestión de eventos (EMS)</li></ul> | Las líneas de datos más recientes hasta un máximo especificado.                                                                                                                                                                                                                                                                                              |

El contenido de los mensajes de AutoSupport puede cambiar entre las versiones de ONTAP.

## Archivos enviados en mensajes semanales de AutoSupport

Los mensajes semanales de AutoSupport contienen datos adicionales de configuración y estado que son útiles para realizar el seguimiento de los cambios que se producen en el sistema a lo largo del tiempo.

La siguiente información se envía en mensajes semanales de AutoSupport:

- Información básica sobre cada subsistema
- Contenido de seleccionado /mroot/etc archivos de directorio
- Archivos de registro
- Resultado de comandos que proporcionan información del sistema
- Información adicional, incluida la información de la base de datos replicada (RDB), las estadísticas de servicio, etc.

## De qué manera AutoSupport OnDemand obtiene instrucciones de entrega del soporte técnico

AutoSupport OnDemand se comunica periódicamente con el soporte técnico para obtener instrucciones de entrega para enviar, reenviar y rechazar mensajes de AutoSupport, así como para cargar archivos de gran tamaño en el sitio de soporte de

NetApp. AutoSupport OnDemand permite enviar mensajes de AutoSupport bajo demanda en lugar de esperar a que se ejecute el trabajo de AutoSupport semanal.

OnDemand de AutoSupport consta de los siguientes componentes:

- Cliente OnDemand de AutoSupport que se ejecuta en cada nodo
- Servicio OnDemand de AutoSupport que reside en el soporte técnico

El cliente OnDemand de AutoSupport sondea periódicamente el servicio AutoSupport OnDemand para obtener instrucciones de entrega del soporte técnico. Por ejemplo, el soporte técnico puede utilizar el servicio AutoSupport OnDemand para solicitar que se genere un nuevo mensaje de AutoSupport. Cuando el cliente AutoSupport OnDemand sondea el servicio AutoSupport OnDemand, el cliente obtiene las instrucciones de entrega y envía el nuevo mensaje de AutoSupport bajo demanda según corresponda.

AutoSupport OnDemand está habilitado de forma predeterminada. Sin embargo, AutoSupport OnDemand utiliza algunos ajustes de AutoSupport para continuar comunicándose con el soporte técnico. AutoSupport OnDemand se comunica automáticamente con el soporte técnico cuando se cumplen los siguientes requisitos:

- AutoSupport está habilitado.
- AutoSupport está configurado para enviar mensajes al soporte técnico.
- AutoSupport se configura para utilizar el protocolo de transporte HTTPS.

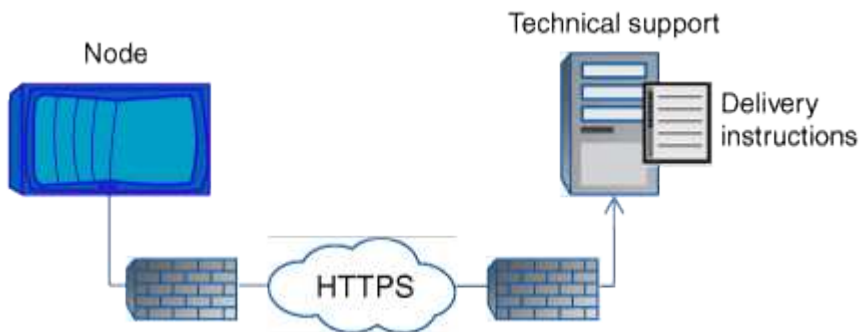
El cliente AutoSupport OnDemand envía solicitudes HTTPS a la misma ubicación de soporte técnico a la que se envían los mensajes de AutoSupport. El cliente AutoSupport OnDemand no acepta conexiones entrantes.



AutoSupport OnDemand utiliza la cuenta de usuario «'AutoSupport'» para comunicarse con la asistencia técnica. ONTAP le impide eliminar esta cuenta.

Si desea deshabilitar AutoSupport OnDemand, pero mantener AutoSupport habilitado, utilice el comando:  
Link: [https://docs.netapp.com/us-en/ontap-cli-9121/system-node-autosupport-modify.html#parameters\[system node autosupport modify -ondemand-state disable\]](https://docs.netapp.com/us-en/ontap-cli-9121/system-node-autosupport-modify.html#parameters[system node autosupport modify -ondemand-state disable]).

En la siguiente ilustración, se muestra cómo AutoSupport OnDemand envía las solicitudes HTTPS al soporte técnico para obtener instrucciones de entrega.



Las instrucciones de entrega pueden incluir solicitudes para que AutoSupport haga lo siguiente:

- Generar nuevos mensajes de AutoSupport.

El soporte técnico puede solicitar nuevos mensajes de AutoSupport como ayuda para la clasificación de problemas.



- Genere nuevos mensajes de AutoSupport que cargan archivos de volcado principales o archivos de archivado de rendimiento en el sitio de soporte de NetApp.

El soporte técnico puede solicitar un volcado de memoria o archivos de archivado de rendimiento que ayuden a clasificar los problemas.

- Retransmita mensajes de AutoSupport generados previamente.

Esta solicitud se produce automáticamente si no se ha recibido un mensaje debido a un fallo de entrega.

- Deshabilite la entrega de mensajes de AutoSupport para eventos de activación específicos.

El soporte técnico puede deshabilitar la entrega de datos que no se utiliza.

## Estructura de los mensajes AutoSupport enviados por correo electrónico

Cuando se envía un mensaje AutoSupport por correo electrónico, el mensaje tiene un asunto estándar, un cuerpo breve y un archivo adjunto grande en formato de archivo 7z que contiene los datos.



Si AutoSupport está configurado para ocultar datos privados, cierta información, como el nombre de host, se omite o se oculta en el encabezado, el asunto, el cuerpo y los datos adjuntos.

### Asunto

La línea de asunto de los mensajes enviados por el mecanismo AutoSupport contiene una cadena de texto que identifica el motivo de la notificación. El formato de la línea del asunto es el siguiente:

Notificación DE grupo HA de *System\_Name (Message) Severity*

- *System\_Name* es el nombre de host o el ID del sistema, según la configuración de AutoSupport

### Cuerpo

El cuerpo del mensaje de AutoSupport contiene la siguiente información:

- Fecha y Marca de hora del mensaje
- Versión de ONTAP en el nodo que generó el mensaje
- El ID del sistema, el número de serie y el nombre de host del nodo que generó el mensaje
- Número de secuencia de AutoSupport
- Nombre y ubicación del contacto SNMP, si se especifica
- El ID del sistema y el nombre de host del partner de alta disponibilidad

### Archivos adjuntos

La información clave de un mensaje de AutoSupport contiene archivos comprimidos en un archivo 7z llamado *body.7z* y adjunto al mensaje.

Los archivos contenidos en el archivo adjunto son específicos del tipo de mensaje AutoSupport.

## Tipos de gravedad de AutoSupport

Los mensajes de AutoSupport tienen tipos de gravedad que le ayudan a entender el propósito de cada mensaje, por ejemplo, para llamar la atención inmediata a un problema de emergencia, o sólo para proporcionar información.

Los mensajes tienen una de las siguientes gravedades:

- **Alerta:** Los mensajes de alerta indican que podría producirse un evento de nivel superior si no realiza alguna acción.

Debe realizar una acción contra los mensajes de alerta en un plazo de 24 horas.

- **Emergencia:** Los mensajes de emergencia se muestran cuando se produce una interrupción.

Usted debe tomar una acción contra los mensajes de emergencia inmediatamente.

- **Error:** Las condiciones de error indican lo que podría suceder si ignora.
- **Aviso:** Condición normal pero significativa.
- **Info:** El mensaje informativo proporciona detalles sobre el problema, que usted puede ignorar.
- **Depurar:** Los mensajes de nivel de depuración proporcionan instrucciones que debe realizar.

Si su organización de soporte interno recibe mensajes de AutoSupport por correo electrónico, la gravedad aparecerá en la línea del asunto del mensaje de correo electrónico.

## Requisitos para usar AutoSupport

Debe utilizar HTTPS con TLSv1,2 o SMTP seguro para la entrega de mensajes de AutoSupport a fin de proporcionar la mejor seguridad y admitir todas las funciones de AutoSupport más recientes. Se rechazarán los mensajes de AutoSupport entregados con cualquier otro protocolo.

### Protocolos compatibles

Todos estos protocolos se ejecutan en IPv4 o IPv6, según la familia de direcciones a la que se resuelve el nombre.

| Protocolo y puerto                 | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HTTPS en el puerto 443             | <p>Este es el protocolo predeterminado. Debe utilizarlo siempre que sea posible.</p> <p>Este protocolo es compatible con AutoSupport OnDemand y la carga de archivos de gran tamaño.</p> <p>El certificado del servidor remoto se valida con el certificado raíz, a menos que se deshabilite la validación.</p> <p>La entrega utiliza una solicitud PUT HTTPS. Con PUT, si la solicitud falla durante la transmisión, la solicitud se reinicia donde se detuvo. Si el servidor que recibe la solicitud no admite PUT, la entrega utiliza una solicitud POST HTTPS.</p>                                                                                                                                                                   |
| HTTP en el puerto 80               | <p>Este protocolo es el más preferido que SMTP.</p> <p>Este protocolo admite cargas de archivos de gran tamaño, pero no AutoSupport OnDemand.</p> <p>La entrega utiliza una solicitud PUT HTTPS. Con PUT, si la solicitud falla durante la transmisión, la solicitud se reinicia donde se detuvo. Si el servidor que recibe la solicitud no admite PUT, la entrega utiliza una solicitud POST HTTPS.</p>                                                                                                                                                                                                                                                                                                                                 |
| SMTP en el puerto 25 u otro puerto | <p>Solo debe utilizar este protocolo si la conexión de red no permite HTTPS.</p> <p>El valor predeterminado del puerto es 25, pero puede configurar AutoSupport para que utilice un puerto diferente.</p> <p>Tenga en cuenta las siguientes limitaciones al utilizar SMTP:</p> <ul style="list-style-type: none"> <li>• No se admiten las cargas de archivos de gran tamaño bajo demanda de AutoSupport.</li> <li>• Los datos no están cifrados.</li> </ul> <p>SMTP envía datos en texto sin cifrar, haciendo que el texto en el mensaje de AutoSupport sea fácil de interceptar y leer.</p> <ul style="list-style-type: none"> <li>• Se pueden introducir limitaciones en la longitud del mensaje y la longitud de la línea.</li> </ul> |

Si configura AutoSupport con direcciones de correo electrónico específicas para su organización de soporte interno o una organización de partner de soporte, esos mensajes siempre los envía SMTP.

Por ejemplo, si utiliza el protocolo recomendado para enviar mensajes al soporte técnico y también desea enviar mensajes a la organización de soporte interno, los mensajes se transportarán mediante HTTPS y SMTP, respectivamente.

AutoSupport limita el tamaño máximo de archivo para cada protocolo. La configuración predeterminada para las transferencias HTTP y HTTPS es 25 MB. El valor predeterminado para las transferencias SMTP es 5 MB. Si el tamaño del mensaje de AutoSupport supera el límite configurado, AutoSupport entregará la mayor parte posible del mensaje. Se puede editar el tamaño máximo modificando la configuración de AutoSupport. Consulte `system node autosupport modify manual` para más información.



AutoSupport anula automáticamente el límite de tamaño máximo de archivo de los protocolos HTTPS y HTTP cuando se generan y envían mensajes de AutoSupport que cargan archivos de volcado principales o de archivo de rendimiento al sitio de soporte de NetApp o un URI especificado. La anulación automática sólo se aplica cuando se cargan archivos mediante el `system node autosupport invoke-core-upload` o la `system node autosupport invoke-performance-archive` comandos.

### Requisitos de configuración

Dependiendo de la configuración de red, el protocolo HTTPS puede requerir una configuración adicional de una URL de proxy. Si HTTPS envía mensajes de AutoSupport al soporte técnico y tiene un proxy, debe identificar la URL de ese proxy. Si el proxy utiliza un puerto distinto del predeterminado, que es 3128, puede especificar el puerto para ese proxy. También puede especificar un nombre de usuario y una contraseña para la autenticación del proxy.

Si utiliza SMTP para enviar mensajes de AutoSupport a la organización de soporte interno o al soporte técnico, debe configurar un servidor de correo externo. El sistema de almacenamiento no funciona como un servidor de correo; requiere un servidor de correo externo en su sitio para enviar correo. El servidor de correo debe ser un host que escucha en el puerto SMTP (25) u otro puerto, y debe estar configurado para enviar y recibir codificación MIME (Extensiones multipropósito de correo Internet) de 8 bits. Los hosts de correo de ejemplo incluyen un host UNIX que ejecuta un servidor SMTP como el programa sendmail y un servidor Windows que ejecuta el servidor Microsoft Exchange. Puede tener uno o más hosts de correo.

### Configure AutoSupport

Puede controlar si la información de AutoSupport se envía al soporte técnico y a la organización de soporte interna, y luego probar que la configuración es correcta.

### Acerca de esta tarea

En ONTAP 9.5 y versiones posteriores, es posible habilitar AutoSupport y modificar su configuración en todos los nodos del clúster de forma simultánea. Cuando un nuevo nodo se une al clúster, el nodo hereda automáticamente la configuración del clúster de AutoSupport. No es necesario actualizar la configuración en cada nodo por separado.



A partir de ONTAP 9.5, el ámbito de la `system node autosupport modify` el comando se encuentra en todo el clúster. La configuración de AutoSupport se modifica en todos los nodos del clúster, incluso cuando el `-node` se especifica la opción. La opción se omite, pero se conserva para la compatibilidad con versiones anteriores de la CLI.

En ONTAP 9.4 y versiones anteriores, el alcance del `system node autosupport modify` el comando es específico del nodo. La configuración de AutoSupport debe modificarse en cada nodo del clúster.

De manera predeterminada, AutoSupport se habilita en cada nodo para enviar mensajes al soporte técnico mediante el protocolo de transporte HTTPS.

Debe utilizar HTTPS con TLSv1,2 o SMTP seguro para la entrega de mensajes de AutoSupport a fin de proporcionar la mejor seguridad y admitir todas las funciones de AutoSupport más recientes.

**Pasos**

- 1. Asegúrese de que AutoSupport esté habilitado:

```
system node autosupport modify -state enable
```

- 2. Si desea que el soporte técnico reciba mensajes de AutoSupport, utilice el comando siguiente:

```
system node autosupport modify -support enable
```

Debe habilitar esta opción si desea habilitar AutoSupport para trabajar con AutoSupport OnDemand o si desea cargar archivos grandes, como archivos de volcado de memoria y de archivo de rendimiento, al soporte técnico o una URL específica.

- 3. Si el soporte técnico está habilitado para recibir mensajes de AutoSupport, especifique el protocolo de transporte que debe utilizar para los mensajes.

Es posible elegir entre las siguientes opciones:

|                                            |                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Si desea...                                | A continuación, configure los siguientes parámetros del <code>system node autosupport modify</code> comando...                                                                                                                                                                                                                   |
| Utilizar el protocolo HTTPS predeterminado | <ul style="list-style-type: none"><li>a. Configurado <code>-transport</code> para <code>https</code>.</li><li>b. Si utiliza un proxy, establezca <code>-proxy-url</code> A la dirección URL de su proxy.<br/>Esta configuración admite la comunicación con AutoSupport OnDemand y la carga de archivos de gran tamaño.</li></ul> |
| Utilice SMTP                               | <p>Configurado <code>-transport</code> para <code>smtp</code>.</p> <p>Esta configuración no admite AutoSupport OnDemand ni la carga de archivos de gran tamaño.</p>                                                                                                                                                              |

- 4. Si desea que su organización de soporte interno o un partner de soporte reciban mensajes de AutoSupport, realice las siguientes acciones:
  - a. Identifique a los destinatarios de su organización estableciendo los siguientes parámetros de `system node autosupport modify` comando:

|                              |           |
|------------------------------|-----------|
| Configurar este parámetro... | A esto... |
|------------------------------|-----------|

|                  |                                                                                                                                                                                                                                                                                      |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -to              | Hasta cinco direcciones de correo electrónico individuales separadas por comas o listas de distribución en su organización de soporte interno que recibirán mensajes clave de AutoSupport                                                                                            |
| -noteto          | Hasta cinco direcciones de correo electrónico individuales separadas por comas o listas de distribución en su organización de soporte interno que recibirán una versión abreviada de los mensajes clave de AutoSupport diseñados para teléfonos móviles y otros dispositivos móviles |
| -partner-address | Hasta cinco direcciones de correo electrónico individuales separadas por comas o listas de distribución en su organización de partners de soporte que recibirán todos los mensajes de AutoSupport                                                                                    |

b. Compruebe que las direcciones se han configurado correctamente enumerando los destinos mediante el `system node autosupport destinations show` comando.

5. Si va a enviar mensajes a su organización de soporte interno o ha elegido el transporte SMTP para mensajes al soporte técnico, configure SMTP estableciendo los siguientes parámetros de `system node autosupport modify` comando:

- Configurado `-mail-hosts` en uno o más hosts de correo, separados por comas.

Puede establecer un máximo de cinco.

Puede configurar un valor de puerto para cada host de correo especificando dos puntos y un número de puerto después del nombre de host de correo: Por ejemplo, `mymailhost.example.com:5678`, donde 5678 es el puerto del host de correo.

- Configurado `-from` A la dirección de correo electrónico que envía el mensaje AutoSupport.

6. Configure DNS.

7. Opcionalmente, agregue opciones de comando si desea cambiar ajustes específicos:

|                                                                                                   |                                                                                                                                                                                                                            |
|---------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Si desea hacer esto...                                                                            | A continuación, configure los siguientes parámetros del <code>system node autosupport modify</code> comando...                                                                                                             |
| Oculte datos privados eliminando, enmascarando o codificando datos confidenciales en los mensajes | Configurado <code>-remove-private-data</code> para <code>true</code> . Si cambia de <code>false</code> para <code>true</code> , Se eliminan todos los archivos de historial de AutoSupport y todos los archivos asociados. |
| Detenga el envío de datos de rendimiento en mensajes periódicos de AutoSupport                    | Configurado <code>-perf</code> para <code>false</code> .                                                                                                                                                                   |

8. Compruebe la configuración general mediante el `system node autosupport show` con el `-node`

parámetro.

9. Verifique el funcionamiento de la AutoSupport mediante el `system node autosupport check show` comando.

Si se informa de algún problema, utilice `system node autosupport check show-details` comando para ver más información.

10. Comprobar que se envían y reciben mensajes de AutoSupport:

- a. Utilice la `system node autosupport invoke` con el `-type` parámetro establecido en test.

```
cluster1::> system node autosupport invoke -type test -node node1
```

- b. Confirme que NetApp recibe sus mensajes de AutoSupport:

el historial de AutoSupport del nodo del sistema muestra `-node local`

El estado del último mensaje AutoSupport saliente debería cambiar a `sent-successful` para todos los destinos de protocolo adecuados.

- a. De manera opcional, si el mensaje de AutoSupport se envía a la organización de soporte interna o a su partner de soporte, consulte el correo electrónico de cualquier dirección que haya configurado para el `-to`, `-noteto`, o. `-partner-address` parámetros de `system node autosupport modify` comando.

## Cargar archivos de volcado principales

Cuando se guarda un archivo de volcado principal, se genera un mensaje de evento. Si el servicio AutoSupport está habilitado y configurado para enviar mensajes al soporte de NetApp, se transmite un mensaje AutoSupport y se le envía un mensaje de correo electrónico de confirmación automatizado.

### Lo que necesitará

- Debe haber configurado AutoSupport con las siguientes opciones:
  - AutoSupport está habilitado en el nodo.
  - AutoSupport está configurado para enviar mensajes al soporte técnico.
  - AutoSupport está configurado para utilizar el protocolo de transporte HTTP o HTTPS.

El protocolo de transporte SMTP no se admite cuando se envían mensajes que incluyen archivos de gran tamaño, como archivos de volcado principales.

### Acerca de esta tarea

También se puede cargar el archivo de volcado principal a través del servicio AutoSupport mediante HTTPS con el `system node autosupport invoke-core-upload` Si lo solicita el soporte de NetApp.

## "Cómo cargar un archivo en NetApp"

### Pasos

1. Vea los archivos de volcado principales de un nodo mediante el `system node coredump show`

comando.

En el siguiente ejemplo, se muestran los archivos de volcado principales para el nodo local:

```
cluster1::> system node coredump show -node local
Node:Type Core Name Saved Panic Time

node:kernel
core.4073000068.2013-09-11.15_05_01.nz true 9/11/2013 15:05:01
```

2. Genere un mensaje de AutoSupport y cargue un archivo de volcado principal con la `system node autosupport invoke-core-upload` comando.

En el siguiente ejemplo, se genera un mensaje de AutoSupport y se envía a la ubicación predeterminada, es decir, al soporte técnico, y el archivo de volcado principal se carga en la ubicación predeterminada, que es el sitio de soporte de NetApp:

```
cluster1::> system node autosupport invoke-core-upload -core-filename
core.4073000068.2013-09-11.15_05_01.nz -node local
```

En el ejemplo siguiente, se genera un mensaje de AutoSupport que se envía a la ubicación especificada en el URI y el archivo de volcado principal se carga en el URI:

```
cluster1::> system node autosupport invoke-core-upload -uri
https://files.company.com -core-filename
core.4073000068.2013-09-11.15_05_01.nz -node local
```

## Cargue archivos de archivado de rendimiento

Puede generar y enviar un mensaje de AutoSupport que contenga un archivo de rendimiento. De forma predeterminada, el soporte técnico de NetApp recibe el mensaje AutoSupport y el archivo de rendimiento se carga en el sitio de soporte de NetApp. Puede especificar un destino alternativo para el mensaje y cargarlo.

### Lo que necesitará

- Debe haber configurado AutoSupport con las siguientes opciones:
  - AutoSupport está habilitado en el nodo.
  - AutoSupport está configurado para enviar mensajes al soporte técnico.
  - AutoSupport está configurado para utilizar el protocolo de transporte HTTP o HTTPS.

El protocolo de transporte SMTP no se admite cuando se envían mensajes que incluyen archivos de gran tamaño, como archivos de archivado de rendimiento.



## Acerca de esta tarea

Debe especificar una fecha de inicio para los datos de archivo de rendimiento que desea cargar. La mayoría de los sistemas de almacenamiento conservan los archivos de rendimiento durante dos semanas, lo que permite especificar una fecha de inicio hasta hace dos semanas. Por ejemplo, si hoy es el 15 de enero, puede especificar una fecha de inicio del 2 de enero.

## Paso

1. Genere un mensaje de AutoSupport y cargue el archivo de archivado de rendimiento mediante la `system node autosupport invoke-performance-archive` comando.

En el siguiente ejemplo, se añaden 4 horas de archivos de archivado de rendimiento desde el 12 de enero de 2015 a un mensaje de AutoSupport y se cargan en la ubicación predeterminada, que es el sitio de soporte de NetApp:

```
cluster1::> system node autosupport invoke-performance-archive -node
local -start-date 1/12/2015 13:42:09 -duration 4h
```

En el siguiente ejemplo, se agregan 4 horas de archivos de rendimiento desde el 12 de enero de 2015 a un mensaje de AutoSupport y se cargan en la ubicación especificada por el URI:

```
cluster1::> system node autosupport invoke-performance-archive -node
local -start-date 1/12/2015 13:42:09 -duration 4h -uri
https://files.company.com
```

## Obtener descripciones de mensajes de AutoSupport

Las descripciones de los mensajes de AutoSupport que recibe están disponibles a través del traductor de syslog de ONTAP.

## Pasos

1. Vaya a la ["Traductor de syslog"](#).
2. En el campo **Versión**, introduzca la versión de ONTAP que está utilizando. En el campo **cadena de búsqueda**, introduzca "callhome". Seleccione **Traducir**.
3. Syslog Translator mostrará alfabéticamente todos los eventos que coincidan con la cadena de mensaje introducida.

## Comandos para gestionar AutoSupport

Utilice la `system node autosupport` Comandos para cambiar o ver la configuración de AutoSupport, mostrar información acerca de mensajes anteriores de AutoSupport y enviar, reenviar o cancelar un mensaje de AutoSupport.

## Configure AutoSupport

| Si desea...                                                                                                                                                                                                                                                                  | Se usa este comando...                                                             |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| Controle si se envían mensajes de AutoSupport                                                                                                                                                                                                                                | <code>system node autosupport modify</code> con la <code>-state</code> parámetro   |
| Controlar si se envían mensajes de AutoSupport al soporte técnico                                                                                                                                                                                                            | <code>system node autosupport modify</code> con la <code>-support</code> parámetro |
| Configure AutoSupport o modifique la configuración de AutoSupport                                                                                                                                                                                                            | <code>system node autosupport modify</code>                                        |
| Habilite y deshabilite los mensajes de AutoSupport a su organización de soporte interno para eventos de activación individuales y especifique informes de subsistema adicionales que se incluirán en los mensajes enviados en respuesta a eventos de activación individuales | <code>system node autosupport trigger modify</code>                                |

#### Muestra información acerca de la configuración de AutoSupport



| Si desea...                                                                                                                    | Se usa este comando...                                                        |
|--------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| Mostrar la configuración de AutoSupport                                                                                        | <code>system node autosupport show</code> con la <code>-node</code> parámetro |
| Vea un resumen de todas las direcciones y direcciones URL que reciben mensajes de AutoSupport                                  | <code>system node autosupport destinations show</code>                        |
| Mostrar los mensajes de AutoSupport que se envían a su organización de soporte interno para eventos de activación individuales | <code>system node autosupport trigger show</code>                             |
| Mostrar el estado de la configuración de AutoSupport, así como la entrega a varios destinos                                    | <code>system node autosupport check show</code>                               |
| Mostrar el estado detallado de la configuración de AutoSupport, así como la entrega a varios destinos                          | <code>system node autosupport check show-details</code>                       |

#### Muestra información acerca de los mensajes anteriores de AutoSupport

| Si desea...                                                                             | Se usa este comando...                            |
|-----------------------------------------------------------------------------------------|---------------------------------------------------|
| Muestra información acerca de uno o más de los 50 mensajes de AutoSupport más recientes | <code>system node autosupport history show</code> |

| Si desea...                                                                                                                                                                                            | Se usa este comando...                                           |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|
| Muestra información sobre los mensajes de AutoSupport recientes generados para cargar archivos de volcado principal o de archivado de rendimiento en el sitio de soporte técnico o un URI especificado | <code>system node autosupport history show-upload-details</code> |
| Vea la información de los mensajes de AutoSupport, incluidos el nombre y el tamaño de cada archivo recopilado para el mensaje, junto con cualquier error                                               | <code>system node autosupport manifest show</code>               |

#### Enviar, reenviar o cancelar mensajes de AutoSupport

| Si desea...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Se usa este comando...                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Retransmitir un mensaje AutoSupport almacenado localmente, identificado por su número de secuencia AutoSupport</p> <div>  <p>Si retransmite un mensaje de AutoSupport y si la compatibilidad ya recibió ese mensaje, el sistema de soporte no creará una incidencia duplicada. Si, por otro lado, el soporte no recibió ese mensaje, entonces el sistema AutoSupport analizará el mensaje y creará un caso, si es necesario.</p> </div> | <code>system node autosupport history retransmit</code>                                                                                                                                                                                                                                                                                                                                   |
| <p>Generar y enviar un mensaje de AutoSupport, por ejemplo, con fines de pruebas</p>                                                                                                                                                                                                                                                                                                                                                                                                                                         | <code>system node autosupport invoke</code> <div>  <p>Utilice la <code>-force</code> Parámetro para enviar un mensaje incluso si AutoSupport está deshabilitado. Utilice la <code>-uri</code> parámetro para enviar el mensaje al destino que especifique en lugar del destino configurado.</p> </div> |
| <p>Cancelar un mensaje de AutoSupport</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <code>system node autosupport history cancel</code>                                                                                                                                                                                                                                                                                                                                       |

#### Información relacionada

["Comandos de ONTAP 9"](#)

#### La información incluida en el manifiesto AutoSupport

El manifiesto AutoSupport ofrece una vista detallada de los archivos recopilados para cada mensaje de AutoSupport. El manifiesto AutoSupport también incluye información sobre los errores de recopilación cuando AutoSupport no puede recopilar los archivos

que necesita.

El manifiesto de AutoSupport incluye la siguiente información:

- Número de secuencia del mensaje AutoSupport
- Qué archivos incluye AutoSupport en el mensaje AutoSupport
- Tamaño de cada archivo, en bytes
- Estado de la colección de manifiesto AutoSupport
- Descripción del error, si AutoSupport no pudo recopilar uno o varios archivos

Puede ver el manifiesto AutoSupport mediante la `system node autosupport manifest show` comando.

El manifiesto AutoSupport se incluye con todos los mensajes de AutoSupport y se presenta en formato XML, lo que significa que puede utilizar un visor XML genérico para leerlo o verlo utilizando el portal Active IQ (anteriormente conocido como My AutoSupport).

### Supresión de casos AutoSupport durante las ventanas de mantenimiento programadas

La supresión de casos de AutoSupport permite impedir que se creen casos innecesarios mediante mensajes de AutoSupport que se activan durante las ventanas de mantenimiento programadas.

Para suprimir casos de AutoSupport, debe invocar manualmente un mensaje de AutoSupport con una cadena de texto con formato especial: `MAINT=xh`. `x` es la duración del plazo de mantenimiento en unidades de horas.

#### Información relacionada

["Cómo impedir la creación automática de casos durante las ventanas de mantenimiento programado"](#)

### Solucionar problemas de AutoSupport cuando no se reciben mensajes

Si el sistema no envía el mensaje de AutoSupport, puede determinar si esto es porque AutoSupport no puede generar el mensaje o no puede entregar el mensaje.

#### Pasos

1. Compruebe el estado de entrega de los mensajes mediante el `system node autosupport history show` comando.
2. Lea el estado.

| Este estado           | Medios                                                                                                                                                                                                                 |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| inicializando         | Se está iniciando el proceso de recopilación. Si este estado es temporal, todo está bien. Sin embargo, si este estado persiste, hay un problema.                                                                       |
| error de recopilación | AutoSupport no puede crear el contenido de AutoSupport en el directorio de spool. Para ver qué está intentando recopilar AutoSupport, introduzca el <code>system node autosupport history show -detail</code> comando. |

| Este estado               | Medios                                                                                                                                                                                                                                                       |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| recogida en curso         | AutoSupport está recopilando contenido de AutoSupport. Para ver la recopilación de AutoSupport, introduzca la <code>system node autosupport manifest show</code> comando.                                                                                    |
| en cola                   | Los mensajes de AutoSupport se ponen en cola para su entrega, pero aún no se han entregado.                                                                                                                                                                  |
| transmitiendo             | AutoSupport proporciona mensajes actualmente.                                                                                                                                                                                                                |
| enviado correctamente     | AutoSupport ha entregado el mensaje correctamente. Para averiguar dónde ha entregado el mensaje AutoSupport, introduzca el <code>system node autosupport history show -delivery</code> comando.                                                              |
| ignorar                   | AutoSupport no tiene destinos para el mensaje. Para ver los detalles de la entrega, introduzca la <code>system node autosupport history show -delivery</code> comando.                                                                                       |
| volver a poner en cola    | AutoSupport intentó entregar mensajes, pero el intento falló. Como resultado, AutoSupport volvió a colocar los mensajes en la cola de entrega para otro intento. Para ver el error, introduzca el <code>system node autosupport history show</code> comando. |
| la transmisión ha fallado | AutoSupport no pudo entregar el mensaje el número especificado de veces y dejó de intentar entregar el mensaje. Para ver el error, introduzca el <code>system node autosupport history show</code> comando.                                                  |
| ondemand-ignore           | El mensaje AutoSupport se procesó correctamente, pero el servicio OnDemand de AutoSupport decidió ignorarlo.                                                                                                                                                 |

3. Ejecute una de las siguientes acciones:

| Para este estado                                                            | Haga esto                                                                                                                                                                                                                                                       |
|-----------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| error de inicialización o recopilación                                      | <p>Póngase en contacto con el soporte de NetApp, porque AutoSupport no puede generar el mensaje. Mencione el siguiente artículo de la base de conocimientos:</p> <p><a href="#">"AutoSupport no puede proporcionar: Estado bloqueado en inicialización"</a></p> |
| se ha producido un error al ignorar, volver a poner en cola o al transmitir | Compruebe que los destinos estén configurados correctamente para SMTP, HTTP o HTTPS porque AutoSupport no puede entregar el mensaje.                                                                                                                            |

## Solucione problemas de entrega de mensajes de AutoSupport a través de HTTP o HTTPS

Si el sistema no envía el mensaje AutoSupport esperado y utiliza HTTP o HTTPS, o la función de actualización automática no está funcionando, puede comprobar una serie de configuraciones para resolver el problema.

### Lo que necesitará

Debe haber confirmado la conectividad de red básica y la búsqueda de DNS:

- El LIF de gestión de nodos debe estar activo para tener el estado operativo y administrativo.
- Debe poder hacer ping a un host en funcionamiento en la misma subred desde la LIF de gestión del clúster (no una LIF en ninguno de los nodos).
- Debe poder hacer ping a un host en funcionamiento fuera de la subred desde la LIF de administración de clústeres.
- Debe poder hacer ping a un host en funcionamiento fuera de la subred desde la LIF de administración de clústeres con el nombre del host (no la dirección IP).

### Acerca de esta tarea

Estos pasos son para casos en los que se ha determinado que AutoSupport puede generar el mensaje, pero no puede entregarlo a través de HTTP o HTTPS.

Si encuentra errores o no puede completar un paso de este procedimiento, determine y resuelva el problema antes de continuar con el siguiente paso.

### Pasos

1. Muestre el estado detallado del subsistema AutoSupport:

```
system node autosupport check show-details
```

Esto incluye verificar la conectividad a los destinos de AutoSupport, mediante el envío de mensajes de prueba y la provisión de una lista de los posibles errores en las opciones de configuración de AutoSupport.

2. Compruebe el estado de la LIF de gestión de nodos:

```
network interface show -home-node local -role node-mgmt -fields
vserver,lif,status-oper,status-admin,address,role
```

La status-oper y.. status-admin los campos deberán devolver «'up'».

3. Registre el nombre de la SVM, el nombre de la LIF y la dirección IP de la LIF para usarlos más adelante.
4. Asegúrese de que DNS esté habilitado y configurado correctamente:

```
vserver services name-service dns show
```

5. Resuelva los errores devueltos por el mensaje de AutoSupport:

```
system node autosupport history show -node * -fields node,seq-
num,destination,last-update,status,error
```

Para obtener ayuda sobre la solución de problemas de los errores devueltos, consulte ["Guía de resolución de ONTAP AutoSupport \(Transport HTTPS y HTTP\)"](#).

6. Confirme que el clúster puede acceder a los servidores que necesita y a Internet correctamente:

- a. `network traceroute -lif node-management_LIF -destination DNS server`
- b. `network traceroute -lif node_management_LIF -destination support.netapp.com`



La dirección `support.netapp.com` en sí mismo no responde a ping/traceroute, pero la información por salto es valiosa.

- c. `system node autosupport show -fields proxy-url`
- d. `network traceroute -node node_management_LIF -destination proxy_url`

Si alguna de estas rutas no funciona, pruebe la misma ruta desde un host en funcionamiento en la misma subred que el clúster, utilizando la utilidad «'traceroute' o «'tracert'» que se encuentra en la mayoría de los clientes de red de terceros. Esto le ayuda a determinar si el problema está en la configuración de red o en la configuración del clúster.

7. Si utiliza HTTPS para el protocolo de transporte AutoSupport, asegúrese de que el tráfico HTTPS pueda salir de la red:

- a. Configure un cliente web en la misma subred que la LIF de gestión de clústeres.

Asegúrese de que todos los parámetros de configuración sean los mismos valores que para la configuración de AutoSupport, incluido el uso del mismo servidor proxy, nombre de usuario, contraseña y puerto.

- b. Acceso `https://support.netapp.com` con el cliente web.

El acceso debe ser correcto. Si no es así, asegúrese de que todos los firewalls estén configurados correctamente para permitir el tráfico HTTPS y DNS, y de que el servidor proxy esté configurado correctamente. Para obtener más información sobre la configuración de la resolución de nombres estáticos para `support.netapp.com`, consulte el artículo de Knowledge base ["Cómo se puede añadir una entrada DE HOST en ONTAP para la versión support.netapp.com?"](#)

8. A partir de ONTAP 9.10.1, si ha activado la función de actualización automática, asegúrese de que dispone de conectividad HTTPS con las siguientes direcciones URL adicionales:

- `https://support-sg-emea.netapp.com`
- `https://support-sg-naeast.netapp.com`
- `https://support-sg-nawest.netapp.com`

## Solucionar los problemas de entrega de mensajes de AutoSupport a través de SMTP

Si el sistema no puede entregar mensajes de AutoSupport a través de SMTP, puede comprobar una serie de opciones para resolver el problema.

### Lo que necesitará

Debe haber confirmado la conectividad de red básica y la búsqueda de DNS:

- El LIF de gestión de nodos debe estar activo para tener el estado operativo y administrativo.
- Debe poder hacer ping a un host en funcionamiento en la misma subred desde la LIF de gestión del clúster (no una LIF en ninguno de los nodos).

- Debe poder hacer ping a un host en funcionamiento fuera de la subred desde la LIF de administración de clústeres.
- Debe poder hacer ping a un host en funcionamiento fuera de la subred desde la LIF de administración de clústeres con el nombre del host (no la dirección IP).

### Acerca de esta tarea

Estos pasos son para casos en los que ha determinado que AutoSupport puede generar el mensaje, pero no puede entregarlo a través de SMTP.

Si encuentra errores o no puede completar un paso de este procedimiento, determine y resuelva el problema antes de continuar con el siguiente paso.

Todos los comandos se introducen en la interfaz de línea de comandos de ONTAP, a menos que se especifique lo contrario.

### Pasos

1. Compruebe el estado de la LIF de gestión de nodos:

```
network interface show -home-node local -role node-mgmt -fields
vserver,lif,status-oper,status-admin,address,role
```

La status-oper y.. status-admin los campos deben regresar up.

2. Registre el nombre de la SVM, el nombre de la LIF y la dirección IP de la LIF para usarlos más adelante.
3. Asegúrese de que DNS esté habilitado y configurado correctamente:

```
vserver services name-service dns show
```

4. Mostrar todos los servidores configurados para ser utilizados por AutoSupport:

```
system node autosupport show -fields mail-hosts
```

Registre todos los nombres de servidor mostrados.

5. Para cada servidor que se muestra en el paso anterior, y. `support.netapp.com`, Asegúrese de que el nodo puede acceder al servidor o a la URL:

```
network traceroute -node local -destination server_name
```

Si alguna de estas rutas no funciona, pruebe la misma ruta desde un host en funcionamiento en la misma subred que el clúster, utilizando la utilidad «'traceroute' o «'tracert'» que se encuentra en la mayoría de los clientes de red de terceros. Esto le ayuda a determinar si el problema está en la configuración de red o en la configuración del clúster.

6. Inicie sesión en el host designado como host de correo y asegúrese de que puede atender solicitudes SMTP:

```
netstat -aAn|grep 25
```

25 Es el número de puerto SMTP del listener.

Se muestra un mensaje similar al siguiente texto:



```
ff64878c tcp 0 0 *.25 *.* LISTEN.
```

7. Desde otro host, abra una sesión Telnet con el puerto SMTP del host de correo:

```
telnet mailhost 25
```

Se muestra un mensaje similar al siguiente texto:

```
220 filer.yourco.com Sendmail 4.1/SMI-4.1 ready at Thu, 30 Nov 2014
10:49:04 PST
```

8. En el símbolo de telnet, asegúrese de que se puede transmitir un mensaje desde su host de correo:

```
HELO domain_name
```

```
MAIL FROM: your_email_address
```

```
RCPT TO: autosupport@netapp.com
```

domain\_name es el nombre de dominio de la red.

Si se devuelve un error que indica que se deniega la retransmisión, la retransmisión no está activada en el host de correo. Póngase en contacto con el administrador del sistema.

9. En el símbolo de telnet, envíe un mensaje de prueba:

```
DATA
```

```
SUBJECT: TESTING
```

```
THIS IS A TEST
```

```
.
```



Asegúrese de introducir el último período (.) en una línea por sí misma. El período indica al host de correo que el mensaje ha finalizado.

Si se devuelve un error, el host de correo no está configurado correctamente. Póngase en contacto con el administrador del sistema.

10. Desde la interfaz de línea de comandos de ONTAP, envíe un mensaje de prueba de AutoSupport a una dirección de correo electrónico de confianza a la que tenga acceso:

```
system node autosupport invoke -node local -type test
```

11. Busque el número de secuencia del intento:

```
system node autosupport history show -node local -destination smtp
```

Busque el número de secuencia para su intento basado en la Marca de hora. Probablemente sea el intento más reciente.

12. Mostrar el error para el intento de mensaje de prueba:

```
system node autosupport history show -node local -seq-num seq_num -fields error
```

Si el error mostrado es `Login denied`, El servidor SMTP no acepta peticiones de envío desde la LIF de administración del clúster. Si no desea cambiar al uso de HTTPS como protocolo de transporte, póngase en contacto con el administrador de red del sitio para configurar las puertas de enlace SMTP para resolver este problema.

Si esta prueba se realiza correctamente pero el mismo mensaje enviado a `mailto:autosupport@netapp.com` no lo hace, asegúrese de que la retransmisión SMTP está activada en todos los hosts de correo SMTP o utilice HTTPS como protocolo de transporte.

Si incluso el mensaje a la cuenta de correo administrada localmente no se realiza correctamente, confirme que los servidores SMTP están configurados para reenviar archivos adjuntos con ambas características:

- El sufijo `"7z"`
- El tipo MIME `"Application/x-7x-Compressed"`.

## Solucione problemas del subsistema AutoSupport

La `system node check show` Los comandos se pueden utilizar para verificar y solucionar los problemas relacionados con la configuración y la entrega de AutoSupport.

### Paso

1. Use los siguientes comandos para mostrar el estado del subsistema AutoSupport.

| Se usa este comando...                            | Para hacer esto...                                                                                                                                                                                          |
|---------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>system node autosupport check show</b>         | Mostrar el estado general del subsistema AutoSupport, como el estado del destino HTTP o HTTPS de AutoSupport, destinos SMTP de AutoSupport, servidor AutoSupport OnDemand y la configuración de AutoSupport |
| <b>system node autosupport check show-details</b> | Mostrar el estado detallado del subsistema AutoSupport, como descripciones detalladas de errores y las acciones correctivas                                                                                 |

## Supervisión del estado

### Supervise el estado de la información general del sistema

Los monitores de estado supervisan proactivamente ciertas condiciones críticas de su clúster y generan alertas si detectan una falla o un riesgo. Si hay alertas activas, el estado del sistema informa de un estado degradado para el clúster. Las alertas incluyen la información que necesita para responder a un estado del sistema degradado.

Si el estado es degradado, puede ver detalles del problema, incluidas la causa probable y las acciones de

recuperación recomendadas. Después de resolver el problema, el estado del sistema vuelve automáticamente a OK.

El estado del sistema refleja varios monitores de estado independientes. Un estado degradado en un monitor de estado individual provoca un estado degradado para el estado general del sistema.

Si quiere más información sobre cómo ONTAP admite los switches de clúster para supervisar el estado del sistema en el clúster, puede consultar el *Hardware Universe*.

["Los switches compatibles del Hardware Universe"](#)

Para obtener información detallada sobre las causas de los mensajes de AutoSupport del monitor de estado del switch de clúster (CSHM) y las acciones necesarias para resolver estas alertas, consulte el artículo de la base de conocimientos.

["Mensaje de AutoSupport: Proceso del monitor de estado CSHM"](#)

## Cómo funciona la supervisión del estado

Los monitores de estado individuales tienen un conjunto de políticas que activan alertas cuando se dan ciertas condiciones. Comprender cómo funciona la supervisión del estado puede ayudarle a responder a problemas y controlar alertas futuras.

La supervisión del estado consta de los siguientes componentes:

- Monitores de salud individuales para subsistemas específicos, cada uno de los cuales tiene su propio estado de salud

Por ejemplo, el subsistema de almacenamiento tiene un monitor de estado de conectividad de nodo.

- Un monitor de estado general del sistema que consolida el estado de los monitores de estado individuales

Un estado degradado en cualquier subsistema único da como resultado un estado degradado para todo el sistema. Si ningún subsistema tiene alertas, el estado general del sistema es correcto.

Cada monitor de estado se compone de los siguientes elementos clave:

- Alertas que el monitor de estado puede generar potencialmente

Cada alerta tiene una definición, que incluye detalles como la gravedad de la alerta y su causa probable.

- Políticas de estado que identifican cuándo se activa cada alerta

Cada política de mantenimiento tiene una expresión de regla, que es la condición o cambio exactos que desencadena la alerta.

Un monitor de estado supervisa y valida continuamente los recursos en su subsistema para comprobar la condición o los cambios de estado. Cuando un cambio de condición o estado coincide con una expresión de regla de una política de estado, el monitor de estado genera una alerta. Una alerta hace que el estado del subsistema y su estado general del sistema se degraden.

## Formas de responder a las alertas de estado del sistema

Cuando se produce una alerta de estado del sistema, puede reconocerla, obtener más información sobre él, reparar la condición subyacente y evitar que vuelva a producirse.

Cuando un monitor de estado genera una alerta, puede responder de cualquiera de las siguientes maneras:

- Obtenga información sobre la alerta, que incluye el recurso afectado, la gravedad de la alerta, la causa probable, el posible efecto y las acciones correctivas.
- Obtenga información detallada sobre la alerta, como el momento en que se planteó la alerta y si alguien más ya ha reconocido dicha alerta.
- Obtenga información relacionada con el estado del recurso o subsistema afectado, como una bandeja o un disco específicos.
- Reconozca la alerta para indicar que alguien está trabajando en el problema e identifíquese como el "acusador".
- Resuelva el problema siguiendo las acciones correctivas proporcionadas en la alerta, como la corrección de cableado para resolver un problema de conectividad.
- Elimine la alerta si el sistema no la borró automáticamente.
- Suprime una alerta para evitar que afecte al estado de un subsistema.

La supresión es útil cuando se entiende un problema. Después de suprimir una alerta, todavía puede ocurrir, pero el estado del subsistema se muestra como "ok-with-suppress". cuando se produce la alerta suprimida.

## Personalización de alertas de estado del sistema

Puede controlar qué alertas genera un monitor de estado mediante la habilitación y la deshabilitación de las políticas de estado del sistema que definen cuándo se activan las alertas. Esto le permite personalizar el sistema de control del estado para su entorno concreto.

Puede obtener más información sobre el nombre de una política mediante la visualización de información detallada sobre una alerta generada o la visualización de definiciones de políticas para un monitor de estado, nodo o ID de alerta específicos.

Deshabilitar políticas de estado es diferente de suprimir alertas. Cuando se suprime una alerta, esta no afecta al estado del subsistema, pero aún puede aparecer la alerta.

Si deshabilita una política, la condición o el estado definidos en la expresión de regla de política ya no activan una alerta.

### Ejemplo de una alerta que desea deshabilitar

Por ejemplo, supongamos que se produce una alerta que no le resulta útil. Utilice la `system health alert show -instance` Comando para obtener el ID de política de la alerta. El ID de política se utiliza en la `system health policy definition show` comando para ver información acerca de la política. Después de revisar la expresión de regla y otra información acerca de la directiva, decide deshabilitar la directiva. Utilice la `system health policy definition modify` comando para deshabilitar la política.

## Cómo activan las alertas de estado los mensajes y eventos de AutoSupport

Las alertas de estado del sistema activan mensajes y eventos de AutoSupport en el sistema de gestión de eventos (EMS), lo que permite supervisar el estado del sistema mediante mensajes de AutoSupport y EMS, además de utilizar el sistema de supervisión de estado directamente.

El sistema envía un mensaje de AutoSupport dentro de los cinco minutos posteriores a una alerta. El mensaje AutoSupport incluye todas las alertas generadas desde el mensaje de AutoSupport anterior, a excepción de las alertas que duplican una alerta para el mismo recurso y la misma causa probable en la semana anterior.


Algunas alertas no activan mensajes de AutoSupport. Una alerta no activa un mensaje de AutoSupport si su política de estado deshabilita el envío de mensajes de AutoSupport. Por ejemplo, una directiva de estado podría deshabilitar los mensajes de AutoSupport de forma predeterminada porque AutoSupport ya genera un mensaje cuando se produce el problema. Puede configurar directivas para que no activen mensajes AutoSupport mediante el `system health policy definition modify` comando.

Puede ver una lista de todos los mensajes de AutoSupport activados por alertas enviados en la semana anterior mediante el `system health autosupport trigger history show` comando.

Las alertas también activan la generación de eventos en el EMS. Se genera un evento cada vez que se crea una alerta y se borra cada vez que se borra una alerta.

## Monitores de estado del clúster disponibles

Existen varios monitores de estado que supervisan diferentes partes de un clúster. Los monitores de estado le ayudan a recuperarse de errores en sistemas ONTAP mediante la detección de eventos, el envío de alertas a usted y la eliminación de eventos según los borre.

| Nombre del monitor de estado (identificador) | Nombre del subsistema (identificador)                                                                               | Específico                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Switch de clúster (switch de clúster)        | Switch (Switch-Health)                                                                                              | <p>Supervisa los switches de red de clúster y los switches de red de gestión para obtener temperatura, utilización, configuración de interfaces, redundancia (solo switches de red de clúster) y funcionamiento de suministro de alimentación y ventilador. El monitor de estado del switch del clúster se comunica con los switches a través de SNMP. SNMPv2c es el valor predeterminado.</p> <div>  <p>A partir de ONTAP 9.2, este monitor puede detectar y generar informes cuando se ha reiniciado un switch de clúster desde el último periodo de sondeo.</p> </div> |
| Estructura MetroCluster                      | Conmutador                                                                                                          | Supervisa la topología de la estructura del back-end de la configuración de MetroCluster y detecta mala configuración como el cableado y la división en zonas incorrectas y los fallos de ISL.                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| MetroCluster Salud                           | Interconexión, RAID y almacenamiento                                                                                | Supervisa los adaptadores FC-VI, los adaptadores del iniciador FC, los agregados y discos subyacentes y los puertos entre clústeres                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Conectividad de nodo (conexión por nodo)     | Operaciones no disruptivas de CIFS (CIFS-NDO)                                                                       | Supervisa conexiones SMB para proporcionar operaciones no disruptivas a aplicaciones de Hyper-V.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Almacenamiento (conexión SAS)                | Supervisa las bandejas, los discos y los adaptadores a nivel de nodo para obtener las rutas y conexiones adecuadas. | Sistema                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

| Nombre del monitor de estado (identificador) | Nombre del subsistema (identificador)            | Específico                                      |
|----------------------------------------------|--------------------------------------------------|-------------------------------------------------|
| no aplicable                                 | Agrega información de otros monitores de estado. | Conectividad del sistema (conexión del sistema) |

## Reciba alertas de estado del sistema automáticamente

Puede ver manualmente las alertas de estado del sistema usando la `system health alert show` comando. Sin embargo, debe suscribirse a mensajes específicos de Event Management System (EMS) para recibir notificaciones automáticamente cuando un monitor de estado genera una alerta.

### Acerca de esta tarea

En el siguiente procedimiento se muestra cómo configurar notificaciones para todos los mensajes `hm.alert.levantados` y todos los mensajes `hm.alert.borrados`.

Todos los mensajes `hm.alert.levantados` y todos los mensajes `hm.alert.borrados` incluyen una captura SNMP. Los nombres de las capturas SNMP son `HealthMonitorAlertRaised` y `HealthMonitorAlertCleared`. Para obtener información acerca de las capturas SNMP, consulte *Network Management Guide*.

### Pasos

1. Utilice la `event destination create` Comando para definir el destino al que desea enviar mensajes de EMS.

```
cluster1::> event destination create -name health_alerts -mail
admin@example.com
```

2. Utilice la `event route add-destinations` comando para enrutar la `hm.alert.raised` y el `hm.alert.cleared` mensaje a un destino.

```
cluster1::> event route add-destinations -messagename hm.alert*
-destinations health_alerts
```

### Información relacionada

["Gestión de redes"](#)

## Responda al estado degradado del sistema

Cuando el estado del sistema es degradado, puede mostrar alertas, leer acerca de la causa probable y acciones correctivas, mostrar información sobre el subsistema degradado y resolver el problema. También se muestran alertas suprimidas para que pueda modificarlas y ver si se han reconocido.

### Acerca de esta tarea

Puede detectar que se generó una alerta mediante un mensaje de AutoSupport o un evento de EMS, o mediante el `system health` comandos.

## Pasos

1. Utilice la `system health alert show` comando para ver las alertas que están afectando al estado del sistema.
2. Lea la causa probable, el posible efecto y las acciones correctivas de la alerta para determinar si puede resolver el problema o necesita más información.
3. Si necesita más información, utilice `system health alert show -instance` comando para ver información adicional disponible para la alerta.
4. Utilice la `system health alert modify` con el `-acknowledge` parámetro para indicar que está trabajando en una alerta específica.
5. Tome medidas correctivas para resolver el problema como se describe en `Corrective Actions` campo de la alerta.

Las acciones correctivas pueden incluir reiniciar el sistema.

Cuando se resuelve el problema, la alerta se borra automáticamente. Si el subsistema no tiene otras alertas, el estado del subsistema cambia a `OK`. Si el estado de todos los subsistemas es correcto, el estado general del sistema cambia a `OK`.

6. Utilice la `system health status show` comando para confirmar que el estado del sistema es `OK`.

Si el estado del sistema no es `OK`, repetir este procedimiento.

## Ejemplo de respuesta al estado degradado del sistema

Al revisar un ejemplo específico de estado del sistema degradado causado por una bandeja que carece de dos rutas a un nodo, puede ver lo que muestra la CLI cuando responde a una alerta.

Después de iniciar ONTAP, compruebe el estado del sistema y detecte que el estado es degradado:

```
cluster1::>system health status show
Status

degraded
```

Muestra las alertas para averiguar dónde está el problema y ver que la bandeja 2 no tiene dos rutas al nodo 1:



```
cluster1::>system health alert show
 Node: node1
 Resource: Shelf ID 2
 Severity: Major
 Indication Time: Mon Nov 10 16:48:12 2013
 Probable Cause: Disk shelf 2 does not have two paths to controller
 node1.
 Possible Effect: Access to disk shelf 2 via controller node1 will be
 lost with a single hardware component failure (e.g.
 cable, HBA, or IOM failure).
 Corrective Actions: 1. Halt controller node1 and all controllers attached
 to disk shelf 2.
 2. Connect disk shelf 2 to controller node1 via two
 paths following the rules in the Universal SAS and ACP Cabling Guide.
 3. Reboot the halted controllers.
 4. Contact support personnel if the alert persists.
```

Se muestran detalles de la alerta para obtener más información, incluido el ID de alerta:

```

cluster1::>system health alert show -monitor node-connect -alert-id
DualPathToDiskShelf_Alert -instance
 Node: node1
 Monitor: node-connect
 Alert ID: DualPathToDiskShelf_Alert
 Alerting Resource: 50:05:0c:c1:02:00:0f:02
 Subsystem: SAS-connect
 Indication Time: Mon Mar 21 10:26:38 2011
 Perceived Severity: Major
 Probable Cause: Connection_establishment_error
 Description: Disk shelf 2 does not have two paths to controller
node1.
 Corrective Actions: 1. Halt controller node1 and all controllers
attached to disk shelf 2.
 2. Connect disk shelf 2 to controller node1 via
two paths following the rules in the Universal SAS and ACP Cabling Guide.
 3. Reboot the halted controllers.
 4. Contact support personnel if the alert
persists.
 Possible Effect: Access to disk shelf 2 via controller node1 will
be lost with a single
 hardware component failure (e.g. cable, HBA, or IOM failure).
 Acknowledge: false
 Suppress: false
 Policy: DualPathToDiskShelf_Policy
 Acknowledger: -
 Suppressor: -
 Additional Information: Shelf uuid: 50:05:0c:c1:02:00:0f:02
 Shelf id: 2
 Shelf Name: 4d.shelf2
 Number of Paths: 1
 Number of Disks: 6
 Adapter connected to IOMA:
 Adapter connected to IOMB: 4d
 Alerting Resource Name: Shelf ID 2

```

Reconoce la alerta para indicar que está trabajando en ella.

```

cluster1::>system health alert modify -node node1 -alert-id
DualPathToDiskShelf_Alert -acknowledge true

```

Fije el cableado entre la bandeja 2 y la nodo 1 y, a continuación, reinicie el sistema. Luego, vuelva a comprobar el estado del sistema y compruebe que el estado es OK:

```
cluster1::>system health status show
Status

OK
```

## Configurar la detección de switches de red de gestión y clústeres

El monitor de estado del switch de clúster intenta automáticamente detectar los switches de red de gestión y clúster mediante el protocolo de detección de Cisco (CDP). Debe configurar el monitor de estado si no puede detectar automáticamente un switch o si no desea usar CDP para la detección automática.

### Acerca de esta tarea

La `system cluster-switch show` el comando enumera los switches que detectó el monitor de estado. Si no ve un switch que esperaba ver en esa lista, el monitor de estado no podrá detectarlo automáticamente.

### Pasos

1. Si desea utilizar CDP para la detección automática, haga lo siguiente:

- a. Asegúrese de que el protocolo de descubrimiento de Cisco (CDP) está habilitado en los switches.

Consulte la documentación de su switch para obtener instrucciones.

- b. Ejecute el siguiente comando en cada nodo del clúster para verificar si CDP está habilitado o deshabilitado:

```
run -node node_name -command options cdpd.enable
```

Si CDP está habilitado, vaya al paso d. Si CDP está desactivado, vaya al paso c.

- c. Ejecute el siguiente comando para habilitar CDP:

```
run -node node_name -command options cdpd.enable on
```

Espere cinco minutos antes de pasar al siguiente paso.

- a. Utilice la `system cluster-switch show` Para verificar si ONTAP ahora puede detectar automáticamente los switches.

2. Si el monitor de estado no puede detectar automáticamente un switch, use el `system cluster-switch create` comando para configurar la detección del switch:

```
cluster1::> system cluster-switch create -device switch1 -address
192.0.2.250 -snmp-version SNMPv2c -community cshml! -model NX5020 -type
cluster-network
```

Espere cinco minutos antes de pasar al siguiente paso.

3. Utilice la `system cluster-switch show` Comando para verificar que ONTAP puede detectar el switch

al que ha añadido información.

## Después de terminar

Compruebe que el monitor de estado puede supervisar los switches.

## Compruebe la supervisión de los switches de red de clúster y de gestión

El monitor de estado del switch de clúster intenta supervisar automáticamente los switches que detecta; sin embargo, es posible que la supervisión no se produzca de manera automática si los switches no se han configurado correctamente. Debe verificar que el monitor de estado esté correctamente configurado para supervisar los switches.

### Pasos

1. Para identificar los switches que detectó el monitor de estado del switch del clúster, introduzca el siguiente comando:

#### ONTAP 9,8 y versiones posteriores

```
system switch ethernet show
```

#### ONTAP 9,7 y anteriores

```
system cluster-switch show
```

Si la `Model` columna muestra el valor `OTHER`, Entonces ONTAP no puede supervisar el conmutador. ONTAP establece el valor en `OTHER` si un switch que detecta automáticamente no es compatible con la supervisión del estado.



Si un switch no se muestra en el resultado del comando, debe configurar la detección del switch.

2. Actualice al software de switch más reciente admitido y consulte el archivo de configuración (RCF) desde el sitio de soporte de NetApp.

### ["Página de descargas de soporte de NetApp"](#)

La cadena de comunidad en el RCF del conmutador debe coincidir con la cadena de comunidad que el monitor de estado está configurado para utilizar. De forma predeterminada, el monitor de estado utiliza la cadena de comunidad `cshml!`.



En este momento, el monitor de estado sólo admite SNMPv2.

Si necesita cambiar información sobre un switch que supervisa el clúster, puede modificar la cadena de comunidad que utiliza el monitor de estado mediante el siguiente comando:

**ONTAP 9,8 y versiones posteriores**

```
system switch ethernet modify
```

**ONTAP 9,7 y anteriores**

```
system cluster-switch modify
```

3. Compruebe que el puerto de gestión del switch está conectado a la red de gestión.

Esta conexión es necesaria para realizar consultas SNMP.

## Comandos para supervisar el estado del sistema

Puede utilizar el `system health` comandos para mostrar información sobre el estado de los recursos del sistema, responder a las alertas y configurar alertas futuras. El uso de los comandos de la CLI le permite ver información en profundidad sobre la configuración del control del estado. Las páginas de manual de los comandos contienen más información.

### Mostrar el estado del estado del sistema

| Si desea...                                                                                | Se usa este comando...                    |
|--------------------------------------------------------------------------------------------|-------------------------------------------|
| Muestre el estado del sistema, que refleja el estado general de cada monitor de estado     | <code>system health status show</code>    |
| Mostrar el estado de los subsistemas para los que está disponible la supervisión de estado | <code>system health subsystem show</code> |

### Mostrar el estado de conectividad de los nodos

| Si desea...                                                                                                                                                                                                               | Se usa este comando...                                                                                                                      |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| Muestra detalles acerca de la conectividad del nodo a la bandeja de almacenamiento, incluida la información de puertos, la velocidad del puerto de HBA, el rendimiento de I/O y la tasa de operaciones de I/O por segundo | <code>storage shelf show -connectivity</code><br><br>Utilice la <code>-instance</code> para mostrar información detallada de cada bandeja.  |
| Muestra información sobre las unidades y los LUN de cabina, incluidos el espacio utilizable, los números de bandeja y bahía y el nombre del nodo propietario                                                              | <code>storage disk show</code><br><br>Utilice la <code>-instance</code> parámetro para mostrar información detallada acerca de cada unidad. |

| Si desea...                                                                                                                             | Se usa este comando...                                                                                                                   |
|-----------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Muestra información detallada sobre los puertos de las bandejas de almacenamiento, incluido el tipo de puerto, la velocidad y el estado | <pre>storage port show</pre> <p>Utilice la <code>-instance</code> parámetro para mostrar información detallada sobre cada adaptador.</p> |

### Gestionar la detección de switches de redes de gestión, almacenamiento y clúster

| Si desea...                                                                                                                                                                                                                                                                                                                                                         | Utilice este comando. (ONTAP 9.8 y posterior)                | Utilice este comando. (ONTAP 9.7 y anterior)                |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|-------------------------------------------------------------|
| Muestre los switches que supervisa el clúster                                                                                                                                                                                                                                                                                                                       | <pre>system switch ethernet show</pre>                       | <pre>system cluster-switch show</pre>                       |
| Muestre los switches que el clúster supervisa actualmente, incluidos los switches que ha eliminado (que se muestran en la columna motivo del resultado del comando), y la información de configuración que necesita para el acceso de red a los switches de red de gestión y clúster.<br><br>Este comando solo está disponible en el nivel de privilegios avanzado. | <pre>system switch ethernet show-all</pre>                   | <pre>system cluster-switch show-all</pre>                   |
| Configurar la detección de un switch no detectado                                                                                                                                                                                                                                                                                                                   | <pre>system switch ethernet create</pre>                     | <pre>system cluster-switch create</pre>                     |
| Modificar la información sobre un conmutador que supervisa el clúster (por ejemplo, nombre de dispositivo, dirección IP, versión SNMP y cadena de comunidad)                                                                                                                                                                                                        | <pre>system switch ethernet modify</pre>                     | <pre>system cluster-switch modify</pre>                     |
| Desactive la supervisión de un interruptor                                                                                                                                                                                                                                                                                                                          | <pre>system switch ethernet modify -disable-monitoring</pre> | <pre>system cluster-switch modify -disable-monitoring</pre> |
| Desactive la detección y supervisión de un switch y elimine la información de configuración del switch                                                                                                                                                                                                                                                              | <pre>system switch ethernet delete</pre>                     | <pre>system cluster-switch delete</pre>                     |

| Si desea...                                                                                                                                                                         | Utilice este comando. (ONTAP 9.8 y posterior)     | Utilice este comando. (ONTAP 9.7 y anterior)     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|--------------------------------------------------|
| Eliminar permanentemente la información de configuración del conmutador almacenada en la base de datos (al hacerlo se vuelve a activar el descubrimiento automático del conmutador) | <code>system switch ethernet delete -force</code> | <code>system cluster-switch delete -force</code> |
| Active el registro automático para que se envíe con mensajes de AutoSupport.                                                                                                        | <code>system switch ethernet log</code>           | <code>system cluster-switch log</code>           |




### Responda a alertas generadas

| Si desea...                                                                                                                                                                     | Se usa este comando...                                      |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|
| Muestra información sobre las alertas generadas, como el recurso y el nodo donde se activó la alerta, y la gravedad y la causa probable de la alerta                            | <code>system health alert show</code>                       |
| Muestra información sobre cada alerta generada                                                                                                                                  | <code>system health alert show -instance</code>             |
| Indique que alguien está trabajando en una alerta                                                                                                                               | <code>system health alert modify</code>                     |
| Reconozca una alerta                                                                                                                                                            | <code>system health alert modify -acknowledge</code>        |
| Suprimir una alerta posterior para que no afecte al estado de un subsistema                                                                                                     | <code>system health alert modify -suppress</code>           |
| Eliminar una alerta que no se borró automáticamente                                                                                                                             | <code>system health alert delete</code>                     |
| Muestra información sobre los mensajes de AutoSupport que se han activado en la última semana, por ejemplo, para determinar si una alerta ha activado un mensaje de AutoSupport | <code>system health autosupport trigger history show</code> |

### Configurar alertas futuras

| Si desea...                                                                                                     | Se usa este comando...                              |
|-----------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|
| Habilite o deshabilite la política que controla si un estado de recurso específico genera una alerta específica | <code>system health policy definition modify</code> |

## Muestra información acerca de cómo se configura la supervisión del estado

| Si desea...                                                                                                | Se usa este comando...                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Muestra información acerca de los monitores de estado, como sus nodos, nombres, subsistemas y estado       | <pre>system health config show</pre> <div> Utilice la <code>-instance</code> parámetro para mostrar información detallada sobre cada monitor de estado.</div>                                                                                                                                                            |
| Muestre información sobre las alertas que un monitor de estado puede generar potencialmente                | <pre>system health alert definition show</pre> <div> Utilice la <code>-instance</code> parámetro para mostrar información detallada sobre cada definición de alerta.</div>                                                                                                                                               |
| Muestra información sobre las políticas de control de estado, que determinan cuándo se generan las alertas | <pre>system health policy definition show</pre> <div> Utilice la <code>-instance</code> parámetro para mostrar información detallada de cada política. Utilice otros parámetros para filtrar la lista de alertas, por ejemplo, el estado de la política (habilitada o no), el monitor de estado, las alertas, etc.</div> |

## Muestra información del entorno

Los sensores le ayudan a supervisar los componentes medioambientales de su sistema. La información que puede mostrar acerca de los sensores medioambientales incluye sus advertencias de tipo, nombre, estado, valor y umbral.

### Paso

1. Para mostrar la información de los sensores medioambientales, utilice `system node environment sensors show` comando.

## Análisis del sistema de archivos

### Descripción general de File System Analytics

El análisis de sistemas de archivos (FSA, File System Analytics) se introdujo por primera vez en ONTAP 9.8 para ofrecer visibilidad en tiempo real de las tendencias de la capacidad de almacenamiento y el uso de ficheros dentro de los volúmenes de ONTAP FlexGroup o FlexVol. Esta funcionalidad nativa elimina la necesidad de herramientas externas y proporciona información clave sobre cómo se utiliza el almacenamiento y si existen oportunidades para optimizar el almacenamiento según las necesidades de su negocio.

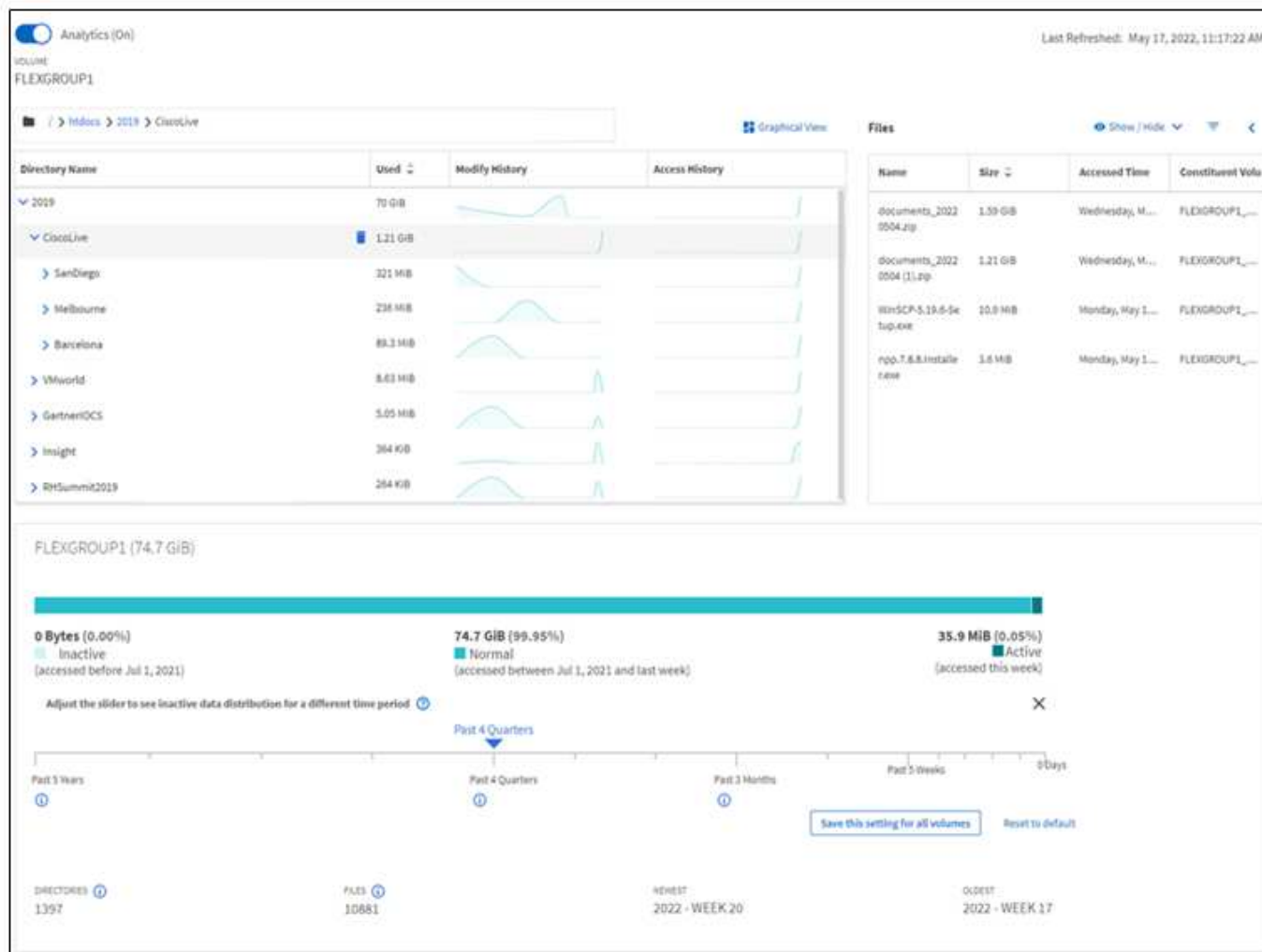


Con FSA, usted tiene visibilidad en todos los niveles de la jerarquía de sistema de archivos de un volumen en NAS. Por ejemplo, puede obtener información sobre uso y capacidad en los niveles de máquina virtual de almacenamiento (SVM), volumen, directorio y archivo. Puede utilizar la FSA para responder preguntas como:

- ¿Qué está llenando el almacenamiento y tengo archivos de gran tamaño que puedo mover a otra ubicación de almacenamiento?
- ¿Cuáles son los volúmenes, directorios y archivos más activos? ¿Está optimizado el rendimiento de mi almacenamiento para las necesidades de mis usuarios?
- ¿Cuántos datos se han añadido el último mes?
- ¿Quiénes son los usuarios de almacenamiento más activos o menos activos?
- ¿Qué cantidad de datos inactivos o inactivos contiene mi almacenamiento primario? ¿Puedo mover los datos a un nivel de datos más bajo coste?
- ¿Los cambios previstos de calidad de servicio afectarán negativamente al acceso a archivos críticos y a los que se accede con frecuencia?

El análisis del sistema de archivos está integrado en System Manager de ONTAP. Las vistas de System Manager proporcionan:

- Visibilidad en tiempo real para una gestión y un funcionamiento de los datos efectivos
- Recopilación y agregación de datos en tiempo real
- Los tamaños y el número de subdirectorios y archivos, junto con los perfiles de rendimiento asociados
- Histogramas de edad de archivo para modificar e historial de acceso



## Tipos de volúmenes admitidos

El análisis de sistemas de archivos está diseñado para proporcionar visibilidad en volúmenes con datos NAS activos, a excepción de las cachés de FlexCache y los volúmenes de destino de SnapMirror.

## Disponibilidad de funciones de análisis de sistemas de archivos

Cada versión de ONTAP amplía el alcance del análisis de sistemas de archivos.

|                                                                                      | ONTAP 9.14.1 | ONTAP 9.13.1 | ONTAP 9.12.1 | ONTAP 9.11.1 | ONTAP 9.10.1 | ONTAP 9.9.1 | ONTAP 9,8 |
|--------------------------------------------------------------------------------------|--------------|--------------|--------------|--------------|--------------|-------------|-----------|
| Visualización en System Manager                                                      | ✓            | ✓            | ✓            | ✓            | ✓            | ✓           | ✓         |
| Análisis de capacidad                                                                | ✓            | ✓            | ✓            | ✓            | ✓            | ✓           | ✓         |
| Información de datos inactivos                                                       | ✓            | ✓            | ✓            | ✓            | ✓            | ✓           | ✓         |
| Compatibilidad con volúmenes que han realizado la transición desde Data ONTAP 7-Mode | ✓            | ✓            | ✓            | ✓            | ✓            | ✓           |           |

|                                                                                 | ONTAP<br>9.14.1 | ONTAP<br>9.13.1 | ONTAP<br>9.12.1 | ONTAP<br>9.11.1 | ONTAP<br>9.10.1 | ONTAP<br>9.9.1 | ONTAP<br>9,8 |
|---------------------------------------------------------------------------------|-----------------|-----------------|-----------------|-----------------|-----------------|----------------|--------------|
| Capacidad para personalizar el período inactivo en System Manager               | ✓               | ✓               | ✓               | ✓               | ✓               | ✓              |              |
| Seguimiento de actividad a nivel de volumen                                     | ✓               | ✓               | ✓               | ✓               | ✓               |                |              |
| Descargue los datos de seguimiento de actividad en CSV                          | ✓               | ✓               | ✓               | ✓               | ✓               |                |              |
| Seguimiento de actividad a nivel de SVM                                         | ✓               | ✓               | ✓               | ✓               |                 |                |              |
| Línea de tiempo                                                                 | ✓               | ✓               | ✓               | ✓               |                 |                |              |
| Análisis del uso                                                                | ✓               | ✓               | ✓               |                 |                 |                |              |
| Opción para activar el análisis del sistema de archivos de forma predeterminada | ✓               | ✓               |                 |                 |                 |                |              |
| Supervisión de progreso de exploración de inicialización                        | ✓               |                 |                 |                 |                 |                |              |

Obtenga más información sobre el análisis del sistema de archivos

## ONTAP File System Analytics

Daniel Tennant  
Director of Software Engineering  
December 13, 2020

© 2020 NetApp, Inc. All rights reserved. — NETAPP CONFIDENTIAL —






### Lecturas adicionales

- ["TR 4687: Directrices de prácticas recomendadas para el análisis del sistema de archivos de ONTAP"](#)
- ["Base de conocimientos: Latencia alta o fluctuante tras activar el análisis del sistema de archivos ONTAP"](#)

## Active File System Analytics

Para recopilar y mostrar datos de uso, como los análisis de capacidad, es necesario habilitar File System Analytics en un volumen.

### Acerca de esta tarea

- A partir de ONTAP 9.8, puede habilitar el análisis del sistema de archivos en un volumen nuevo o existente. Si actualiza un sistema a ONTAP 9.8 o posterior, asegúrese de que todos los procesos de actualización se han completado antes de habilitar el análisis del sistema de archivos.
- Según el tamaño y el contenido del volumen, la habilitación del análisis puede llevar tiempo mientras ONTAP procesa los datos existentes en el volumen. System Manager muestra el progreso y presenta datos de análisis cuando se completa. Si necesita información más precisa sobre el progreso de inicialización, puede utilizar el comando CLI de ONTAP `volume analytics show`.

A partir de ONTAP 9.14.1, ONTAP proporciona seguimiento de progreso para la exploración de inicialización, además de notificaciones sobre eventos de limitación que afectan al progreso de la exploración.

Para obtener más información relacionada con la secuencia de inicialización, consulte [Consideraciones sobre la adquisición](#).

### Pasos

Puede habilitar el análisis del sistema de archivos con el Administrador del sistema de ONTAP o la CLI.

#### System Manager

| En ONTAP 9.8 y 9.9.1                                                                                                                                                                                                                                                        | A partir de ONTAP 9.10.1                                                                                                                                                                                                                                                                                            |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ol style="list-style-type: none"> <li>1. Seleccione <b>almacenamiento &gt; volúmenes</b>.</li> <li>2. Seleccione el volumen deseado y, a continuación, seleccione <b>Explorer</b>.</li> <li>3. Seleccione <b>Activar análisis</b> o <b>Desactivar análisis</b>.</li> </ol> | <ol style="list-style-type: none"> <li>1. Seleccione <b>almacenamiento &gt; volúmenes</b>.</li> <li>2. Seleccione el volumen deseado. En el menú volumen individual, seleccione <b>sistema de archivos &gt; Explorador</b>.</li> <li>3. Seleccione <b>Activar análisis</b> o <b>Desactivar análisis</b>.</li> </ol> |

#### CLI

##### Active File System Analytics con la CLI

1. Ejecute el siguiente comando:  

```
volume analytics on -vserver svm_name -volume volume_name [-foreground {true|false}]
```

De forma predeterminada, el comando se ejecuta en primer plano; ONTAP muestra el progreso y presenta datos de análisis cuando se completa. Si necesita información más precisa, puede ejecutar el comando en segundo plano mediante la `-foreground false` y, a continuación, utilice la `volume analytics show` Comando para mostrar el progreso de inicialización en la CLI.
2. Después de habilitar correctamente el análisis del sistema de archivos, utilice System Manager o la API REST DE ONTAP para mostrar los datos analíticos.


## Modificar la configuración predeterminada de análisis del sistema de archivos

A partir de ONTAP 9.13.1, se puede modificar la configuración de SVM o de los clústeres para habilitar el análisis del sistema de archivos de forma predeterminada en los volúmenes nuevos.

### System Manager

Si utiliza System Manager, puede modificar la configuración de la máquina virtual de almacenamiento o del clúster para permitir los análisis de capacidad y el seguimiento de actividad durante la creación del volumen de forma predeterminada. La habilitación predeterminada solo se aplica a los volúmenes creados después de modificar la configuración, no a los volúmenes existentes.

### Modificar la configuración de análisis del sistema de archivos en un clúster

1. En System Manager, vaya a **Configuración del clúster**.
2. En **Configuración del clúster**, revise la pestaña Configuración del sistema de archivos. Para modificar la configuración, seleccione la .
3. En el campo **Seguimiento de actividad**, introduzca los nombres de las SVM para habilitar Seguimiento de actividad de forma predeterminada. Si deja el campo vacío, el seguimiento de actividad quedará deshabilitado en todas las SVM.

Desactive la casilla **Activar en nuevas máquinas virtuales de almacenamiento** para desactivar el Seguimiento de actividad de forma predeterminada en las nuevas máquinas virtuales de almacenamiento.

4. En el campo **Analytics**, introduzca los nombres de las máquinas virtuales de almacenamiento para las que desea habilitar la analítica de capacidad de forma predeterminada. Si deja el campo vacío, los análisis de capacidad quedarán deshabilitados en todas las SVM.

Desactive la casilla **Enable on new storage VMs** para desactivar los análisis de capacidad de forma predeterminada en las nuevas máquinas virtuales de almacenamiento.

5. Seleccione **Guardar**.

### Modificar la configuración de análisis del sistema de archivos en una SVM

1. Seleccione la SVM que desea modificar, a continuación **Configuración de la máquina virtual de almacenamiento**.
2. En la tarjeta **File System Analytics**, utilice los botones para activar o desactivar el Seguimiento de actividad y el análisis de capacidad para todos los volúmenes nuevos en la máquina virtual de almacenamiento.

### CLI

Puede configurar la máquina virtual de almacenamiento para habilitar el análisis del sistema de archivos de forma predeterminada en los nuevos volúmenes mediante la interfaz de línea de comandos de ONTAP.

### Habilite File System Analytics de forma predeterminada en una SVM

1. Modifique la SVM para habilitar los análisis de capacidad y el seguimiento de actividad de forma predeterminada en todos los volúmenes recién creados:  

```
vserver modify -vserver svm_name -auto-enable-activity-tracking true -auto-enable-analytics true
```

## Ver la actividad del sistema de archivos

Después de habilitar File System Analytics (FSA), puede ver el contenido del directorio raíz de un volumen seleccionado ordenado por el espacio utilizado en cada subárbol.

Seleccione cualquier objeto del sistema de archivos para examinar el sistema de archivos y mostrar información detallada sobre cada objeto de un directorio. La información sobre los directorios también se puede visualizar gráficamente. Con el paso del tiempo, se muestran los datos históricos de cada subárbol. El espacio utilizado no se ordena si hay más de 3000 directorios.

### Explorador

La pantalla File System Analytics **Explorer** consta de tres áreas:

- Vista en árbol de directorios y subdirectorios; lista ampliable que muestra el nombre, el tamaño, el historial de modificación y el historial de acceso.
- Archivos; muestra el nombre, tamaño y tiempo de acceso del objeto seleccionado en la lista de directorios.
- Comparación de datos activos e inactivos para el objeto seleccionado en la lista de directorios.

A partir de ONTAP 9.9.1, se puede personalizar el rango que se informará. El valor predeterminado es un año. En función de estas personalizaciones, puede tomar medidas correctivas, como mover volúmenes y modificar la política de organización en niveles.

La hora de acceso se muestra de forma predeterminada. Sin embargo, si el valor predeterminado del volumen se ha modificado desde la CLI (mediante el establecimiento del `-atime-update` opción a. `false` con la `volume modify`), entonces sólo se muestra la última hora modificada. Por ejemplo:

- La vista de árbol no mostrará el **historial de acceso**.
- La vista de archivos se modificará.
- La vista de datos activa/inactiva se basará en el tiempo modificado (`mtime`).

Mediante estas pantallas, puede examinar lo siguiente:

- Las ubicaciones de los sistemas de archivos consumen más espacio
- Información detallada sobre un árbol de directorios, incluido el recuento de archivos y subdirectorios dentro de directorios y subdirectorios
- Ubicaciones del sistema de archivos que contienen datos antiguos (por ejemplo, arboles, temp o log)

Tenga en cuenta lo siguiente al interpretar la salida FSA:

- La FSA muestra dónde y cuándo están en uso sus datos, no cuántos datos se están procesando. Por ejemplo, un gran consumo de espacio por parte de los archivos modificados o a los que se ha accedido recientemente no indica necesariamente que haya cargas elevadas de procesamiento del sistema.
- La forma en que la pestaña **Explorador de volúmenes** calcula el consumo de espacio para FSA podría ser diferente de otras herramientas. En particular, podría haber diferencias significativas en comparación con el consumo informado en **Resumen de volumen** si el volumen tiene las funciones de eficiencia del almacenamiento activadas. Esto se debe a que la pestaña **Explorador de volúmenes** no incluye el ahorro de eficiencia.
- Debido a las limitaciones de espacio en la visualización de directorios, no es posible ver una profundidad de directorio superior a 8 niveles en *List View*. Para ver los directorios con más de 8 niveles de

profundidad, debe cambiar a *Graphical View*, localizar el directorio deseado y, a continuación, volver a *List View*. Esto permitirá espacio adicional en la pantalla.

## Pasos

1. Vea el contenido del directorio raíz de un volumen seleccionado:

| En ONTAP 9.8 y 9.9.1                                                                                                                  | A partir de ONTAP 9.10.1                                                                                                                                                |
|---------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Haga clic en <b>almacenamiento &gt; volúmenes</b> , seleccione el volumen deseado y, a continuación, haga clic en <b>Explorador</b> . | Seleccione <b>almacenamiento &gt; volúmenes</b> , seleccione el volumen deseado. En el menú volumen individual, seleccione <b>sistema de archivos &gt; Explorador</b> . |

## Activar seguimiento de actividad

A partir de ONTAP 9.10.1, el análisis del sistema de archivos incluye una función de seguimiento de actividades que le permite identificar objetos activos y descargar los datos como un archivo CSV. A partir de ONTAP 9.11.1, el seguimiento de la actividad se amplía al ámbito de SVM. A partir de ONTAP 9.11.1, el Administrador del sistema incluye una línea de tiempo para el seguimiento de actividades, lo que le permite buscar hasta cinco minutos de datos de seguimiento de actividades.

El seguimiento de actividad permite la supervisión en cuatro categorías:

- Directorios
- Archivos
- Clientes
- Usuarios

En cada categoría supervisada, el seguimiento de actividad mostrará IOPS de lectura, IOPS de escritura, rendimiento de lectura y rendimiento de escritura. Consultas sobre la actualización de seguimiento de actividad cada 10 a 15 segundos relacionadas con puntos calientes vistos en el sistema durante el intervalo de cinco segundos anterior.

La información de seguimiento de la actividad es aproximada, y la precisión de los datos depende de la distribución del tráfico de I/o entrante.

Al ver el seguimiento de actividad en System Manager a nivel de volumen, sólo se actualizará activamente el menú del volumen expandido. Si la vista de cualquier volumen se contrae, no se actualizará hasta que se expanda la visualización del volumen. Puede detener las actualizaciones con el botón **Pausa Actualizar**. Los datos de actividad se pueden descargar en formato CSV que mostrará todos los datos de un momento específico capturados para el volumen seleccionado.

Con la función de línea de tiempo disponible a partir de ONTAP 9.11.1, puede conservar un registro de la actividad de punto de acceso en un volumen o SVM, actualizando de forma continua aproximadamente cada cinco segundos y conservando los cinco minutos anteriores de datos. Los datos de la escala de tiempo sólo se conservan para los campos que son áreas visibles de la página. Si contrae una categoría de seguimiento o se desplaza para que la escala de tiempo esté fuera de la vista, la escala de tiempo dejará de recopilar datos. De forma predeterminada, las líneas de tiempo están desactivadas y se desactivarán automáticamente cuando salga de la ficha actividad.

## Activar seguimiento de actividad para un único volumen

Puede habilitar el seguimiento de actividad con ONTAP System Manager o la interfaz de línea de comandos.

### Acerca de esta tarea

Si utiliza RBAC con la API REST de ONTAP o System Manager, deberá crear roles personalizados para gestionar el acceso al seguimiento de actividades. Consulte [Control de acceso basado en roles](#) para este proceso.

#### System Manager

##### Pasos

1. Seleccione **almacenamiento > volúmenes**. Seleccione el volumen deseado. En el menú volumen individual, seleccione sistema de archivos y, a continuación, seleccione la ficha actividad.
2. Asegúrese de que **Activity Tracking** está activado para ver informes individuales en los directorios principales, archivos, clientes y usuarios.
3. Para analizar los datos a mayor profundidad sin actualizaciones, seleccione **Pausa Actualizar**. También puede descargar los datos para tener un registro CSV del informe.

#### CLI

##### Pasos

1. Activar seguimiento de actividad:

```
volume activity-tracking on -vserver svm_name -volume volume_name
```

2. Compruebe si el estado Seguimiento de actividad de un volumen está activado o desactivado con el comando:

```
volume activity-tracking show -vserver svm_name -volume volume_name -state
```

3. Una vez habilitada, use el administrador del sistema de ONTAP o la API REST de ONTAP para mostrar los datos de seguimiento de actividad.

## Habilite el seguimiento de actividad para varios volúmenes

Puede habilitar el seguimiento de actividades para varios volúmenes con System Manager o la interfaz de línea de comandos.

### Acerca de esta tarea

Si utiliza RBAC con la API REST de ONTAP o System Manager, deberá crear roles personalizados para gestionar el acceso al seguimiento de actividades. Consulte [Control de acceso basado en roles](#) para este proceso.



## System Manager

### Habilite para volúmenes específicos

1. Seleccione **almacenamiento > volúmenes**. Seleccione el volumen deseado. En el menú volumen individual, seleccione sistema de archivos y, a continuación, seleccione la ficha actividad.
2. Seleccione los volúmenes en los que desea habilitar el seguimiento de actividad. En la parte superior de la lista de volúmenes, seleccione el botón **más opciones**. Seleccione **Activar seguimiento de actividad**.
3. Para ver el seguimiento de actividad en el nivel de SVM, seleccione la SVM específica que desea ver en **almacenamiento > volúmenes**. Vaya a la pestaña sistema de archivos y luego a Activity y verá datos de los volúmenes que tienen activado Activity Tracking.

### Habilitar para todos los volúmenes

1. Seleccione **almacenamiento > volúmenes**. Seleccione una SVM del menú.
2. Vaya a la ficha **sistema de archivos**, seleccione la ficha **más** para activar el seguimiento de actividad en todos los volúmenes de la SVM.

## CLI

A partir de ONTAP 9.13.1, puede habilitar el seguimiento de actividades para varios volúmenes mediante la interfaz de línea de comandos de ONTAP.

### Pasos

1. Activar seguimiento de actividad:

```
volume activity-tracking on -vserver svm_name -volume [*|!volume_names]
```

Uso \* Para habilitar el seguimiento de actividad para todos los volúmenes en la máquina virtual de almacenamiento especificada.

Uso ! Seguimiento de los nombres de volúmenes para habilitar el seguimiento de actividad para todos los volúmenes en la SVM, excepto los volúmenes con nombre.

2. Confirme que la operación se ha realizado correctamente:

```
volume show -fields activity-tracking-state
```

3. Una vez habilitada, use el administrador del sistema de ONTAP o la API REST de ONTAP para mostrar los datos de seguimiento de actividad.

## Habilite la analítica de uso

A partir de ONTAP 9.12.1, puede habilitar el análisis de uso para ver qué directorios de un volumen están utilizando la mayor cantidad de espacio. Puede ver el número total de directorios de un volumen o el número total de archivos de un volumen. Los informes están limitados a los 25 directorios que utilizan la mayor parte del espacio.

Los análisis de directorios grandes se actualizan cada 15 minutos. Puede supervisar el refrescamiento más reciente comprobando la última marca de tiempo refrescada en la parte superior de la página. También puede hacer clic en el botón Descargar para descargar datos en un libro de Excel. La operación de descarga se ejecuta en segundo plano y presenta la información más reciente del volumen seleccionado. Si el análisis

vuelve sin ningún resultado, asegúrese de que el volumen está en línea. Eventos como SnapRestore harán que el Análisis del sistema de archivos reconstruya su lista de directorios grandes.

### Pasos

1. Seleccione **almacenamiento > volúmenes**. Seleccione el volumen deseado.
2. En el menú volumen individual, seleccione **sistema de archivos**. A continuación, seleccione la ficha **uso**.
3. Cambie el conmutador **Analytics** para activar el análisis de uso.
4. System Manager mostrará un gráfico de barras que identifica los directorios con el tamaño más grande en orden descendente.



ONTAP puede mostrar datos parciales o ningún dato mientras se recopila la lista de directorios principales. El progreso de la exploración puede encontrarse en la pestaña **uso** que se muestra durante la exploración.

Para obtener más información sobre un directorio específico, puede hacerlo [ver la actividad en un sistema de archivos](#).

## Adopte medidas correctivas basadas en análisis

A partir de ONTAP 9.9.1, puede tomar medidas correctivas basadas en los datos actuales y los resultados deseados directamente desde las pantallas de análisis del sistema de archivos.

### Eliminar directorios y archivos

En la pantalla del explorador, puede seleccionar directorios o archivos individuales que desea eliminar. Los directorios se eliminan con la funcionalidad de eliminación rápida de directorios de baja latencia. (FAST Directory delete también está disponible a partir de ONTAP 9.9.1 sin análisis activados).

### Pasos

1. Haga clic en **almacenamiento > volúmenes** y, a continuación, en **Explorador**.

Al pasar el ratón sobre un archivo o carpeta, aparece la opción para eliminar. Sólo puede eliminar un objeto cada vez.



Cuando se eliminan directorios y archivos, los nuevos valores de capacidad de almacenamiento no se muestran inmediatamente.

## Asignación de costes de medios en niveles de almacenamiento para comparar los costes de las ubicaciones de almacenamiento de datos inactivas

El coste del medio es un valor que usted asigna en función de su evaluación de los costes de almacenamiento, que se representan como la moneda por GB que elija. Cuando se establece, System Manager usa el costo de medios asignado para proyectar el ahorro estimado cuando se mueven volúmenes.

El coste de los medios establecido no es persistente; sólo se puede establecer para una única sesión de explorador.

### Pasos

1. Haga clic en **Almacenamiento > Niveles** y, a continuación, haga clic en **Establecer coste de medios** en

los mosaicos de nivel local (agregado) deseados.

Asegúrese de seleccionar los niveles activo e inactivo para permitir la comparación.

2. Introduzca un tipo de moneda y un importe.


Al introducir o cambiar el coste del material, el cambio se realiza en todos los tipos de material.

### **Mueva volúmenes para reducir los costes de almacenamiento**

Según los análisis mostrados y las comparaciones de costes en medios, puede trasladar volúmenes a un almacenamiento menos costoso en niveles locales.

Solo se puede comparar y mover un volumen cada vez.

#### **Pasos**

1. Después de habilitar la visualización de costo de medios, haga clic en **almacenamiento > niveles** y, a continuación, haga clic en **volúmenes**.
2. Para comparar las opciones de destino de un volumen, haga clic en  Para el volumen, haga clic en **mover**.
3. En la pantalla **Seleccionar nivel local de destino**, seleccione niveles de destino para mostrar la diferencia de coste estimada.
4. Después de comparar las opciones, seleccione el nivel deseado y haga clic en **mover**.

### **Control de acceso basado en roles con Análisis del sistema de archivos**

A partir de ONTAP 9.12.1, ONTAP incluye un rol predefinido denominado control de acceso basado en roles (RBAC) `admin-no-fsa`. La `admin-no-fsa` el rol concede privilegios a nivel de administrador, pero impide que el usuario realice operaciones relacionadas con `files` Extremo (es decir, análisis del sistema de archivos) en la interfaz de línea de comandos de ONTAP, la API DE REST y System Manager.

Para obtener más información sobre `admin-no-fsa` función, consulte [Roles predefinidos para administradores de clúster](#).

Si utiliza una versión de ONTAP publicada antes de ONTAP 9.12.1, tendrá que crear un rol dedicado para controlar el acceso al análisis del sistema de archivos. En las versiones de ONTAP anteriores a ONTAP 9.12.1, debe configurar los permisos de RBAC a través de la interfaz de línea de comandos de ONTAP o la API DE REST de ONTAP.

## System Manager

A partir de ONTAP 9.12.1, puede configurar permisos de RBAC para análisis de sistemas de archivos con System Manager.

### Pasos

1. Seleccione **Cluster > Settings**. En **Seguridad**, vaya a **usuarios y roles** y seleccione ➔.
2. En **roles**, seleccione **+ Add**.
3. Escriba un nombre para el rol. En atributos de función, configure el acceso o las restricciones para la función de usuario proporcionando el adecuado "Extremos de API". Consulte la tabla siguiente para ver las rutas principales y las rutas secundarias para configurar restricciones o acceso al análisis del sistema de archivos.

| Restricción                                               | Ruta primaria        | Ruta secundaria                                                                                                                                                                             |
|-----------------------------------------------------------|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Seguimiento de actividad en volúmenes                     | /api/storage/volumes | <ul style="list-style-type: none"><li>• /:uuid/top-metrics/directories</li><li>• /:uuid/top-metrics/files</li><li>• /:uuid/top-metrics/clients</li><li>• /:uuid/top-metrics/users</li></ul> |
| Seguimiento de actividad en las SVM                       | /api/svm/svms        | <ul style="list-style-type: none"><li>• /:uuid/top-metrics/directories</li><li>• /:uuid/top-metrics/files</li><li>• /:uuid/top-metrics/clients</li><li>• /:uuid/top-metrics/users</li></ul> |
| Todas las operaciones de análisis del sistema de archivos | /api/storage/volumes | /:uuid/files                                                                                                                                                                                |

Puede utilizar /\*/ En lugar de un UUID para establecer la política para todos los volúmenes o SVM en el extremo.

Elija los privilegios de acceso para cada extremo.

4. Seleccione **Guardar**.
5. Para asignar el rol a un usuario o a un usuario, consulte [Control del acceso de administradores](#).

### CLI

Si utiliza una versión de ONTAP publicada antes de ONTAP 9.12.1, utilice la interfaz de línea de comandos de ONTAP para crear un rol personalizado.

## Pasos

1. Cree una función predeterminada para tener acceso a todas las funciones.

Esto debe hacerse antes de crear la función restrictiva para asegurarse de que la función sólo se limita en el seguimiento de actividad:

```
security login role create -cmddirname DEFAULT -access all -role storageAdmin
```

2. Cree el rol restrictivo:

```
security login role create -cmddirname "volume file show-disk-usage" -access none -role storageAdmin
```

3. Autorice a los roles para acceder a los servicios web de la SVM:

- `rest` Para llamadas a la API DE REST
- `security` para protección mediante contraseña
- `sysmgr` Para acceder a System Manager

```
vserver services web access create -vserver svm-name -name rest -role storageAdmin
```

```
vserver services web access create -vserver svm-name -name security -role storageAdmin
```

```
vserver services web access create -vserver svm-name -name sysmgr -role storageAdmin
```

4. Cree un usuario.

Debe emitir un comando `CREATE` distinto para cada aplicación que desee aplicar al usuario. Llamar crea varias veces en el mismo usuario simplemente aplica todas las aplicaciones a ese usuario y no crea un nuevo usuario cada vez. La `http` El parámetro del tipo de aplicación se aplica a la API REST de ONTAP y System Manager.

```
security login create -user-or-group-name storageUser -authentication -method password -application http -role storageAdmin
```

5. Ahora, con las credenciales de usuario nuevas, puede iniciar sesión en System Manager o usar la API DE REST de ONTAP para acceder a los datos de análisis de sistemas de archivos.

## Más información

- [Roles predefinidos para administradores de clúster](#)
- [Controle el acceso de administradores con System Manager](#)
- ["Obtenga más información acerca de los roles de RBAC y la API DE REST de ONTAP"](#)

## Consideraciones para el análisis del sistema de archivos

Debe conocer ciertos límites de uso e impactos de rendimiento potenciales asociados

con la implementación de los análisis del sistema de archivos.

## Relaciones protegidas por SVM

Si ha habilitado File System Analytics en los volúmenes que contienen SVM se encuentran en una relación de protección, los datos de análisis no se replican en la SVM de destino. Si la SVM de origen debe volver a sincronizarse en una operación de recuperación, debe volver a habilitar manualmente los análisis de los volúmenes deseados una vez que se recupera.

## Consideraciones de rendimiento

En algunos casos, la activación del análisis del sistema de archivos podría afectar negativamente al rendimiento durante la recopilación inicial de metadatos. Esto se suele ver en sistemas con un aprovechamiento máximo. Para evitar habilitar análisis en dichos sistemas, puede utilizar las herramientas de supervisión del rendimiento de System Manager de ONTAP.

Si experimenta un aumento significativo en la latencia, consulte el artículo de la base de conocimientos ["Una latencia elevada o fluctuante después de activar el análisis del sistema de archivos ONTAP de NetApp"](#).

## Consideraciones sobre la adquisición

Cuando se habilita el análisis de capacidad, ONTAP realiza un análisis de inicialización para los análisis de capacidad. El análisis accede a los metadatos de todos los archivos de los volúmenes para los que están habilitados los análisis de capacidad. No se leen datos de archivos durante el análisis. A partir de ONTAP 9.14.1, puede realizar un seguimiento del progreso del análisis con la API REST, en la pestaña **Explorer** del Administrador del sistema o con el `volume analytics show` Comando de la CLI. Si hay un evento de limitación, ONTAP proporciona una notificación.

Una vez que se completa el análisis, File System Analytics se actualiza continuamente en tiempo real a medida que el sistema de archivos cambia sin necesidad de volver a ejecutar el análisis.

El tiempo necesario para la exploración es proporcional al número de directorios y archivos del volumen. Como el análisis recoge metadatos, el tamaño del archivo no afecta el tiempo de análisis.

Para obtener más información sobre la secuencia de inicialización, consulte ["TR-4867: Directrices de prácticas recomendadas para análisis de sistemas de archivos"](#).

## Mejores prácticas

Debe iniciar el análisis en los volúmenes que no comparten agregados. Puede ver qué agregados alojan actualmente los volúmenes con el comando:

```
volume show -volume comma-separated-list_of_volumes -fields aggr-list
```

Mientras se ejecuta el análisis, los volúmenes siguen sirviendo al tráfico de cliente. Se recomienda iniciar la exploración durante los períodos en los que se anticipa un tráfico de cliente más bajo.

Si aumenta el tráfico del cliente, consumirá recursos del sistema y el análisis tardará más tiempo.

A partir de ONTAP 9.12.1, se puede pausar la recogida de datos en System Manager y con la CLI de ONTAP.

- Si utiliza la CLI de ONTAP:
  - Puede pausar la recopilación de datos con el comando: `volume analytics initialization pause -vserver svm_name -volume volume_name`

- Una vez que el tráfico del cliente se ha ralentizado, puede reanudar la recopilación de datos con el comando: `volume analytics initialization resume -vserver svm_name -volume volume_name`

- Si está utilizando System Manager, en la vista **Explorer** del menú de volumen, utilice los botones **Pausar la recopilación de datos** y **Reanudar la recopilación de datos** para administrar el escaneo.

## Configuración de EMS

### Información general de la configuración de EMS

Puede configurar ONTAP 9 para que envíe importantes notificaciones de eventos de EMS (Event Management System) directamente a una dirección de correo electrónico, un servidor de syslog, un host de capturas de protocolo simple de red de gestión (SNMP) o una aplicación webhook para que se le informe de inmediato de los problemas del sistema que requieren atención urgente.

Dado que las notificaciones de eventos importantes no están habilitadas de forma predeterminada, debe configurar EMS para que envíe notificaciones a una dirección de correo electrónico, a un servidor de syslog, a un host de capturas de SNMP o a una aplicación webhook.

Revise las versiones específicas de cada versión de ["Referencia de ONTAP 9 EMS"](#).

Si la asignación de eventos de EMS utiliza conjuntos de comandos ONTAP obsoletos (como el destino de eventos o la ruta de eventos), se recomienda actualizar la asignación. ["Aprenda a actualizar el mapa de EMS desde comandos de ONTAP obsoletos"](#).

### Configure las notificaciones de eventos de EMS y los filtros con System Manager

Puede usar System Manager para configurar cómo el sistema de gestión de eventos (EMS) envía notificaciones de eventos de modo que se puedan notificar de los problemas del sistema que requieren su atención.

| Versión de ONTAP                     | Con System Manager, podrá...                                                                                                                                                                                        |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ONTAP 9.12.1 y versiones posteriores | Especifique el protocolo TLS (Seguridad de la capa de transporte) cuando envíe eventos a servidores de syslog remotos.                                                                                              |
| ONTAP 9.10.1 y posteriores           | Configurar las direcciones de correo electrónico, los servidores de syslog y las aplicaciones de webhook, así como los hosts de capturas SNMP.                                                                      |
| ONTAP 9.7 a 9.10.0                   | Configurar solo los hosts de capturas de SNMP. Es posible configurar otro destino de EMS con la interfaz de línea de comandos de ONTAP. Consulte <a href="#">"Información general de la configuración de EMS"</a> . |

Puede realizar los siguientes procedimientos:

- [\[add-ems-destination\]](#)
- [\[create-ems-filter\]](#)

- [\[edit-ems-destination\]](#)
- [\[edit-ems-filter\]](#)
- [\[delete-ems-destination\]](#)
- [\[delete-ems-filter\]](#)

#### Información relacionada



- ["Referencia de EMS de ONTAP"](#)
- ["Uso de la interfaz de línea de comandos para configurar los hosts de capturas de SNMP para recibir notificaciones de eventos"](#)

### Añada un destino de notificación de eventos de EMS

Puede usar System Manager para especificar dónde desea enviar mensajes de EMS.

A partir de ONTAP 9.12.1, los eventos EMS se pueden enviar a un puerto designado en un servidor de syslog remoto a través del protocolo de seguridad de la capa de transporte (TLS). Para obtener más detalles, consulte `event notification destination create` [página de manual](#).

#### Pasos

1. Haga clic en **clúster > Configuración**.
2. En la sección **Administración de notificaciones**, haga clic en , A continuación, haga clic en **Ver destinos de evento**.
3. En la página **Administración de notificaciones**, seleccione la ficha **Destinos de eventos**.
4. Haga clic en  **Add**.
5. Especifique un nombre, un tipo de destino EMS y filtros.



Si es necesario, puede agregar un filtro nuevo. Haga clic en **Agregar un nuevo filtro de sucesos**.

6. Según el tipo de destino de EMS seleccionado, especifique lo siguiente:

| Para configurar...                         | Especificar o seleccionar...                                                                                                                                                          |
|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host de capturas de SNMP                   | <ul style="list-style-type: none"> <li>• Nombre de TrapHost</li> </ul>                                                                                                                |
| Correo electrónico<br>(A partir de 9.10.1) | <ul style="list-style-type: none"> <li>• Dirección de correo electrónico de destino</li> <li>• Servidor de correo</li> <li>• Dirección de correo electrónico del remitente</li> </ul> |






|                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Servidor de syslog<br>(A partir de 9.10.1) | <ul style="list-style-type: none"> <li>Nombre de host o dirección IP del servidor</li> <li>Puerto de syslog (9.12.1 y posterior)</li> <li>Transporte de syslog (a partir de 9.12.1)</li> </ul> <p>Al seleccionar <b>cifrado TCP</b> se activa el protocolo de seguridad de la capa de transporte (TLS). Si no se introduce ningún valor para <b>puerto Syslog</b>, se utiliza un valor predeterminado basado en la selección <b>Transporte Syslog</b>.</p> |
| Webhook<br>(A partir de 9.10.1)            | <ul style="list-style-type: none"> <li>URL de Webhook</li> <li>Autenticación de cliente (seleccione esta opción para especificar un certificado de cliente)</li> </ul>                                                                                                                                                                                                                                                                                     |

## Cree un nuevo filtro de notificación de eventos EMS

A partir de ONTAP 9.10.1, es posible usar System Manager para definir nuevos filtros personalizados que especifiquen las reglas para el manejo de las notificaciones de EMS.

### Pasos

- Haga clic en **clúster > Configuración**.
- En la sección **Administración de notificaciones**, haga clic en , A continuación, haga clic en **Ver destinos de eventos**.
- En la página **Administración de notificaciones**, seleccione la ficha **Filtros de sucesos**.
- Haga clic en  **Add**.
- Especifique un nombre y seleccione si desea copiar reglas de un filtro de eventos existente o agregar nuevas reglas.
- En función de su elección, realice los siguientes pasos:



| Si elige....                                         | A continuación, realice estos pasos...                                                                                                                                                                                                                                                                 |
|------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Copiar reglas del filtro de sucesos existente</b> | <ol style="list-style-type: none"> <li>Seleccione un filtro de sucesos existente.</li> <li>Modifique las reglas existentes.</li> <li>Si es necesario, agregue otras reglas haciendo clic en  <b>Add</b>.</li> </ol> |
| <b>Añadir nuevas reglas</b>                          | Especifique el tipo, patrón de nombre, gravedad y tipo de captura SNMP para cada nueva regla.                                                                                                                                                                                                          |

## Edite un destino de notificación de eventos de EMS

A partir de ONTAP 9.10.1, puede utilizar System Manager para cambiar la información del destino de notificaciones de eventos.

### Pasos

- Haga clic en **clúster > Configuración**.

2. En la sección **Administración de notificaciones**, haga clic en  , A continuación, haga clic en **Ver destinos de evento**.
3. En la página **Administración de notificaciones**, seleccione la ficha **Destinos de eventos**.
4. Junto al nombre del destino del evento, haga clic en  , A continuación, haga clic en **Editar**.
5. Modifique la información del destino del evento y, a continuación, haga clic en **Guardar**.



### Edite un filtro de notificación de eventos EMS

A partir de ONTAP 9.10.1, es posible usar System Manager para modificar los filtros personalizados y cambiar la forma en que se manejan las notificaciones de eventos.



No puede modificar filtros definidos por el sistema.

#### Pasos

1. Haga clic en **clúster > Configuración**.
2. En la sección **Administración de notificaciones**, haga clic en  , A continuación, haga clic en **Ver destinos de eventos**.
3. En la página **Administración de notificaciones**, seleccione la ficha **Filtros de sucesos**.
4. Junto al nombre del filtro de eventos, haga clic en  , A continuación, haga clic en **Editar**.
5. Modifique la información del filtro de sucesos y haga clic en **Guardar**.



### Elimine un destino de notificación de eventos de EMS

A partir de ONTAP 9.10.1, es posible usar System Manager para eliminar un destino de notificación de eventos de EMS.



No puede eliminar destinos SNMP.

#### Pasos

1. Haga clic en **clúster > Configuración**.
2. En la sección **Administración de notificaciones**, haga clic en  , A continuación, haga clic en **Ver destinos de eventos**.
3. En la página **Administración de notificaciones**, seleccione la ficha **Destinos de eventos**.
4. Junto al nombre del destino del evento, haga clic en  , Luego haga clic en **Eliminar**.


### Elimine un filtro de notificación de eventos EMS


A partir de ONTAP 9.10.1, se puede usar System Manager para eliminar filtros personalizados.



No puede eliminar filtros definidos por el sistema.

#### Pasos

1. Haga clic en **clúster > Configuración**.
2. En la sección **Administración de notificaciones**, haga clic en  , A continuación, haga clic en **Ver destinos de eventos**.
3. En la página **Administración de notificaciones**, seleccione la ficha **Filtros de sucesos**.

4. Junto al nombre del filtro de eventos, haga clic en , A continuación, haga clic en **Eliminar**.

## Configure las notificaciones de eventos de EMS con la CLI

### Flujo de trabajo de configuración de EMS

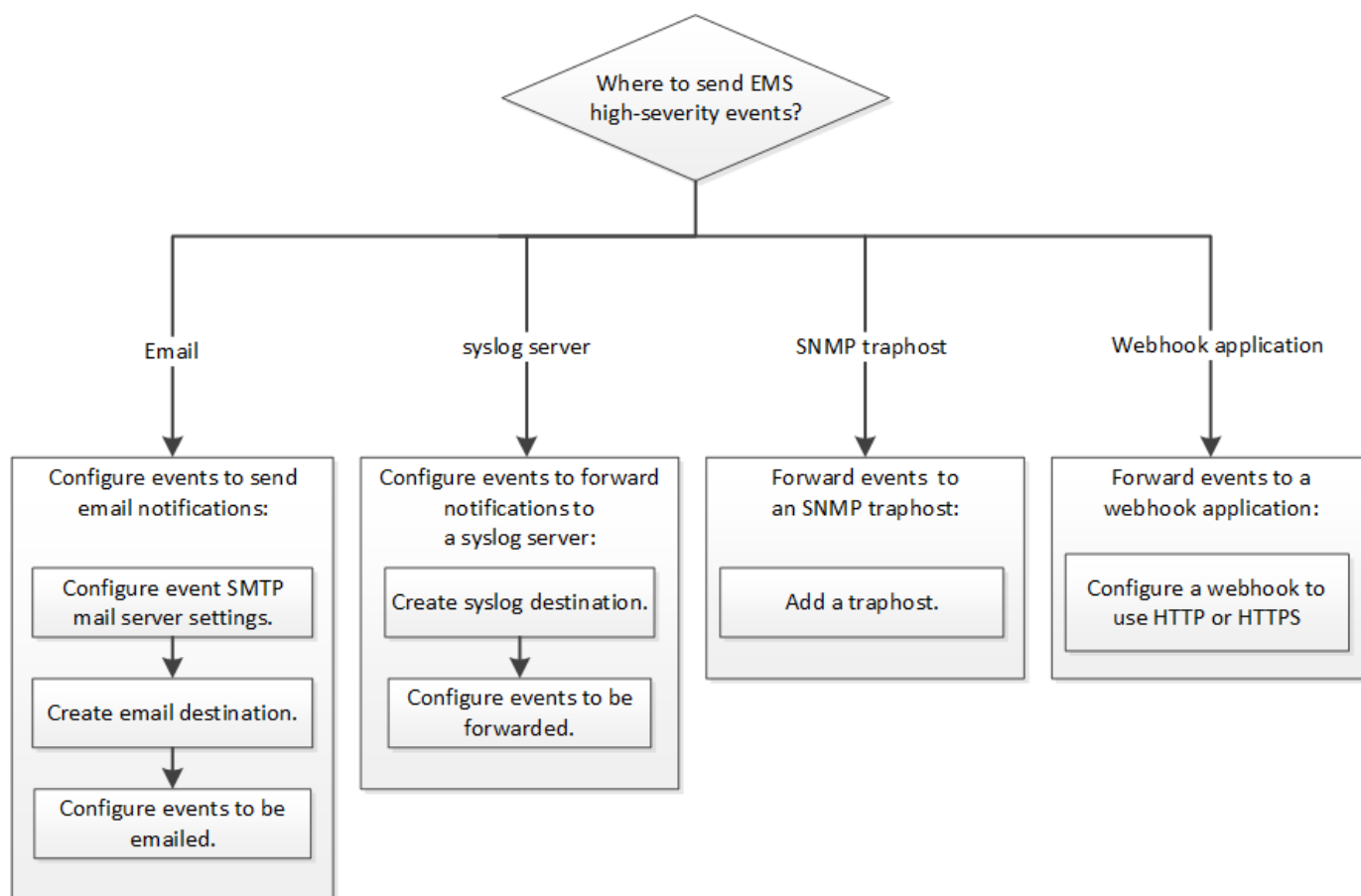
Debe configurar las notificaciones de eventos de EMS importantes para que se envíen como correo electrónico, se reenvíen a un servidor de syslog, se reenvíen a un host de capturas de SNMP o se reenvíen a una aplicación de webhook. Esto le ayuda a evitar interrupciones en el sistema tomando medidas correctivas de forma puntual.

#### Acerca de esta tarea

Si el entorno ya contiene un servidor de syslog para añadir los eventos registrados de otros sistemas, como servidores y aplicaciones, resulta más fácil utilizar el mismo servidor de syslog para enviar las notificaciones de eventos importantes de sistemas de almacenamiento.

Si el entorno no contiene ningún servidor de syslog, resulta más fácil usar un correo electrónico para enviar las notificaciones de eventos importantes.

Si ya ha reenviado notificaciones de eventos a un host de capturas de SNMP, es posible que desee supervisar dicho host de capturas para buscar eventos importantes.



#### Opciones

- Configure EMS para que envíe notificaciones de eventos.

| Si desea que...                                                                       | Consulte...                                                                                                |
|---------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| EMS envíe notificaciones de eventos importantes a una dirección de correo electrónico | <a href="#">Configure eventos de EMS importantes para que envíen notificaciones por correo electrónico</a> |
| EMS reenvíe notificaciones de eventos importantes a un servidor de syslog             | <a href="#">Configure eventos de EMS importantes para reenviar notificaciones a un servidor de syslog</a>  |
| EMS reenvíe notificaciones de eventos a un host de capturas de SNMP                   | <a href="#">Configure los hosts de capturas de SNMP para recibir notificaciones de eventos</a>             |
| Si desea que EMS reenvíe notificaciones de eventos a una aplicación webhook           | <a href="#">Configure eventos EMS importantes para reenviar notificaciones a una aplicación webhook</a>    |

### Configure eventos de EMS importantes para que envíen notificaciones por correo electrónico

Para recibir notificaciones por correo electrónico acerca de los eventos más importantes, debe configurar EMS para que envíe mensajes por correo electrónico de los eventos que representan actividades importantes.

#### Lo que necesitará

El DNS debe haberse configurado en el clúster para resolver las direcciones de correo electrónico.

#### Acerca de esta tarea

Puede realizar esta tarea en cualquier momento que el clúster esté en ejecución. Para ello, introduzca los comandos en la línea de comandos de ONTAP.

#### Pasos

1. Configure las opciones del servidor de correo SMTP de eventos:

```
event config modify -mail-server mailhost.your_domain -mail-from
cluster_admin@your_domain
```

2. Cree un destino de correo electrónico para las notificaciones de eventos:

```
event notification destination create -name storage-admins -email
your_email@your_domain
```

3. Configure los eventos importantes para que envíen notificaciones por correo electrónico:

```
event notification create -filter-name important-events -destinations storage-
admins
```

### Configuración de eventos de EMS importantes para reenviar notificaciones a un servidor de syslog

Para registrar las notificaciones de los eventos más graves en un servidor de syslog, debe configurar EMS para reenviar las notificaciones de los eventos que representan actividades importantes.

## Lo que necesitará

El DNS debe haberse configurado en el clúster para resolver el nombre del servidor de syslog.

## Acerca de esta tarea

Si el entorno no contiene un servidor de syslog para las notificaciones de eventos, primero debe crear uno. Si el entorno ya contiene un servidor de syslog para registrar eventos de otros sistemas, se recomienda usarlo para las notificaciones de eventos importantes.

Puede realizar esta tarea en cualquier momento que el clúster esté en ejecución. Para ello, introduzca los comandos en la CLI de ONTAP.

A partir de ONTAP 9.12.1, los eventos EMS se pueden enviar a un puerto designado en un servidor de syslog remoto a través del protocolo de seguridad de la capa de transporte (TLS). Hay dos nuevos parámetros disponibles:

### **tcp-encrypted**

Cuando `tcp-encrypted` se especifica para la `syslog-transport`, ONTAP verifica la identidad del host de destino validando su certificado. El valor predeterminado es `udp-unencrypted`.

### **syslog-port**

El valor predeterminado `syslog-port` el parámetro depende del valor del `syslog-transport` parámetro. Si `syslog-transport` se establece en `tcp-encrypted`, `syslog-port` tiene el valor predeterminado 6514.

Para obtener más detalles, consulte `event notification destination create` [página de manual](#).

## Pasos

1. Cree un destino de servidor de syslog para los eventos importantes:

```
event notification destination create -name syslog-ems -syslog syslog-server-address -syslog-transport {udp-unencrypted|tcp-unencrypted|tcp-encrypted}
```

A partir de ONTAP 9.12.1, se pueden especificar los siguientes valores para `syslog-transport`:

- ° `udp-unencrypted` - Protocolo de datagramas de usuario sin seguridad
- ° `tcp-unencrypted` - Protocolo de control de la transmisión sin seguridad
- ° `tcp-encrypted` - Protocolo de control de la transmisión con seguridad de la capa de transporte (TLS)

El protocolo predeterminado es `udp-unencrypted`.

2. Configure los eventos importantes de manera que reenvíen notificaciones al servidor de syslog:

```
event notification create -filter-name important-events -destinations syslog-ems
```

## Configure los hosts de capturas de SNMP para recibir notificaciones de eventos

Para recibir notificaciones de eventos en un host de capturas de SNMP, debe configurar un host de capturas.

## Lo que necesitará

- Se debe habilitar SNMP y las capturas de SNMP en el clúster.



SNMP y las capturas de SNMP se habilitan de forma predeterminada.

- El DNS debe haberse configurado en el clúster para resolver los nombres de host de capturas.

## Acerca de esta tarea

Si no tiene un host de capturas de SNMP configurado para recibir notificaciones de eventos (capturas de SNMP), debe añadir uno.

Puede realizar esta tarea en cualquier momento que el clúster esté en ejecución. Para ello, introduzca los comandos en la línea de comandos de ONTAP.

## Paso

1. Si su entorno no tiene un host de capturas de SNMP configurado para recibir notificaciones de eventos, añada uno:

```
system snmp traphost add -peer-address snmp_traphost_name
```

Todas las notificaciones de eventos que SNMP admite de forma predeterminada se reenvían al host de capturas de SNMP.

## Configure eventos EMS importantes para reenviar notificaciones a una aplicación webhook

Puede configurar ONTAP para reenviar notificaciones de eventos importantes a una aplicación webhook. Los pasos de configuración necesarios dependen del nivel de seguridad que elija.

### Prepare la configuración del reenvío de eventos EMS

Hay varios conceptos y requisitos que debe tener en cuenta antes de configurar ONTAP para reenviar notificaciones de eventos a una aplicación webhook.

### Aplicación Webhook

Necesita una aplicación de webhook capaz de recibir las notificaciones de eventos de ONTAP. Un webhook es una rutina de devolución de llamada definida por el usuario que amplía la capacidad de la aplicación remota o el servidor donde se ejecuta. El cliente llama o activa a los enlaces web (en este caso ONTAP) enviando una solicitud HTTP a la dirección URL de destino. Específicamente, ONTAP envía una solicitud HTTP POST al servidor que aloja la aplicación webhook junto con los detalles de notificación de eventos formateados en XML.

## Opciones de seguridad

Hay varias opciones de seguridad disponibles en función de cómo se utilice el protocolo de seguridad de la capa de transporte (TLS). La opción que elija determina la configuración de ONTAP que requiere.



TLS es un protocolo criptográfico que se utiliza ampliamente en Internet. Proporciona privacidad, así como integridad de datos y autenticación mediante uno o varios certificados de clave pública. Los certificados son emitidos por autoridades de certificados de confianza.

## HTTP

Es posible utilizar HTTP para transportar las notificaciones de eventos. Con esta configuración, la conexión no es segura. Las identidades del cliente ONTAP y de la aplicación webhook no se verifican. Además, el tráfico de red no está cifrado ni protegido. Consulte ["Configure un destino de webhook para utilizar HTTP"](#) para obtener detalles de la configuración.

## HTTPS

Para mayor seguridad, puede instalar un certificado en el servidor que aloja la rutina de webhook. ONTAP utiliza el protocolo HTTPS para verificar la identidad del servidor de aplicaciones webhook, así como de ambas partes, para garantizar la privacidad e integridad del tráfico de red. Consulte ["Configure un destino de webhook para utilizar HTTPS"](#) para obtener detalles de la configuración.

### HTTPS con autenticación mutua

Puede mejorar aún más la seguridad HTTPS mediante la instalación de un certificado de cliente en el sistema ONTAP que emite las solicitudes webhook. Además ONTAP de verificar la identidad del servidor de aplicaciones webhook y proteger el tráfico de red, la aplicación webhook verifica la identidad del cliente ONTAP. Esta autenticación de par bidireccional se conoce como *Mutual TLS*. Consulte ["Configure un destino de webhook para utilizar HTTPS con autenticación mutua"](#) para obtener detalles de la configuración.

### Información relacionada

- ["Protocolo de seguridad de la capa de transporte \(TLS\) versión 1.3"](#)

### Configure un destino de webhook para utilizar HTTP

Puede configurar ONTAP para reenviar notificaciones de eventos a una aplicación webhook mediante HTTP. Esta es la opción menos segura pero la más sencilla de configurar.

### Pasos

1. Cree un nuevo destino `restapi-ems` para recibir los eventos:

```
event notification destination create -name restapi-ems -rest-api-url
http://<webhook-application>
```

En el comando anterior, debe utilizar el esquema **HTTP** para el destino.

2. Cree una notificación que vincule el `important-events` filtre con la `restapi-ems` destino:

```
event notification create -filter-name important-events -destinations restapi-
ems
```

### Configure un destino de webhook para utilizar HTTPS

Puede configurar ONTAP para reenviar notificaciones de eventos a una aplicación de webhook mediante HTTPS. ONTAP utiliza el certificado de servidor para confirmar la identidad de la aplicación webhook y proteger el tráfico de red.

### Antes de empezar

- Genere una clave privada y un certificado para el servidor de aplicaciones de webhook
- Tenga el certificado raíz disponible para instalar en ONTAP

### Pasos

1. Instale la clave privada y los certificados del servidor adecuados en el servidor que aloja la aplicación webhook. Los pasos de configuración específicos dependen del servidor.
2. Instale el certificado raíz de servidor en ONTAP:

```
security certificate install -type server-ca
```

El comando solicitará el certificado.

3. Cree el `restapi-ems` destino para recibir los eventos:

```
event notification destination create -name restapi-ems -rest-api-url
https://<webhook-application>
```

En el comando anterior, debe usar el esquema **HTTPS** para el destino.

4. Cree la notificación que vincula el `important-events` filtrar con el nuevo `restapi-ems` destino:

```
event notification create -filter-name important-events -destinations restapi-
ems
```

#### Configure un destino de webhook para utilizar HTTPS con autenticación mutua

Puede configurar ONTAP para reenviar notificaciones de eventos a una aplicación de webhook mediante HTTPS con autenticación mutua. Con esta configuración hay dos certificados. ONTAP utiliza el certificado de servidor para confirmar la identidad de la aplicación webhook y proteger el tráfico de red. Además, la aplicación que aloja el webhook utiliza el certificado de cliente para confirmar la identidad del cliente ONTAP.

#### Antes de empezar

Debe hacer lo siguiente antes de configurar ONTAP:

- Genere una clave privada y un certificado para el servidor de aplicaciones de webhook
- Tenga el certificado raíz disponible para instalar en ONTAP
- Genere una clave privada y un certificado para el cliente ONTAP

#### Pasos

1. Realice los dos primeros pasos de la tarea ["Configure un destino de webhook para utilizar HTTPS"](#) Instalar el certificado de servidor para que ONTAP pueda verificar la identidad del servidor.
2. Instale los certificados raíz e intermedios adecuados en la aplicación webhook para validar el certificado de cliente.
3. Instale el certificado de cliente en ONTAP:

```
security certificate install -type client
```

El comando solicitará la clave privada y el certificado.

4. Cree el `restapi-ems` destino para recibir los eventos:

```
event notification destination create -name restapi-ems -rest-api-url
https://<webhook-application> -certificate-authority <issuer of the client
certificate> -certificate-serial <serial of the client certificate>
```



En el comando anterior, debe utilizar el esquema **HTTPS** para el destino.

5. Cree la notificación que vincula el `important-events` filtrar con el nuevo `restapi-ems` destino:

```
event notification create -filter-name important-events -destinations restapi-ems
```

## Actualizar asignación de eventos de EMS obsoleta

### Modelos de asignación de eventos EMS

Antes de ONTAP 9.0, los eventos de EMS solo podían asignarse a destinos de eventos en función de la correspondencia entre el patrón de nombres de eventos. Los conjuntos de comandos de la ONTAP (`event destination`, `event route`) Que usan este modelo siguen estando disponibles en las últimas versiones de ONTAP, pero han sido obsoletas empezando por ONTAP 9.0.

A partir de ONTAP 9.0, la práctica recomendada para la asignación de destinos de eventos EMS de ONTAP es utilizar el modelo de filtro de eventos más escalable en el que la coincidencia de patrones se realiza en varios campos, mediante la `event filter`, `event notification`, y `event notification destination` conjuntos de comandos.

Si la asignación de EMS se configura con los comandos obsoletos, debe actualizar la asignación para utilizar los `event filter`, `event notification`, y `event notification destination` conjuntos de comandos.

Hay dos tipos de destinos de eventos:

1. **Destinos generados por el sistema:** Hay cinco destinos de eventos generados por el sistema (creados de forma predeterminada)

- `allevents`
- `asup`
- `criticals`
- `pager`
- `traphost`

Algunos de los destinos generados por el sistema tienen un propósito especial. Por ejemplo, el destino `asup` enruta los eventos `callhome.*` al módulo AutoSupport de ONTAP para generar mensajes AutoSupport.

2. **Destinos creados por el usuario:** Se crean manualmente mediante el `event destination create` comando.

```
cluster-1::event*> destination show
```

| Name | Mail Dest. | SNMP Dest. | Syslog Dest. | Hide |
|------|------------|------------|--------------|------|
|------|------------|------------|--------------|------|

Params

|       |       |       |       |       |
|-------|-------|-------|-------|-------|
| ----- | ----- | ----- | ----- | ----- |
| ----- |       |       |       |       |

allevents

-

-

-

false

asup

-

-

-

false

criticals

-

-

-

false

pager

-

-

-

false

traphost

-

-

-

false

5 entries were displayed.

+

```
cluster-1::event*> destination create -name test -mail test@xyz.com
```

This command is deprecated. Use the "event filter", "event notification destination" and "event notification" commands, instead.

+

```
cluster-1::event*> destination show
```

+

Hide

| Name | Mail Dest. | SNMP Dest. | Syslog Dest. |
|------|------------|------------|--------------|
|------|------------|------------|--------------|

Params

|       |       |       |       |
|-------|-------|-------|-------|
| ----- | ----- | ----- | ----- |
| ----- |       |       |       |

allevents

-

-

-

false

asup

-

-

-

false

criticals

-

-

-

false

pager

-

-

-

false

test

test@xyz.com

-

-

false

traphost

-

-

-

false

6 entries were displayed.

En el modelo obsoleto, los eventos EMS se asignan individualmente a un destino mediante el `event route add-destinations` comando.

```
cluster-1::event*> route add-destinations -message-name raid.aggr.*
-destinations test
This command is deprecated. Use the "event filter", "event notification
destination" and "event notification" commands, instead.
4 entries were acted on.
```

```
cluster-1::event*> route show -message-name raid.aggr.*
```

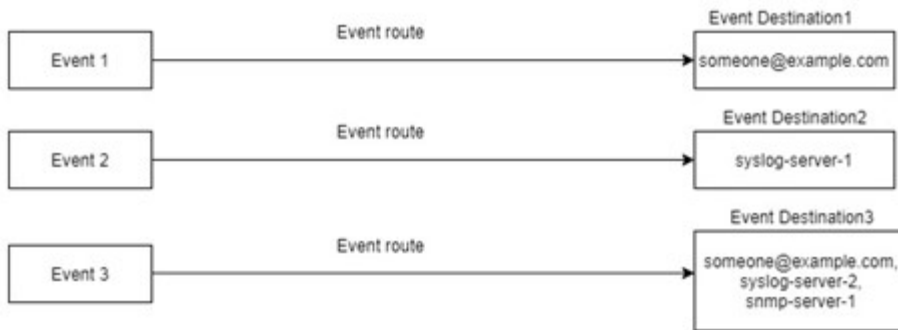
| Time                       | Severity      | Destinations | Freq | Threshd |
|----------------------------|---------------|--------------|------|---------|
| raid.aggr.autoGrow.abort   | NOTICE        | test         | 0    | 0       |
| raid.aggr.autoGrow.success | NOTICE        | test         | 0    | 0       |
| raid.aggr.lock.conflict    | INFORMATIONAL | test         | 0    | 0       |
| raid.aggr.log.CP.count     | DEBUG         | test         | 0    | 0       |

4 entries were displayed.

El nuevo mecanismo de notificaciones de eventos de EMS más escalable se basa en filtros de eventos y destinos de notificaciones de eventos. Consulte el siguiente artículo de la base de conocimientos para obtener información detallada sobre el nuevo mecanismo de notificación de eventos:

- ["Descripción general del sistema de gestión de eventos para ONTAP 9"](#)

Legacy routing based model



Event notification based model



### Actualice la asignación de eventos de EMS desde comandos ONTAP obsoletos

Si la asignación de eventos de EMS se configura actualmente con los conjuntos de comandos ONTAP obsoletos (event destination, event route), debe seguir este procedimiento para actualizar la asignación para utilizar event filter, event notification, y event notification destination conjuntos de comandos.

#### Pasos

1. Enumere todos los destinos de eventos del sistema mediante event destination show comando.

```
cluster-1::event*> destination show
```

Hide

| Name | Mail Dest. | SNMP Dest. | Syslog Dest. |
|------|------------|------------|--------------|
|------|------------|------------|--------------|

Params

|           |              |   |   |
|-----------|--------------|---|---|
| allevents | -            | - | - |
| false     |              |   |   |
| asup      | -            | - | - |
| false     |              |   |   |
| criticals | -            | - | - |
| false     |              |   |   |
| pager     | -            | - | - |
| false     |              |   |   |
| test      | test@xyz.com | - | - |
| false     |              |   |   |
| traphost  | -            | - | - |
| false     |              |   |   |

6 entries were displayed.

2. Para cada destino, enumere los eventos que se están asignando con el `event route show -destinations <destination name>` comando.

```
cluster-1::event*> route show -destinations test
```

| Time                       | Message       | Severity | Destinations | Threshd | Freq |
|----------------------------|---------------|----------|--------------|---------|------|
| raid.aggr.autoGrow.abort   | NOTICE        | test     | 0            | 0       |      |
| raid.aggr.autoGrow.success | NOTICE        | test     | 0            | 0       |      |
| raid.aggr.lock.conflict    | INFORMATIONAL | test     | 0            | 0       |      |
| raid.aggr.log.CP.count     | DEBUG         | test     | 0            | 0       |      |

4 entries were displayed.

3. Cree una correspondiente `event filter` lo que incluye todos estos subconjuntos de eventos. Por ejemplo, si desea incluir solo el `raid.aggr.*` sucesos, utilice un comodín para el `message-name` parámetro al crear el filtro. También puede crear filtros para eventos individuales.



Es posible crear hasta 50 filtros de eventos.

```
cluster-1::event*> filter create -filter-name test_events

cluster-1::event*> filter rule add -filter-name test_events -type
include -message-name raid.aggr.*

cluster-1::event*> filter show -filter-name test_events
Filter Name Rule Rule Message Name SNMP Trap Type
Severity
 Position Type

test_events
 1 include raid.aggr.* * *
 2 exclude * * *
2 entries were displayed.
```

4. Cree un event notification destination para cada uno de los event destination Extremos (es decir, SMTP/SNMP/syslog)

```
cluster-1::event*> notification destination create -name dest1 -email
test@xyz.com

cluster-1::event*> notification destination show
Name Type Destination

dest1 email test@xyz.com (via "localhost" from
"admin@localhost", configured in "event config")
snmp-traphost snmp - (from "system snmp traphost")
2 entries were displayed.
```

5. Cree una notificación de eventos asignando el filtro de eventos al destino de notificación de eventos.

```
cluster-1::event*> notification create -filter-name asup_events
-destinations dest1

cluster-1::event*> notification show
ID Filter Name Destinations

1 default-trap-events snmp-traphost
2 asup_events dest1
2 entries were displayed.
```

6. Repita los pasos 1-5 para cada uno event destination eso tiene una event route asignación.



Los eventos enrutados a destinos de SNMP se deben asignar a `snmp-traphost` destino de notificaciones de eventos. El destino del host de capturas de SNMP utiliza el host de capturas de SNMP configurado del sistema.

```
cluster-1::event*> system snmp traphost add 10.234.166.135

cluster-1::event*> system snmp traphost show
 scspr2410142014.gdl.englab.netapp.com
(scspr2410142014.gdl.englab.netapp.com) <10.234.166.135> Community:
public

cluster-1::event*> notification destination show -name snmp-traphost

 Destination Name: snmp-traphost
 Type of Destination: snmp
 Destination: 10.234.166.135 (from "system snmp
traphost")
 Server CA Certificates Present?: -
 Client Certificate Issuing CA: -
 Client Certificate Serial Number: -
 Client Certificate Valid?: -
```

# Referencia de comandos de la ONTAP

Para cada versión principal de ONTAP, los comandos CLI disponibles con más frecuencia (páginas manuales de ONTAP o páginas de manual) se combinan en un *Command reference*. Estas referencias de comandos explican cómo utilizar los comandos de la CLI en cada versión de ONTAP. Las páginas de manual también están disponibles en la línea de comandos de ONTAP con el `man` comando.

## Referencias de comandos para versiones compatibles de ONTAP

- ["ONTAP 9.14.1"](#)
- ["ONTAP 9.13.1"](#)
- ["ONTAP 9.12.1"](#)
- ["ONTAP 9.11.1"](#)
- ["ONTAP 9.10.1"](#)
- ["ONTAP 9.9.1"](#)
- ["ONTAP 9,8"](#)
- ["ONTAP 9,7"](#)
- ["ONTAP 9,6"](#)
- ["ONTAP 9,5"](#)
- ["ONTAP 9,3"](#)

## Referencias de comandos para versiones de soporte limitadas de ONTAP (solo PDF)

- ["ONTAP 9,4"](#)
- ["ONTAP 9,2"](#)
- ["ONTAP 9,1"](#)
- ["ONTAP 9,0"](#)

## Herramienta de comparación de CLI

Puede aprender acerca de los cambios en los comandos de la interfaz de línea de comandos (CLI) entre las versiones de ONTAP mediante la ["Herramienta de comparación de CLI"](#) En el sitio de soporte de NetApp.

### Lecturas adicionales

- [Use la interfaz de línea de comandos de ONTAP](#)
- [Métodos para navegar por los directorios de comandos de la CLI](#)



# Avisos legales

Los avisos legales proporcionan acceso a las declaraciones de copyright, marcas comerciales, patentes y mucho más.

## Derechos de autor

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

## Marcas comerciales

NETAPP, el logotipo de NETAPP y las marcas enumeradas en la página de marcas comerciales de NetApp son marcas comerciales de NetApp, Inc. Los demás nombres de empresas y productos son marcas comerciales de sus respectivos propietarios.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

## Estadounidenses

Puede encontrar una lista actual de las patentes propiedad de NetApp en:

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

## Política de privacidad

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

## Código abierto

Los archivos de notificación proporcionan información sobre los derechos de autor y las licencias de terceros que se utilizan en software de NetApp.

## ONTAP

["Aviso para ONTAP 9.14.1"](#)  
["Aviso para ONTAP 9.14.0"](#)  
["Aviso para ONTAP 9.13.1"](#)  
["Aviso para ONTAP 9.12.1"](#)  
["Aviso para ONTAP 9.12.0"](#)  
["Aviso para ONTAP 9.11.1"](#)  
["Aviso para ONTAP 9.10.1"](#)  
["Aviso para ONTAP 9.10.0"](#)  
["Aviso para ONTAP 9.9.1"](#)  
["Aviso para ONTAP 9.8"](#)  
["Aviso para ONTAP 9,7"](#)  
["Aviso para ONTAP 9,6"](#)  
["Aviso para ONTAP 9,5"](#)  
["Aviso para ONTAP 9,4"](#)  
["Aviso para ONTAP 9,3"](#)  
["Aviso para ONTAP 9,2"](#)

"Aviso para ONTAP 9,1"

## **MEDIADOR ONTAP para MCC IP**

"9.9.1 Aviso PARA EL MEDIADOR de ONTAP para MCC IP"

"9.8 Aviso PARA EL MEDIADOR de ONTAP para MCC IP"

"9,7 Aviso para MEDIADOR DE ONTAP para MCC IP"

## Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

## Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.