NetApp Informes técnicos

NetApp Technical Reports

NetApp
June 05, 2026

Tabla de contenidos

NetApp Informes técnicos

Informes técnicos de ONTAP y aplicaciones y bases de datos

ONTAP es la base para la gestión y la protección de datos de numerosas tecnologías de aplicaciones y bases de datos empresariales. Los siguientes informes técnicos ofrecen orientación sobre las prácticas recomendadas de NetApp y los procedimientos de implementación para Microsoft SQL Server, MySQL, Oracle, PostgreSQL, SAP HANA y Epic.

Microsoft SQL Server

SQL Server es la base de la plataforma de datos de Microsoft y ofrece rendimiento de misión crítica con tecnologías en memoria y información más rápida sobre cualquier dato, ya sea en las instalaciones o en el cloud.

"Práctica recomendada para Microsoft SQL Server con ONTAP" Obtenga más información sobre cómo los administradores de almacenamiento y de bases de datos pueden implementar correctamente Microsoft SQL Server en sistemas de almacenamiento ONTAP.

Esta documentación sustituye al informe técnico publicado anteriormente *TR-4590: Guía de mejores prácticas para Microsoft SQL Server con ONTAP.*

"TR-4976: Rendimiento de Microsoft SQL Server virtualizado en sistemas NetApp AFF A-Series y C-Series" Conozca las características de rendimiento de Microsoft SQL Server mediante los sistemas de NetApp AFF A-Series y C-Series, así como orientación sobre cómo seleccionar el sistema adecuado en función de la carga de trabajo.

"TR-4714: Prácticas recomendadas para Microsoft SQL Server con SnapCenter" Descubre cómo implementar correctamente Microsoft SQL Server en almacenamiento de ONTAP utilizando la tecnología SnapCenter para la protección de datos.

MySQL

Este documento describe los requisitos de configuración y proporciona orientación sobre el ajuste y la configuración del almacenamiento para poner en marcha MySQL en ONTAP.

"Base de datos MySQL en mejores prácticas de NetApp ONTAP" MySQL y sus variantes, como MariaDB y Percona, son ampliamente utilizados en muchas aplicaciones empresariales. Estas aplicaciones van desde sitios de redes sociales globales y sistemas de comercio electrónico masivos hasta sistemas de alojamiento SMB que contienen miles de instancias de bases de datos. Conozca los requisitos de configuración y las instrucciones sobre el ajuste y la configuración del almacenamiento para implementar MySQL en ONTAP.

Esta documentación sustituye al informe técnico publicado previamente *TR-4722: Base de datos MySQL sobre mejores prácticas de NetApp ONTAP.*

Oracle

ONTAP está diseñado para bases de datos de Oracle. Durante décadas, ONTAP se ha optimizado para las demandas específicas de las I/O de las bases de datos relacionales y se crearon varias funciones de ONTAP

específicamente para satisfacer las necesidades de las bases de datos de Oracle e incluso a petición de la misma Oracle Inc.

"Bases de datos de Oracle en ONTAP" Obtenga más información sobre las prácticas recomendadas que permiten a los administradores de almacenamiento y bases de datos implementar Oracle con éxito en el almacenamiento de ONTAP.

"Protección de datos de Oracle con ONTAP" Obtenga más información sobre las prácticas recomendadas que permiten a los administradores de almacenamiento y de bases de datos realizar correctamente el backup, la recuperación, la replicación y proporcionar recuperación ante desastres a Oracle en almacenamiento de ONTAP.

"Recuperación ante desastres de Oracle con ONTAP" Obtenga más información sobre las prácticas recomendadas, los procedimientos de prueba y otras consideraciones para operar bases de datos de Oracle en una continuidad de negocio de MetroCluster y SnapMirror.

"Migración de bases de datos de Oracle a sistemas de almacenamiento de ONTAP" Conozca las consideraciones generales para planificar una estrategia de migración, los tres niveles diferentes en los que se lleva a cabo el movimiento de datos y detalla algunos de los diversos procedimientos disponibles.

> La documentación enlazada anteriormente sustituye a estos informes técnicos *TR-3633 publicados anteriormente: Bases de datos Oracle en ONTAP; TR-4591: Protección de datos de Oracle: Backup, recuperación, replicación; TR-4592: Oracle en MetroCluster; y TR-4534: Migración de bases de datos de Oracle a sistemas de almacenamiento de NetApp*

"TR-4969: Rendimiento de bases de datos de Oracle en AFF A-Series y C-Series"
ONTAP es una potente plataforma de gestión de datos con funcionalidades nativas que incluyen compresión en línea, actualizaciones de hardware no disruptivas y la capacidad de importar un LUN desde una cabina de almacenamiento externa. Es posible agrupar hasta 24 nodos en clúster y proporcionar datos de forma simultánea a través de los protocolos Sistema de archivos de red (NFS), Bloque de mensajes del servidor (SMB), iSCSI, Fibre Channel (FC) y Memoria no volátil rápida (NVMe). Además, la tecnología Snapshot es la base para crear decenas de miles de backups en línea y clones de bases de datos completamente operativos. Además del amplio conjunto de funcionalidades de ONTAP, hay una gran variedad de requisitos de usuario, como necesidades de tamaño de la base de datos, requisitos de rendimiento y protección de datos. Obtenga información sobre el rendimiento de las bases de datos sin sistema operativo con los sistemas de almacenamiento de AFF, incluidas la serie A y la serie C, y abarca tanto los máximos como la diferencia práctica entre las dos opciones de AFF.

"TR-4971: Rendimiento virtualizado de bases de datos Oracle en AFF A-Series y C-Series"
ONTAP es una potente plataforma de gestión de datos con funcionalidades nativas que incluyen compresión en línea, actualizaciones de hardware no disruptivas y la capacidad de importar un LUN desde una cabina de almacenamiento externa. Es posible agrupar hasta 24 nodos en clúster y proporcionar datos de forma simultánea a través de los protocolos Sistema de archivos de red (NFS), Bloque de mensajes del servidor (SMB), iSCSI, Fibre Channel (FC) y Memoria no volátil rápida (NVMe). Además, la tecnología Snapshot es la base para crear decenas de miles de backups en línea y clones de bases de datos completamente operativos. Además del amplio conjunto de funcionalidades de ONTAP, hay una gran variedad de requisitos de usuario, como necesidades de tamaño de la base de datos, requisitos de rendimiento y protección de datos. Obtenga información sobre el rendimiento de las bases de datos virtualizadas con los sistemas de almacenamiento AFF, incluidas la serie A y la serie C, y abarca tanto los máximos como la diferencia práctica entre las dos opciones de AFF.

"TR-4695: Organización en niveles de almacenamiento de base de datos con FabricPool"
Obtenga información sobre las ventajas y las opciones de configuración de FabricPool con varias bases de datos, incluido el sistema de gestión de bases de datos relacionales de Oracle (RDBMS).

"TR-4899: Conmutación por error transparente de aplicaciones de base de datos de Oracle con sincronización activa de SnapMirror" La sincronización activa de SnapMirror (anteriormente SM-BC) y Oracle Real Application Cluster (RAC) pueden proporcionar recuperación tras fallos transparente de aplicaciones (TAF) y continuidad en caso de interrupciones del servicio del sitio y desastres reales. Obtenga información sobre las directrices de configuración y las prácticas recomendadas de una cabina de almacenamiento de AFF con SnapMirror Active Sync como componente de almacenamiento de Oracle RAC.

"TR-4876:multitenancy de Oracle con la solución de ONTAP y prácticas recomendadas de puesta en marcha" Obtenga más información sobre las prácticas recomendadas por la solución sobre cómo aprovisionar, gestionar y proteger bases de datos multitenant de Oracle usando el almacenamiento de ONTAP para maximizar los beneficios tanto de las bases de datos multitenant de Oracle como de las funciones del software ONTAP.

PostgreSQL

PostgreSQL viene con variantes que incluyen PostgreSQL, PostgreSQL Plus y EDB Postgres Advanced Server (EPAS). PostgreSQL suele ponerse en marcha como base de datos de back-end para aplicaciones de varios niveles. NetApp ONTAP es una opción excelente para ejecutar bases de datos PostgreSQL en cuanto a su fiabilidad, alto rendimiento y eficacia.

"Base de datos PostgreSQL en mejores prácticas de ONTAP" PostgreSQL viene con variantes que incluyen PostgreSQL, PostgreSQL Plus y EDB Postgres Advanced Server (EPAS). PostgreSQL suele ponerse en marcha como base de datos de back-end para aplicaciones de varios niveles. Es compatible con paquetes de middleware comunes (como PHP, Java, Python, Tcl/Tk, ODBC, etc.). JDBC) y, desde siempre, ha sido una opción popular para los sistemas de gestión de bases de datos de código abierto. Conozca los requisitos de configuración y las instrucciones sobre el ajuste y la configuración del almacenamiento para implementar PostgreSQL en ONTAP.

Esta documentación sustituye al informe técnico publicado previamente *TR-4770: Base de datos PostgreSQL sobre mejores prácticas de ONTAP*.

SAP HANA

"Soluciones de bases de datos SAP HANA en ONTAP" Las mejores prácticas para configurar, gestionar y automatizar soluciones SAP se pueden encontrar en la página de soluciones SAP de NetApp.

Épica

"Epic en las mejores prácticas de ONTAP" Una guía para comprender las prácticas recomendadas para la puesta en marcha de Epic en las instalaciones y en el cloud, además de cumplir los estándares de configuración para una puesta en marcha adecuada en ONTAP.

Esta documentación sustituye al informe técnico publicado previamente *TR-3923: Mejores prácticas de NetApp para Epic*.

Informes técnicos sobre continuidad empresarial

NetApp ofrece una amplia gama de soluciones que racionalizan dónde residen los datos y las aplicaciones para mejorar el rendimiento de forma rentable. Protección de datos, replicación y disponibilidad continua: La gestión de datos de ONTAP puede simplificar la protección de datos con una gestión de políticas que solo necesita configurar y olvidarse, a la vez que permite la continuidad del negocio con MetroCluster y SnapMirror Active Sync.

Estos informes técnicos se amplían en "Sincronización activa de SnapMirror de ONTAP" la documentación de y "ONTAP MetroCluster" del producto.

Sincronización activa de SnapMirror (anteriormente SM-BC)

"TR-4878: Sincronización activa con SnapMirror" SnapMirror Active Sync es una solución de almacenamiento de disponibilidad continua con granularidad a nivel de aplicación, disponible para ONTAP que se ejecute en sistemas de almacenamiento AFF o All SAN Array (ASA), para satisfacer las necesidades de objetivo de punto de recuperación 0 y objetivo de tiempo de recuperación 0 para las aplicaciones empresariales más cruciales.

MetroCluster

"TR-4705: Arquitectura y diseño de la solución NetApp MetroCluster"
Este documento describe los conceptos de diseño y arquitectura de alto nivel para las funciones de MetroCluster en ONTAP.

IP de MetroCluster

"TR-4689: Dirección IP de NetApp MetroCluster" MetroCluster es una solución de almacenamiento de disponibilidad continua para ONTAP que se ejecuta en sistemas FAS y AFF. MetroCluster IP es un producto de última generación que utiliza un entramado de almacenamiento back-end basado en Ethernet. MetroCluster IP proporciona una configuración altamente redundante para satisfacer las necesidades de las aplicaciones empresariales más importantes. MetroCluster IP se incluye en ONTAP y proporciona conectividad NAS y SAN a los clientes y servidores que utilizan almacenamiento de ONTAP.

FC de MetroCluster

"TR-4375: FC de NetApp MetroCluster" MetroCluster proporciona una disponibilidad de datos continua en centros de datos separados geográficamente para aplicaciones críticas para la empresa. Obtenga más información sobre las prácticas recomendadas, las decisiones de diseño y las configuraciones compatibles con MetroCluster FC.

Informes técnicos de protección de datos y recuperación ante desastres de ONTAP

SnapMirror es una solución de replicación unificada rentable y fácil de usar en todo el Data Fabric. Replica datos a altas velocidades mediante LAN o WAN. Proporciona alta disponibilidad de datos y replicación de datos rápida para las aplicaciones vitales para el negocio, como Microsoft Exchange, Microsoft SQL Server y Oracle, tanto en entornos virtuales como tradicionales. Al replicar datos en uno o varios sistemas de almacenamiento de ONTAP y actualizar continuamente los datos secundarios, estos están siempre al día y disponibles cuando los necesite. No se requieren servidores de replicación externos.

Estos informes técnicos se amplían en "Protección de datos y recuperación ante desastres de ONTAP"la documentación del producto.

SnapMirror

Asíncrono SnapMirror

"TR-4015: Prácticas recomendadas y configuración asíncrona de SnapMirror" Conozca las prácticas recomendadas para configurar la replicación asíncrona de SnapMirror (SM-A) de volúmenes, grupos de consistencia y máquinas virtuales de almacenamiento (recuperación de desastres de SVM).

"TR-4678: Protección de datos y backup de volúmenes ONTAP FlexGroup"
Conozca las recomendaciones para la protección de datos y el backup para FlexGroup Volumes. Los temas incluyen copias Snapshot, SnapMirror y otras soluciones de protección de datos y backup.

SnapMirror síncrono

"TR-4733: Prácticas recomendadas y configuración síncrona de SnapMirror" Obtenga información sobre las prácticas recomendadas para configurar la replicación síncrona de SnapMirror (SM-S).

Recuperación ante desastres en tres centros de datos de SnapMirror

"TR-4832: Recuperación ante desastres de tres centros de datos mediante SnapMirror de NetApp para ONTAP 9,7" Obtenga información sobre una configuración de recuperación ante desastres de tres centros de datos con la tecnología ONTAP SnapMirror para la replicación.

Aplicaciones e infraestructura con SnapMirror

"TR-4900: VMware Site Recovery Manager con ONTAP" ONTAP ha sido una solución de almacenamiento líder para entornos VMware vSphere desde su introducción en el centro de datos moderno en 2002, y continúa añadiendo funcionalidades innovadoras para simplificar la gestión y reducir los costes. Obtenga información sobre la solución ONTAP recomendada para VMware Site Recovery Manager (SRM), el software de recuperación ante desastres (DR) líder del sector de VMware, que incluye la información de producto más reciente y las prácticas recomendadas para simplificar la puesta en marcha, reducir el riesgo y simplificar la gestión continua.

Ciberalmacén de ONTAP

"Ciberalmacén de ONTAP" El ciberalmacén basado en ONTAP de NetApp ofrece a las organizaciones una solución completa y flexible para proteger sus activos de datos más importantes. Gracias a la separación lógica con metodologías de refuerzo sólidas, ONTAP permite crear entornos de almacenamiento aislados y seguros que son resilientes frente a ciberamenazas en constante evolución. Con ONTAP, puede garantizar la confidencialidad, la integridad y la disponibilidad de sus datos y mantener la agilidad y la eficiencia de su infraestructura de almacenamiento.

Informes técnicos sobre volúmenes de ONTAP FlexCache y FlexGroup

Las soluciones de almacenamiento conectado a la red (NAS) de NetApp simplifican la gestión de datos y ayudan a seguir el ritmo de crecimiento a la vez que se optimizan los costes. Las soluciones NAS de ONTAP proporcionan operaciones no disruptivas, una eficiencia contrastada y una escalabilidad fluida dentro de una arquitectura unificada. Con la tecnología de ONTAP, NAS de escalado horizontal aprovecha el ecosistema masivo de ONTAP, con una visión y un liderazgo de innovación significativos para una innovación futura agresiva.

Estos informes técnicos se amplían en "Volumen de ONTAP FlexCache" la documentación de y "Volumen de ONTAP FlexGroup" del producto.

FlexCache

"TR-4743: FlexCache en ONTAP"
FlexCache es una tecnología de almacenamiento en caché que crea réplicas dispersas y editables de volúmenes en los mismos clústeres ONTAP o en diferentes. Puede acercar los datos y los archivos al usuario para obtener un rendimiento más rápido y menos espacio físico. Descubra cómo se puede usar FlexCache y las prácticas recomendadas, los límites y las consideraciones para el diseño y la implementación.

Reescritura de FlexCache

"Reescritura de FlexCache" La anotación-back de FlexCache, que se presenta en ONTAP 9.15.1, es un modo alternativo de operación para la escritura en una caché. La anotación permite que la escritura se confirme en un almacenamiento estable en la caché y se reconozca en el cliente sin esperar a que los datos lleguen al origen. Los datos se vuelven a vaciar de forma asíncrona en el origen. El resultado es un sistema de archivos distribuido globalmente que permite operaciones de escritura a velocidades casi locales para cargas de trabajo y entornos específicos, lo que ofrece importantes ventajas en cuanto a rendimiento.

Volúmenes de FlexGroup

"TR-4571: Prácticas recomendadas y guía de implementación de NetApp ONTAP FlexGroup Volumes"
Obtén más información sobre FlexGroup Volumes, prácticas recomendadas y consejos de implementación. Los volúmenes FlexGroup son una evolución de contenedores NAS de escalado horizontal de ONTAP que combinan una capacidad casi infinita con un rendimiento predecible y de baja latencia en cargas de trabajo con un uso intensivo de metadatos.

"TR-4678: Protección de datos y backup de volúmenes FlexGroup"
Descubra la protección de datos y el backup para volúmenes de FlexGroup, incluidas copias Snapshot, SnapMirror y otras soluciones de backup y protección de datos.

Informes técnicos de NAS de ONTAP

Las soluciones de almacenamiento conectado a la red (NAS) de NetApp simplifican la gestión de datos y ayudan a seguir el ritmo de crecimiento a la vez que se optimizan los costes. Las soluciones NAS de ONTAP proporcionan operaciones no disruptivas, eficiencia y escalabilidad perfecta dentro de una arquitectura unificada. Con la tecnología de NetApp ONTAP, NAS de escalado horizontal aprovecha el ecosistema masivo de ONTAP, con una visión y un liderazgo de innovación significativos para una innovación futura agresiva.

Estos informes técnicos se amplían en "Gestión del almacenamiento NAS de ONTAP" la documentación de y "Administración del almacenamiento de ONTAP S3" del producto.

NFS

"TR-4067: Prácticas recomendadas y guía de implementación de NFS en ONTAP"
Descubra conceptos básicos, información de soporte, consejos de configuración y prácticas recomendadas para NFS en ONTAP.

"TR-4962: NFSv4,2 atributos extendidos"
Obtenga información sobre cómo habilitar y usar los atributos extendidos de NFSv4,2 en ONTAP 9.12.1 y versiones posteriores.

SMB

"TR-4740: Multicanal de SMB 3,0"
Microsoft introdujo Multichannel en el protocolo SMB 3,0 con el objetivo de mejorar el protocolo SMB3 abordando las limitaciones de rendimiento y fiabilidad de SMB1 y SMB2. Obtenga información sobre la función multicanal de ONTAP, incluidas sus capacidades, prácticas recomendadas y resultados de pruebas de rendimiento.

Multiprotocolo

"TR-4887: Información general y prácticas recomendadas de NAS multiprotocolo en ONTAP"
Descubra cómo funciona el acceso NAS multiprotocolo en ONTAP y las prácticas recomendadas para entornos multiprotocolo.

ONTAP S3

"TR-4814: S3 en mejores prácticas de ONTAP" Obtén información sobre las prácticas recomendadas para usar el servicio Simple Storage Service (S3) de Amazon con el software ONTAP, así como las funcionalidades y configuraciones para usar ONTAP como almacén de objetos con aplicaciones S3 nativas o como destino de organización en niveles de FabricPool.

Servicios de nombres

"TR-4523: Balanceo de carga de DNS en ONTAP"
Aprenda a configurar ONTAP para su uso con metodologías de equilibrio de carga de DNS, incluido DNS en

ONTAP, varios métodos de configuración y prácticas recomendadas.

"TR-4668: Guía de prácticas recomendadas de servicios de nombres"
Conozca las prácticas recomendadas, los límites y las consideraciones que se deben tener en cuenta en la implementación de soluciones de almacenamiento conectado a la red (NAS), como CIFS/SMB y NFS en ONTAP.

"TR-4835: Cómo configurar LDAP en la gestión de identidades NAS multiprotocolo de ONTAP"
Aprenda a configurar la gestión de identidades del protocolo ligero de acceso a directorios (LDAP) en ONTAP para NAS multiprotocolo.

Seguridad NAS

"TR-4616: Kerberos de NFS en ONTAP"
Obtenga más información sobre Kerberos de NFS en ONTAP, incluidos los pasos de configuración con los clientes de Active Directory y Red Hat Enterprise Linux (RHEL).

Informes técnicos de red de ONTAP

ONTAP proporciona una variedad de diferentes capacidades y configuraciones de red para satisfacer las aplicaciones más exigentes de escalabilidad horizontal. Gracias a las funciones y capacidades de red, las empresas pueden crear un acceso fiable y seguro a sus datos.

Estos informes técnicos se amplían en "Gestión de red de ONTAP"la documentación del producto.

"Informe técnico TR-4949: BGP/VIP con ONTAP en el centro de datos"
Aprenda a implementar rápidamente una configuración BGP básica en ONTAP.

Informes técnicos de SAN de ONTAP

El almacenamiento SAN de ONTAP ofrece una experiencia SAN simplificada que proporciona alta disponibilidad para las bases de datos críticas para la misión de su organización y otras cargas de trabajo SAN. Gracias a la mejor integración de servicios de datos con bases de datos de Oracle, SAP y Microsoft SQL Server, además de VMware y otros hipervisores líderes, la solución SAN de ONTAP ofrece una rentabilidad de la inversión acelerada para las aplicaciones de bases de datos empresariales.

Estos informes técnicos se amplían en "Gestión de almacenamiento SAN de ONTAP"la documentación del producto.

"TR-4080: Prácticas recomendadas para SAN modernas en ONTAP"
Obtenga información sobre los protocolos de bloque en ONTAP y las prácticas de recomendaciones.

"TR-4684: Implementación y configuración de SAN modernas con NVMe sobre entramados (NVMe-oF)"
Descubra cómo implementar y configurar los transportes NVMe over Fabrics (NVMe over Fibre Channel y NVMe over TCP). Los temas incluyen el diseño, la implementación, la configuración, directrices de gestión y prácticas recomendadas para crear soluciones SAN modernas de alto rendimiento y altamente disponibles que utilicen protocolos y transportes NVMe.

"TR-4968: Integridad y disponibilidad de datos de cabinas All-SAN de NetApp"
Descubra cómo funcionan las distintas funciones de protección e integridad de datos de un sistema de cabina All SAN para conseguir el máximo tiempo de actividad de las aplicaciones, además de las prácticas recomendadas para diseñar, implementar y gestionar una red SAN.

"Solución flash SAN moderna conectada al cloud"
Esta arquitectura verificada de NetApp ha sido diseñada y verificada conjuntamente por NetApp, VMware yBroadcom. Utiliza las últimas soluciones de tecnología Brocade, Emulex y VMware vSphere junto con el almacenamiento all-flash de NetApp, que establece un nuevo estándar en el almacenamiento SAN empresarial y la protección de datos que ofrecerá un valor empresarial superior.

Seguridad

Informes técnicos de seguridad de ONTAP

ONTAP continúa evolucionando, con la seguridad como parte integral de la solución. Los últimos lanzamientos de ONTAP incluyen numerosas funciones de seguridad que son de gran valor para que tu organización proteja sus datos en el cloud híbrido, evite ataques de ransomware y cumpla las prácticas recomendadas del sector. Estas nuevas funciones también favorecen el avance de su organización hacia un modelo de Confianza Cero.

Estos informes técnicos se amplían en "Seguridad y cifrado de datos ONTAP"la documentación del producto.

Ciberalmacén de ONTAP

"Ciberalmacén de ONTAP" El ciberalmacén basado en ONTAP de NetApp ofrece a las organizaciones una solución completa y flexible para proteger sus activos de datos más importantes. Gracias a la separación lógica con metodologías de refuerzo sólidas, ONTAP permite crear entornos de almacenamiento aislados y seguros que son resilientes frente a ciberamenazas en constante evolución. Con ONTAP, puede garantizar la confidencialidad, la integridad y la disponibilidad de sus datos y mantener la agilidad y la eficiencia de su infraestructura de almacenamiento.

Ransomware

"TR-4572: La solución de NetApp para ransomware" Descubre cómo ha evolucionado el ransomware y cómo identificar ataques, evitar la propagación y recuperarte lo más rápido posible con la solución de NetApp para el ransomware. Las directrices y las soluciones proporcionadas en este documento están diseñadas para ayudar a las organizaciones a ofrecer soluciones ciberresilientes y cumplir, al mismo tiempo, los objetivos de seguridad prescritos para la confidencialidad, integridad y disponibilidad de los sistemas de información.

"TR-4526: ALMACENAMIENTO WORM conforme a la normativa con NetApp SnapLock"
Muchas empresas confían en el uso de un almacenamiento de datos WORM para satisfacer los requisitos de cumplimiento de normativas o simplemente añadir otra capa a su estrategia de protección de datos. Descubra cómo integrar SnapLock, la solución WORM en ONTAP, en entornos que requieran el almacenamiento de datos WORM.

Confianza cero

"NetApp y Zero Trust" Zero Trust tradicionalmente ha sido un enfoque centrado en la red del diseño del micronúcleo y el perímetro (MCAP) para proteger los datos, los servicios, las aplicaciones o los activos con controles conocidos como puerta de enlace de segmentación. ONTAP adopta un enfoque centrado en los datos de Zero Trust en el que el sistema de administración del almacenamiento se convierte en la puerta de enlace de segmentación para proteger y supervisar el acceso a los datos de nuestros clientes. En concreto, el motor de confianza cero de FPolicy y el ecosistema de partners de FPolicy se convierten en un centro de control que permite comprender en detalle los patrones de acceso a los datos normales y aberrantes e identificar las amenazas internas.

Autenticación multifactor

"TR-4647: Autenticación multifactor en prácticas recomendadas de ONTAP y guía de implementación"

Conozca la funcionalidad de autenticación multifactor de ONTAP para el acceso administrativo mediante la autenticación de CLI de System Manager, Active IQ Unified Manager y ONTAP Secure Shell (SSH).

"TR-4717: Autenticación SSH de ONTAP con una tarjeta de acceso común"
Aprenda a configurar y probar clientes SSH de terceros, junto con el software ActivClient, para autenticar a un administrador de almacenamiento ONTAP a través de la clave pública almacenada en una tarjeta de acceso común (CAC) cuando se configura en ONTAP.

Multi-tenancy

"TR-4160: Multi-tenancy seguro en ONTAP"
Descubra cómo implementar una multitenencia segura mediante máquinas virtuales de almacenamiento en ONTAP, incluidas las consideraciones de diseño y las prácticas recomendadas.

Estándares

"TR-4401: PCI-DSS 4,0 y ONTAP"
Aprenda cómo validar un sistema con el estándar PCI DSS 4,0 y cumplir con los requisitos de los controles que aplica a un sistema NetApp ONTAP.

Control de acceso basado en atributos

"Control de acceso basado en atributos con ONTAP" Aprenda a configurar las etiquetas de seguridad NFSv4,2 y los atributos extendidos (xattrs) para admitir el control de acceso basado en roles (RBAC) y el control de acceso basado en atributos (ABAC), una estrategia de autorización que define los permisos basados en los atributos del usuario, los recursos y el entorno.

Solución de NetApp para ransomware

La cartera de protección de NetApp y ransomware

El ransomware sigue siendo una de las amenazas más importantes que causan interrupciones en el negocio en 2024. Según los "Estado Sophos del ransomware 2024"datos, los ataques de ransomware afectaron al 72 % de su público encuestado. Los ataques de ransomware han evolucionado hasta ser más sofisticados y dirigidos, donde los actores encargados de amenazas emplean técnicas avanzadas como la inteligencia artificial para maximizar su impacto y sus beneficios.

Las organizaciones deben mirar por toda su postura de seguridad, desde el perímetro, la red, la identidad y la aplicación, y donde los datos se encuentran en el nivel de almacenamiento, para asegurar esas capas. Adoptar un enfoque de ciberprotección en la capa de almacenamiento centrado en los datos es crucial en el panorama actual de amenazas. Aunque ninguna solución individual puede frustrar todos los ataques, utilizar una cartera de soluciones que incluya colaboraciones y terceros ofrece una defensa en capas.

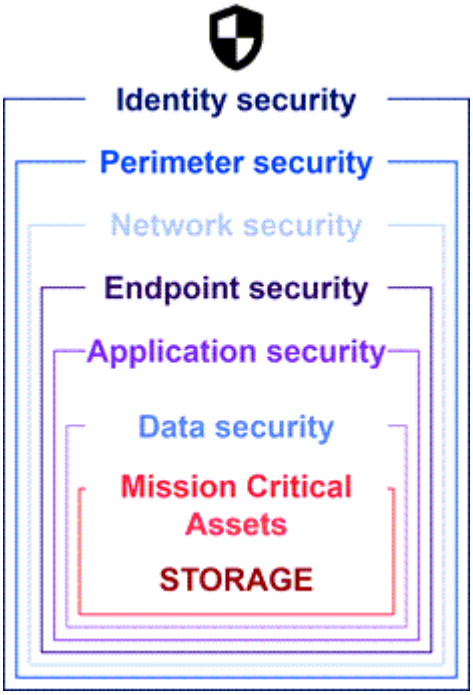
El Gama de productos de NetApp ofrece varias herramientas eficaces para la visibilidad, detección y corrección que ayudan a detectar el ransomware de manera temprana, prevenir la propagación y recuperarse rápidamente, si es necesario, para evitar costosos tiempos de inactividad. Las soluciones tradicionales de defensa en capas siguen siendo comunes, como las que utilizan las soluciones de terceros y de socios para la visibilidad y la detección. La corrección efectiva sigue siendo una parte crucial de la respuesta a cualquier amenaza. El enfoque único del sector que aprovecha la tecnología Snapshot de NetApp inmutable y la solución de aislamiento lógico de SnapLock son factores diferenciadores en el sector y una práctica

recomendada en el ámbito de las capacidades de remediación del ransomware.

A partir de julio de 2024, el contenido del informe técnico *TR-4572: NetApp Ransomware Protection*, que se publicó anteriormente como PDF, está disponible en docs.netapp.com.

Los datos son el destino principal

Los ciberdelincuentes atacan cada vez más los datos directamente, reconociendo su valor. Si bien la seguridad del perímetro, la red y las aplicaciones son importantes, se pueden omitir. Centrarse en la protección de los datos en su origen, la capa de almacenamiento, proporciona una última línea crucial de defensa. Obtener acceso a los datos de producción, cifrarlos o hacerlos inaccesibles es el objetivo de los ataques de ransomware. Para lograrlo, los atacantes deben haber traspasado ya las defensas existentes implementadas por las organizaciones en la actualidad, desde el perímetro hasta la seguridad de las aplicaciones.



Desafortunadamente, muchas organizaciones no aprovechan las funcionalidades de seguridad en la capa de datos. Aquí es donde entra en juego la cartera de productos de protección contra ransomware de NetApp, que te protege en la última línea de defensa.

El coste real del ransomware

El pago del rescate en sí no es el mayor efecto económico en una empresa. Aunque el pago no es insignificante, palidece en comparación con el coste de tiempo de inactividad de sufrir un incidente de ransomware.

Los pagos de rescates son solo un elemento de los costes de recuperación cuando se trata de eventos de ransomware. Salvo los rescates pagados, en 2024 organizaciones indicaron un coste medio de recuperación tras un ataque de ransomware de 2,73M 000 dólares, un aumento de casi 1M 000 dólares desde los 1,82M 000 millones registrados en 2023, según el "2024 Sophos State of Ransomware (Estado del ransomware de Sophos)" informe. Para las organizaciones que dependen en gran medida de la disponibilidad de TECNOLOGÍA, como el comercio electrónico, el comercio de acciones y el cuidado sanitario, los costes pueden aumentar hasta 10 veces o más.

Los costos de los seguros cibernéticos también continúan aumentando dada la probabilidad muy real de un ataque de ransomware en las compañías aseguradas.

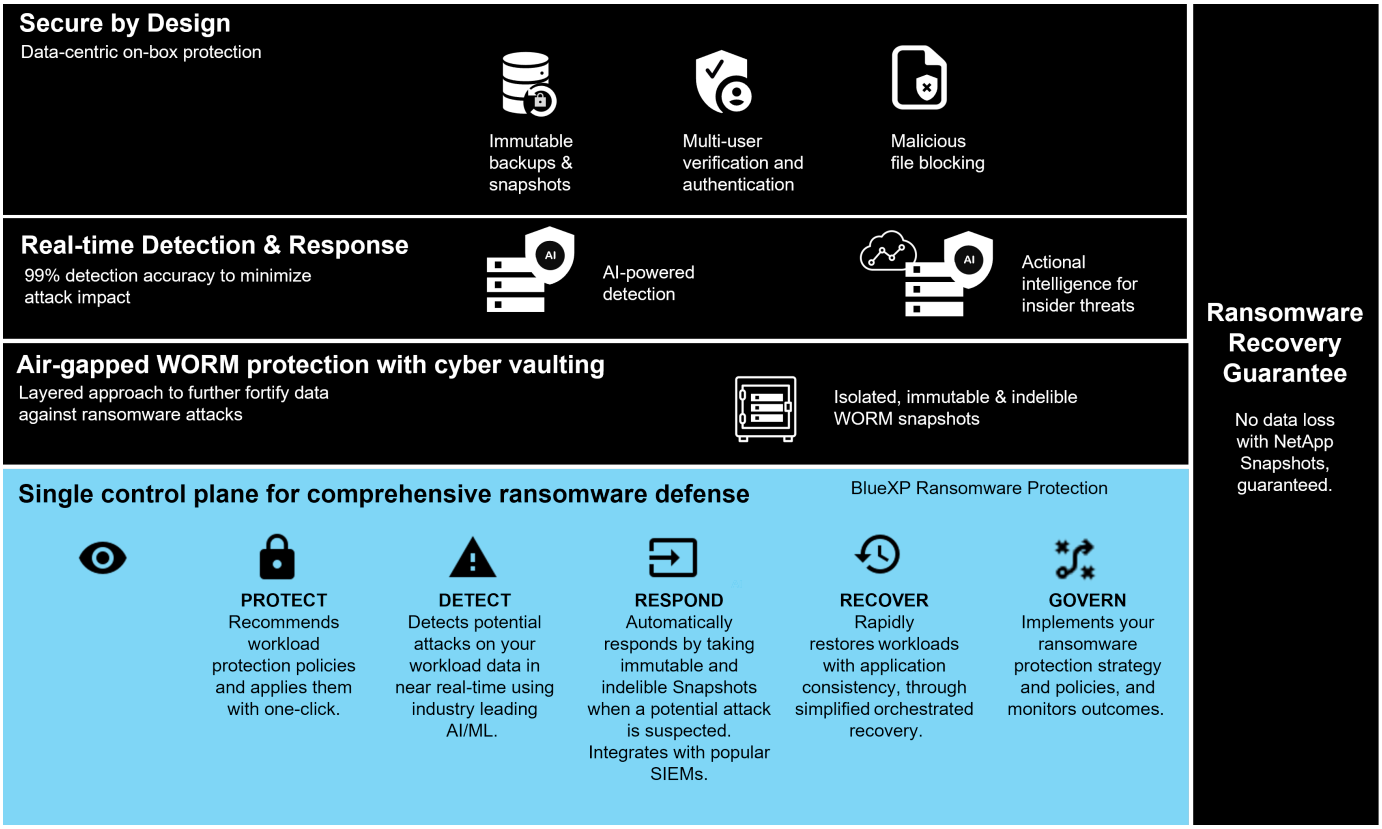
Protección frente a ransomware en la capa de datos

NetApp entiende que su política de seguridad es amplia y profunda en toda su organización, desde el perímetro hasta el lugar donde residen los datos en la capa de almacenamiento. Su pila de seguridad es compleja y debe proporcionar seguridad en todos los niveles de su pila tecnológica.

La protección en tiempo real en la capa de datos es incluso más importante y tiene requisitos exclusivos. Para ser eficaces, las soluciones en esta capa deben ofrecer estos atributos críticos:

- **Seguridad por diseño** para minimizar la posibilidad de un ataque exitoso
- **Detección y respuesta en tiempo real** para minimizar el impacto de un ataque exitoso
- **Protección WORM con aire ACONDICIONADO** para aislar copias de seguridad de datos críticos
- **Un solo plano de control** para una defensa integral contra ransomware

NetApp puede proporcionar todo esto y mucho más.



La cartera de productos de protección frente a ransomware de NetApp

NetApp "protección contra ransomware incorporada"ofrece una defensa en tiempo real, sólida y con múltiples facetas para tus datos cruciales. Los algoritmos avanzados de detección impulsados por IA supervisan continuamente los patrones de datos, identificando rápidamente posibles amenazas de ransomware con una precisión del 99 %. Al reaccionar rápidamente a los ataques, nuestro almacenamiento puede realizar instantáneas rápidamente de los datos y proteger las copias, lo que garantiza una rápida recuperación.

Para reforzar aún más los datos, "copias cibernéticas"la funcionalidad de NetApp aísla los datos con una

brecha lógica. Al proteger los datos cruciales, garantizamos una continuidad de negocio rápida.

NetApp"Protección contra ransomware de NetApp" reduce las cargas operativas con un único plano de control para coordinar y ejecutar de forma inteligente una defensa contra ransomware centrada en la carga de trabajo de extremo a extremo, de modo que pueda identificar y proteger datos críticos de la carga de trabajo en riesgo con un solo clic, detectar y responder de forma precisa y automática para limitar el impacto de un posible ataque y recuperar cargas de trabajo en minutos, no en días, salvaguardando sus valiosos datos de carga de trabajo y minimizando las interrupciones costosas.

Como solución de ONTAP nativa e integrada que protege el acceso no autorizado a los datos, "Verificación multi-admin (MAV)" cuenta con un sólido conjunto de funciones que garantizan que operaciones como la eliminación de volúmenes, la creación de usuarios administrativos adicionales o la eliminación de copias Snapshot solo se puedan ejecutar después de las aprobaciones de, al menos, un segundo administrador designado. De este modo, se evita que administradores comprometidos, malintencionados o inexpertos realicen cambios no deseados o eliminen datos. Puede configurar tantos aprobadores de administrador designados como desee antes de eliminar una instantánea.

NetApp ONTAP aborda el requisito de "Autenticación multifactor (MFA)" la autenticación basada en web en System Manager y de la interfaz de línea de comandos de SSH.

La protección frente al ransomware de NetApp ofrece tranquilidad en un panorama de amenazas en constante evolución. Su enfoque integral no solo defiende las variantes actuales de ransomware, sino que también se adapta a las amenazas emergentes, proporcionando seguridad a largo plazo para su infraestructura de datos.

Obtenga información sobre otras opciones de protección

- "Protección frente al ransomware del asesor digital"
- "Data Infrastructure Insights Almacenamiento Carga de trabajo Seguridad"
- "FPolicy"
- "SnapLock y copias Snapshot a prueba de manipulaciones"

Garantía de recuperación frente a ransomware

NetApp ofrece una garantía para restaurar los datos de las instantáneas en caso de que se produzca un ataque de ransomware. Nuestra garantía: Si no podemos ayudarle a restaurar los datos de la snapshot, corregiremos. La garantía está disponible en las nuevas adquisiciones de sistemas AFF A-Series, AFF C-Series, ASA y FAS.

Leer más

- "Descripción del servicio de garantía de recuperación"
- "Blog de garantía de recuperación frente al ransomware".

Información relacionada

- "Página de recursos del sitio de soporte de NetApp"
- "Seguridad de los productos de NetApp"

SnapLock y snapshots a prueba de manipulaciones para la protección contra el ransomware

Un arma vital en el arsenal de NetApp es SnapLock, que ha demostrado ser altamente eficaz para proteger contra las amenazas de ransomware. Al evitar la eliminación de

datos no autorizados, SnapLock proporciona una capa adicional de seguridad, garantizando que los datos cruciales permanecen intactos y accesibles incluso en caso de ataques malintencionados.

Cumplimiento de normativas SnapLock

SnapLock Compliance (SLC) proporciona una protección indeleble para los datos. SLC prohíbe la eliminación de datos incluso cuando un administrador intenta reinicializar la cabina. A diferencia de otros productos de la competencia, SnapLock Compliance no es vulnerable a los hacks de ingeniería social a través de los equipos de soporte de esos productos. Los datos protegidos por volúmenes de SnapLock Compliance se pueden recuperar hasta que los datos hayan alcanzado su fecha de vencimiento.

Para habilitar SnapLock, "ONTAP One"se necesita una licencia.

Leer más

- "Documentación de SnapLock"

Snapshots a prueba de manipulación

Las copias Snapshot a prueba de manipulaciones (TPS) proporcionan un método rápido y cómodo de proteger los datos de actos malintencionados. A diferencia de SnapLock Compliance, TPS se utiliza normalmente en sistemas primarios en los que el usuario puede proteger los datos durante un tiempo determinado y dejarlos localmente para recuperaciones rápidas o donde no es necesario replicar datos fuera del sistema primario. TPS utiliza las tecnologías SnapLock para evitar que la instantánea principal sea eliminada incluso por un administrador de ONTAP que esté utilizando el mismo período de retención de SnapLock. La eliminación de snapshots se evita aunque el volumen no tenga la función SnapLock habilitada, aunque las snapshots no tengan la misma naturaleza indeleble de los volúmenes de SnapLock Compliance.

Para hacer instantáneas a prueba de manipulaciones, se requiere una "ONTAP One" licencia.

Leer más

- "Bloquea una snapshot para protegerte frente a ataques de ransomware".

Bloqueo de archivos FPolicy

FPolicy bloquea los archivos no deseados para que no se almacenen en su dispositivo de almacenamiento de clase empresarial. FPolicy también le ofrece una forma de bloquear las extensiones de archivos de ransomware conocidas. Un usuario sigue teniendo permisos de acceso completo a la carpeta principal, pero FPolicy no permite que un usuario almacene los archivos que marca su administrador como bloqueados. No importa si esos archivos son archivos MP3 o extensiones de archivos ransomware conocidos.

Bloquea archivos maliciosos con el modo nativo de FPolicy

El modo nativo de FPolicy de NetApp (una evolución del nombre, Política de archivos) es un marco de bloqueo de extensiones de archivos que le permite bloquear las extensiones de archivos no deseadas para que entren en su entorno. Ha formado parte de ONTAP durante más de una década y es increíblemente útil para ayudarte a protegerte contra el ransomware. Este motor de confianza cero es valioso porque obtienes medidas de seguridad adicionales más allá de los permisos de la lista de control de acceso (ACL).

En ONTAP System Manager y en la NetApp Console, hay disponible una lista de más de 3000 extensiones de

archivos como referencia.

> Algunas extensiones pueden ser legítimas en su entorno y bloquearlas puede dar lugar a problemas inesperados. Cree su propia lista que sea adecuada para su entorno antes de configurar las FPolicy nativas.

El modo nativo de FPolicy se incluye en todas las licencias de ONTAP.

Leer más

- "Blog: Lucha contra el ransomware: Tercera parte: FPolicy de ONTAP, otra potente herramienta nativa (también gratuita)"

Habilite el análisis de comportamiento de usuarios y entidades (UEBA) con el modo externo de FPolicy

El modo externo de FPolicy es un marco de notificación y control de actividad de archivos que proporciona visibilidad de la actividad de archivos y usuarios. Una solución externa puede utilizar estas notificaciones para realizar análisis basados en IA con el fin de detectar comportamientos maliciosos.

El modo externo de FPolicy también se puede configurar para que espere a la aprobación del servidor FPolicy antes de permitir que pasen determinadas actividades. Se pueden configurar múltiples normativas de este tipo en un clúster, lo que le proporciona una gran flexibilidad.

> Los servidores FPolicy deben responder a las solicitudes de FPolicy si se configuran para proporcionar la aprobación; de lo contrario, el rendimiento del sistema de almacenamiento puede verse afectado de forma negativa.

El modo externo FPolicy se incluye en "Todas las licencias de ONTAP".

Leer más

- "Blog: Lucha contra el ransomware: Cuarta parte: UBA y ONTAP con el modo externo FPolicy."

Data Infrastructure Insights Almacenamiento Carga de trabajo Seguridad

Storage Workload Security (SWS) es una característica de NetApp Data Infrastructure Insights que mejora enormemente la postura de seguridad, la capacidad de recuperación y la responsabilidad de un entorno ONTAP . SWS adopta un enfoque centrado en el usuario y rastrea toda la actividad de archivos de cada usuario autenticado en el entorno. Utiliza análisis avanzados para establecer patrones de acceso normales y estacionales para cada usuario. Estos patrones se utilizan para identificar rápidamente comportamientos sospechosos sin necesidad de firmas de ransomware.

Cuando SWS detecta un posible ransomware o la eliminación de datos, puede tomar acciones automáticas como:

- Tome una copia Snapshot del volumen afectado.
- Bloquee la cuenta de usuario y la dirección IP sospechosa de actividad maliciosa.
- Enviar una alerta a los administradores.

Debido a que puede tomar acciones automatizadas para detener rápidamente una amenaza interna, así como rastrear cada actividad de archivos, SWS hace que la recuperación de un evento de ransomware sea mucho más simple y rápida. Con las herramientas avanzadas de auditoría y análisis forense integradas, los usuarios

pueden ver inmediatamente qué volúmenes y archivos se vieron afectados por un ataque, de qué cuenta de usuario procede el ataque y qué acción maliciosa se realizó. Las snapshots automáticas mitigan los daños y aceleran la restauración de archivos.

Las alertas de la protección autónoma contra ransomware (ARP) de ONTAP también se pueden ver en SWS, lo que proporciona una única interfaz para los clientes que usan ARP y SWS para protegerse de ataques de ransomware.

Leer más

- "Data Infrastructure Insights de NetApp"

Detección y respuesta integradas de NetApp ONTAP basadas en IA

A medida que las amenazas de ransomware se vuelven más y más sofisticadas, también lo deberían hacer tus mecanismos de defensa. La protección autónoma contra ransomware (ARP) de NetApp cuenta con la tecnología de la IA con la detección inteligente de anomalías integrada en ONTAP. Activa la acción para añadir otra capa de defensa a tu resiliencia cibernética.

ARP y ARP/AI se pueden configurar a través de la interfaz de gestión integrada de ONTAP, System Manager y se habilitan por volumen.

Protección de ransomware autónoma (ARP)

La protección autónoma contra ransomware (ARP), otra solución nativa integrada de ONTAP desde 9.10.1, analiza la actividad de archivos de cargas de trabajo de volúmenes de almacenamiento en NAS y la entropía de datos para detectar automáticamente potencial ransomware. ARP ofrece a los administradores detección en tiempo real, conocimientos y un punto de recuperación de datos para una detección potencial de ransomware sin precedentes on-box.

En el caso de ONTAP 9.15,1 y versiones anteriores que admiten ARP, ARP comienza en el modo de aprendizaje para aprender la actividad de datos de cargas de trabajo típicas. Esto puede tardar siete días en la mayoría de los entornos. Una vez completado el modo de aprendizaje, ARP cambiará automáticamente al modo activo y comenzará a buscar actividad de carga de trabajo anormal que podría ser ransomware.

Si se detecta actividad anormal, se realiza inmediatamente una instantánea automática que proporciona un punto de restauración lo más cercano posible al momento del ataque con un mínimo de datos infectados. Simultáneamente, se genera una alerta automática (configurable) que permite a los administradores ver la actividad anormal del archivo para que puedan determinar si la actividad es realmente maliciosa y tomar las medidas adecuadas.

Si la actividad es una carga de trabajo esperada, los administradores pueden marcarla fácilmente como un falso positivo. ARP aprende este cambio como actividad normal de la carga de trabajo y ya no lo marca como un ataque potencial en el futuro.

Para habilitar ARP, "ONTAP One"se requiere una licencia.

Leer más

- "Protección autónoma de ransomware"

Protección autónoma contra ransomware/IA (ARP/AI)

Con la introducción como versión preliminar tecnológica en ONTAP 9.15,1, ARP/AI lleva los sistemas de almacenamiento NAS a la detección en tiempo real integrada al siguiente nivel. La nueva tecnología de detección impulsada por la IA está entrenada en más de un millón de archivos y varios ataques de ransomware conocidos. Además de las señales utilizadas en ARP, ARP/AI también detecta el cifrado de encabezados. La potencia de la IA y las señales adicionales permiten que ARP/AI ofrezca una precisión de detección superior al 99%. Esto ha sido validado por SE Labs, un laboratorio de pruebas independiente que le dio a ARP/AI su calificación AAA más alta.

Dado que la formación de los modelos ocurre de forma continua en la nube, ARP/AI no requiere un modo de aprendizaje. Está activo en el momento en que se enciende. El entrenamiento continuo también implica que ARP/IA siempre se valida frente a nuevos tipos de ataques de ransomware a medida que se producen. ARP/AI también incluye funcionalidades de actualización automática que ofrecen nuevos parámetros a todos los clientes para mantener actualizada la detección de ransomware. Todas las demás funcionalidades de detección, información y punto de recuperación de datos de ARP se mantienen para ARP/AI.

Para habilitar ARP/AI, "ONTAP One"se requiere una licencia.

Leer más

- "Blog: La solución de detección de ransomware en tiempo real basada en IA de NetApp logra la calificación AAA"

Protección WORM aislada con copia digital en ONTAP

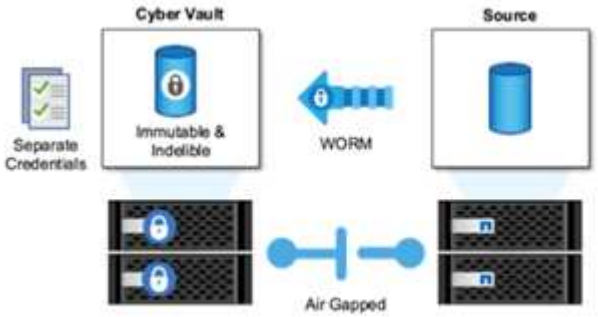
El enfoque de NetApp de un ciberalmacén es una arquitectura de referencia creada específicamente para un ciberalmacén con brecha lógica. Este enfoque aprovecha las tecnologías de refuerzo de la seguridad y cumplimiento de normativas, como SnapLock, para permitir copias Snapshot inalterables e indelebles.

Cyber vaulting con SnapLock Compliance y una red desconectada lógica

Una tendencia creciente es que los atacantes destruyan las copias de seguridad y, en algunos casos, incluso las cifren. Es por ello que muchos en el sector de la ciberseguridad recomiendan usar copias de seguridad aisladas como parte de una estrategia general de resiliencia cibernética.

El problema es que las brechas de aire tradicionales (cintas y soportes fuera de línea) pueden aumentar significativamente el tiempo de restauración, lo que aumenta el tiempo de inactividad y los costos generales asociados. Incluso un enfoque más moderno de una solución de brecha de aire puede resultar problemático. Por ejemplo, si el almacén de copia de seguridad se abre temporalmente para recibir nuevas copias de seguridad y, a continuación, desconecta y cierra su conexión de red a los datos primarios para que vuelvan a estar «fuera de juego», un atacante podría aprovechar la apertura temporal. Durante el tiempo en que la conexión está en línea, un atacante podría atacar para comprometer o destruir los datos. Este tipo de configuración también suele añadir complejidad no deseada. Un espacio de aire lógico es un excelente

sustituto de un espacio de aire tradicional o moderno, ya que tiene los mismos principios de protección de la seguridad mientras se mantiene el backup online. Con NetApp, puede solucionar la complejidad del intercambio de aire en cinta o disco mediante el intercambio de aire lógico, lo que se puede lograr con copias Snapshot y NetApp SnapLock Compliance inmutables.



NetApp lanzó la función SnapLock hace más de 10 años para abordar los requisitos de cumplimiento de normativas relacionados con los datos, como la ley de portabilidad y responsabilidad del seguro médico (HIPAA), Sarbanes-Oxley, y otras normas relativas a los datos normativos. También puede almacenar snapshots primarias en volúmenes de SnapLock para que las copias se puedan comprometer A WORM, lo que evita su eliminación. Hay dos versiones de licencia de SnapLock: SnapLock Compliance y SnapLock Enterprise. En cuanto a la protección frente a ransomware, NetApp recomienda SnapLock Compliance porque puede establecer un período de retención específico durante el cual las snapshots se bloquean y no se pueden eliminar, incluso para los administradores de ONTAP o el soporte de NetApp.

Leer más

- "Blog: Descripción general de ciberalmacén de ONTAP"

Snapshots a prueba de manipulación

Aunque aprovechar SnapLock Compliance como una barrera aérea lógica proporciona la máxima protección a la hora de evitar que los atacantes eliminen sus copias de backup, sí requiere que mueva las copias Snapshot con SnapVault a un volumen secundario habilitado para SnapLock. Por ello, muchos clientes ponen en marcha esta configuración en el almacenamiento secundario en la red. Esto puede prolongar los tiempos de restauración en comparación con la restauración de copias Snapshot de volúmenes primarios en el almacenamiento primario.

A partir de ONTAP 9.12.1, las copias Snapshot a prueba de manipulaciones proporcionan una protección prácticamente de nivel SnapLock Compliance para las copias Snapshot en el almacenamiento primario y en volúmenes primarios. No es necesario almacenar la instantánea mediante SnapVault en un volumen de SnapManager secundario. Las copias Snapshot a prueba de manipulaciones usan la tecnología SnapLock para evitar que se elimine la copia Snapshot primaria, incluso por un administrador completo de ONTAP con el mismo período de retención de SnapLock. De este modo, se pueden acelerar los tiempos de restauración y se puede hacer backup de un volumen FlexClone mediante una copia Snapshot protegida a prueba de manipulaciones, algo que no se puede hacer con una copia Snapshot tradicional de SnapLock Compliance en bóveda.

La principal diferencia entre copias Snapshot de SnapLock Compliance y a prueba de manipulaciones es que SnapLock Compliance no permite que la cabina ONTAP se inicialice y se borre si existen volúmenes SnapLock Compliance con copias Snapshot en bóveda que todavía no han alcanzado su fecha de vencimiento. Para hacer snapshots a prueba de manipulaciones, se necesita una licencia de SnapLock Compliance.

Leer más

- "Bloquea una snapshot para protegerte frente a ataques de ransomware"

Protección frente al ransomware del asesor digital

Digital Advisor powered by Active IQ simplifica el cuidado proactivo y la optimización del almacenamiento NetApp con inteligencia procesable para una gestión óptima de datos. Impulsado por datos de telemetría de nuestra base instalada altamente diversa, utiliza técnicas avanzadas de IA y ML para descubrir oportunidades para reducir el riesgo y mejorar el rendimiento y la eficiencia de tu entorno de almacenamiento.

No solo puede "Asesor digital de NetApp" ayudar "eliminar las vulnerabilidades de seguridad", sino que también proporciona información y orientación específicas para la protección contra el ransomware. Una tarjeta de bienestar dedicada muestra las acciones necesarias y los riesgos abordados, por lo que puede estar seguro de que sus sistemas cumplen con las recomendaciones de mejores prácticas.

Los riesgos y las acciones rastreadas en la página de bienestar de la defensa contra ransomware incluyen los siguientes (y muchos más):

- El recuento de volúmenes de snapshots es bajo, lo que reduce la protección contra potenciales ataques de ransomware.
- FPolicy no está habilitado para todas las máquinas virtuales de almacenamiento (SVM) configuradas para protocolos NAS.

Para ver cómo la protección frente al ransomware está en acción, consulte "Asesor digital".

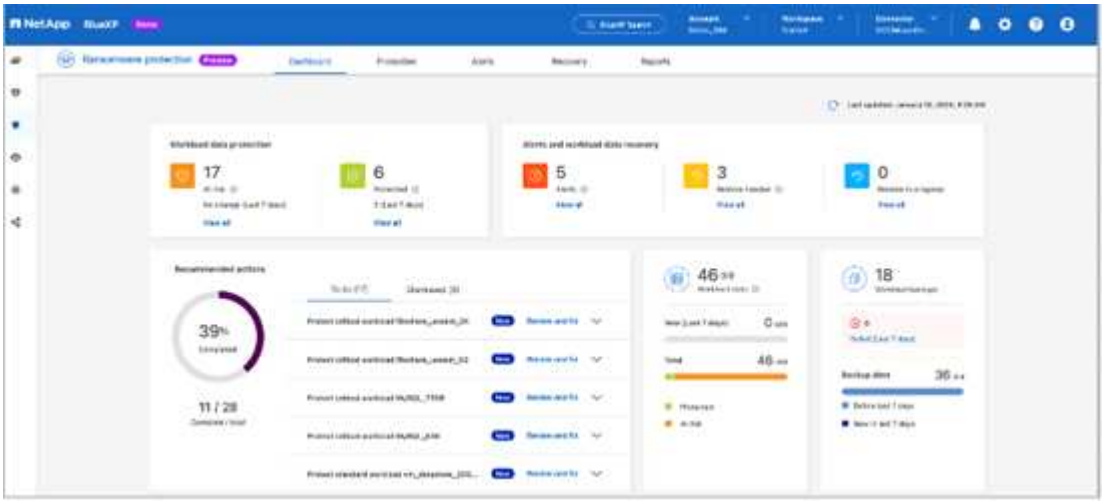
Resiliencia integral con protección contra ransomware de NetApp

Es importante que la detección de ransomware se produzca lo antes posible para poder prevenir su propagación y evitar tiempos de inactividad costosos. Sin embargo, una estrategia eficaz de detección de ransomware debe incluir más de una sola capa de protección. La protección contra ransomware de NetApp adopta un enfoque integral que incluye capacidades en tiempo real en el dispositivo que se extienden a los servicios de datos mediante la NetApp Console y una solución aislada y en capas para el almacenamiento cibernético.

Protección contra ransomware de NetApp

La NetApp Console es un único plano de control para orquestar de forma inteligente una defensa integral

contra ransomware centrada en la carga de trabajo. La protección contra ransomware de NetApp reúne las potentes funciones de resiliencia cibernética de ONTAP, como ARP, FPolicy e instantáneas a prueba de manipulaciones, y los servicios de datos de NetApp , como NetApp Backup and Recovery. También agrega recomendaciones y orientación con flujos de trabajo automatizados para brindar una defensa de extremo a extremo a través de una única interfaz de usuario. Opera a nivel de carga de trabajo para garantizar que las aplicaciones que ejecutan su negocio estén protegidas y puedan recuperarse lo más rápido posible en caso de un ataque.



Beneficios para el cliente:

- La preparación asistida contra el ransomware reduce la sobrecarga operativa y mejora la eficacia
- La detección de anomalías impulsada por IA/ML ofrece mayor precisión y una respuesta más rápida para contener el riesgo
- La restauración guiada coherente con las aplicaciones permite recuperar cargas de trabajo de forma más fácil y en unos minutos

"Protección contra ransomware de NetApp"hace que estas funciones del NIST sean más fáciles de lograr:

- Automáticamente **Descubra** y priorice los datos en el almacenamiento de NetApp **con un enfoque en las principales cargas de trabajo basadas en aplicaciones**.
- **Protección con un solo clic** de copia de seguridad de datos de carga de trabajo superior, configuración inmutable, segura, bloqueo de archivos maliciosos y diferentes dominios de seguridad.
- * Detecte con precisión* ransomware de la forma más rápida posible utilizando **detección de anomalías basada en IA de próxima generación.**
- Respuesta automatizada y flujos de trabajo e integración con las principales soluciones **SIEM y XDR.**
- Restaure rápidamente los datos utilizando una **recuperación orquestada** simplificada para acelerar el tiempo de actividad de las aplicaciones.
- Implementa tu **estrategia** y **políticas** de protección contra ransomware, y **monitorea resultados**.

NetApp y Zero Trust

NetApp y Zero Trust

Zero Trust tradicionalmente ha sido un enfoque centrado en la red del diseño del micronúcleo y el perímetro (MCAP) para proteger los datos, los servicios, las

aplicaciones o los activos con controles conocidos como puerta de enlace de segmentación. NetApp ONTAP está adoptando un enfoque centrado en los datos de Zero Trust en el que el sistema de gestión del almacenamiento se convierte en la puerta de enlace de segmentación para proteger y supervisar el acceso a los datos de nuestros clientes. En concreto, el motor de confianza cero de FPolicy y el ecosistema de partners de FPolicy se convierten en un centro de control que permite comprender en detalle los patrones de acceso a los datos normales y aberrantes e identificar las amenazas internas.

A partir de julio de 2024, el contenido del informe técnico *TR-4829: NetApp y confianza cero: Habilitar un modelo de confianza cero* centrado en los datos, que anteriormente se publicó como PDF, está disponible en docs.netapp.com.

Los datos son los activos más importantes con los que cuenta la organización. Las amenazas internas son la causa del 18% de las violaciones de datos, según el 2022 "Informe de investigación de infracciones de datos de Verizon". Las organizaciones pueden aumentar su vigilancia mediante la puesta en marcha de controles de confianza cero (Zero Trust) líderes en el sector en torno a los datos con el software de gestión de datos de NetApp ONTAP.

¿Qué es Zero Trust?

El modelo Zero Trust fue desarrollado por primera vez por John Kindervag en Forrester Research. Prevé la seguridad de la red desde dentro hacia fuera en lugar de desde fuera hacia dentro. El enfoque de confianza cero de dentro hacia fuera identifica el micronúcleo y el perímetro (MCAP). El MCAP es una definición interior de datos, servicios, aplicaciones y activos que debe protegerse mediante un completo conjunto de controles. El concepto de perímetro exterior seguro es obsoleto. Las entidades de confianza que se pueden autenticar correctamente a través del perímetro pueden hacer que la organización sea vulnerable a los ataques. Por definición, las personas con información privilegiada ya se encuentran dentro del perímetro seguro. Los empleados, contratistas y partners son personas con información privilegiada y deben poder operar con los controles adecuados para desempeñar sus funciones dentro de la infraestructura de la organización.

Zero Trust fue mencionado como una tecnología que ofrece promesa al DoD en septiembre de 2019 "FY19-23 DoD Estrategia de Modernización Digital". Define Zero Trust como «Una estrategia de ciberseguridad que incorpora la seguridad en toda la arquitectura con el fin de detener las violaciones de datos. Este modelo de seguridad centrado en datos elimina la idea de redes, dispositivos, personas o procesos de confianza o no confiables y cambia a niveles de confianza basados en múltiples atributos que permiten políticas de autenticación y autorización bajo el concepto de acceso con menos privilegios. Implementar la confianza cero requiere repensar cómo utilizamos la infraestructura existente para implementar la seguridad mediante el diseño de una manera más sencilla y eficiente a la vez que se permiten operaciones sin obstáculos».

En agosto de 2020, el NIST publicó "Special Pub 800-207 Zero Trust Arquitectura" (ZTA). ZTA se centra en proteger los recursos, no los segmentos de la red, porque la ubicación de la red ya no se ve como el componente principal de la postura de seguridad del recurso. Los recursos son datos e informática. Las estrategias ZTA son para arquitectos de redes empresariales. ZTA introduce una nueva terminología de los conceptos originales de Forrester. Los mecanismos de protección denominados punto de decisión de política (PDP) y punto de aplicación de políticas (PEP) son análogos a una puerta de enlace de segmentación de Forrester. ZTA presenta cuatro modelos de implementación:

- Implementación basada en gateway o agente de dispositivo
- Instalación basada en enclave (algo similar al Forrester MCAP)
- Despliegue basado en portal de recursos

- Sandboxing de aplicaciones de dispositivos

Para los fines de esta documentación, utilizamos los conceptos y la terminología de Forrester Research en lugar de la ZTA de NIST.

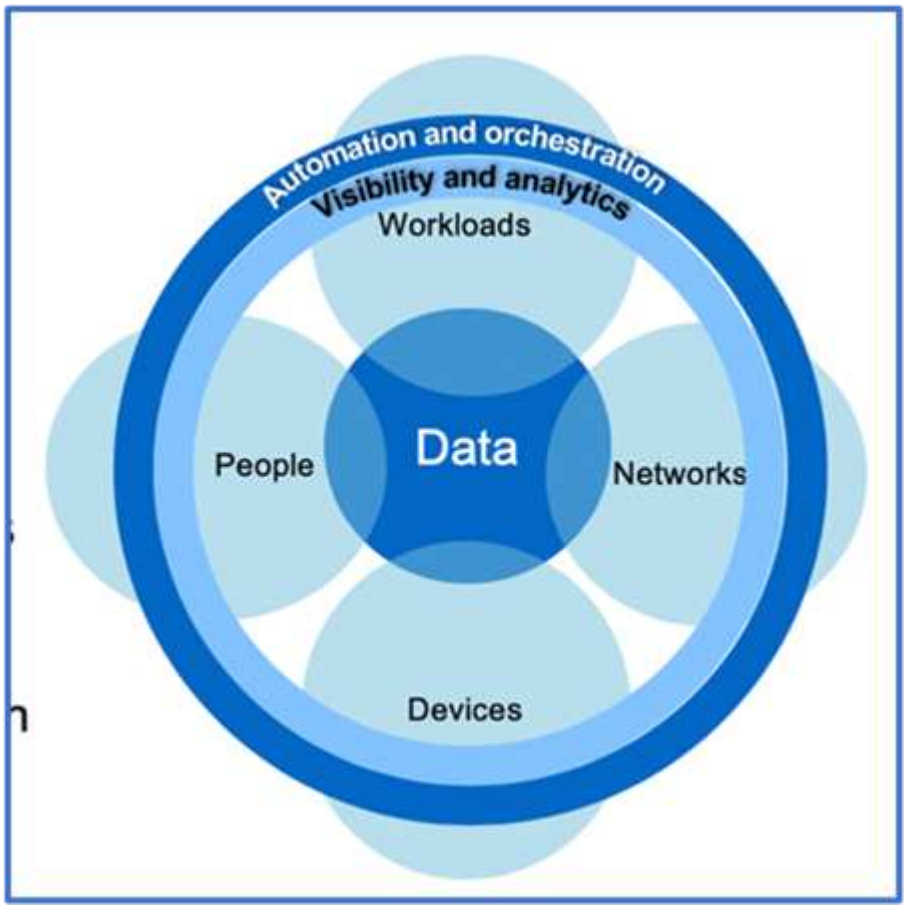
Recursos de seguridad

Para obtener información sobre la creación de informes sobre vulnerabilidades e incidentes, las respuestas de seguridad de NetApp y la confidencialidad del cliente, consulte la "Portal de seguridad de NetApp".

Diseñe un enfoque de Zero Trust centrado en los datos con ONTAP

Una red de confianza cero se define por un enfoque centrado en los datos en el que los controles de seguridad deben estar lo más cerca posible de los datos. Las funcionalidades de ONTAP y el ecosistema de partners de FPolicy de NetApp pueden ofrecer los controles necesarios para el modelo de confianza cero centrado en datos.

ONTAP es un software de gestión de datos de alta seguridad de NetApp, y el motor de confianza cero de FPolicy es una funcionalidad de ONTAP líder del sector que proporciona una interfaz de notificaciones de eventos granular basada en archivos. Los partners de FPolicy de NetApp pueden usar esta interfaz para facilitar el acceso a los datos en ONTAP.



Cree un MCAP centrado en los datos de confianza cero

Para diseñar un MCAP de confianza cero centrado en los datos, siga estos pasos:

1. Identifique la ubicación de todos los datos de la organización.
2. Clasifique los datos.
3. Elimine de forma segura los datos que ya no necesite.
4. Comprender qué roles deben tener acceso a las clasificaciones de datos.
5. Aplique el principio de privilegio mínimo para aplicar los controles de acceso.
6. Use la autenticación multifactor para el acceso administrativo y el acceso a los datos.
7. Utilice el cifrado para los datos en reposo y los datos en tránsito.
8. Supervisar y registrar todo el acceso.
9. Alerte de accesos o comportamientos sospechosos.

Identifique la ubicación de todos los datos de la organización

La funcionalidad FPolicy de ONTAP junto con el ecosistema de partners de alianza de NetApp formado por partners de FPolicy le permite identificar dónde existen los datos de su organización y quién tiene acceso a ellos. Esto se hace con el análisis del comportamiento del usuario, que identifica si los patrones de acceso a los datos son válidos. Más detalles sobre el análisis del comportamiento del usuario se discuten en Supervisar y registrar todo el acceso. Si no entiende dónde están sus datos y quién tiene acceso a ellos, el análisis de comportamiento del usuario puede proporcionar una línea base para construir la clasificación y la política a partir de observaciones empíricas.

Clasifique los datos

En la terminología del modelo Zero Trust, la clasificación de datos implica la identificación de datos tóxicos. Los datos tóxicos son datos confidenciales que no deben exponerse fuera de una organización. La divulgación de datos tóxicos podría violar el cumplimiento normativo y dañar la reputación de una organización. En términos de cumplimiento normativo, los datos tóxicos incluyen datos del titular de la tarjeta para "Estándar de seguridad de datos del sector de tarjetas de pago (PCI-DSS)" , datos personales para la UE "Reglamento general sobre la protección de datos (GDPR)" , o datos de atención sanitaria para el "Ley de Portabilidad y Responsabilidad de Seguros Médicos (HIPAA)" . Puedes utilizar NetApp "NetApp Data Classification" (anteriormente conocido como Cloud Data Sense), un conjunto de herramientas impulsado por IA, para escanear, analizar y categorizar automáticamente sus datos.

Deseche de forma segura los datos que ya no necesite

Después de clasificar los datos de su organización, puede descubrir que algunos de sus datos ya no son necesarios o relevantes para la función de su organización. La retención de datos innecesarios es una responsabilidad, y dichos datos deben ser eliminados. Para ver un mecanismo avanzado para borrar datos de forma criptográfica, consulte la descripción de la purga segura en el cifrado de datos en reposo.

Comprender qué roles deben tener acceso a las clasificaciones de datos y aplicar el principio de privilegio mínimo para aplicar los controles de acceso

La asignación de acceso a datos confidenciales y la aplicación del principio de privilegio mínimo significa dar a las personas de su organización acceso a solo los datos necesarios para realizar sus trabajos. Este proceso implica el control de acceso basado en roles ("RBAC"), que se aplica al acceso a los datos y al acceso administrativo.

Con ONTAP, puede utilizarse una máquina virtual de almacenamiento (SVM) para segmentar el acceso a los datos de la organización por parte de los inquilinos dentro de un clúster de ONTAP. Es posible aplicar el control de acceso basado en roles al acceso a los datos, así como al acceso administrativo a la SVM. RBAC también se puede aplicar en el nivel administrativo del clúster.

Además de RBAC, puede utilizar ONTAP "verificación multiadministrativa" (MAV) para requerir que uno o más administradores aprueben comandos `volume delete` como o `volume snapshot delete`. Una vez que MAV está activado, la modificación o desactivación de MAV requiere la aprobación del administrador de MAV.

Otra forma de proteger las instantáneas es con ONTAP "bloqueo de instantáneas". El bloqueo de snapshots es una función de SnapLock en la que las instantáneas se vuelven indelebles manual o automáticamente con un período de retención en la política de snapshots de volúmenes. El bloqueo de instantáneas también se denomina bloqueo de instantáneas a prueba de manipulaciones. El objetivo del bloqueo de instantáneas es impedir que los administradores malintencionados o que no sean de confianza eliminen snapshots de los sistemas de ONTAP principales y secundarios. Se puede lograr una rápida recuperación de snapshots bloqueadas en sistemas principales para restaurar volúmenes dañados por el ransomware.

Use la autenticación multifactor para el acceso administrativo y el acceso a los datos

Además del control de acceso basado en roles administrativo del clúster, "Autenticación multifactor (MFA)" es posible poner en funcionamiento para el acceso administrativo web de ONTAP y para el acceso por línea de comandos de Secure Shell (SSH). La MFA para el acceso administrativo es un requisito para las organizaciones del sector público de EE. UU. O las que deben seguir la PCI-DSS. MFA hace que sea imposible para un atacante comprometer una cuenta usando solo un nombre de usuario y contraseña. La MFA requiere dos o más factores independientes para autenticarse. Un ejemplo de autenticación de dos factores es algo que posee un usuario, como una clave privada, y algo que un usuario conoce, como una contraseña. El acceso web administrativo a ONTAP System Manager o ActiveIQ Unified Manager está habilitado con Security Assertion Markup Language (SAML) 2,0. El acceso a la línea de comandos SSH utiliza autenticación encadenada de dos factores con una clave pública y una contraseña.

Puede controlar el acceso de usuarios y máquinas a través de API con las capacidades de gestión de acceso e identidad en ONTAP:

- Usuario:
  - **Autenticación y autorización.** Mediante las funcionalidades del protocolo NAS para SMB y NFS.
  - **Auditoría.** Syslog de acceso y eventos. Registro de auditorías detallado del protocolo CIFS para probar las políticas de autenticación y autorización. Auditoría granular de FPolicy precisa de acceso NAS detallado a nivel de archivo.
- Dispositivo:
  - **Autenticación.** Autenticación basada en certificados para el acceso a API.
  - **Autorización.** Control de acceso basado en roles (RBAC) predeterminado o personalizado.
  - **Auditoría.** Syslog de todas las acciones realizadas.

Utilice el cifrado para los datos en reposo y los datos en tránsito

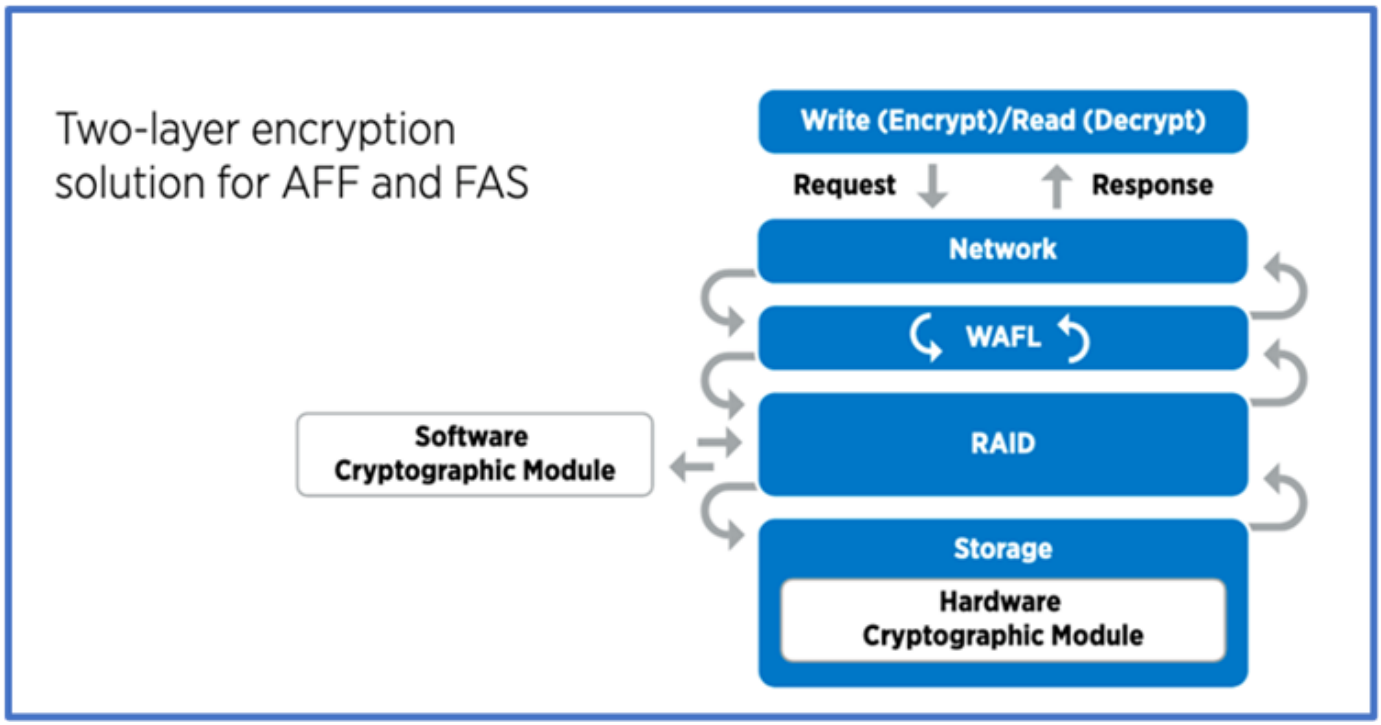
Cifrado de los datos en reposo

Cada día se cumplen nuevos requisitos para mitigar los riesgos del sistema de almacenamiento y las deficiencias en la infraestructura cuando una organización reasigna unidades, devuelve unidades defectuosas o actualiza unidades de mayor tamaño vendiéndolas o canjeándolas. Los ingenieros de almacenamiento, como administradores y operadores de datos, deben gestionar y mantener los datos de forma segura a lo largo de su ciclo de vida. "NetApp Storage Encryption (NSE), NetApp Volume Encryption (NVE), y NetApp Aggregate Encryption" le ayudamos a cifrar todos sus datos en reposo todo el tiempo, sean tóxicos o no, y sin afectar a las operaciones diarias. "NSE" Es una solución de hardware ONTAP "datos en reposo" que utiliza unidades de autocifrado validadas FIPS 140-2 de nivel 2. "NVE y NAE" Son una solución de software de ONTAP "datos en reposo" que hace uso de "Módulo criptográfico NetApp validado FIPS 140-2 nivel 1"la . Con NVE y NAE, pueden utilizarse unidades de disco duro o unidades de estado sólido para el cifrado de datos en

reposo. Además, pueden utilizarse unidades NSE para proporcionar una solución de cifrado nativa por capas que ofrezca redundancia de cifrado y seguridad adicional. Si se rompe una capa, la segunda capa aún protege los datos. Estas funcionalidades hacen que ONTAP esté bien posicionado para "cifrado preparado para quantum".

NVE también proporciona una funcionalidad denominada "limpieza segura" que elimina criptográficamente los datos tóxicos de las fugas de datos cuando los archivos confidenciales se escriben en un volumen no clasificado.

"Gestión de claves incorporada (OKM)"El , que es el gestor de claves integrado en ONTAP, o "aprobada" "gestores de claves externos" puede usarse con NSE y NVE para almacenar material de claves de forma segura.



Como se ve en la figura anterior, se puede combinar el cifrado basado en hardware y software. Esta función permitió "Validación de ONTAP en las soluciones comerciales para el programa clasificado de la NSA" el almacenamiento de datos confidenciales.

Cifrado de datos en tránsito

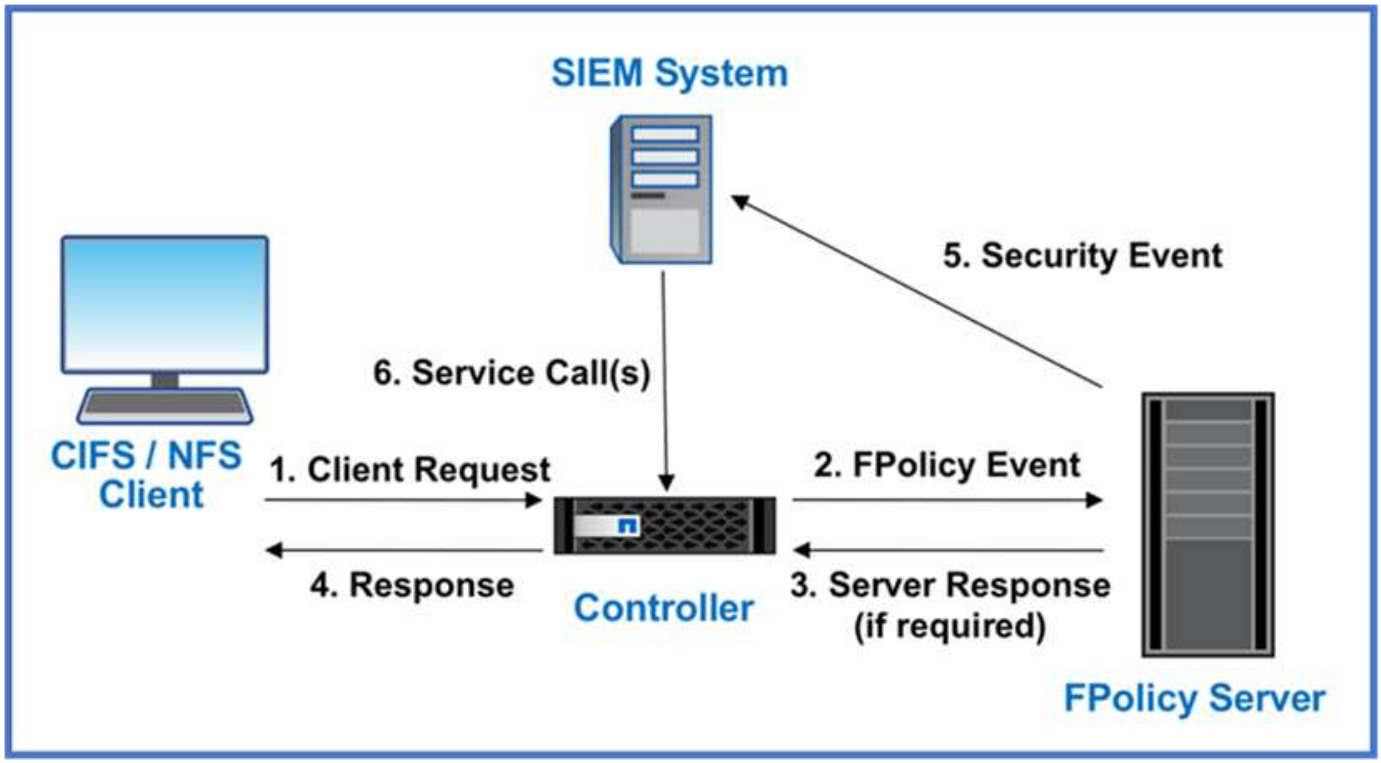
El cifrado de datos en tiempo real de ONTAP protege el acceso a los datos de usuario y el acceso al plano de control. El acceso a los datos del usuario puede cifrarse mediante el cifrado SMB 3,0 para el acceso a recursos compartidos de Microsoft CIFS o por krb5P para Kerberos 5 NFS. El acceso a los datos del usuario también puede cifrarse con "IPSec" para CIFS, NFS e iSCSI. El acceso al plano de control está cifrado con Transport Layer Security (TLS). ONTAP proporciona "FIPS"el modo de cumplimiento para el acceso al plano de control, que habilita algoritmos aprobados por FIPS y deshabilita los algoritmos que no están aprobados por FIPS. La replicación de datos está cifrada con "cifrado de pares de clústeres". Esto proporciona cifrado para las tecnologías ONTAP SnapVault y SnapMirror.

Supervisar y registrar todo el acceso

Una vez implementadas las políticas de RBAC, debe implementar supervisión activa, auditoría y alertas. El motor de confianza cero FPolicy de NetApp ONTAP junto con "Ecosistema de partners FPolicy de NetApp", proporciona los controles necesarios para el modelo de confianza cero centrado en datos. NetApp ONTAP es

un software de gestión de datos de alta seguridad y "FPolicy" una funcionalidad ONTAP líder del sector que proporciona una interfaz granular de notificaciones de eventos basada en archivos. Los partners de FPolicy de NetApp pueden usar esta interfaz para facilitar el acceso a los datos en ONTAP. La funcionalidad FPolicy de ONTAP, junto con el ecosistema de partners de alianza de NetApp formado por partners de FPolicy, le permite identificar dónde existen los datos de su organización y quién tiene acceso a ellos. Esto se hace con el análisis del comportamiento del usuario, que identifica si los patrones de acceso a los datos son válidos. El análisis de comportamiento del usuario se puede utilizar para alertar de acceso a datos sospechosos o aberrantes que estén fuera del patrón normal y, si es necesario, tomar medidas para denegar el acceso.

Los partners de FPolicy van más allá del análisis de comportamiento del usuario hacia el aprendizaje automático (ML) y la inteligencia artificial (IA) para ofrecer una mayor fidelidad a los eventos y menos falsos positivos, si los hay. Todos los eventos deben registrarse en un servidor de syslog o en un sistema de gestión de información y eventos de seguridad (SIEM) que también pueda emplear ML e AI.



De NetApp "Seguridad de la carga de trabajo de almacenamiento DII" utiliza la interfaz FPolicy y el análisis del comportamiento del usuario en sistemas de almacenamiento ONTAP locales y en la nube para brindarle alertas en tiempo real sobre el comportamiento malicioso del usuario. Storage Workload Security protege los datos de la organización contra el uso indebido por parte de usuarios maliciosos o comprometidos a través del aprendizaje automático avanzado y la detección de anomalías. Storage Workload Security puede identificar ataques de ransomware u otros comportamientos maliciosos, invocar instantáneas y poner en cuarentena a usuarios maliciosos. Storage Workload Security también tiene una capacidad forense para ver con gran detalle las actividades de los usuarios y las entidades. La seguridad de la carga de trabajo de almacenamiento es parte de NetApp Data Infrastructure Insights.

Además de la seguridad de las cargas de trabajo de almacenamiento, ONTAP cuenta con una funcionalidad de detección de ransomware incorporada conocida como "Protección autónoma de ransomware" ARP. ARP utiliza el aprendizaje automático para determinar si una actividad anormal de archivos indica que un ataque de ransomware está en curso y llama a una instantánea y alerta a los administradores. Seguridad de carga de trabajo de almacenamiento se integra con ONTAP para recibir eventos ARP y ofrece una capa de análisis adicional y respuestas automáticas.

Obtenga más información sobre los comandos descritos en este procedimiento en el "Referencia de

comandos del ONTAP".

Controles de orquestación y automatización de la seguridad de NetApp externos a ONTAP

La automatización le permite realizar un proceso o procedimiento con una asistencia humana mínima. Gracias a la automatización, las organizaciones pueden escalar sus puestas en marcha de confianza cero más allá de los procedimientos manuales para defenderse frente a actividades engañosas que también están automatizadas.

Ansible es una herramienta de aprovisionamiento de software de código abierto, gestión de configuración y puesta en marcha de aplicaciones. Se ejecuta en muchos sistemas similares a Unix, y puede configurar tanto sistemas similares a Unix como Microsoft Windows. Incluye su propio lenguaje declarativo para describir la configuración del sistema. Ansible fue escrito por Michael DeHaan y adquirido por Red Hat en 2015. Ansible no tiene agentes, se conecta temporalmente de forma remota a través de SSH o Administración remota de Windows (lo que permite la ejecución remota de PowerShell) para realizar tareas. NetApp ha desarrollado más que "150 Módulos Ansible para software ONTAP", lo que permite una mayor integración con el marco de automatización de Ansible. Los módulos de Ansible para NetApp proporcionan un conjunto de instrucciones para definir el estado deseado y transmitirlo al entorno NetApp de destino. Los módulos se incorporarán para dar soporte a tareas como configurar licencias, crear agregados y máquinas virtuales de almacenamiento, crear volúmenes y restaurar instantáneas, entre otras. Una función de Ansible ha sido "Publicado en GitHub" específica de la guía de implementación de funcionalidades unificadas para departamentos de NetApp (UC).

Al utilizar los módulos disponibles de la biblioteca, los usuarios pueden desarrollar fácilmente playbooks de Ansible y personalizarlos para sus propias aplicaciones y necesidades empresariales para automatizar tareas mundanas. Después de escribir un playbook, puede ejecutarlo para ejecutar la tarea especificada, lo que ahorra tiempo y mejora la productividad. NetApp ha creado y compartido playbooks de muestra que puede utilizar directamente o personalizar según sus necesidades.

Data Infrastructure Insights es una herramienta de monitoreo de infraestructura que le brinda visibilidad de su infraestructura completa. Con Data Infrastructure Insights, puede supervisar, solucionar problemas y optimizar todos sus recursos, incluidas sus instancias de nube pública y sus centros de datos privados. Data Infrastructure Insights puede reducir el tiempo medio de resolución en un 90 % y evitar que el 80 % de los problemas de la nube afecten a los usuarios finales. También puede reducir los costos de infraestructura en la nube en un promedio del 33% y reducir su exposición a amenazas internas al proteger sus datos con inteligencia procesable. La capacidad de seguridad de la carga de trabajo de almacenamiento de Data Infrastructure Insights permite el análisis del comportamiento del usuario con IA y ML para alertar cuando se producen comportamientos aberrantes del usuario debido a una amenaza interna. Para ONTAP, Storage Workload Security utiliza el motor Zero Trust FPolicy.

Puesta en marcha de cloud híbrido y confianza cero

NetApp es la autoridad de datos para la nube híbrida. NetApp ofrece una variedad de opciones para ampliar los sistemas de gestión de datos locales a la nube híbrida con Amazon Web Services (AWS), Microsoft Azure, Google Cloud y otros proveedores de nube líderes. Las soluciones de nube híbrida de NetApp admiten los mismos controles de seguridad Zero Trust que están disponibles con los sistemas ONTAP locales y el almacenamiento definido por software ONTAP Select .

Puede ampliar fácilmente la capacidad en nubes públicas sin las restricciones típicas de CAPEX mediante el uso de servicios de archivos nativos de la nube de clase empresarial para AWS (FSxN), Google Cloud (GCNV) y Azure NetApp Files para Microsoft Azure. Ideales para cargas de trabajo intensivas en datos, como

análisis y DevOps, estos servicios de datos en la nube combinan almacenamiento elástico bajo demanda como servicio de NetApp con gestión de datos ONTAP en una oferta completamente administrada.

ONTAP permite el movimiento de datos entre sus sistemas ONTAP locales y el entorno de almacenamiento de AWS, Google Cloud o Azure con el software de replicación de datos SnapMirror de NetApp .

Control de acceso basado en atributos

Control de acceso basado en atributos con ONTAP

A partir de la versión 9.12.1, puede configurar ONTAP con NFSv4,2 etiquetas de seguridad y atributos extendidos (xattrs) para admitir el control de acceso basado en roles (RBAC) con atributos y el control de acceso basado en atributos (ABAC).

ABAC es una estrategia de autorización que define permisos basados en atributos de usuario, atributos de recursos y condiciones ambientales. La integración de ONTAP con etiquetas de seguridad NFS v4,2 y xattrs cumple con los estándares NIST para soluciones ABAC, como se establece en la Publicación Especial 800-162 del NIST.

Puede utilizar etiquetas de seguridad NFS v4,2 y xattrs para asignar archivos atributos y etiquetas definidos por el usuario. ONTAP puede integrarse con el software de gestión de acceso e identidad orientado a ABAC para aplicar políticas de control de acceso granular a archivos y carpetas basadas en estos atributos y etiquetas.

Información relacionada

- "Aproximaciones a ABAC con ONTAP"
- "NFS en NetApp ONTAP: Prácticas recomendadas y guía de implementación"

Enfoques para el control de acceso basado en atributos (ABAC) en ONTAP

ONTAP proporciona varios métodos que puede utilizar para lograr el control de acceso basado en atributos (ABAC) a nivel de archivo, incluidas las etiquetas de seguridad de NFS v4,2 y los atributos extendidos (xattrs) mediante NFS.

Etiquetas de seguridad de NFS v4,2

A partir de ONTAP 9,9.1, se admite la función NFS v4,2 llamada NFS.

Las etiquetas de seguridad NFS v4,2 son una forma de administrar el acceso granular a archivos y carpetas mediante el uso de etiquetas SELinux y el control de acceso obligatorio (MAC). Estas etiquetas MAC se almacenan con archivos y carpetas y funcionan junto con permisos UNIX y ACL de NFS v4.x.

La compatibilidad con las etiquetas de seguridad NFS v4,2 implica que ONTAP ahora reconoce y comprende la configuración de etiqueta SELinux del cliente NFS. Las etiquetas de seguridad de NFS v4,2 se tratan en RFC-7204.

Entre los casos de uso de las etiquetas de seguridad de NFS v4,2 se encuentran los siguientes:

- Etiquetado MAC de imágenes de máquinas virtuales (VM)
- Clasificación de seguridad de datos para el sector público (secreto, alto secreto y otras clasificaciones)
- Cumplimiento de normativas de seguridad

- Linux sin disco

Habilite etiquetas de seguridad de NFS v4.2

Puede habilitar o deshabilitar las etiquetas de seguridad de NFS v4,2 con el siguiente comando (se requiere privilegio avanzado):

```
vserver nfs modify -vserver <svm_name> -v4.2-seclabel <disabled|enabled>
```

Obtenga más información sobre `vserver nfs modify` en el "Referencia de comandos del ONTAP".

Modos de aplicación de etiquetas de seguridad NFS v4,2

A partir de ONTAP 9,9.1, ONTAP admite los siguientes modos de aplicación:

- **Modo de servidor limitado**: ONTAP no puede hacer cumplir las etiquetas, pero puede almacenarlas y transmitirlas.

  La capacidad de cambiar las etiquetas MAC depende del cliente para hacer cumplir.

- **Modo invitado**: Si el cliente no está etiquetado como NFS-Aware (v4,1 o inferior), las etiquetas MAC no se transmiten.

  ONTAP no admite actualmente el modo completo (almacenamiento y aplicación de etiquetas MAC).

Ejemplos de etiquetas de seguridad NFS v4,2

En el siguiente ejemplo de configuración se muestran los conceptos que utilizan Red Hat Enterprise Linux versión 9,3 (Plow).

El usuario `jrsmith`, creado en función de las credenciales de John R. Smith, tiene el siguiente Privileges de cuenta:

- Nombre de usuario = `jrsmith`
- Privileges = `uid=1112(jrsmith) gid=1112(jrsmith) groups=1112(jrsmith) context=user_u:user_r:user_t:s0`

Hay dos roles: La cuenta admin que es un usuario y usuario con privilegios `jrsmith`, como se describe en la siguiente tabla Privileges MLS:

Usuarios	Función	Tipo	Niveles
`admins`	`sysadm_r`	`sysadm_t`	`t:s0`
`jrsmith`	`user_r`	`user_t`	`t:s1 - t:s4`

En este entorno de ejemplo, el usuario `jrsmith` tiene acceso a los archivos en los niveles `s0` a `s3`. Podemos mejorar las clasificaciones de seguridad existentes, como se describe a continuación, para garantizar que los

administradores no tengan acceso a datos específicos del usuario.

- s0 = datos de usuario administrador de privilegios
- s0 = datos no clasificados
- s1 = confidencial
- s2 = datos secretos
- s3 = datos secretos superiores

Ejemplo de etiquetas de seguridad NFS v4,2 con MCS

Además de la Seguridad multinivel (MLS), otra capacidad llamada Seguridad de varias categorías (MCS) le permite definir categorías como proyectos.

Etiqueta de seguridad de NFS	Valor
`entitySecurityMark`	`t:s01 = UNCLASSIFIED`

Atributos extendidos (xattrs)

A partir de ONTAP 9.12.1, ONTAP admite xattrs. Xattrs permite que los metadatos se asocien con archivos y directorios más allá de lo que proporciona el sistema, como las listas de control de acceso (ACL) o los atributos definidos por el usuario.

Para implementar xattrs, puede usar `setfattr` las utilidades de línea de comandos y `getfattr` en Linux. Estas herramientas proporcionan una manera poderosa de administrar metadatos adicionales para archivos y directorios. Se deben usar con cuidado, ya que el uso inadecuado puede conducir a un comportamiento inesperado o problemas de seguridad. Consulte siempre `setfattr` las páginas del manual y `getfattr` u otra documentación fiable para obtener instrucciones de uso detalladas.

Cuando xattrs está habilitado en un sistema de archivos ONTAP, los usuarios pueden configurar, modificar y recuperar atributos arbitrarios en los archivos. Estos atributos se pueden utilizar para almacenar información adicional sobre el archivo que no es capturado por el conjunto estándar de atributos de archivo, como la información de control de acceso.

Hay varios requisitos y límites para el uso de xattrs en ONTAP:

- Red Hat Enterprise Linux 8,4 o posterior
- Ubuntu 22.04 o posterior
- Cada archivo puede tener hasta 128 xattrs
- Las claves xattr están limitadas a 255 bytes
- El tamaño de clave o valor combinado es de 1.729 bytes por xattr
- Los directorios y archivos pueden tener xattrs
- Para establecer y recuperar xattrs, `w` o bits de modo de escritura deben estar activados para el usuario y el grupo

Los Xattrs se utilizan dentro del espacio de nombres del usuario y no tienen ningún significado intrínseco al propio ONTAP. En cambio, sus aplicaciones prácticas son determinadas y gestionadas exclusivamente por la aplicación del lado cliente que interactúa con el sistema de archivos.

Ejemplos de casos de uso de xattr:

- Registro del nombre de la aplicación responsable de la creación de un archivo
- Mantener una referencia al mensaje de correo electrónico del que se obtuvo un archivo
- Establecimiento de un marco de categorización para organizar objetos de archivo
- Etiquetar archivos con la URL de su fuente de descarga original

Comandos para gestionar xattrs

- `setfattr` define un atributo extendido de un archivo o directorio:

  ```
  setfattr -n <attribute_name> -v <attribute_value> <file or directory name>
  ```

  Comando de ejemplo:

  ```
  setfattr -n user.comment -v test example.txt
  ```

- `getfattr` recupera el valor de un atributo extendido específico o muestra todos los atributos extendidos de un archivo o directorio:

  Atributo Específico:
  `getfattr -n <attribute_name> <file or directory name>`

  Todos los atributos:
  `getfattr <file or directory name>`

  Comando de ejemplo:

  ```
  getfattr -n user.comment example.txt
  ```

Ejemplos de pares de valores de clave xattr

En la siguiente tabla se muestran dos ejemplos de pares de valores de clave xattr:

xattr	Valor
`user.digitalIdentifier`	`CN=John Smith jrsmith, OU=Finance, OU=U.S.ACME, O=US, C=US`
`user.countryOfAffiliations`	`USA`

Permisos de usuario con ACE para xattrs

Una entrada de control de acceso (ACE) es un componente dentro de una ACL que define los derechos o permisos de acceso otorgados a un usuario individual o a un grupo de usuarios para un recurso específico, como un archivo o directorio. Cada ACE especifica el tipo de acceso permitido o denegado y está asociado a

un principal de seguridad en particular (identidad de usuario o grupo).

Entrada de control de acceso (ACE) necesaria para xattrs

- Recuperar xattr: Los permisos necesarios para que un usuario lea los atributos extendidos de un archivo o directorio. La “R” significa que el permiso de lectura es necesario.
- Set xattrs: Los permisos necesarios para modificar o definir los atributos extendidos. “A”, “w” y “T” representan diferentes ejemplos de permisos, tales como agregar, escribir y un permiso específico relacionado con xattrs.
- Archivos: Los usuarios necesitan agregar, escribir y potencialmente un permiso especial relacionado con xattrs para establecer atributos extendidos.
- Directorios: Se requiere un permiso específico “T” para establecer atributos extendidos.

Tipo de archivo	Recuperar xattr	Establezca xattrs
Archivo	R	A,w,T
Directorio	R	T

Integración con el software de control de acceso e identidad ABAC

Para aprovechar al máximo las capacidades de ABAC, ONTAP puede integrarse con un software de gestión de acceso e identidad orientado a ABAC.

En un sistema ABAC, el Punto de Aplicación de Políticas (PEP) y el Punto de Decisión de Políticas (PDP) desempeñan un papel crucial. El PEP es responsable de hacer cumplir las políticas de control de acceso, mientras que el PDP toma la decisión de conceder o denegar el acceso basado en las políticas.

En una configuración práctica, una organización utilizaría una combinación de etiquetas de seguridad NFS y xattrs. Estos se utilizan para representar una variedad de metadatos, incluida la clasificación, la seguridad, la aplicación y el contenido, que son fundamentales en la toma de decisiones ABAC.xattrs, por ejemplo, se puede utilizar para almacenar los atributos de recursos que el PDP utiliza para su proceso de toma de decisiones. Se puede definir un atributo para representar el nivel de clasificación de un archivo (por ejemplo, «Sin clasificar», «Confidencial», «Secreto» o «Secreto superior»). A continuación, el PDP podría utilizar este atributo para aplicar una política que restringe el acceso de los usuarios a archivos que tienen un nivel de clasificación igual o inferior a su nivel de autorización.

> Este contenido asume que los servicios de identidad, autenticación y acceso del cliente incluyen como mínimo un PEP y un PDP que actúan como intermediarios para el acceso al sistema de archivos.

Ejemplo de flujo de proceso para ABAC

1. El usuario presenta credenciales (por ejemplo, PKI, OAuth, SAML) para acceder al sistema a PEP y obtiene resultados de PDP.

   La función del PEP es interceptar la solicitud de acceso del usuario y reenviarla al PDP.

2. A continuación, el PDP evalúa esta solicitud con respecto a las políticas establecidas de ABAC.

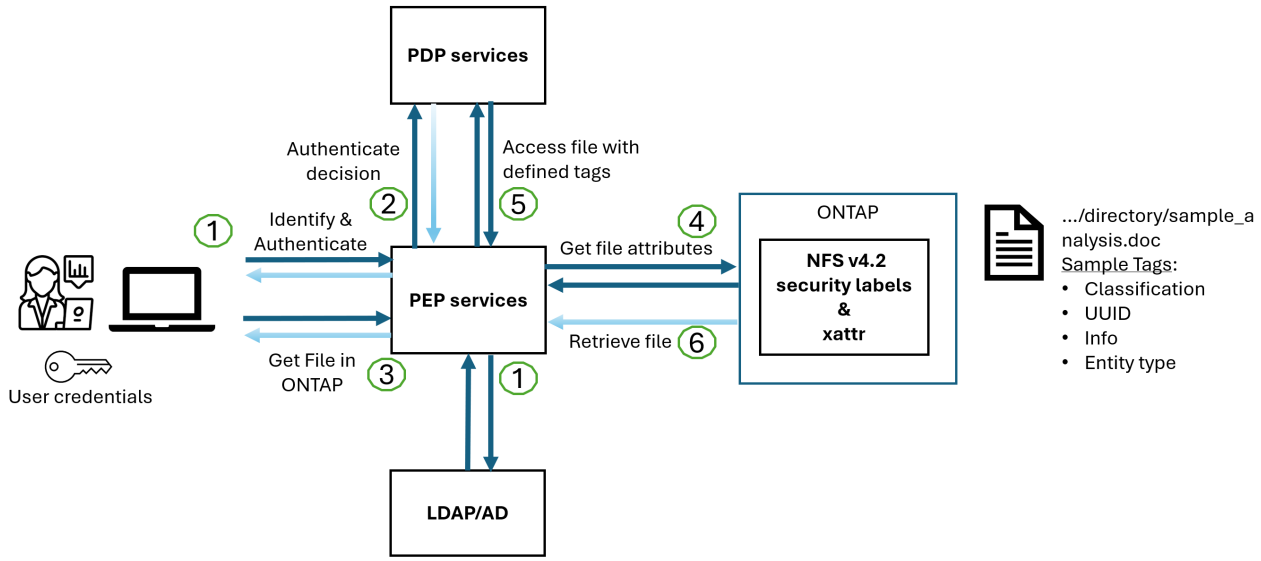
   Estas políticas tienen en cuenta varios atributos relacionados con el usuario, el recurso en cuestión y el entorno circundante. Basándose en estas políticas, el PDP toma una decisión de acceso para permitir o denegar y luego comunica esta decisión al PEP.

   PDP proporciona una política a PEP para hacer cumplir. El PEP entonces aplica esta decisión, ya sea

otorgando o denegando la solicitud de acceso del usuario según la decisión del PDP.

3. Después de una solicitud correcta, el usuario solicita un archivo almacenado en ONTAP (AFF, AFF-C, por ejemplo).
4. Si la solicitud se realiza correctamente, PEP obtiene etiquetas de control de acceso de granularidad fina del documento.
5. PEP solicita una política para el usuario basada en los certificados de ese usuario.
6. PEP toma una decisión basada en la política y las etiquetas si el usuario tiene acceso al archivo y permite al usuario recuperar el archivo.

El acceso real se puede realizar mediante tokens.



Clonado ONTAP y SnapMirror

Las tecnologías de clonado y SnapMirror de ONTAP están diseñadas para proporcionar funciones de replicación y clonado de datos eficientes y fiables, lo que garantiza que todos los aspectos de los datos de archivos, incluidos los xattrs, se preservan y transfieren junto con el fichero. Los xattrs son esenciales al almacenar metadatos adicionales asociados a un archivo, como etiquetas de seguridad, información de control de acceso y datos definidos por el usuario, lo que son esenciales para mantener el contexto y la integridad del archivo.

Cuando se clona un volumen con tecnología FlexClone de ONTAP, se crea una réplica exacta del volumen que puede escribirse. Este proceso de clonación es instantáneo y ocupa poco espacio, e incluye todos los datos y metadatos de ficheros, lo que garantiza que xattrs se repliquen en su totalidad. De igual modo, SnapMirror garantiza que los datos se dupliquen en un sistema secundario con una fidelidad total. Esto incluye xattrs, que son cruciales para las aplicaciones que dependen de estos metadatos para funcionar correctamente.

Al incluir xattrs en operaciones de clonado y de replicación, NetApp ONTAP garantiza que todo el conjunto de datos, con todas sus características, esté disponible y sea consistente en sistemas de almacenamiento primario y secundario. Este enfoque integral de la gestión de datos es vital para las organizaciones que necesitan una protección de datos consistente, una recuperación rápida y el cumplimiento de normativas y estándares normativos. También simplifica la gestión de los datos en diferentes entornos, ya sea local o en el cloud, lo que proporciona a los usuarios la seguridad de que los datos están completos y que no se alteran

durante estos procesos.

Las etiquetas de seguridad NFS v4,2 tienen las advertencias definidas en 2.

Auditoría de cambios en las etiquetas

La auditoría de cambios en xattrs o etiquetas de seguridad NFS es un aspecto crítico de la administración y seguridad del sistema de archivos. Las herramientas de auditoría estándar del sistema de archivos permiten la supervisión y el registro de todos los cambios en un sistema de archivos, incluidas las modificaciones en xattrs y etiquetas de seguridad.

En entornos Linux, el `auditd` daemon se utiliza comúnmente para establecer la auditoría de eventos del sistema de archivos. Permite a los administradores configurar reglas para vigilar las llamadas del sistema específicas relacionadas con los cambios de xattr, `setxattr` como , `lsetxattr` y `fsetxattr` para definir atributos y, `lremovexattr` y `fremovexattr` para `removexattr` eliminar atributos.

FPolicy de ONTAP amplía estas funciones al proporcionar un sólido marco para la supervisión en tiempo real y el control de las operaciones de archivos. FPolicy se puede configurar para admitir diversos eventos xattr, lo que ofrece un control granular de las operaciones de archivos y la capacidad de aplicar directivas de gestión de datos completas.

Para los usuarios que utilizan xattrs, especialmente en entornos NFS v3 y NFS v4, solo se admiten ciertas combinaciones de operaciones de archivos y filtros para la supervisión. A continuación se detalla la lista de combinaciones de filtros y operaciones de archivos admitidas para la supervisión de FPolicy de los eventos de acceso a archivos NFS v3 y NFS v4:

Operaciones de archivos admitidas	Filtros compatibles
`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`

Ejemplo de un fragmento de log auditd para una operación setattr:

```
type=SYSCALL msg=audit(1713451401.168:106964): arch=c000003e syscall=188
success=yes exit=0 a0=7fac252f0590 a1=7fac251d4750 a2=7fac252e50a0 a3=25
items=1 ppid=247417 pid=247563 auid=1112 uid=1112 gid=1112 euid=1112
suid=1112 fsuid=1112 egid=1112 sgid=1112 fsgid=1112 tty=pts0 ses=141
comm="python3" exe="/usr/bin/python3.9"
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
key="*set-xattr*"ARCH=x86_64 SYSCALL=**setxattr** AUID="jrsmith"
UID="jrsmith" GID="jrsmith" EUID="jrsmith" SUID="jrsmith"
FSUID="jrsmith" EGID="jrsmith" SGID="jrsmith" FSGID="jrsmith"
```

Habilitar "FPolicy de ONTAP" para los usuarios que trabajan con xattrs proporciona una capa de visibilidad y control que es esencial para mantener la integridad y la seguridad del sistema de archivos. Al aprovechar las capacidades avanzadas de supervisión de FPolicy, las organizaciones pueden garantizar que se realicen un

seguimiento, se auditen y se alineen con sus estándares de seguridad y cumplimiento. Este enfoque proactivo de la gestión de sistemas de archivos es la razón por la que habilitar FPolicy de ONTAP es una opción muy recomendada para cualquier organización que busque mejorar sus estrategias de protección y gobierno de los datos.

Ejemplos de control del acceso a los datos

La siguiente entrada de ejemplo para los datos almacenados en el certificado PKI de John R. Smith muestra cómo se puede aplicar el enfoque de NetApp a un archivo y proporcionar un control de acceso detallado.

> Estos ejemplos tienen fines ilustrativos y es responsabilidad del cliente determinar los metadatos asociados a las etiquetas de seguridad y xattrs de NFS v4,2. Los detalles sobre la actualización y la retención de etiquetas se omiten para mayor simplicidad.

Ejemplo de valores de certificado PKI

Clave	Valor
Entidad SecurityMark	t:S01 = SIN CLASIFICAR

Información	{
	"commonName": {
	"value": "Smith John R jrsmith"
	},
	"emailAddresses": [
	{
	"value": "jrsmith@dod.mil"
	}
	],
	"employeeId": {
	"value": "00000387835"
	},
	"firstName": {
	"value": "John"
	},
	"lastName": {
	"value": "Smith"
	},
	"telephoneNumber": {
	"value": "938/260-9537"
	},
	"uid": {
	"value": "jrsmith"
	}
	}

Clave	Valor
especificación	DoD
uuid	b4111349-7875-4115-ad30-0928565f2e15

AdminOrganization	{
	"value": "DoD"
	}

reuniones informativas	[
	{
	"value": "ABC1000"
	},
	{
	"value": "DEF1001"
	},
	{
	"value": "EFG2000"
	}
	]

CitizenshipStatus	{
	"value": "US"
	}

Clave	Valor

mínimo	[
	{
	"value": "TS"
	},
	{
	"value": "S"
	},
	{
	"value": "C"
	},
	{
	"value": "U"
	}
	]

PaisOfAfiliaciones	[
	{
	"value": "USA"
	}
	]

Identificador digital	{
	"classification": "UNCLASSIFIED",
	"value": "cn=smith john r jrsmith, ou=dod, o=u.s.
	government, c=us"
	}

DissemTos	{
	"value": "DoD"
	}

DutyOrganization	{
	"value": "DoD"
	}

Clave	Valor

Tipo de entidad	<pre>{
	"value": "GOV"
	}</pre>

FineAccessControls	<pre>[
	{
	"value": "SI"
	},
	{
	"value": "TK"
	},
	{
	"value": "NSYS"
	}
	]</pre>

Estos derechos de PKI muestran los detalles de acceso de John R. Smith, incluido el acceso por tipo de datos y atribución.

En situaciones en las que los metadatos de IC-TDF se almacenan por separado del archivo, NetApp aboga por una capa adicional de control de acceso detallado. Esto implica almacenar la información de control de acceso tanto a nivel de directorio como en asociación con cada archivo. Por ejemplo, considere las siguientes etiquetas vinculadas a un archivo:

- Etiquetas de seguridad de NFS v4,2: Se utilizan para tomar decisiones de seguridad
- Xattrs: Proporcionar información complementaria pertinente al archivo y los requisitos del programa organizativo

Los siguientes pares clave-valor son ejemplos de metadatos que podrían almacenarse como xattrs y ofrecen información detallada sobre el creador del archivo y las clasificaciones de seguridad asociadas. Estos metadatos pueden ser aprovechados por las aplicaciones cliente para tomar decisiones de acceso informadas y para organizar archivos de acuerdo con los estándares y requisitos de la organización.

Ejemplo de pares clave-valor xattr

Clave	Valor
`user.uuid`	`"761d2e3c-e778-4ee4-997b-3bb9a6a1d3fa"`
`user.entitySecurityMark`	`"UNCLASSIFIED"`

Clave	Valor
`user.specification`	`"INFO"`

Clave	Valor

user.Info	{
	"commonName": {
	"value": "Smith John R jrsmith"
	},
	"currentOrganization": {
	"value": "TUV33"
	},
	"displayName": {
	"value": "John Smith"
	},
	"emailAddresses": [
	"jrsmith@example.org"
	],
	"employeeId": {
	"value": "00000405732"
	},
	"firstName": {
	"value": "John"
	},
	"lastName": {
	"value": "Smith"
	},
	"managers": [
	{
	"value": ""
	}
	],
	"organizations": [
	{
	"value": "TUV33"
	},
	{
	"value": "WXY44"
	}
	],
	"personalTitle": {
	"value": ""
	},
	"secureTelephoneNumber": {
	"value": "506-7718"
	},
	"telephoneNumber": {
	"value": "264/160-7187"
	},
	"title": {
	"value": "Software Engineer"
	},

Clave	Valor
`user.geo_point`	`[-78.7941, 35.7956]`

```
    }
}
```

Información relacionada

- "NFS en NetApp ONTAP: Prácticas recomendadas y guía de implementación"
- "Referencia de comandos del ONTAP"
- Solicitud de comentarios (RFC)
  - "RFC 7204: Requisitos para NFS con etiqueta"
  - "RFC 2203: Especificación del protocolo RPCSEC_GSS"
  - "RFC 3530: Protocolo de sistema de archivos de red (NFS) versión 4"

Seguridad reforzada

Guías de refuerzo de seguridad de ONTAP

Estos informes técnicos ofrecen directrices sobre cómo fortalecer NetApp ONTAP y otros productos de NetApp.

Estos informes técnicos se amplían en "Seguridad y cifrado de datos ONTAP"la documentación del producto.

Guías de refuerzo

"TR-4569: Guía de refuerzo de la seguridad para NetApp ONTAP" Aprenda a configurar NetApp ONTAP para ayudar a las organizaciones a cumplir los objetivos de seguridad prescritos para la confidencialidad, la integridad y la disponibilidad de los sistemas de información.

"Guía de seguridad reforzada para herramientas de ONTAP para VMware vSphere" Aprenda a configurar las herramientas de ONTAP para VMware vSphere para ayudar a las empresas a cumplir los objetivos de seguridad prescritos de la confidencialidad, la integridad y la disponibilidad de los sistemas de información.

"TR-4957: Guía de refuerzo de la seguridad para NetApp SnapCenter"
Aprenda a configurar el software NetApp SnapCenter para ayudar a las organizaciones a cumplir los objetivos de seguridad prescritos sobre la confidencialidad, la integridad y la disponibilidad de los sistemas de información.

"TR-4963: Guía de refuerzo de la seguridad: NetApp Backup and Recovery para aplicaciones"Aprenda a configurar NetApp Cloud Backup for Applications para ayudar a las organizaciones a cumplir los objetivos de seguridad prescritos para la confidencialidad, integridad y disponibilidad del sistema de información.

"TR-4943: Guía de refuerzo de la seguridad para NetApp Active IQ Unified Manager"
Aprenda a configurar NetApp Active IQ Unified Manager para ayudar a las organizaciones a cumplir los objetivos de seguridad prescritos para la confidencialidad, la integridad y la disponibilidad de los sistemas de información.

"TR-4945: Guía de refuerzo de la seguridad para SDK de capacidad de gestión de NetApp"
Aprenda a configurar el SDK de capacidad de gestión de NetApp (NMSDK) para ayudar a las organizaciones a cumplir los objetivos de seguridad prescritos para la confidencialidad, la integridad y la disponibilidad de los sistemas de información.

"Guía de refuerzo de seguridad para host y base de datos de MetroCluster tiebreaker" Aprenda a configurar el host y la base de datos de NetApp MetroCluster tiebreaker para ayudar a las organizaciones a cumplir los objetivos de seguridad prescritos para la confidencialidad, la integridad y la disponibilidad de los sistemas de información.

Directrices de refuerzo de seguridad de ONTAP

Información general sobre el refuerzo de la seguridad de ONTAP

ONTAP ofrece un conjunto de controles que permiten fortalecer el sistema operativo de almacenamiento de ONTAP, el software para la gestión de datos líder del sector. Utilice

las directrices y los ajustes de configuración de ONTAP para ayudar a su organización a cumplir los objetivos de seguridad prescritos de confidencialidad, integridad y disponibilidad del sistema de información.

La evolución del panorama actual de amenazas presenta a una organización retos únicos para proteger sus activos más valiosos: Los datos y la información. Las amenazas y vulnerabilidades avanzadas y dinámicas a las que nos enfrentamos son cada vez más sofisticadas. Junto con un aumento en la eficacia de las técnicas de ofuscación y reconocimiento por parte de los posibles intrusos, los administradores de sistemas deben abordar la seguridad de los datos y la información de manera proactiva.

A partir de julio de 2024, el contenido del informe técnico *TR-4569: Guía de refuerzo de la seguridad para ONTAP*, publicado anteriormente como PDF, está disponible en docs.netapp.com.

Validación de imágenes ONTAP

ONTAP proporciona mecanismos para garantizar que la imagen ONTAP sea válida durante la actualización y en el momento del inicio.

Renovación de la validación de imágenes

La firma de código ayuda a verificar que las imágenes ONTAP que se instalan mediante actualizaciones de imágenes no disruptivas o actualizaciones de imágenes, CLI o API de ONTAP automatizadas y no disruptivas se producen de forma auténtica mediante NetApp y no se han alterado. La validación de imágenes de actualización se introdujo en ONTAP 9,3.

Esta función es una mejora de la seguridad sin intervención para la actualización o reversión de ONTAP. No se espera que el usuario haga nada diferente excepto para verificar opcionalmente la firma de nivel superior `image.tgz` .

Validación de imagen en tiempo de arranque

A partir de ONTAP 9,4, el arranque seguro de la interfaz de firmware extensible unificada (UEFI) está habilitado para los sistemas NetApp AFF A800, AFF A220, FAS2750 y FAS2720 y los sistemas de próxima generación subsiguientes que utilizan BIOS UEFI.

Durante el encendido, el cargador de arranque valida la base de datos de la lista blanca de claves de inicio seguro con la firma asociada a cada módulo cargado. Después de validar y cargar cada módulo, el proceso de arranque continúa con la inicialización de ONTAP. Si la validación de firma falla para cualquier módulo, el sistema se reinicia.

Estos elementos se aplican a las imágenes ONTAP y a la plataforma BIOS.

Cuentas de administrador de almacenamiento local

Roles, aplicaciones y autenticación de ONTAP

ONTAP proporciona a la empresa condicionada por la seguridad la capacidad de brindar acceso granular a distintos administradores mediante diferentes métodos y aplicaciones de inicio de sesión. Esto ayuda a los clientes a crear un modelo de confianza cero centrado en los datos.

Estas son las funciones disponibles para los administradores de máquinas virtuales de almacenamiento y administradores. Se especifican los métodos de aplicación de inicio de sesión y los métodos de autenticación de inicio de sesión.

Funciones

Con el control de acceso basado en roles, los usuarios solo tienen acceso a los sistemas y las opciones requeridas para sus roles y funciones de trabajo. La solución RBAC de ONTAP limita el acceso administrativo de los usuarios al nivel permitido por el rol que tengan definido, lo que permite a los administradores gestionar usuarios según el rol asignado. ONTAP ofrece varios roles predefinidos. Los operadores y administradores pueden crear, modificar o suprimir roles de control de acceso personalizados, y pueden especificar restricciones de cuenta para roles específicos.

Roles predefinidos para 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	• Todos los directorios de comandos (`DEFAULT`) • `security login rest-role` • `security login role`

Solo lectura	• `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
• `set` • `system node autosupport`	Ninguno	Todos los demás directorios de comandos (`DEFAULT`)
`backup`	Todo	`vserver services ndmp`
Solo lectura	`volume`	Ninguno
Todos los demás directorios de comandos (`DEFAULT`)	`readonly`	Todo

• `security login password` Sólo para gestionar la contraseña local y la información de claves de la cuenta de usuario propia • `set`	Ninguno	`security`
Solo lectura	Todos los demás directorios de comandos (`DEFAULT`)	`none`

`autosupport`El rol se asigna a la `autosupport` cuenta predefinida, que usa AutoSupport OnDemand. ONTAP le impide modificar o eliminar la `autosupport` cuenta. ONTAP también le impide asignar `autosupport` el rol a otras cuentas de usuario.

Roles predefinidos para administradores de máquinas virtuales de almacenamiento (SVM)

Nombre del rol	Funcionalidades
`vsadmin`	• Administrar la contraseña local y la información de clave de la cuenta de usuario propia • Gestionar volúmenes, excepto movimientos de volúmenes • Gestión de cuotas, qtrees, snapshots y ficheros • Gestionar las LUN • Realice operaciones de SnapLock, excepto la supresión con privilegios • Configurar protocolos: NFS, SMB, iSCSI, FC, FCoE y NVMe/FC y NVMe/TCP • Configurar servicios: DNS, LDAP y NIS • Supervisar trabajos • Supervise las conexiones de red y la interfaz de red • Supervise el estado de la SVM

`vsadmin-volume`	• Administrar la contraseña local y la información de clave de la cuenta de usuario propia • Gestionar volúmenes, excepto movimientos de volúmenes • Gestión de cuotas, qtrees, snapshots y ficheros • Gestionar las LUN • Configurar protocolos: NFS, SMB, iSCSI, FC, FCoE y NVMe/FC y NVMe/TCP • Configurar servicios: DNS, LDAP y NIS • Supervise la interfaz de red • Supervise el estado de la SVM
`vsadmin-protocol`	• Administrar la contraseña local y la información de clave de la cuenta de usuario propia • Configurar protocolos: NFS, SMB, iSCSI, FC, FCoE y NVMe/FC y NVMe/TCP • Configurar servicios: DNS, LDAP y NIS • Gestionar las LUN • Supervise la interfaz de red • Supervise el estado de la SVM
`vsadmin-backup`	• Administrar la contraseña local y la información de clave de la cuenta de usuario propia • Gestione las operaciones de NDMP • Haga que un volumen restaurado sea de lectura/escritura • Permite gestionar relaciones de SnapMirror y snapshots • Ver información de volúmenes y redes

`vsadmin-snaplock`	• Administrar la contraseña local y la información de clave de la cuenta de usuario propia • Gestionar volúmenes, excepto movimientos de volúmenes • Gestión de cuotas, qtrees, snapshots y ficheros • Realizar operaciones de SnapLock, incluida la supresión con privilegios • Configurar protocolos: NFS y SMB • Configurar servicios: DNS, LDAP y NIS • Supervisar trabajos • Supervise las conexiones de red y la interfaz de red
`vsadmin-readonly`	• Administrar la contraseña local y la información de clave de la cuenta de usuario propia • Supervise el estado de la SVM • Supervise la interfaz de red • Ver volúmenes y LUN • Ver servicios y protocolos

Métodos de aplicación

El método de aplicación especifica el tipo de acceso del método de inicio de sesión. Los valores posibles incluyen `console`, `http`, `ontapi`, `rsh`, `snmp`, `service-processor`, `ssh`, y `telnet`.

Configurar este parámetro `service-processor` para otorgar al usuario acceso a Service Processor. Cuando este parámetro se define en `service-processor`, el `-authentication-method` parámetro se debe definir en `password` porque el procesador de servicios sólo admite `password` la autenticación. Las cuentas de usuario de SVM no pueden acceder a Service Processor. Por lo tanto, los operadores y administradores no pueden utilizar el `-vserver` parámetro cuando este parámetro se define en `service-processor`.

Para restringir aún más el acceso al `service-processor` comando, utilice el comando `system service-processor ssh add-allowed-addresses`. El comando `system service-processor api-service` se puede utilizar para actualizar las configuraciones y los certificados.

Por motivos de seguridad, Telnet y el Shell remoto (RSH) están deshabilitados de forma predeterminada porque NetApp recomienda el shell seguro (SSH) para el acceso remoto seguro. Si hay un requisito o una necesidad única de Telnet o RSH, deben estar activados.

El `security protocol modify` comando modifica la configuración existente en todo el cluster de RSH y Telnet. Active RSH y Telnet en el cluster definiendo el campo Activado en `true`.

Métodos de autenticación

El parámetro del método de autenticación especifica el método de autenticación utilizado para inicios de sesión.

Método de autenticación	Descripción
`cert`	Autenticación de certificado SSL
`community`	Cadenas de comunidad SNMP
`domain`	Autenticación de Active Directory
`nsswitch`	Autenticación LDAP o NIS
`password`	Contraseña
`publickey`	Autenticación de clave pública
`usm`	Modelo de seguridad de usuario SNMP

No se recomienda el uso de NIS debido a las debilidades de seguridad del protocolo.

A partir de ONTAP 9,3, la autenticación encadenada de dos factores está disponible para cuentas SSH locales `admin` que utilizan `publickey` y `password` como los dos métodos de autenticación. Además del `-authentication-method` campo del `security login` comando, se ha agregado un nuevo campo denominado `-second-authentication-method`. `publickey`O `password` se puede especificar como el `-authentication-method` o el `-second-authentication-method`. Sin embargo, durante la autenticación SSH, el orden está siempre `publickey` con autenticación parcial, seguido de la solicitud de contraseña para la autenticación completa.

```
[user@host01 ~]$ ssh ontap.netapp.local
Authenticated with partial success.
Password:
cluster1::>
```

A partir de ONTAP 9,4, `nsswitch` se puede utilizar como un segundo método de autenticación con `publickey`.

A partir de ONTAP 9.12.1, FIDO2 también se puede usar para la autenticación SSH usando un dispositivo de autenticación de hardware YubiKey u otros dispositivos compatibles con FIDO2.

A partir de ONTAP 9,13.1:

- `domain` las cuentas se pueden utilizar como un segundo método de autenticación con `publickey`.
- Contraseña de un solo uso basada en tiempo (`totp`) es un código de acceso temporal generado por un algoritmo que utiliza la hora actual del día como uno de sus factores de autenticación para el segundo método de autenticación.
- La revocación de claves públicas es compatible con claves públicas SSH, así como con certificados que se comprobarán para su caducidad/revocación durante SSH.

Para obtener más información sobre la autenticación multifactor (MFA) para el administrador del sistema de ONTAP, Active IQ Unified Manager y SSH, consulte "TR-4647: Autenticación multifactor en ONTAP 9".

Cuentas administrativas predeterminadas

Se debe restringir la cuenta de administrador porque se permite el acceso al rol de

administrador mediante todas las aplicaciones. La cuenta de diagnóstico (diag) permite acceder al shell del sistema y se debe reservar solo para que el soporte técnico realice tareas de solución de problemas.

Hay dos cuentas administrativas predeterminadas `admin` : Y `diag`.

Las cuentas huérfanas son un vector de seguridad importante que a menudo conduce a vulnerabilidades, incluida la escalada de privilegios. Se trata de cuentas innecesarias y no utilizadas que permanecen en el repositorio de cuentas de usuario. Son principalmente cuentas predeterminadas que nunca se usaron o para las que las contraseñas nunca se actualizaron o cambiaron. Para solucionar este problema, ONTAP admite la eliminación y el cambio de nombre de las cuentas.

No puedes eliminar ni renombrar cuentas integradas. Si un administrador elimina la cuenta, al reiniciar, la cuenta integrada se volverá a crear. **NetApp recomienda** bloquear cualquier cuenta integrada que no necesites con el comando lock.

Aunque las cuentas huérfanas son un problema de seguridad importante, **NetApp recomienda encarecidamente** probar el efecto de eliminar cuentas del repositorio de cuentas local.

Enumerar las cuentas locales

Para mostrar las cuentas locales, ejecute `security login show` el comando.

```
cluster1::*> security login show -vserver cluster1

vserver: cluster1
                              Authentication             Acct   Is-Nsswitch
User/Group Name  Application Method    Role Name         Locked Group
---------------- ----------- --------- ----------------- ------ -----------
admin            console     password  admin             no     no
admin            http        password  admin             no     no
admin            ontapi      password  admin             no     no
admin            service-processor password admin        no     no
admin            ssh         password  admin             no     no
autosupport      console     password  autosupport       no     no
6 entries were displayed.
```

Establezca la contraseña de la cuenta de diagnóstico (diag)

El sistema de almacenamiento se proporciona una cuenta de diagnóstico llamada `diag` . Puede utilizar `diag` la cuenta para realizar tareas de solución de problemas en la `systemshell`. La `diag` cuenta es la única cuenta que se puede utilizar para acceder al systemshell a través del `diag` comando con privilegios `systemshell`.

El systemshell y la cuenta asociada `diag` están pensados para fines de diagnóstico de bajo nivel. Su acceso requiere el nivel de privilegio de diagnóstico y se reserva solo para utilizarse con orientación del soporte técnico para realizar tareas de solución de problemas. Ni la `diag` cuenta ni la `systemshell` está destinada a fines administrativos generales.

Antes de empezar

Antes de acceder a `systemshell`, debe definir `diag` la contraseña de la cuenta mediante el `security login password` comando. Debe utilizar principios de contraseña seguros y cambiar la `diag` contraseña a intervalos regulares.

Pasos

1. Establezca `diag` la contraseña de usuario de la cuenta:

```
cluster1::> set -privilege diag

Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? \{y|n}: y

cluster1::*> systemshell -node node-01
    (system node systemshell)
diag@node-01's password:

Warning: The system shell provides access to low-level
diagnostic tools that can cause irreparable damage to
the system if not used properly. Use this environment
only when directed to do so by support personnel.

node-01%
```

Verificación de varios administradores

A partir de ONTAP 9.11.1, puede usar la verificación multiadministrador (MAV) para permitir que ciertas operaciones, como la eliminación de volúmenes o snapshots, se ejecuten solo 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.

La configuración de MAV consiste en lo siguiente:

- "Creación de uno o más grupos de aprobación de administrador".
- "Activación de la función de verificación multiadministradora".
- "Adición o modificación de reglas".

Después de la configuración inicial, solo los administradores de un grupo de aprobación MAV (administradores de MAV) pueden modificar estos elementos.

Cuando MAV está activado, la realización de todas las operaciones protegidas requiere tres pasos:

1. Cuando un usuario inicia la operación, un "se genera la solicitud".
2. Antes de que se pueda ejecutar, el número requerido de "Los administradores de MAV deben aprobar".
3. Después de la aprobación, el usuario completa la operación.

MAV no se ha diseñado para su uso con volúmenes o flujos de trabajo que implican una gran automatización, ya que cada tarea automatizada requiere aprobación antes de que se pueda completar la operación. Si desea utilizar la automatización y MAV conjuntamente, NetApp recomienda que utilice consultas para operaciones de MAV específicas. Por ejemplo, puede aplicar `volume delete` reglas MAV solo a volúmenes en los que la automatización no esté involucrada, y puede designar esos volúmenes con un esquema de nomenclatura particular.

Para obtener información más detallada sobre MAV, consulte la "Documentación de verificación multiadministrador de ONTAP".

Bloqueo de instantáneas

El bloqueo de snapshots es una función de SnapLock en la que las instantáneas se vuelven indelebles manual o automáticamente con un período de retención en la política de snapshots de volúmenes. El objetivo del bloqueo de instantáneas es impedir que los administradores malintencionados o que no sean de confianza eliminen snapshots del sistema de ONTAP principal o secundario.

El bloqueo de instantáneas se introdujo en ONTAP 9.12.1. El bloqueo de instantáneas también se denomina bloqueo de instantáneas a prueba de manipulaciones. Aunque requiere la licencia de SnapLock y la inicialización del reloj de cumplimiento, el bloqueo de instantáneas no está relacionado con SnapLock Compliance o SnapLock Enterprise. No existe un administrador de almacenamiento de confianza, como sucede con SnapLock Enterprise y no protege la infraestructura de almacenamiento físico subyacente, como sucede con el cumplimiento de normativas de SnapLock. Esta es una mejora con respecto a la copia snapshot de SnapVault en un sistema secundario. Puede conseguirse una rápida recuperación de snapshots bloqueadas en sistemas principales para restaurar volúmenes dañados por el ransomware.

Para obtener más información, consulte la "documentación de bloqueo de instantáneas".

Configure el acceso de API basado en certificados

En lugar de utilizar la autenticación basada en certificado y el ID de usuario para la API de REST o el acceso de la API de SDK de capacidad de gestión de NetApp para ONTAP.

> Como alternativa a la autenticación basada en certificados para la API de REST, utilice "Autenticación basada en token OAuth 2,0".)

Puede generar e instalar un certificado autofirmado en ONTAP, tal y como se describe en estos pasos.

Pasos

1. Con OpenSSL, genere un certificado ejecutando el siguiente comando:

```
openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout test.key
-out test.pem \> -subj "/C=US/ST=NC/L=RTP/O=NetApp/CN=cert_user"
Generating a 2048 bit RSA private key
..............+++
............................+++
writing new private key to 'test.key'
```

Este comando genera un certificado público denominado `test.pem` y una clave privada denominada `key.out`. El nombre común, CN, corresponde al ID de usuario de ONTAP.

2. Instale el contenido del certificado público en formato de correo mejorado de privacidad (pem) en ONTAP ejecutando el siguiente comando y pegando el contenido del certificado cuando se le solicite:

```
security certificate install -type client-ca -vserver cluster1

Please enter Certificate: Press <Enter> when done
```

3. Active ONTAP para permitir el acceso del cliente a través de SSL y defina el ID de usuario para el acceso a la API.

```
security ssl modify -vserver cluster1 -client-enabled true
security login create -user-or-group-name cert_user -application ontapi
-authmethod cert -role admin -vserver cluster1
```

En el siguiente ejemplo, el ID de usuario `cert_user` ahora está habilitado para utilizar acceso a API autenticado con certificado. Un script de Python de SDK de gestión simple que utiliza `cert_user` para mostrar la versión de ONTAP aparece de la siguiente manera:

```
#!/usr/bin/python

import sys
sys.path.append("/home/admin/netapp-manageability-sdk-9.5/netapp-
manageability-sdk-9.5/lib/python/NetApp")
from NaServer import *

cluster = "cluster1"
transport = "HTTPS"
port = 443
style = "CERTIFICATE"
cert = "test.pem"
key = "test.key"

s = NaServer(cluster, 1, 30)
s.set_transport_type(transport)
s.set_port(port)
s.set_style(style)
s.set_server_cert_verification(0)
s.set_client_cert_and_key(cert, key)

api = NaElement("system-get-version")
output = s.invoke_elem(api)
if (output.results_status() == "failed"):
    r = output.results_reason()
    print("Failed: " + str(r))
    sys.exit(2)

ontap_version = output.child_get_string("version")
print ("V: " + ontap_version)
```

El resultado del script muestra la versión de ONTAP.

```
./version.py

V: NetApp Release 9.5RC1: Sat Nov 10 05:13:42 UTC 2018
```

4. Para realizar una autenticación basada en certificados con la API REST DE ONTAP, complete los siguientes pasos:
   a. En ONTAP, defina el ID de usuario para el acceso http:

```
security login create -user-or-group-name cert_user -application http
-authmethod cert -role admin -vserver cluster1
```

b. En su cliente Linux, ejecute el siguiente comando que genera la versión de ONTAP como resultado:

```
curl -k --cert-type PEM --cert ./test.pem --key-type PEM --key
./test.key -X GET "https://cluster1/api/cluster?fields=version"
{
    "version": {
        "full": "NetApp Release 9.7P1: Thu Feb 27 01:25:24 UTC 2020",
        "generation": 9,
        "major": 7,
        "minor": 0
    },
    "_links": {
        "self": {
            "href": "/api/cluster"
        }
    }
}
```

Más información

- "Autenticación basada en certificados con el SDK de capacidad de gestión de NetApp para ONTAP".

Autenticación basada en token OAuth 2,0 de ONTAP para la API de REST

Como alternativa a la autenticación basada en certificados, puede utilizar la autenticación basada en tokens OAuth 2,0 para la API REST.

A partir de ONTAP 9.14.1, 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.

Los tokens OAuth 2,0 reemplazan las contraseñas para la autenticación de cuentas de usuario.

Para obtener más información sobre el uso de OAuth 2,0, consulte la "Documentación de ONTAP sobre autenticación y autorización mediante OAuth 2,0".

Parámetros de inicio de sesión y contraseña

Una postura de seguridad efectiva se adhiere a las políticas organizativas establecidas, directrices y cualquier gobierno o estándares que se apliquen a la organización. Algunos ejemplos de estos requisitos incluyen la vida útil del nombre de usuario, los requisitos de longitud de contraseña, los requisitos de caracteres y el almacenamiento de dichas cuentas. La solución ONTAP ofrece características y funciones para abordar estos problemas de seguridad.

Nuevas funciones de cuenta local

Para admitir las políticas, directrices o estándares de cuentas de usuario de una organización, incluida la gobernanza, ONTAP admite las siguientes funciones:

- Configuración de políticas de contraseñas para aplicar un número mínimo de dígitos, caracteres en minúsculas o caracteres en mayúsculas
- Se requiere un retraso después de un intento fallido de inicio de sesión
- Definición del límite inactivo de la cuenta
- Vencimiento de una cuenta de usuario
- Mostrando un mensaje de advertencia de caducidad de contraseña
- Notificación de una conexión no válida

Los ajustes configurables se gestionan mediante el comando security login role config modify.

Compatibilidad con SHA-512

Para mejorar la seguridad de las contraseñas, ONTAP 9 admite la función hash de contraseña SHA-2 y utiliza por defecto SHA-512 para hash de contraseñas recién creadas o modificadas. Los operadores y administradores también pueden caducar o bloquear cuentas según sea necesario.

Las cuentas de usuario de ONTAP 9 preexistentes con contraseñas sin modificar siguen utilizando la función hash MD5 después de la actualización a ONTAP 9,0 o posterior. Sin embargo, NetApp recomienda encarecidamente que estas cuentas de usuario migren a la solución SHA-512 más segura al hacer que los usuarios cambien sus contraseñas.

La funcionalidad hash de contraseña le permite realizar las siguientes tareas:

- Muestra las cuentas de usuario que coinciden con la función hash especificada:

```
cluster1::*> security login show -user-or-group-name NewAdmin -fields
hash-function
vserver  user-or-group-name application authentication-method hash-
function
-------- ------------------ ----------- ---------------------
-------------
cluster1 NewAdmin           console     password              sha512
cluster1 NewAdmin           ontapi      password              sha512
cluster1 NewAdmin           ssh         password              sha512
```

- Las cuentas Expire que utilizan una función hash especificada (por ejemplo, MD5), que obliga a los usuarios a cambiar sus contraseñas en el siguiente inicio de sesión:

```
cluster1::*> security login expire-password -vserver * -username * -hash
-function md5
```

- Bloquear cuentas con contraseñas que utilizan la función hash especificada.

```
cluster1::*> security login lock -vserver * -username * -hash-function
md5
```

La función hash de contraseña es desconocida para el usuario interno `autosupport` de la SVM administrativa del clúster. Este problema es cosmético. La función hash es desconocida porque este usuario interno no tiene una contraseña configurada por defecto.

- Para ver la función hash de contraseña del `autosupport` usuario, ejecute los siguientes comandos:

```
::> set advanced
::> security login show -user-or-group-name autosupport -instance

                    Vserver: cluster1
      User Name or Group Name: autosupport
                  Application: console
        Authentication Method: password
     Remote Switch IP Address: -
                    Role Name: autosupport
               Account Locked: no
                 Comment Text: -
      Whether Ns-switch Group: no
       Password Hash Function: unknown
Second Authentication Method2: none
```

- Para establecer la función hash de contraseña (valor por defecto: SHA512), ejecute el siguiente comando:

```
::> security login password -username autosupport
```

  No importa en qué se establezca la contraseña.

```
security login show -user-or-group-name autosupport -instance

                      Vserver: cluster1
      User Name or Group Name: autosupport
                  Application: console
        Authentication Method: password
     Remote Switch IP Address: -
                    Role Name: autosupport
               Account Locked: no
                 Comment Text: -
      Whether Ns-switch Group: no
       Password Hash Function: sha512
Second Authentication Method2: none
```

Parámetros de contraseña

La solución de ONTAP admite parámetros de contraseña que abordan los requisitos y las directrices de las políticas de la organización y los respaldan.

A partir de 9.14.1, se aumenta la complejidad y las reglas de bloqueo para las contraseñas que se aplican solo a las nuevas instalaciones de ONTAP.

Todas las contraseñas deben ser distintas del nombre de usuario.

Atributo	Descripción	Predeterminado	Rango
`username-minlength`	Longitud mínima de nombre de usuario requerida	3	3-16
`username-alphanum`	Nombre de usuario alfanumérico	deshabilitado	Activado/Desactivado
`passwd-minlength`	Longitud mínima requerida de contraseña	8	3-64
`passwd-alphanum`	Contraseña alfanumérica	activado	Activado/Desactivado
`passwd-min-special-chars`	Número mínimo de caracteres especiales requeridos en la contraseña	0	0-64
`passwd-expiry-time`	Tiempo de caducidad de la contraseña (en días)	Ilimitado, lo que significa que las contraseñas nunca caducan	0-ilimitado 0 == vence ahora

Atributo	Descripción	Predeterminado	Rango
`require-initial-passwd-update`	Requerir la actualización inicial de la contraseña en el primer inicio de sesión	Deshabilitado	Activado/Desactivado Cambios permitidos a través de la consola o SSH
`max-failed-login-attempts`	Número máximo de intentos fallidos	0, no bloquee la cuenta	-
`lockout-duration`	Período máximo de bloqueo (en días)	El valor predeterminado es 0, lo que significa que la cuenta está bloqueada durante un día	-
`disallowed-reuse`	No permitir las últimas N contraseñas	6	El mínimo es 6
`change-delay`	Retraso entre cambios de contraseña (en días)	0	-
`delay-after-failed-login`	Retraso tras cada intento de inicio de sesión fallido (en segundos)	4	-
`passwd-min-lowercase-chars`	Número mínimo de caracteres alfabéticos en minúscula necesarios en la contraseña	0, que no requiere caracteres en minúsculas	0-64
`passwd-min-uppercase-chars`	Núm. Mínimo de caracteres alfabéticos en mayúsculas necesario	0, que no requiere caracteres en mayúsculas	0-64
`passwd-min-digits`	Número mínimo de dígitos necesarios en la contraseña	0, que no requiere dígitos	0-64
`passwd-expiry-warn-time`	Mostrar mensaje de advertencia antes del vencimiento de la contraseña (en días)	Ilimitado, lo que significa que nunca advierta sobre la caducidad de la contraseña	0, lo que significa advertir al usuario sobre la caducidad de la contraseña cada vez que se inicia sesión correctamente
`account-expiry-time`	La cuenta caduca en N días	Ilimitado, lo que significa que las cuentas nunca caducan	La hora de vencimiento de la cuenta debe ser mayor que el límite inactivo de la cuenta
`account-inactive-limit`	Duración máxima de la inactividad antes del vencimiento de la cuenta (en días)	Ilimitado, lo que significa que las cuentas inactivas nunca caducan	El límite inactivo de la cuenta debe ser inferior al tiempo de vencimiento de la cuenta

Ejemplo

```
cluster1::*> security login role config show -vserver cluster1 -role admin

                                        Vserver: cluster1
                                      Role Name: admin
                  Minimum Username Length Required: 3
                            Username Alpha-Numeric: disabled
                  Minimum Password Length Required: 8
                            Password Alpha-Numeric: enabled
Minimum Number of Special Characters Required in the Password: 0
                       Password Expires In (Days): unlimited
   Require Initial Password Update on First Login: disabled
                Maximum Number of Failed Attempts: 0
                    Maximum Lockout Period (Days): 0
                      Disallow Last 'N' Passwords: 6
            Delay Between Password Changes (Days): 0
     Delay after Each Failed Login Attempt (Secs): 4
Minimum Number of Lowercase Alphabetic Characters Required in the
Password: 0
Minimum Number of Uppercase Alphabetic Characters Required in the
Password: 0
Minimum Number of Digits Required in the Password: 0
Display Warning Message Days Prior to Password Expiry (Days): unlimited
                        Account Expires in (Days): unlimited
Maximum Duration of Inactivity before Account Expiration (Days): unlimited
```

Métodos de administración del sistema

Estos son parámetros importantes para fortalecer la administración del sistema ONTAP.

Acceso en línea de comandos

Establecer un acceso seguro a los sistemas es una parte fundamental del mantenimiento de una solución segura. Las opciones de acceso a la línea de comandos más comunes son SSH, Telnet y RSH. De estos, SSH es la mejor práctica más segura y estándar en el sector para el acceso remoto en línea de comandos. NetApp recomienda encarecidamente el uso de SSH para el acceso de línea de comandos a la solución ONTAP.

Configuraciones de SSH

El `security ssh show` comando muestra las configuraciones de los algoritmos de intercambio de claves SSH, los cifrados y los algoritmos MAC para el clúster y las SVM. El método de intercambio de claves utiliza estos algoritmos y cifrados para especificar cómo se generan las claves de sesión única para el cifrado y la autenticación y cómo se lleva a cabo la autenticación del servidor.

```
cluster1::> security ssh show

Vserver       Ciphers       Key Exchange Algorithms     MAC Algorithms
--------  ----------------  --------------------------  --------------
nsadhanacluster-2
                aes256-ctr,   diffie-helman-group-      hmac-sha2-256
                aes192-ctr,    exchange-sha256,         hmac-sha2-512
                aes128-ctr    ecdh-sha2-nistp384
vs0             aes128-gcm    curve25519-sha256         hmac-sha1
vs1             aes256-ctr,   diffie-hellman-group-     hmac-sha1-96
                aes192-ctr,   exchange-sha256           hmac-sha2-256
                aes128-ctr,   ecdh-sha2-nistp384        hmac-sha2-256-
                3des-cbc,     ecdh-sha2-nistp512        etm
                aes128-gcm                              hmac-sha2-512
3 entries were displayed.
```

Banners de inicio de sesión

Los banners de inicio de sesión permiten a una organización presentar a cualquier operador, administradores e incluso a los intrusos los términos y condiciones de uso aceptable, e indican a quién se le permite acceder al sistema. Este enfoque es útil para establecer las expectativas de acceso y uso del sistema. El `security login banner modify` comando modifica el banner de inicio de sesión. El banner de inicio de sesión se muestra justo antes del paso de autenticación durante el proceso de inicio de sesión del dispositivo de la consola y SSH. El texto del banner debe estar entre comillas dobles (' '), como se muestra en el siguiente ejemplo.

```
cluster1::> security login banner modify -vserver cluster1 -message
"Authorized users ONLY!"
```

Parámetros del banner de inicio de sesión

Parámetro	Descripción
`vserver`	Use este parámetro para especificar la SVM con el banner modificado. Utilice el nombre de la SVM de administrador del clúster para modificar el mensaje de nivel del clúster. El mensaje del nivel del clúster se usa como predeterminado para las SVM de datos que no tienen un mensaje definido.

Parámetro	Descripción
`message`	Este parámetro opcional se puede usar para especificar un mensaje de banner de inicio de sesión. Si el clúster tiene establecido un mensaje de banner de inicio de sesión, todas las SVM de datos también utilizan el banner de inicio de sesión del clúster. Al configurar el banner de inicio de sesión de una SVM de datos, se anula la visualización del banner de inicio de sesión del clúster. Para restablecer un banner de inicio de sesión de SVM de datos y usar el banner de inicio de sesión del clúster, use este parámetro con el valor «-». Si utiliza este parámetro, el banner de inicio de sesión no puede contener nuevas líneas (también conocidas como ends of lines [EOLs] o saltos de línea). Para introducir un mensaje de banner de inicio de sesión con nuevas líneas, no especifique ningún parámetro. Se le pedirá que introduzca el mensaje de forma interactiva. Los mensajes introducidos de forma interactiva pueden contener nuevas líneas. Los caracteres no ASCII deben utilizar Unicode UTF-8.
`uri`	`(ftp
http):///(hostname	IPv4` Utilice este parámetro para especificar el URI desde el cual se descarga el banner de inicio de sesión. El mensaje no debe superar los 2048 bytes de longitud. Los caracteres no ASCII se deben proporcionar como Unicode UTF-8.

Mensaje del día

El `security login motd modify` comando actualiza el mensaje del día (MOTD).

Hay dos categorías de MOTD: El MOTD a nivel de clúster y el MOTD a nivel de SVM de datos. Un usuario que inicie sesión en el clustershell de una SVM de datos puede ver dos mensajes: El MOTD a nivel de clúster seguido por el MOTD a nivel de SVM para esa SVM.

El administrador del clúster puede habilitar o deshabilitar el MOTD a nivel de clúster en cada SVM de forma individual si es necesario. Si el administrador del clúster deshabilita el MOTD a nivel de clúster para una SVM, el usuario que inicie sesión en la SVM no verá el mensaje a nivel de clúster. Solo un administrador del clúster puede habilitar o deshabilitar el mensaje a nivel del clúster.

Parámetro MOTD	Descripción
Vserver	Utilice este parámetro para especificar la SVM para la que se modifica el MOTD. Utilice el nombre de la SVM de administrador del clúster para modificar el mensaje de nivel del clúster.

Parámetro MOTD	Descripción
mensaje	Este parámetro opcional se puede utilizar para especificar un mensaje. Si utiliza este parámetro, MOTD no puede contener nuevas líneas. Si no especifica ningún parámetro que no sea el `-vserver` parámetro, se le pedirá que introduzca el mensaje de forma interactiva. Los mensajes introducidos de forma interactiva pueden contener nuevas líneas. Los caracteres no ASCII se deben proporcionar como Unicode UTF-8. El mensaje puede contener contenido generado dinámicamente mediante las siguientes secuencias de escape: • `\\` - Un solo carácter de contragolpe • `\b` - Sin salida (compatible solo con Linux) • `\C` - Nombre del clúster • `\d` - Fecha actual como se establece en el nodo de inicio de sesión • `\t` - Hora actual como se establece en el nodo de inicio de sesión • `\I` - Dirección IP de LIF entrante (imprime la consola para un `console` inicio de sesión) • `\l` - Nombre del dispositivo de inicio de sesión (imprime la consola para un `console` inicio de sesión) • `\L` - Último login para el usuario en cualquier nodo del cluster • `\m` - Arquitectura de la máquina • `\n` - Nodo o nombre de SVM de datos • `\N` - Nombre del usuario que inicia sesión • `\o` - Igual que \O. Suministrado para compatibilidad con Linux. • `\O` - Nombre de dominio DNS del nodo. Tenga en cuenta que la salida depende de la configuración de red y puede estar vacía. • `\r` - Número de versión de software • `\s` - Nombre del sistema operativo • `\u` - Número de sesiones de clustershell activas en el nodo local. Para el administrador de clúster: Todos los usuarios de clustershell. Para el administrador de SVM de datos: Solo sesiones activas para esa SVM de datos. • `\U` - Igual que `\u`, pero tiene `user` o `users` anexado • `\v` - Cadena efectiva de la versión del clúster • `\W` - Sesiones activas en todo el clúster para el usuario que inicia sesión (`who`)

Para obtener más información sobre la configuración del mensaje del día en ONTAP, consulte la "Documentación de ONTAP sobre el mensaje del día".

Tiempo de espera de sesión de la CLI

El tiempo de espera predeterminado de la sesión de la CLI es de 30 minutos. El tiempo de espera es importante para evitar sesiones obsoletas y el respaldo continuo de sesiones.

Utilice `system timeout show` el comando para ver el tiempo de espera actual de la sesión de la CLI. Para configurar el valor de tiempo de espera, utilice `system timeout modify -timeout <minutes>` el comando.

Acceso web con System Manager de NetApp ONTAP

Si un administrador de ONTAP prefiere usar una interfaz gráfica en lugar de la CLI para acceder a un clúster y gestionarlo, use el administrador del sistema de NetApp ONTAP. Se incluye con ONTAP como servicio web, habilitado de forma predeterminada, y accesible mediante un navegador. Dirija el navegador al nombre de host si utiliza DNS o la dirección IPv4 o IPv6 a través de `https://cluster-management-LIF`.

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 para continuar con el acceso o instalar un certificado digital firmado por una entidad de certificación (CA) en el clúster para la autenticación del servidor.

A partir de ONTAP 9,3, la autenticación del lenguaje de marcado de aserción de seguridad (SAML) es una opción para ONTAP System Manager.

Autenticación SAML para ONTAP System Manager

SAML 2,0 es un estándar de la industria ampliamente adoptado que permite a cualquier proveedor de identidad (IDP) que cumpla con SAML de terceros realizar MFA utilizando mecanismos únicos para el IDP que elija la empresa y como fuente de inicio de sesión único (SSO).

Hay tres roles definidos en la especificación SAML: El principal, el IdP y el proveedor de servicios. En la implementación de ONTAP, un principal es el administrador del clúster que obtiene acceso a ONTAP mediante ONTAP System Manager o NetApp Active IQ Unified Manager. El IdP es un software IdP de terceros. A partir de ONTAP 9,3, los Servicios Federados de Active Directory de Microsoft (ADFS) y el IdP de código abierto Shibboleth son compatibles. A partir de ONTAP 9.12.1, Cisco DUO es un IDP compatible. El proveedor de servicios es la funcionalidad SAML integrada en ONTAP que utiliza ONTAP System Manager o la aplicación web Active IQ Unified Manager.

A diferencia del proceso de configuración de dos factores de SSH, una vez que se activa la autenticación SAML, el acceso de ONTAP System Manager o Service Processor de ONTAP requiere que todos los administradores existentes se autentiquen mediante el IdP de SAML. No es necesario realizar cambios en las cuentas de usuario del clúster. Cuando se habilita la autenticación SAML, se añade un nuevo método de autenticación de `saml` a los usuarios existentes con roles de administrador para `http` y `ontapi` aplicaciones.

Una vez habilitada la autenticación SAML, es necesario definir cuentas nuevas adicionales que requieren acceso SAML IdP en ONTAP con el rol de administrador y el método de autenticación saml para `http` las aplicaciones y `ontapi` . Si la autenticación SAML está deshabilitada en algún momento, estas cuentas nuevas requieren que se defina el `password` método de autenticación con el rol de administrador para `http` las aplicaciones y `ontapi` y la adición de `console` la aplicación para la autenticación ONTAP local en ONTAP System Manager.

Una vez habilitado el IdP de SAML, el IdP realiza la autenticación para el acceso de ONTAP System Manager mediante los métodos disponibles para IdP, como el protocolo ligero de acceso a directorios (LDAP), Active Directory (AD), Kerberos, contraseña, etc. Los métodos disponibles son únicos para el IdP. Es importante que las cuentas configuradas en ONTAP tengan ID de usuario que se asignen a los métodos de autenticación de IdP.

Los IDP validados por NetApp son Microsoft ADFS, Cisco DUO y Shibboleth IDP de código abierto.

A partir de ONTAP 9.14.1, Cisco DUO se puede utilizar como un segundo factor de autenticación para SSH.

Para obtener más información sobre MFA para el administrador del sistema de ONTAP, Active IQ Unified Manager y SSH, consulte "TR-4647: Autenticación multifactor en ONTAP 9".

Información de System Manager de ONTAP

A partir de ONTAP 9.11.1, System Manager de ONTAP proporciona información para ayudar a los administradores de clúster a simplificar sus tareas diarias. La información sobre seguridad se basa en las recomendaciones de este informe técnico.

Información sobre seguridad	Determinación
Telnet está activado	NetApp recomienda Secure Shell (SSH) para el acceso remoto seguro.
Shell remoto (RSH) está activado	NetApp recomienda SSH para un acceso remoto seguro.
AutoSupport está utilizando un protocolo no seguro	AutoSupport no está configurado para ser enviado a través de enlace:HTTPS.
El banner de inicio de sesión no está configurado en el clúster a nivel del clúster	Advertencia si el banner de inicio de sesión no está configurado para el clúster.
SSH está utilizando cifrados no seguros	Advertencia si SSH utiliza cifrados no seguros.
Hay muy pocos servidores NTP configurados	Advertencia si el número de servidores NTP configurados es inferior a tres.
El usuario administrador predeterminado no está bloqueado	Cuando no se utiliza ninguna cuenta administrativa predeterminada (admin o diag) para iniciar sesión en System Manager y estas cuentas no están bloqueadas, la recomendación es bloquearlas.
Defensa contra ransomware: Los volúmenes no tienen políticas de Snapshot	No hay una política de Snapshot adecuada anexada a uno o varios volúmenes.
Protección contra ransomware: Deshabilita la eliminación automática de copias Snapshot	La eliminación automática de Snapshot se establece para uno o varios volúmenes.
No se supervisan los volúmenes de ataques de ransomware	La protección autónoma contra ransomware es compatible con varios volúmenes, pero aún no configurada.
Las SVM no están configuradas para la protección autónoma frente al ransomware	La protección autónoma contra ransomware es compatible con varias SVM, pero aún no configurada.
FPolicy nativo no configurado	FPolicy no está establecido para SVM NAS.
Habilita el modo activo autónomo de protección frente a ransomware	Varios volúmenes completaron el modo de aprendizaje y se puede activar el modo activo
El cumplimiento de la normativa global FIPS 140-2 está desactivado	El cumplimiento de la normativa global FIPS 140-2 no está activado.
El clúster no está configurado para notificaciones	Los correos electrónicos, los WebHooks o los hosts de capturas de SNMP no están configurados para recibir notificaciones.

Para obtener más información acerca de los detalles de ONTAP System Manager, consulte la "Documentación de información de System Manager de ONTAP".

Tiempo de espera de sesión de System Manager

Puede cambiar el tiempo de espera de inactividad de sesión de System Manager. El tiempo de espera de inactividad predeterminado es de 30 minutos. Un tiempo de espera es importante para evitar sesiones obsoletas y el respaldo de sesiones.

Si se configura SAML, la configuración del IdP controla el tiempo de espera de inactividad.

Pasos

1. Seleccione **Cluster > Settings**.
2. En **Configuración de la interfaz de usuario**, seleccione .
3. En el cuadro **Tiempo de espera de inactividad**, escriba un valor de minutos entre 2 y 180 o escriba “0” para desactivar el tiempo de espera.
4. Seleccione **Guardar**.

Protección autónoma contra ransomware de ONTAP

Para complementar el análisis del comportamiento de los usuarios para la Seguridad de las cargas de trabajo de almacenamiento, la protección autónoma frente al ransomware de ONTAP analiza las cargas de trabajo de volumen y la entropía para detectar el ransomware y realiza una instantánea y notifica al administrador cuando se sospecha de un ataque.

Además de la detección y prevención de ransomware mediante el análisis del comportamiento del usuario (UBA) externo de FPolicy con NetApp Data Infrastructure Insights Storage Workload Security y el ecosistema de socios de NetApp FPolicy, ONTAP 9.10.1 presenta protección autónoma contra ransomware. La protección autónoma contra ransomware de ONTAP utiliza una capacidad de aprendizaje automático (ML) incorporada que analiza la actividad de la carga de trabajo del volumen más la entropía de los datos para detectar ransomware automáticamente. Monitorea la actividad que es diferente a la de UBA para poder detectar ataques que UBA no detecta.

Para obtener información más detallada sobre esta capacidad, consulte "Soluciones de NetApp para ransomware" o "Documentación autónoma de protección contra ransomware de ONTAP".

Auditoría del sistema de administración de almacenamiento

Asegure la integridad de la auditoría de eventos descargando eventos de ONTAP en un servidor syslog remoto. Este servidor podría ser un sistema de gestión de eventos de información de seguridad como Splunk.

Enviar syslog

La información de registro y auditoría es muy valiosa para las organizaciones desde el punto de vista del soporte y la disponibilidad. Además, la información y los detalles que contienen los registros (syslog) y los informes y resultados de auditorías suelen ser de carácter confidencial. Para mantener los controles y la política de seguridad, es imprescindible que las organizaciones gestionen los datos de registro y auditoría de forma segura.

Descargar la información de syslog es necesario para limitar el alcance o la huella de una intrusión en un solo sistema o solución. Por ello, NetApp recomienda descargar la información de syslog de forma segura en una

ubicación segura de almacenamiento o retención.

Cree un destino de reenvío de logs

Utilice `cluster log-forwarding create` el comando para crear destinos de reenvío de registros para el registro remoto.

Parámetros

Use los siguientes parámetros para configurar `cluster log-forwarding create` el comando:

- **Destino host.** Este nombre es el nombre de host o la dirección IPv4 o IPv6 del servidor al que desea reenviar los logs.

```
-destination <Remote InetAddress>
```

- **Puerto de destino.** Este es el puerto en el que recibe el servidor de destino.

```
[-port <integer>]
```

- **Protocolo de reenvío de registros.** Este protocolo se utiliza para enviar mensajes al destino.

```
[-protocol \{udp-unencrypted|tcp-unencrypted|tcp-encrypted}]
```

  El protocolo de reenvío de registros puede usar uno de los valores siguientes:

  - `udp-unencrypted`. Protocolo de datagramas de usuario sin seguridad.
  - `tcp-unencrypted`. TCP sin seguridad.
  - `tcp-encrypted`. TCP con seguridad de la capa de transporte (TLS).
- **Verificar la identidad del servidor de destino.** Cuando este parámetro se define en TRUE, la identidad del destino de reenvío de logs se verifica validando su certificado. El valor se puede establecer en verdadero sólo cuando se selecciona el valor en `tcpencrypted` el campo de protocolo.

```
[-verify-server \{true|false}]
```

- **Instalación Syslog.** Este valor es la utilidad syslog que se debe utilizar para los registros reenviados.

```
[-facility <Syslog Facility>]
```

- **Salte la prueba de conectividad.** Normalmente, el `cluster log-forwarding create` comando comprueba que se puede acceder al destino enviando un ping de protocolo de mensajes de control de Internet (ICMP) y genera un error si no se puede acceder a él. Al definir este valor `true` se omite la comprobación de ping para que pueda configurar el destino cuando no se pueda acceder a él.

```
[-force [true]]
```

NetApp recomienda el uso `cluster log-forwarding` del comando para forzar la conexión a un `-tcp-encrypted` tipo.

Notificación de eventos

Proteger la información y los datos que salen de un sistema es vital para mantener y gestionar la política de seguridad del sistema. Los eventos generados por la solución de ONTAP ofrecen una gran cantidad de información acerca de qué se encuentra la solución, la información procesada y mucho más. La vitalidad de estos datos destaca la necesidad de gestionarlos y migrarlos de forma segura.

El `event notification create` comando envía una nueva notificación de un conjunto de eventos definidos por un filtro de eventos a uno o más destinos de notificación. Los siguientes ejemplos muestran la configuración de notificaciones de eventos y `event notification show` el comando, que muestra los filtros y los destinos de notificación de eventos configurados.

```
cluster1::> event notification create -filter-name filter1 -destinations
 email_dest,syslog_dest,snmp-traphost

cluster1::> event notification show
ID     Filter Name       Destinations
-----  ----------------  -----------------
1 filter1 email_dest, syslog_dest, snmp-traphost
```

Cifrado del almacenamiento en ONTAP

Para proteger los datos confidenciales en caso de que un disco sea robado, devuelto o reasignado mediante el cifrado de almacenamiento de NetApp basado en hardware o el cifrado de volúmenes de NetApp basado en software/el cifrado de agregados de NetApp. Ambos mecanismos son validados FIPS-140-2 y cuando se utilizan mecanismos basados en hardware con mecanismos basados en software, la solución califica para el programa de soluciones comerciales para clasificados (CSfC). Permite una protección de seguridad mejorada para los datos secretos y secretos en reposo, tanto a nivel de hardware como de software.

El cifrado de datos en reposo es importante para proteger los datos confidenciales en caso de robo, devolución o reasignación de un disco.

ONTAP 9 cuenta con tres soluciones de cifrado de datos en reposo conforme a la normativa FIPS 140-2:

- El cifrado en almacenamiento de NetApp (NSE) es una solución de hardware que usa unidades de autocifrado.
- El cifrado de volúmenes de NetApp (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.

- El cifrado de agregados de NetApp (NAE) es una solución de software que permite el cifrado de cualquier volumen de datos en cualquier tipo de unidad, donde se habilita con claves únicas para cada agregado.

NSe, NVE y NAE pueden usar la gestión de claves externa o el gestor de claves incorporado (OKM). El uso de NSE, NVE y NAE no afecta a las funciones de eficiencia del almacenamiento de ONTAP. Sin embargo, los volúmenes NVE se excluyen de la deduplicación de agregados. Los volúmenes NAE participan en la deduplicación agregada y se benefician de ella.

OKM proporciona una solución de cifrado independiente para datos en reposo con NSE, NVE o NAE.

NVE, NAE y OKM usan el CryptoMod de ONTAP. CryptoMod aparece en la lista CMVP de módulos validados FIPS 140-2-2. Consulte "Certificado FIPS 140-2 n.o 4144".

Para iniciar la configuración de OKM, utilice el `security key-manager onboard enable` comando. Para configurar gestores de claves del protocolo de interoperabilidad de gestión de claves (KMIP) externas, utilice `security key-manager external enable` el comando. A partir de ONTAP 9,6, se admite el multi-tenancy para los gestores de claves externos. Utilice el `-vserver <vserver name>` parámetro para habilitar la gestión de claves externa para una SVM específica. Antes de 9,6, el `security key-manager setup` comando se utilizaba para configurar OKM y gestores de claves externos. Para la gestión de claves incorporada, esta configuración guía al operador o administrador a través de la configuración de la clave de acceso y los parámetros adicionales para la configuración de OKM.

En el siguiente ejemplo se proporciona una parte de la configuración:

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

Enter the following commands at any time
"help" or "?" if you want to have a question clarified,
"back" if you want to change your answers to previous questions, and
"exit" if you want to quit the key manager setup wizard. Any changes
you made before typing "exit" will be applied.

Restart the key manager setup wizard with "security key-manager setup". To
accept a default
or omit a question, do not enter a value.

Would you like to configure onboard key management? {yes, no} [yes]:
Enter the cluster-wide passphrase for onboard key management. To continue
the configuration, enter the passphrase, otherwise
type "exit":
Re-enter the cluster-wide passphrase:
After configuring onboard key management, save the encrypted configuration
data
in a safe location so that you can use it if you need to perform a manual
recovery
operation. To view the data, use the "security key-manager backup show"
command.
```

A partir de ONTAP 9,4, puede utilizar `-enable-cc-mode` la opción true con `security key-manager setup` para solicitar que los usuarios introduzcan la frase de acceso después de un reinicio. Para ONTAP 9,6 y versiones posteriores, la sintaxis del comando es `security key-manager onboard enable -cc -mode-enabled yes`.

A partir de ONTAP 9,4, se puede utilizar esta `secure-purge` función con privilegios avanzados para «restregar» datos de forma no disruptiva en los volúmenes habilitados para NVE. El barrido de datos en un volumen cifrado garantiza que no puedan recuperarse del medio físico. El siguiente comando purga de forma segura los archivos eliminados en vol1 en la SVM VS1:

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume vol1
```

A partir de ONTAP 9,7, NAE y NVE se habilitan de forma predeterminada si la licencia VE está vigente, se configuran OKM o los gestores de claves externos y NSE no se utiliza. Los volúmenes NAE se crean de forma predeterminada en los agregados de NAE, y los volúmenes NVE se crean de forma predeterminada en agregados no NAE. Para anular esto, introduzca el siguiente comando:

```
cluster1::*> options -option-name
encryption.data_at_rest_encryption.disable_by_default true
```

A partir de ONTAP 9,6, se puede usar un ámbito de SVM 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 utiliza un SVM diferente (o un conjunto de SVM) para servir datos. Solo el administrador de SVM para un inquilino determinado tiene acceso a las claves de ese inquilino. Para obtener más información, consulte "Habilite la gestión de claves externa en ONTAP 9,6 y versiones posteriores" en la documentación de ONTAP.

A partir de ONTAP 9.11.1, puede configurar la conectividad con servidores de gestión de claves externos en clúster designando servidores de claves primarios y secundarios en una SVM. Para obtener más información, consulte "configurar servidores de claves externas en clúster" en la documentación de ONTAP.

A partir de ONTAP 9.13.1, es posible configurar servidores externos del gestor de claves en System Manager. Para obtener más información, consulte "Gestione gestores de claves externos" en la documentación de ONTAP.

Cifrado de la replicación de datos

Para complementar el cifrado de datos en reposo, puedes cifrar el tráfico de replicación de datos de ONTAP entre clústeres usando TLS con una clave precompartida para SnapMirror, SnapVault o FlexCache.

Al replicar datos para recuperación ante desastres, almacenamiento en caché o backup, debe proteger esos datos durante el transporte por el cable de un clúster de ONTAP a otro. De este modo, se evitan ataques maliciosos de tipo man-in-the-middle contra datos confidenciales mientras están en movimiento.

A partir de ONTAP 9.6, el cifrado de cluster peering proporciona soporte de cifrado TLS 1.2 AES-256 GCM para las funciones de replicación de datos de ONTAP como SnapMirror, SnapVault y FlexCache. El cifrado se configura mediante una clave precompartida (PSK) entre dos cluster peers.

A partir de ONTAP 9.15.1, el cifrado de cluster peering proporciona compatibilidad con el cifrado TLS 1.3 AES-256 GCM para las funciones de replicación de datos de ONTAP, como SnapMirror, SnapVault y FlexCache. El cifrado se configura mediante una clave precompartida (PSK) entre dos cluster peers.

Los clientes que usan tecnologías como NSE, NVE y NAE para proteger los datos en reposo también pueden usar el cifrado de datos de extremo a extremo actualizando a ONTAP 9.6 o posterior para usar el cifrado de clúster peering.

El cluster peering cifra todos los datos entre los cluster peers. Por ejemplo, cuando usas SnapMirror, toda la información de peering y todas las relaciones SnapMirror entre el clúster de origen y el clúster de destino están cifradas. No puedes enviar datos en texto claro entre cluster peers si tienes activado el cifrado de cluster peering.

A partir de ONTAP 9.6, las nuevas relaciones entre iguales de clúster tienen el cifrado activado por defecto. Para activar el cifrado en las relaciones entre iguales de clúster que se crearon antes de ONTAP 9.6, debes actualizar el clúster de origen y el clúster de destino a 9.6. Además, debes usar el comando `cluster peer modify` para cambiar tanto los clústeres de origen como los de destino para que utilicen el cifrado de relaciones entre iguales de clúster.

Puedes convertir una relación entre iguales existente para usar el cifrado de clústeres en ONTAP 9.6 como se muestra en el siguiente ejemplo:

```
On the destination cluster peer:

cluster2::> cluster peer modify cluster1 -auth-status-admin use-
authentication -encryption-protocol-proposed tls-psk

When prompted enter a passphrase.

On the source cluster peer:

cluster1::> cluster peer modify cluster2 -auth-status-admin use-
authentication -encryption-protocol-proposed tls-psk

When prompted enter the same passphrase you created in the previous step.
```

Cifrado de datos en tránsito IPsec

Los clientes que usan tecnologías de cifrado de datos en reposo como el cifrado del almacenamiento de NetApp (NSE) o el cifrado de volúmenes de NetApp (NVE) y el cifrado de paridad de clústeres (CPE) para el tráfico de replicación de datos ahora pueden utilizar el cifrado de extremo a extremo entre el cliente y el almacenamiento en su estructura de datos multicloud híbrida actualizando a ONTAP 9,8 o versiones posteriores, y utilizando IPSec. IPSec ofrece una alternativa al cifrado NFS o SMB/CIFS y es la única opción de cifrado en tránsito para el tráfico iSCSI.

En algunas situaciones, es posible que haya un requisito de proteger todos los datos de clientes transportados a través del cable (o en tránsito) hacia la SVM de ONTAP. De este modo, se evita la repetición y los ataques maliciosos de intermediario contra datos confidenciales mientras están en movimiento.

A partir de ONTAP 9,8, el protocolo de seguridad de Internet (IPsec) ofrece compatibilidad con cifrado integral para todo el tráfico IP entre un cliente y una SVM de ONTAP. El cifrado de datos IPSec para todo el tráfico IP incluye protocolos NFS, iSCSI y SMB/CIFS. IPSec proporciona la única opción de cifrado en vuelo para el tráfico iSCSI.

Proporcionar cifrado NFS por cable es uno de los casos de uso principales de IPsec. Antes de ONTAP 9,8, el cifrado por cable NFS requería la configuración y la configuración de Kerberos para utilizar krb5p para cifrar datos NFS en tránsito. No siempre es sencillo ni fácil de lograr en todos los entornos del cliente.

Los clientes que usan tecnologías de cifrado de datos en reposo como el cifrado del almacenamiento de NetApp (NSE) o el cifrado de volúmenes de NetApp (NVE) y el cifrado de paridad de clústeres (CPE) para el tráfico de replicación de datos ahora pueden utilizar el cifrado de extremo a extremo entre el cliente y el almacenamiento en su estructura de datos multicloud híbrida actualizando a ONTAP 9,8 o versiones posteriores, y utilizando IPSec.

IPSec es un estándar IETF. ONTAP utiliza IPsec en modo de transporte. También aprovecha la versión 2 del protocolo de intercambio de claves de Internet (IKE), que utiliza una clave precompartida (PSK) para negociar material clave entre el cliente y ONTAP con IPv4 o IPv6. De forma predeterminada, IPsec utiliza el cifrado Suite-B AES-GCM de 256 bits. Suite-B AES-GMAC256 y AES-CBC256 con cifrado de 256 bits también son compatibles.

Aunque la funcionalidad IPsec debe estar habilitada en el clúster, se aplica a direcciones IP de SVM individuales mediante el uso de una entrada de base de datos de política de seguridad (SPD). La entrada de directiva (SPD) contiene la dirección IP del cliente (subred IP remota), la dirección IP de SVM (subred IP local), el conjunto de cifrado que se va a utilizar y el secreto precompartido (PSK) necesario para autenticarse a través de IKEv2 y establecer la conexión IPsec. Además de la entrada de directiva IPsec, el cliente debe configurarse con la misma información (IP local y remota, PSK y conjunto de cifrado) antes de que el tráfico pueda fluir a través de la conexión IPsec. A partir de ONTAP 9.10.1, se añade el soporte de autenticación de certificados IPsec. Esto elimina los límites de la política IPsec y activa el soporte del sistema operativo Windows para IPsec.

Si hay un firewall entre el cliente y la dirección IP de SVM, debe permitir los protocolos ESP y UDP (puertos 500 y 4500), tanto de entrada (entrada) como de salida (salida), para que la negociación IKEv2 se realice correctamente y, por lo tanto, permita el tráfico IPsec.

Para el cifrado de tráfico de paridad de clústeres y SnapMirror de NetApp, se recomienda el cifrado de pares de clústeres (CPE) en IPsec para garantizar una seguridad en tránsito por la red. CPE tiene un mejor rendimiento para estas cargas de trabajo que IPsec. No necesita una licencia para IPsec y no hay restricciones de importación o exportación.

Puede habilitar IPsec en el clúster y crear una entrada SPD para un único cliente y una única dirección IP SVM, como se muestra en el siguiente ejemplo:

```
On the Destination Cluster Peer

cluster1::> security ipsec config modify -is-enabled true

cluster1::> security ipsec policy create -vserver vs1 -name test34 -local
-ip-subnets 192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32

When prompted enter and confirm the pre shared secret (PSK).
```

Información relacionada

"Prepárese para usar la seguridad IP en la red ONTAP"

Modo FIPS y gestión TLS y SSL en ONTAP

La norma FIPS 140-2 especifica los requisitos de seguridad para los módulos criptográficos dentro de los sistemas de seguridad que protegen la información confidencial en sistemas informáticos y de telecomunicaciones. El estándar FIPS 140-2 se aplica *específicamente* al módulo criptográfico, en lugar del producto, la arquitectura, los datos o el ecosistema. El módulo criptográfico es el componente específico (hardware, software, firmware o una combinación de los tres) que implementa funciones de seguridad aprobadas por el NIST.

La habilitación del cumplimiento FIPS 140-2 tiene efectos en otros sistemas y comunicaciones internos y externos a ONTAP 9. NetApp recomienda encarecidamente probar esta configuración en un sistema no de producción que tenga acceso a la consola.

Desde el soporte de ONTAP 9.11.1 y TLS 1,3, puede validar FIPS 140-3.

La configuración FIPS se aplica a ONTAP y a la plataforma BMC.

Configuración FIPS-Mode de NetApp ONTAP

NetApp ONTAP tiene una configuración en modo FIPS que instancia un nivel de seguridad añadido al plano de control:

- A partir de ONTAP 9.11.1, cuando se habilita el modo de cumplimiento de FIPS 140-2, TLSv1, TLSv1,1 y SSLv3 están deshabilitados y solo TSLv1,2 y TSLv1,3 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. TLSv1,2 o TLSv1,3 permanecerán habilitados según la configuración anterior.
- Para las versiones de ONTAP anteriores a 9.11.1 cuando se habilita el modo de cumplimiento de FIPS 140-2, tanto TLSv1 como SSLv3 están deshabilitados y solo TLSv1,1 y TLSv1,2 se encuentran 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.
- "Módulo de seguridad criptográfica de NetApp (NCSM)", Que es FIPS 140-2 nivel 1 validado, proporciona el cumplimiento basado en software.

NIST ha enviado un estándar FIPS-140-3, y NCSM tendrá validaciones FIPS-140-2 y FIPS-140-3. Todas las validaciones FIPS 140-2 pasarán al estado histórico el 21 de septiembre de 2026, que es cinco años después del último día para el envío de nuevos certificados.

Habilite el modo de cumplimiento de normativas FIPS-140-2 y FIPS-140-3

A partir de ONTAP 9, puede habilitar el modo de cumplimiento FIPS-140-2 y FIPS-140-3 para las interfaces del plano de control para todo el clúster.

- "Active FIPS"
- "Ver el estado de FIPS"

Habilitación y protocolos FIPS

El `security config modify` comando permite modificar la configuración de seguridad existente en todo el clúster. Si habilita el modo conforme a FIPS, el clúster selecciona automáticamente solo los protocolos TLS.

- Utilice el `-supported-protocols` parámetro para incluir o excluir protocolos TLS independientemente del modo FIPS. De manera predeterminada, el modo FIPS está deshabilitado y los protocolos TLSv1,3 (a partir de ONTAP 9.11.1) y TLSv1,2 están habilitados.
- Las versiones anteriores de ONTAP tenían activados de forma predeterminada los siguientes protocolos TLS:
  - TLSv1,1 (deshabilitado de forma predeterminada a partir de ONTAP 9.12.1)
  - TLSv1 (deshabilitado de forma predeterminada a partir de ONTAP 9,8)
- Para obtener compatibilidad con versiones anteriores, ONTAP admite la adición de SSLv3 a la lista de protocolos compatibles cuando el modo FIPS está deshabilitado.

Habilitación y cifrados FIPS

- Use `-supported-cipher-suites` el parámetro para configurar solo el estándar de cifrado avanzado (AES) o AES y 3DES.
- Puede desactivar los cifrados débiles como RC4 especificando `!RC4`. Por defecto, el valor de cifrado soportado es `ALL:!LOW:!aNULL:!EXP:!eNULL`. Esta configuración significa que todos los conjuntos de cifrado admitidos para los protocolos están habilitados, excepto los que utilizan algoritmos de cifrado de 64 o 56 bits sin autenticación, sin cifrado, sin exportaciones y conjuntos de cifrado de bajo cifrado.
- Seleccione un conjunto de cifrado que esté disponible con el protocolo seleccionado correspondiente. Una configuración no válida puede provocar que algunas funcionalidades no funcionen correctamente.
- Para obtener la sintaxis correcta de la cadena de cifrado, consulte el "cifrados" en OpenSSL (publicado por la base de software OpenSSL). A partir de ONTAP 9.9.1 y versiones posteriores, ya no es necesario reiniciar todos los nodos manualmente después de modificar la configuración de seguridad.

Refuerzo de la seguridad de SSH y TLS

La administración SSH de ONTAP 9 requiere un cliente OpenSSH 5,7 o posterior. Los clientes SSH deben negociar con el algoritmo de clave pública del algoritmo de firma digital de curva elíptica (ECDSA) para que la conexión sea exitosa.

Para reforzar la seguridad TLS, habilite solo TLS 1,2 y utilice conjuntos de cifrado capaces de secreto directo perfecto (PFS). PFS es un método de intercambio de claves que, cuando se utiliza en combinación con protocolos de cifrado como TLS 1,2, ayuda a evitar que un atacante descifre todas las sesiones de red entre un cliente y un servidor.

Active conjuntos de cifrado compatibles con TLSv1,2 y PFS

Para habilitar sólo conjuntos de cifrado compatibles con TLS 1,2 y PFS, utilice el `security config modify` comando desde el nivel de privilegio avanzado.

> Antes de cambiar la configuración de la interfaz SSL, asegúrese de que el cliente admite los cifrados DHE y ECDHE al conectarse a ONTAP para mantener la conectividad con ONTAP.

Ejemplo

```
cluster1::*> security config modify -interface SSL -supported-protocols
TLSv1.2 -supported-cipher-suites
PSK:DHE:ECDHE:!LOW:!aNULL:!EXP:!eNULL:!3DES:!kDH:!kECDH
```

Confirmar `y` para cada petición de datos. Para obtener más información sobre PFS, consulte este "Blog de NetApp".

Información relacionada

"Federal Information Processing Standard (FIPS), publicación 140"

Cree un certificado digital firmado por CA

Para muchas organizaciones, el certificado digital autofirmado para el acceso web de ONTAP no cumple con sus políticas de InfoSec. En sistemas de producción, se recomienda que NetApp instale un certificado digital firmado por CA para utilizarlo en la

autenticación del clúster o SVM como servidor SSL.

Puede usar `security certificate generate-csr` el comando para generar una solicitud de firma de certificación (CSR) y `security certificate install` el comando para instalar el certificado que recibe de la CA.

Pasos

1. Para crear un certificado digital firmado por la CA de la organización, realice lo siguiente:
   a. Generar una CSR.
   b. Siga el procedimiento de su organización para solicitar un certificado digital mediante la CSR de la CA de su organización. Por ejemplo, mediante la interfaz web de Microsoft Active Directory Certificate Services, vaya a `<CA_server_name>/certsrv` y solicite un certificado.
   c. Instale el certificado digital en ONTAP.

Protocolo de estado de certificado en línea

El protocolo de estado de certificados en línea (OCSP) permite que las aplicaciones de ONTAP que utilizan comunicaciones TLS, como LDAP o TLS, reciban el estado de certificado digital cuando OCSP está habilitado. La aplicación recibe una respuesta firmada que indica que el certificado solicitado es válido, revocado o desconocido.

OCSP permite determinar el estado actual de un certificado digital sin que sea necesario disponer de listas de revocación de certificados (CRL).

De manera predeterminada, la comprobación del estado de los certificados OCSP está deshabilitada. Se puede activar con el comando `security config ocsp enable -app name`, donde el nombre de la aplicación puede ser `autosupport`, , `audit_log`, , , , `fabricpool` `ems` `kmip` `ldap_ad` `ldap_nis_namemap`, o `all`. El comando requiere un nivel de privilegio avanzado.

Gestión de SSHv2

El `security ssh modify` comando reemplaza las configuraciones existentes de los algoritmos de intercambio de claves SSH, los cifrados o los algoritmos MAC para el clúster o una SVM con los ajustes de configuración que especifique.

NetApp recomienda lo siguiente:

- Use contraseñas para las sesiones de usuario.
- Utilice una clave pública para el acceso a la máquina.

Cifrados e intercambios de claves compatibles

Cifrados	Intercambio de claves
aes256-ctr	diffie-hellman-group-exchange-sha256 (SHA-2)
aes192-ctr	diffie-hellman-group-exchange-sha1 (SHA-1)
aes128-ctr	diffie-hellman-group14-sha1 (SHA-1)

Cifrados	Intercambio de claves
aes256-cbc	diffie-hellman-group1-sha1 (SHA-1)
aes192-cbc	-
aes128-cbc	-
aes128-gcm	-
aes256-gcm	-
3des-cbc	-

Compatibilidad con AES y 3DES cifrados simétricos

ONTAP también admite los siguientes tipos de cifrados simétricos AES y 3DES (también conocidos como cifrados):

- hmac-sha1
- hmac-sha1-96
- hmac-md5
- hmac-md5-96
- hmac-ripemd160
- umac-64
- umac-64
- umac-128
- hmac-sha2-256
- hmac-sha2-512
- hmac-sha1-etm
- hmac-sha1-96-etm
- hmac-sha2-256-etm
- hmac-sha2-512-etm
- hmac-md5-etm
- hmac-md5-96-etm
- hmac-ripemd160-etm
- umac-64-etm
- umac-128-etm

La configuración de gestión de SSH se aplica a ONTAP y a la plataforma BMC.

AutoSupport de NetApp

La función AutoSupport de ONTAP permite supervisar de manera proactiva el estado del sistema y enviar automáticamente mensajes y detalles al soporte técnico de NetApp, al equipo de soporte interno de su organización o a un partner de soporte. De manera

predeterminada, los mensajes de AutoSupport en el soporte técnico de NetApp se habilitan cuando el sistema de almacenamiento se configura por primera vez. Además, AutoSupport comienza a enviar mensajes al soporte técnico de NetApp 24 horas después de que está habilitado. Este periodo de 24 horas se puede configurar. Para aprovechar la comunicación con el equipo de soporte interno de una organización, se debe completar la configuración del host de correo.

Solo el administrador del clúster puede realizar una gestión de AutoSupport (configuración). El administrador de SVM no tiene acceso a AutoSupport. Es posible deshabilitar la función AutoSupport. Sin embargo, NetApp recomienda habilitarlo porque AutoSupport ayuda a acelerar la identificación y la resolución de problemas en caso de que surja un problema 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 detalles sobre los mensajes de AutoSupport, incluidos los contenidos en los distintos mensajes y los distintos tipos de mensajes, consulte "Asesor digital de NetApp" la documentación.

Los mensajes AutoSupport contienen datos confidenciales, incluidos, entre otros, los siguientes elementos:

- Archivos de registro
- Datos contextuales relativos a subsistemas específicos
- Datos de configuración y estado
- Datos de rendimiento

AutoSupport admite HTTPS y SMTP para los protocolos de transporte. Debido a la naturaleza sensible de los mensajes de AutoSupport, NetApp recomienda encarecidamente utilizar HTTPS como protocolo de transporte predeterminado para enviar mensajes de AutoSupport a la compatibilidad de NetApp.

Además, debe aprovechar `system node autosupport modify` el comando para especificar los destinos de los datos de AutoSupport (por ejemplo, soporte técnico de NetApp, operaciones internas de una organización o partners). Este comando también permite especificar los detalles específicos de AutoSupport que se deben enviar (por ejemplo, datos de rendimiento, archivos de registro, etc.).

Para deshabilitar por completo AutoSupport, utilice `system node autosupport modify -state disable` el comando.

Protocolo de hora de red

Aunque ONTAP permite configurar manualmente la zona horaria, la fecha y la hora del clúster, debe configurar los servidores de protocolo de hora de redes (NTP) para sincronizar la hora del clúster con al menos tres servidores NTP externos.

Los problemas pueden surgir cuando la hora del clúster no es precisa. Aunque ONTAP permite configurar manualmente la zona horaria, la fecha y la hora en el clúster, debe configurar los servidores de protocolo de tiempo de redes (NTP) para sincronizar la hora del clúster con servidores NTP externos.

A partir de ONTAP 9.5, puede configurar el servidor NTP con autenticación simétrica.

Puede asociar un máximo de 10 servidores NTP externos mediante el `cluster time-service ntp server create` comando. Para la redundancia y la calidad del servicio de tiempo, debe asociar al menos tres servidores NTP externos al clúster.

Para obtener detalles sobre la configuración de NTP en ONTAP, consulte "Gestionar la hora del clúster (solo administradores de clúster)".

Cuentas locales del sistema de archivos NAS (grupo de trabajo de CIFS)

La autenticación de clientes de grupo de trabajo proporciona una capa adicional de seguridad a la solución ONTAP que es consistente con una postura de autenticación de dominio tradicional. Utilice el `vserver cifs session show` comando para mostrar numerosos detalles relacionados con la postura, incluida la información de IP, el mecanismo de autenticación, la versión de protocolo y el tipo de autenticación.

A partir de ONTAP 9, puede configurar un servidor CIFS en un grupo de trabajo con clientes CIFS que se autentiquen en el servidor utilizando usuarios y grupos definidos localmente. La autenticación de clientes de grupo de trabajo proporciona una capa adicional de seguridad a la solución ONTAP que es consistente con una postura de autenticación de dominio tradicional. Para configurar el servidor CIFS, utilice `vserver cifs create` el comando. Tras crear el servidor CIFS, puede unirlo a un dominio CIFS o unirlo a un grupo de trabajo. Para unirse a un grupo de trabajo, utilice el `-workgroup` parámetro. A continuación se muestra un ejemplo de configuración:

```
cluster1::> vserver cifs create -vserver vs1 -cifs-server CIFSSERVER1
-workgroup Sales
```

Un servidor CIFS en modo grupo de trabajo solo es compatible con la autenticación de Windows NT LAN Manager (NTLM) y no admite la autenticación de Kerberos.

NetApp recomienda utilizar la función de autenticación NTLM con grupos de trabajo CIFS para mantener la política de seguridad de su organización. Para validar la política de seguridad CIFS, NetApp recomienda el uso `vserver cifs session show` del comando para mostrar numerosos detalles relacionados con la postura, incluida la información IP, el mecanismo de autenticación, la versión de protocolo y el tipo de autenticación.

Auditoría del sistema de archivos NAS

Los sistemas de archivos NAS ocupan un espacio más presente en el panorama de amenazas actual, las funciones de auditoría son cruciales para respaldar la visibilidad.

La seguridad requiere validación. ONTAP proporciona más eventos y detalles de auditoría en toda la solución. Como los sistemas de archivos NAS ocupan un espacio cada vez mayor en el panorama de amenazas actual, las funciones de auditoría son fundamentales para apoyar la visibilidad. Gracias a la capacidad de auditoría mejorada en ONTAP, los detalles de auditoría de CIFS son más abundantes que nunca. Los detalles clave, incluidos los siguientes, se registran con los eventos creados:

- Acceso a archivos, carpetas y recursos compartidos
- Archivos creados, modificados o eliminados
- Acceso de lectura a archivo realizado
- Intentos fallidos de leer o escribir archivos
- Cambios de permisos de carpeta

Cree una configuración de auditoría

Debe habilitar la auditoría de CIFS para generar eventos de auditoría. Utilice `vserver audit create` el comando para crear una configuración de auditoría. De forma predeterminada, el registro de auditoría utiliza un método de rotación según el tamaño. Puede utilizar una opción de rotación basada en el tiempo si se especifica en el campo Parámetros de rotación. Los detalles adicionales de configuración de rotación de auditoría de log incluyen el programa de rotación, los límites de rotación, los días de rotación de la semana y el tamaño de rotación. El siguiente texto proporciona una configuración de ejemplo que representa una configuración de auditoría mediante una rotación mensual basada en el tiempo programada para todos los días de la semana a las 12:30.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-rotate-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule
-hour 12 -rotate-schedule-minute 30
```

Eventos de auditoría CIFS

Los eventos de auditoría CIFS son los siguientes:

- **File Share**: Genera un evento de auditoría cuando se agrega, modifica o elimina un recurso compartido de red CIFS mediante los comandos relacionados `vserver cifs share` .
- **Cambio de política de auditoría**: Genera un evento de auditoría cuando la política de auditoría está deshabilitada, habilitada o modificada usando los comandos relacionados `vserver audit` .
- **Cuenta de usuario**: Genera un evento de auditoría cuando se crea o elimina un usuario local de CIFS o UNIX; se habilita, deshabilita o modifica una cuenta de usuario local; o se restablece o cambia una contraseña. Este evento utiliza `vserver cifs users-and-groups local-group` el comando o el comando relacionado `vserver services name-service unix-user` .
- **Grupo de seguridad**: Genera un evento de auditoría cuando se crea o elimina un grupo de seguridad local CIFS o UNIX mediante el `vserver cifs users-and-groups local-group` comando o el comando relacionado `vserver services name-service unix-group` .
- **Cambio de política de autorización**: Genera un evento de auditoría cuando se otorgan o revocan derechos para un usuario de CIFS o un grupo CIFS mediante el `vserver cifs users-and-groups privilege` comando.

> Esta funcionalidad se basa en la función de auditoría del sistema, que permite a un administrador revisar lo que el sistema permite y realiza desde la perspectiva de un usuario de datos.

Efecto de las API de REST en la auditoría NAS

ONTAP incluye la capacidad de las cuentas de administrador de acceder a archivos SMB/CIFS o NFS y manipularlos usando las API de REST. Aunque los administradores de ONTAP solo pueden ejecutar las API de REST, los comandos de la API de REST omiten el registro de auditoría del sistema NAS. Además, los administradores de ONTAP también pueden omitir los permisos de archivos cuando utilizan las API DE REST. Sin embargo, las acciones del administrador con API REST en los archivos se capturan en el registro del historial de comandos del sistema.

Crear rol de API de REST sin acceso

Puede evitar que los administradores de ONTAP utilicen las API DE REST para acceder a los archivos mediante la creación de un rol de API DE REST que no tiene acceso a volúmenes de ONTAP mediante REST. Para provisionar este rol, realice los siguientes pasos.

> La API de REST /api/storage/volumes se utiliza para algo más que el acceso a archivos. Es utilizada por System Manager y otras interfaces GUI para crear, ver y modificar volúmenes.

Pasos

1. Crear un nuevo rol DE REST que no tenga acceso a los volúmenes de almacenamiento, pero que tenga acceso a la API de REST.

```
cluster1::> security login rest-role create nofiles -vserver cluster1
"/api/storage/volumes" -access none
cluster1::> security login rest-role create nofiles -vserver cluster1
"/api" -access all
```

2. Asigne la cuenta de administrador al nuevo rol de API DE REST que creó en el paso anterior.

```
cluster1::> security login modify -user-or-group-name user1 -application
http -authentication-method password -vserver cluster1 -role nofile
```

> Si desea impedir que la cuenta de administrador de clúster de ONTAP integrada utilice las API DE REST para acceder a los archivos, primero debe "cree una nueva cuenta de administrador y desactive o elimine la cuenta integrada".

Configure y habilite la firma y el sellado CIFS SMB

Puede configurar y habilitar la firma SMB que proteja la seguridad del Data Fabric garantizando que el tráfico entre clientes y sistemas de almacenamiento no se vea comprometido por ataques de reinyección y de intermediario. La firma SMB protege al verificar que los mensajes SMB tengan firmas válidas.

Acerca de esta tarea

El protocolo SMB constituye un vector de amenazas para las arquitecturas y los sistemas de archivos. Para abordar este vector, la solución ONTAP 9 utiliza firma y sellado SMB estándar del sector. La firma SMB protege la seguridad del Data Fabric al garantizar que el tráfico entre clientes y los sistemas de almacenamiento no se vea comprometido por ataques de reinyección y de intermediario. Para ello, verifica que los mensajes SMB tengan firmas válidas.

Aunque la firma SMB está deshabilitada de forma predeterminada en interés del rendimiento, NetApp recomienda encarecidamente habilitarla. Además, la solución de ONTAP admite el cifrado SMB, que también se conoce como sellado. Este enfoque permite el transporte seguro de datos de recurso por recurso. De manera predeterminada, el cifrado SMB está deshabilitado. Sin embargo, NetApp recomienda que habilite el cifrado SMB.

La firma y el sellado LDAP ahora son compatibles con SMB 2,0 y versiones posteriores. La firma (protección

contra manipulación) y el sellado (cifrado) permiten una comunicación segura entre SVM y los servidores de Active Directory. El cifrado acelerado AES nuevas instrucciones (Intel AES NI) ahora es compatible con SMB 3,0 y versiones posteriores. AES-NI mejora el algoritmo de AES y acelera el cifrado de datos en las familias de procesadores compatibles.

Pasos

1. Para configurar y habilitar la firma SMB, utilice `vserver cifs security modify` el comando y verifique que el `-is-signing-required` parámetro se establezca en `true`. Consulte el siguiente ejemplo de configuración:

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock
-skew 3 -kerberos-ticket-age 8 -is-signing-required true
```

2. Para configurar y habilitar el sellado y el cifrado SMB, utilice `vserver cifs security modify` el comando y verifique que el `-is-smb-encryption-required` parámetro se haya establecido en `true`. Consulte el siguiente ejemplo de configuración:

```
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
```

Protección para NFS

Las reglas de exportación son los elementos funcionales de una política de exportación. Las reglas de exportación coinciden con las solicitudes de acceso de cliente de un volumen con los parámetros específicos que configura para determinar cómo se manejan las solicitudes de acceso de 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 control de acceso es fundamental para mantener una postura segura. Por lo tanto, ONTAP utiliza la función de políticas de exportación para limitar el acceso al volumen NFS a los clientes que coincidan con parámetros específicos. Las políticas de exportación contienen una o varias reglas de exportación que procesan cada solicitud de acceso de cliente. Cada volumen tiene asociada una política de exportación para configurar el acceso de clientes al volumen. El resultado de este proceso determina si al cliente se le otorga o se deniega (con un mensaje de denegación de permiso) el acceso al volumen. En este proceso también se determina el nivel de acceso al volumen.

Debe haber una política de exportación con reglas de exportación en una máquina virtual de almacenamiento para que los clientes accedan a los datos. Una SVM puede contener varias políticas 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 más reglas. Si no hay reglas que coincidan, se deniega el acceso al cliente.

Las reglas de exportación determinan los permisos de acceso del cliente aplicando los siguientes criterios:

- Protocolo de acceso a archivos utilizado por el cliente que envía la solicitud (por ejemplo, NFSv4 o SMB)
- Un identificador de cliente (por ejemplo, nombre de host o dirección IP)
- Tipo de seguridad utilizado por el cliente para autenticar (por ejemplo, Kerberos v5, NTLM o AUTH_SYS)

Si una regla especifica varios criterios y el cliente no coincide con uno o más de ellos, la regla no se aplica.

Un ejemplo de política de exportación contiene una regla de exportación con los parámetros siguientes:

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

El tipo de seguridad determina el nivel de acceso que recibe un cliente. Los tres niveles de acceso son de sólo lectura, de lectura y escritura y de superusuario (para clientes con ID de usuario `0`). Dado que el nivel de acceso determinado por el tipo de seguridad se evalúa en este orden, debe observar las reglas enumeradas:

Reglas para parámetros de nivel de acceso en reglas de exportación

Para que un cliente obtenga los siguientes niveles de acceso	Estos parámetros de acceso deben coincidir con el tipo de seguridad del cliente
Usuario normal de solo lectura	Sólo lectura (`-rorule`)
Lectura y escritura normal del usuario	Sólo lectura (`-rorule`) y lectura-escritura (`-rwrule`)
Sólo lectura de superusuario	Sólo lectura (`-rorule`) y. `-superuser`
Lectura y escritura de superusuario	Sólo lectura (`-rorule`) y lectura-escritura (`-rwrule`) y. `-superuser`

A continuación, se muestran tipos de seguridad válidos para cada uno de estos tres parámetros de acceso:

- Cualquiera
- Ninguno
- Nunca

Estos tipos de seguridad no son válidos para su uso con el `-superuser` parámetro:

- krb5
- ntlm
- act

Reglas para los resultados de los parámetros de acceso

Si el tipo de seguridad del cliente…	Entonces…
Coincide con un tipo de seguridad especificado en el parámetro de acceso.	El cliente recibe acceso para ese nivel con su propio ID de usuario.
No coincide con un tipo de seguridad especificado, pero el parámetro de acceso incluye la opción `none`.	El cliente recibe acceso para ese nivel y recibe el usuario anónimo con el ID de usuario especificado por el `-anon` parámetro.
No coincide con un tipo de seguridad especificado y el parámetro de acceso no incluye la opción `none`.	El cliente no recibe ningún acceso para ese nivel. Esta restricción no se aplica al `-superuser` parámetro porque este parámetro siempre incluye ninguno, incluso cuando no se ha especificado.

Kerberos 5 y Krb5p

A partir de ONTAP 9, se admite la autenticación Kerberos 5 con servicio de privacidad (krb5p). El modo de autenticación krbp5 es seguro y protege contra la manipulación y la escucha de datos empleando sumas de comprobación para cifrar todo el tráfico entre cliente y servidor. La solución ONTAP es compatible con el cifrado AES de 128 bits y 256 bits para Kerberos. El servicio de privacidad incluye la verificación de la integridad de los datos recibidos, la autenticación de los usuarios y el cifrado de los datos antes de la transmisión.

La opción krb5p está más presente en la función de política de exportación, donde se establece como una opción de cifrado. El método de autenticación krb5p se puede usar como parámetro de autenticación, tal como se muestra en el ejemplo siguiente:

```
cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
10.22.32.42 -volume flex_vol -authentication-method krb5p -protocol nfs3
-access- type read
```

Active la firma y el sellado del protocolo ligero de acceso a directorios

Se admiten la firma y el sellado para habilitar la seguridad de la sesión en consultas enviadas a un servidor LDAP. Este enfoque proporciona una alternativa a la seguridad de sesión LDAP-over-TLS.

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. La configuración de seguridad de sesiones en una SVM se corresponde con las disponibles en el servidor LDAP. De forma predeterminada, la firma y el sellado LDAP están deshabilitados.

Pasos

1. Para habilitar esta función, ejecute `vserver cifs security modify` el comando con `session-security-for-ad-ldap` el parámetro.

   Opciones para las funciones de seguridad de LDAP:

   - **Ninguno**: Por defecto, sin firma o sellado
   - **Signo**: Firmar tráfico LDAP
   - **Sello**: Firma y cifra el tráfico LDAP

   > Los parámetros de signo y sello son acumulativos, lo que significa que si se utiliza la opción de signo, el resultado es LDAP con firma. Sin embargo, si se utiliza la opción de sellado, el resultado es tanto el signo como el sello. Además, si no se especifica un parámetro para este comando, el valor predeterminado es none.

   A continuación se muestra un ejemplo de configuración:

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock
-skew 3 -kerberos-ticket-age 8 -session-security-for-ad-ldap seal
```

Cree y utilice una instancia de NetApp FPolicy

Puede crear y utilizar un FPolicy, un componente de infraestructura de la solución ONTAP que permite a las aplicaciones de los partners supervisar y establecer permisos de acceso a archivos. Una de las aplicaciones más potentes es la seguridad de cargas de trabajo de almacenamiento, una aplicación SaaS de NetApp que proporciona visibilidad y control centralizados de todos los accesos a los datos corporativos en entornos de cloud híbrido para garantizar que se cumplan los objetivos de seguridad y cumplimiento de normativas.

El control de acceso es un concepto clave de la seguridad. La visibilidad y la capacidad de responder al acceso a archivos y a las operaciones con archivos son cruciales para mantener su política de seguridad. Para proporcionar visibilidad y control de acceso a los archivos, la solución ONTAP usa la función FPolicy de NetApp.

Se pueden establecer políticas de archivo por tipos de archivo. FPolicy determina la forma en que el sistema de almacenamiento maneja las solicitudes de sistemas cliente individuales en operaciones como crear, abrir, cambiar nombre y eliminar. A partir de ONTAP 9, el marco de notificaciones de acceso a archivos de FPolicy se ha mejorado con controles de filtrado y resiliencia ante breves interrupciones de red.

Pasos

1. Para aprovechar la función FPolicy, primero debe crear la política de FPolicy con `vserver fpolicy policy create` el comando.

Además, debe usar el `-events` parámetro si utiliza FPolicy para obtener visibilidad y colección de eventos. La granularidad adicional que proporciona ONTAP permite filtrar y acceder a él según el nivel de control de los nombres de usuario. Para controlar los privilegios y el acceso con nombres de usuario, especifique el `-privilege-user-name` parámetro.

En el siguiente texto, se proporciona un ejemplo de creación de FPolicy:

```
cluster1::> vserver fpolicy policy create -vserver vs1.example.com
-policy-name vs1_pol -events cserver_evt,v1e1 -engine native -is
-mandatory true -allow-privileged-access no -is-passthrough-read-enabled
false
```

2. Después de crear la política de FPolicy, debe habilitarla con `vserver fpolicy enable` el comando. Este comando también establece la prioridad o la secuencia de la entrada de FPolicy.

La secuencia de FPolicy es importante porque, si varias políticas se han suscrito al mismo evento de acceso a archivos, la secuencia dicta el orden en que se otorga o deniega el acceso.

El siguiente texto proporciona una configuración de ejemplo para habilitar la política de FPolicy y validar la configuración con `vserver fpolicy show` el comando:

```
cluster1::> vserver fpolicy enable -vserver vs2.example.com -policy-name
vs2_pol -sequence-number 5

cluster1::> vserver fpolicy show
Vserver                 Policy Name                  Sequence  Status
Engine
----------------------- ---------------------------- --------  -------
-------
vs1.example.com         vs1_pol
vs2.example.com         vs2_pol
 external
2 entries were displayed.
```

Mejoras de FPolicy

ONTAP 9 incluye las mejoras de FPolicy descritas en las siguientes secciones.

Controles de filtrado

Hay nuevos filtros disponibles para `SetAttr` y para eliminar notificaciones en las actividades del directorio.

Resiliencia asincrónica

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.

Características de seguridad de los roles de LIF en ONTAP

Una LIF es una dirección IP o un nombre de puerto a nivel mundial (WWPN) con características asociadas, como un rol, un puerto de inicio, un nodo de inicio, una lista de puertos a los que se deben conmutar por error 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. Es crucial comprender las características de seguridad de cada rol de LIF.

Roles LIF

Los roles de LIF pueden ser los siguientes:

- **Data LIF**: Una LIF asociada a una SVM y utilizada para comunicarse con los clientes.
- **Cluster LIF**: Una LIF utilizada para transportar tráfico intraclúster entre nodos de un cluster.
- **Node management LIF**: Una LIF que proporciona una dirección IP dedicada para administrar un nodo en particular en un clúster.
- **Cluster management LIF**: Un LIF que proporciona una única interfaz de gestión para todo el clúster.
- **Intercluster LIF**: Una LIF utilizada para la comunicación entre clústeres, la copia de seguridad y la replicación.

Características de seguridad de cada rol de LIF

	LIF de datos	LIF del clúster	LIF de gestión de nodos	LIF de gestión del clúster	LIF de interconexión de clústeres
¿Requiere 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
¿Es personalizable el firewall?	Sí	No	Sí	Sí	Sí

- Dado que la LIF de clúster está completamente abierta sin política de firewall configurable, debe estar en una subred IP privada en una red aislada segura.
- Los roles de LIF nunca deben exponerse a Internet.

Para obtener más información sobre cómo proteger los LIF, consulte "Configurar políticas de firewall para LIF". Esta página también proporciona detalles sobre las políticas de servicio LIF a partir de ONTAP 9.10.1.

Para obtener más información sobre cómo crear una nueva política de servicio, consulte la `network interface service-policy create` comando en el "Referencia de comandos."

Protocolo y seguridad de puertos

Además de realizar operaciones y funciones de seguridad integradas, el endurecimiento de una solución también debe incluir mecanismos de seguridad externos. El aprovechamiento de dispositivos de infraestructura adicionales, como firewalls, sistemas de prevención de intrusiones (IPSs) y otros dispositivos de seguridad, para filtrar y limitar el acceso a ONTAP es una forma eficaz de establecer y mantener una postura de seguridad estricta. Esta información es un componente clave para filtrar y limitar el acceso al entorno y sus recursos.

Los protocolos y puertos comúnmente utilizados

Servicio	Puerto/protocolo	Descripción
`SSH`	22/TCP	Inicio de sesión SSH
`telnet`	23/TCP	Inicio de sesión remoto
`Domain`	53/TCP	Servidor de nombres de dominio
`HTTP`	80/TCP 80/UDP	HTTP
`rpcbind`	111/TCP 111/UDP	Llamada a procedimiento remoto
`NTP`	123/UDP	Protocolo de hora de red
`msrpc`	135/TCP	Llamada a procedimiento remoto de Microsoft
`Netbios-name`	137/TCP 137/UDP	Servicio de nombres NetBIOS
`netbios-ssn`	139/TCP	Sesión de servicio NetBIOS
`SNMP`	161/UDP	SNMP
`HTTPS`	443/TCP	Enlace seguro:http
`microsoft-ds`	445/TCP	Servicios de directorio de Microsoft
`IPsec`	500/UDP	Seguridad del protocolo de Internet
`mount`	635/UDP	Montaje NFS
`named`	953/UDP	Daemon de nombres
`NFS`	2049/UDP 2049/TCP	Daemon del servidor NFS
`nrv`	2050/TCP	Protocolo de volumen remoto de NetApp

Servicio	Puerto/protocolo	Descripción
iscsi	3260/TCP	Puerto de destino iSCSI
Lockd	4045/TCP 4045/UDP	Daemon de bloqueo NFS
NFS	4046/TCP	Protocolo NFS mountd
acp-proto	4046/UDP	Protocolo de contabilidad
rquotad	4049/UDP	Protocolo rquotad NFS
krb524	4444/UDP	Kerberos 524
IPsec	4500/UDP	Seguridad del protocolo de Internet
acp	5125/UDP 5133/UDP 5144/TCP	Puerto de control alternativo para el disco
Mdns	5353/UDP	DNS de multidifusión
HTTPS	5986/UDP	Puerto HTTPS: Protocolo binario de escucha
TELNET	8023/TCP	Telnet de ámbito de nodo
HTTPS	8443/TCP	7MTT herramienta GUI a través de xref:./ontap-security-hardening/HTTPS
RSH	8514/TCP	RSH de ámbito de nodo
KMIP	9877/TCP	Puerto de cliente KMIP (solo host local interno)
ndmp	10000/TCP	NDMP
cifs puerto de testigo	40001/TCP	Puerto de testigo CIFS
TLS	50000/TCP	Seguridad de la capa de transporte
Iscsi	65200/TCP	Puerto iSCSI
SSH	65502/TCP	Shell seguro
vsun	65503/TCP	vsun

Puertos internos de NetApp

Puerto/protocolo	Descripción
900	RPC del clúster de NetApp
902	RPC del clúster de NetApp
904	RPC del clúster de NetApp
905	RPC del clúster de NetApp
910	RPC del clúster de NetApp
911	RPC del clúster de NetApp
913	RPC del clúster de NetApp

Puerto/protocolo	Descripción
914	RPC del clúster de NetApp
915	RPC del clúster de NetApp
918	RPC del clúster de NetApp
920	RPC del clúster de NetApp
921	RPC del clúster de NetApp
924	RPC del clúster de NetApp
925	RPC del clúster de NetApp
927	RPC del clúster de NetApp
928	RPC del clúster de NetApp
929	RPC del clúster de NetApp
931	RPC del clúster de NetApp
932	RPC del clúster de NetApp
933	RPC del clúster de NetApp
934	RPC del clúster de NetApp
935	RPC del clúster de NetApp
936	RPC del clúster de NetApp
937	RPC del clúster de NetApp
939	RPC del clúster de NetApp
940	RPC del clúster de NetApp
951	RPC del clúster de NetApp
954	RPC del clúster de NetApp
955	RPC del clúster de NetApp
956	RPC del clúster de NetApp
958	RPC del clúster de NetApp
961	RPC del clúster de NetApp
963	RPC del clúster de NetApp
964	RPC del clúster de NetApp
966	RPC del clúster de NetApp
967	RPC del clúster de NetApp
7810	RPC del clúster de NetApp
7811	RPC del clúster de NetApp
7812	RPC del clúster de NetApp
7813	RPC del clúster de NetApp

Puerto/protocolo	Descripción
7814	RPC del clúster de NetApp
7815	RPC del clúster de NetApp
7816	RPC del clúster de NetApp
7817	RPC del clúster de NetApp
7818	RPC del clúster de NetApp
7819	RPC del clúster de NetApp
7820	RPC del clúster de NetApp
7821	RPC del clúster de NetApp
7822	RPC del clúster de NetApp
7823	RPC del clúster de NetApp
7824	RPC del clúster de NetApp

Sistemas de almacenamiento

AFX

NetApp visión general de AFX: aprende sobre NetApp AFX

NetApp AFX sigue siendo ONTAP, simplemente es una forma diferente de aprovechar las ventajas de ONTAP. NetApp AFX ofrece una arquitectura desagregada para cargas de trabajo NAS y de objetos, mientras sigue proporcionando el software ONTAP con todas las funciones que ya conoces y te encantan.

Una evolución de la innovación: NetApp ONTAP

NetApp ONTAP se creó en 1992 como una nueva forma de servir cargas de trabajo NFS a múltiples clientes, mientras revolucionaba el rendimiento, la resiliencia de los datos, las copias en un punto en el tiempo y más. Originalmente solo era compatible con NFSv2, pero a medida que crecía la demanda de versiones de NFS más recientes, otros protocolos de datos y más funciones de protección de datos, NetApp ONTAP tuvo que evolucionar.

A continuación se muestra una cronología abreviada de algunas de las principales evoluciones de ONTAP que han tenido lugar en los últimos 30 años.

La evolución de NetApp ONTAP

Década	Funciones
1990s	NFSv2, NFSv3, CIFS, instantáneas, sistema de archivos WAFL, AutoSupport, SnapMirror
2000s	SnapVault, SnapLock, NFSv4, protocolos de bloques, FlexVols, FlexClone, GX/escalado horizontal, deduplicación, clones de archivo
2010s	ONTAP en clúster, eficiencias de almacenamiento en línea, NFSv4.1/pNFS, NVMe, RAID-TEC, volúmenes FlexGroup, cifrado de volúmenes, AFF, Cloud Volumes ONTAP, QoS, FabricPool, Azure NetApp Files (ANF), Google Cloud NetApp Volumes (GCNV), All SAN Array (ASA)
2020s	SnapMirror Business Continuity, FlexCache, ONTAP S3, IPsec, Protección autónoma contra ransomware, SnapMirror dentro y fuera de ANF y GCNV, Amazon FSxN, ASAr2, NetApp AFX you are here

NetApp personalidades de ONTAP

Durante años, ONTAP funcionó como una única plataforma unificada, combinando archivos, bloques y objetos en un único sistema. Esto posicionó a ONTAP como la navaja suiza del centro de datos, una plataforma que podía hacer todo lo que le pidieras.

Sin embargo, a medida que las aplicaciones evolucionaron y los requisitos de los centros de datos cambiaron con una serie de cambios en el sector de TI, creció la demanda de plataformas que pudieran hacer cosas

específicas. Como resultado, ahora hay algunas formas diferentes de consumir ONTAP.

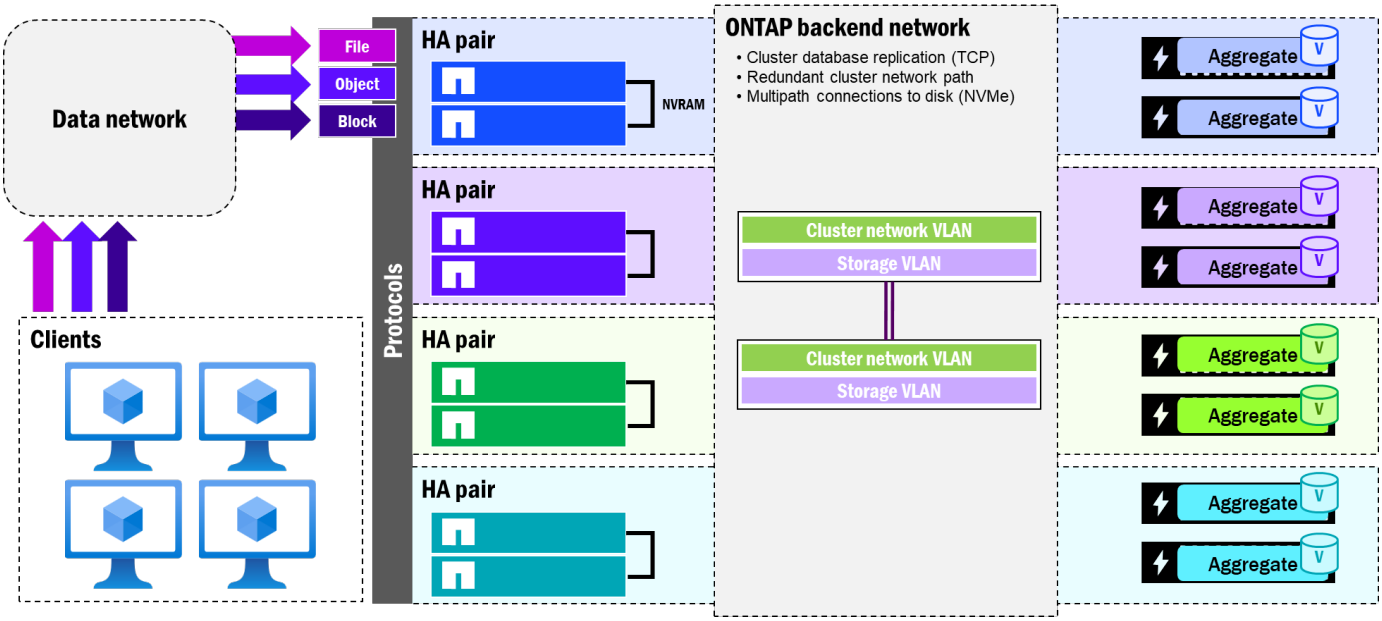
NetApp ONTAP personalidades

Personalidad de ONTAP	Descripción
ONTAP unificado	El mismo ONTAP de siempre, que sigue desarrollándose y mejorándose activamente.
Todas las matrices SAN	ONTAP que solo admite iSCSI, FCP y NVMe sobre FC/TCP y proporciona funcionalidad de controlador activo/activo, así como conceptos desagregados en ASAr2.
ONTAP residente en la nube	ONTAP que se ejecuta en la nube; ya sea en sistemas de metal desnudo ubicados en un centro de datos en la nube o en instancias de ONTAP virtualizadas.
ONTAP/AFX desagregado	ONTAP mediante arquitectura desagregada para cargas de trabajo NAS y de objetos de alto rendimiento.

Visión general de la arquitectura ONTAP unificada

El siguiente diagrama muestra la arquitectura general de ONTAP unificado, con una descripción de cómo encaja todo a continuación.

Arquitectura general de ONTAP



Algunos aspectos clave de la arquitectura de ONTAP:

- Soporte de archivos, objetos y bloques
- Los protocolos se sirven a través de una red de datos de cliente front-end
- Se pueden agrupar varios nodos independientes

- Cada nodo puede proporcionar direcciones IP flotantes independientes para casos de uso de datos y gestión
- Los nodos agrupados en clúster se conectan a un conmutador backend proporcionado por NetApp a través de una VLAN de clúster
- Los nodos se presentan como pares de HA para proporcionar resiliencia en caso de cortes de hardware o de energía
- Los pares de HA tienen tarjetas NVRAM conectadas directamente que se replican para proteger las escrituras
- A cada nodo se le asigna al menos un agregado y posee un subconjunto del número total de discos
- En las conmutaciones por error, los discos de un nodo se reasignan al socio de alta disponibilidad (y solo al socio de alta disponibilidad)
- Las estanterías de discos suelen estar conectadas directamente a los nodos mediante cableado multivía, pero los sistemas de gama alta introducen el concepto de redes de almacenamiento en el mismo conmutador backend del clúster
- Los volúmenes (FlexVols y FlexGroup volumes) proporcionan los puntos de entrada al almacenamiento para el acceso a los datos

¿Qué es NetApp AFX?

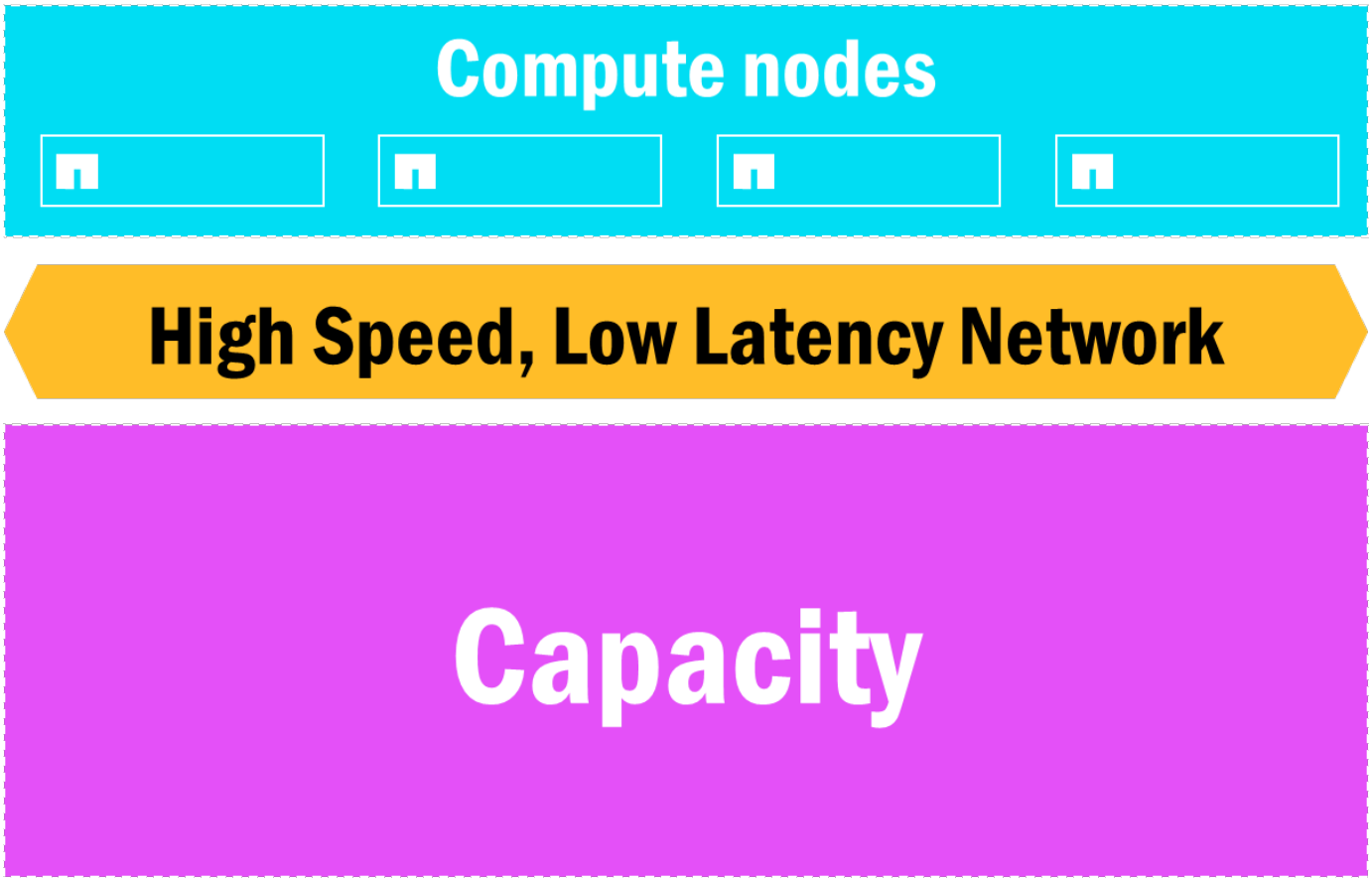
Hay que tener en cuenta que NetApp AFX sigue siendo ONTAP.

Es simplemente una forma diferente de aprovechar las ventajas de ONTAP. La misma imagen que instalarías para tus sistemas Unified ONTAP o All SAN Array es la misma que se utiliza con NetApp AFX. El código base es idéntico, pero la forma en que los sistemas arrancan determina qué ruta de código se sigue, cómo se presenta el almacenamiento backend y qué funciones y protocolos son compatibles.

NetApp AFX ofrece una arquitectura desagregada para cargas de trabajo NAS y de objetos sin dejar de proporcionar el software de ONTAP que ya conoces y te encanta. ONTAP desagregado hace referencia a una arquitectura de almacenamiento en la que cada nodo controlador de NetApp ve la misma capacidad mediante switches de red redundantes y una red de alta velocidad y baja latencia. Este enfoque permite que los nodos controladores y la capacidad de almacenamiento se amplíen de forma independiente para satisfacer mejor las necesidades de las distintas cargas de trabajo de alto rendimiento. En otras palabras, cuando necesites más rendimiento, simplemente añade nodos controladores. Si necesitas más capacidad, añade shelf enclosures. Esto les da a los administradores de almacenamiento la flexibilidad de presentar una solución de almacenamiento más rentable a sus usuarios finales.

Dado que ningún nodo controlador posee discos de forma independiente, tampoco existen agregados físicos con sus propias limitaciones de capacidad y rendimiento. En su lugar, la capacidad se presenta como un modelo compartido con el que todos los nodos pueden interactuar y que ONTAP puede gestionar automáticamente.

ONTAP desagregado



Términos y conceptos clave

A continuación encontrarás términos directamente relacionados con AFX. Para terminología específica de ONTAP, consulta la documentación del producto.

"Documentación del producto ONTAP".

ONTAP desagregado

Se refiere a la nueva arquitectura impulsada por ONTAP que ofrece la posibilidad de escalar el cómputo y la capacidad de forma independiente entre sí. El término "ONTAP desagregado" no es un nombre de producto, sino un medio para diferenciar entre ONTAP unificado y las arquitecturas NetApp AFX.

NetApp AFX

NetApp AFX es el nombre oficial del producto para la arquitectura desagregada de ONTAP y se anunció en NetApp Insight 2025.

Nodos de cómputo

Un nodo de computación en NetApp AFX se refiere al nodo controlador de almacenamiento (y a menudo se utiliza indistintamente en la documentación). Estos nodos no tienen disco integrado y están pensados para ser totalmente modulares y permitir la escala independiente que proporciona la arquitectura ONTAP desagregada.

Zona de disponibilidad de almacenamiento

Una zona de disponibilidad de almacenamiento (SAZ) es el único grupo de capacidad en un clúster AFX de NetApp, donde todos los discos se comparten entre todos los nodos. La SAZ permite funcionalidades como

capacidad compartida, alto rendimiento, deduplicación global y más.

Novedades en NetApp AFX

Esta sección cubre las últimas actualizaciones de NetApp AFX y se actualizará con cada nueva versión. Vuelve aquí periódicamente para obtener nueva información, pero también revisa las notas de la versión.

¿Cuáles son las novedades de la última versión de NetApp ONTAP para AFX?

Última publicación:

ONTAP 9.19.1RC1 (a partir de mayo de 2026)

Nuevas funciones en NetApp AFX:

- Deduplicación global
- Eficiencia de almacenamiento dinámica
- Readahead avanzado
- compatibilidad con 32 nodos
- Compatibilidad con 32PB
- 512 volúmenes constituyentes por volumen FlexGroup

Historial de versiones

Versión	Fecha	Historial de versiones de documentos
Versión 1.0	junio de 2026	Lanzamiento inicial

Cómo la arquitectura NetApp AFX difiere de ONTAP unificado

NetApp AFX introduce diferencias arquitectónicas significativas respecto a ONTAP unificado en cómo se presenta el almacenamiento, cómo interactúan los nodos con los discos y cómo se gestiona la capacidad.

Anteriormente, mostramos una imagen general de cómo la arquitectura unificada de ONTAP proporciona almacenamiento de archivos, objetos y bloques de datos a través de pares de HA conectados directamente que poseen sus propios conjuntos de discos y presentan capacidad física a través de agregados de discos. En esta sección, analizaremos con más detalle algunas de las principales diferencias entre las arquitecturas unificadas de ONTAP y NetApp AFX.

Cómo saber si un sistema está ejecutando NetApp AFX

La principal forma de ver si tu sistema está ejecutando NetApp AFX es ejecutar el siguiente comando:

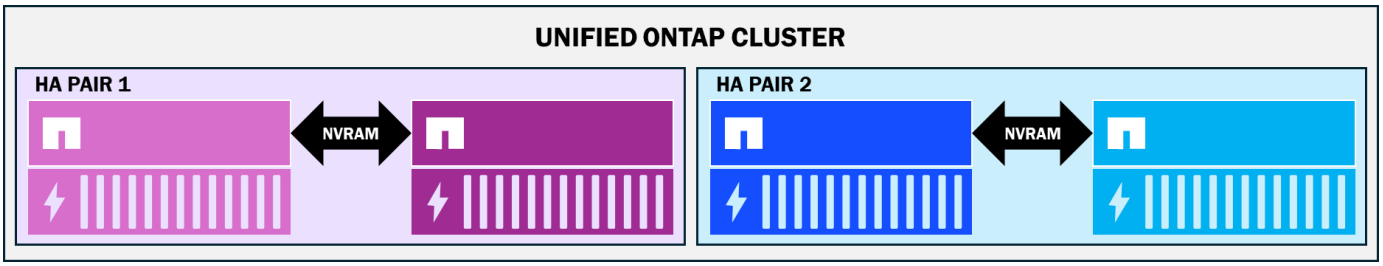
```
AFX::> node show -fields personality
node             personality
---------------- -----------
afx-01           AFX
afx-02           AFX
```

Otra pista es la nueva Storage Availability Zone, pero ese también es un concepto disponible en NetApp All-SAN Arrays (ASA). Puedes ver tu capacidad a través de ese comando.

```
AFX::> storage availability-zone show
                     Availability Zone Name: storage_availability_zone_0
                     Availability Zone UUID: 545cb59f-32e9-11f1-a2f5-
d039eabdd925
                                 Total Size: 69.59TB
                              Physical Used: 837.1GB
                       Physical Used Percent: 1%
                                  Available: 68.77TB
                              Metadata Used: 837.1GB
                  Log and Recovery Metadata: 834.6GB
                              Delayed Frees: 2.50GB
 Physical User Data Without Snapshot Copies: 17.24MB
  Logical User Data Without Snapshot Copies: 17.24MB
   Efficiency Ratio Without Snapshot Copies: 1.00:1
              Space Full Threshold Percent: 98%
        Space Nearly Full Threshold Percent: 95%
```

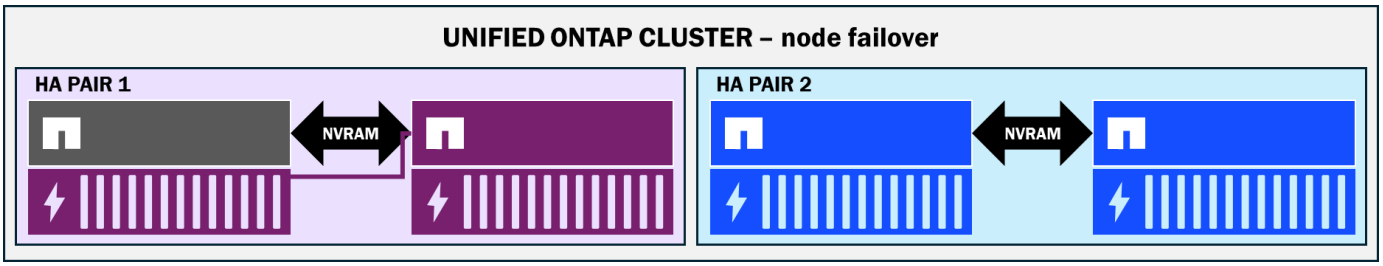
Relaciones entre nodos y discos

En la arquitectura unificada de ONTAP, las lecturas y escrituras se dirigen a un subconjunto específico de discos. Así que, aunque tengas 24 estanterías de discos en un clúster de 24 nodos (una estantería por nodo), en cualquier momento cada nodo solo puede acceder directamente a una estantería de discos, lo que limita la capacidad y el rendimiento disponibles en el clúster.



Además, como la NVRAM está conectada directamente entre pares de HA, los nodos deben residir físicamente uno al lado del otro y están más estrechamente acoplados como objetivos de conmutación por error. Por ejemplo, cuando un nodo conmuta por error a su nodo asociado, los únicos discos a los que tiene acceso físico son los discos del dominio del par de HA.

Clúster ONTAP unificado durante la conmutación por error de HA

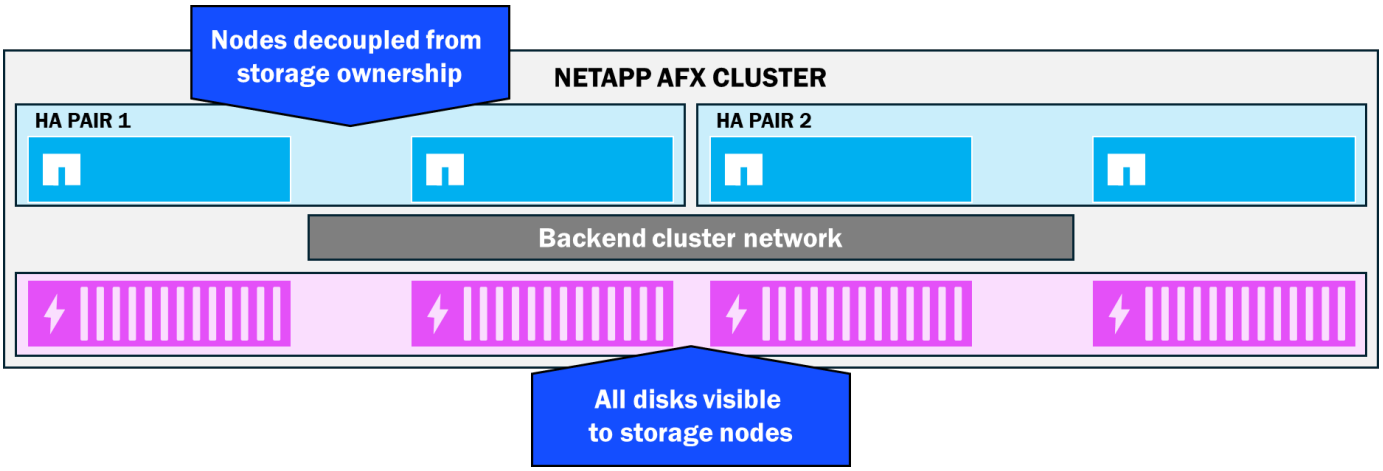


En NetApp AFX, hay algunos cambios importantes en la forma en que los discos se presentan a los nodos de cálculo.

Todos los discos son visibles para todos los nodos de almacenamiento—sin propiedad de disco

En NetApp AFX, los nodos y las estanterías están todos conectados al mismo switch backend, lo que hace posible que ONTAP amplíe el dominio de visibilidad global de los discos a toda la pila. Como resultado, ningún nodo posee discos específicos. En su lugar, todos los discos participan en un único pool de capacidad llamado Storage Availability Zone, que proporciona una gestión de capacidad más sencilla y un mayor potencial de rendimiento (más discos disponibles significa más rendimiento disponible).

NetApp Zona de disponibilidad de almacenamiento AFX

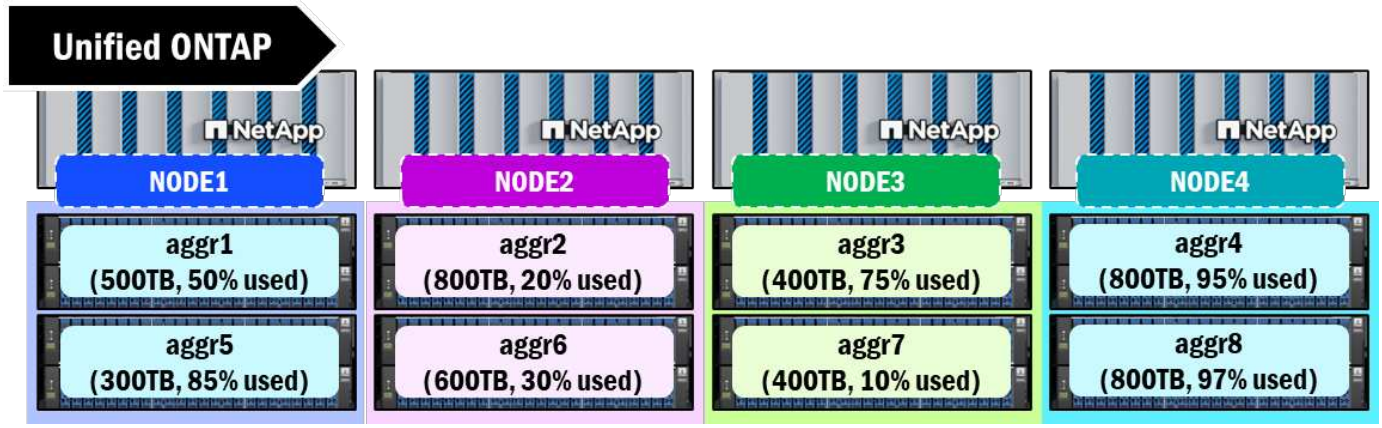


No más agregados físicos

Unified ONTAP agrupa los discos en grupos RAID y luego los combina en una construcción de capacidad conocida como agregado. Este agregado es la forma en que la capacidad física se presenta al almacenamiento y es el límite de espacio disponible para crear volúmenes para servir datos a los usuarios finales. Cada nodo debe tener al menos un agregado asignado y estos agregados tienen un límite actual de 800TB. Una vez alcanzado ese límite, no hay más espacio disponible para escrituras adicionales.

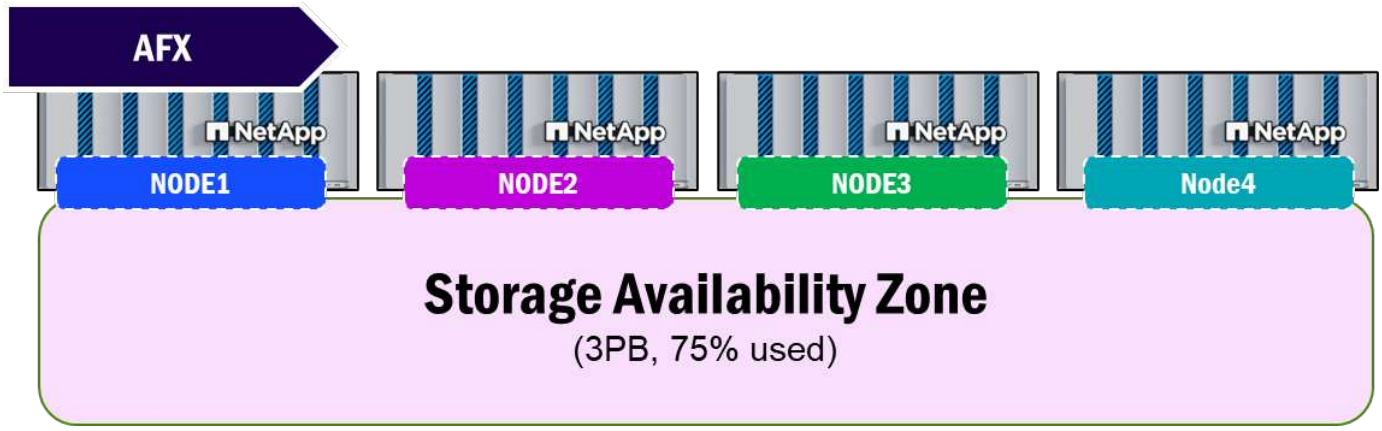
Los agregados físicos también pueden presentar algunos desafíos de gestión de capacidad, ya que los administradores de almacenamiento a veces tendrán que mover manualmente los volúmenes para mantener un equilibrio de capacidad entre los nodos del clúster. Estos desafíos también pueden magnificarse cuando se aprovecha una arquitectura de volumen de escalado horizontal (como un volumen FlexGroup). Los agregados también pueden variar en tamaño, cantidad de discos, tipos de disco, etc., lo que también puede crear algunas diferencias de rendimiento a medida que atraviesas los nodos.

Agregados en ONTAP unificado



NetApp AFX toma el concepto de un agregado físico y lo virtualiza, lo convierte en un agregado gestionado por ONTAP y, a continuación, traslada la gestión de la capacidad física de una metodología por nodo a otra por clúster a través de la nueva Storage Availability Zone. Este grupo único de capacidad proporciona un enfoque de gestión de espacio del tipo "lo que ves es lo que hay".

NetApp Zona de disponibilidad de almacenamiento AFX



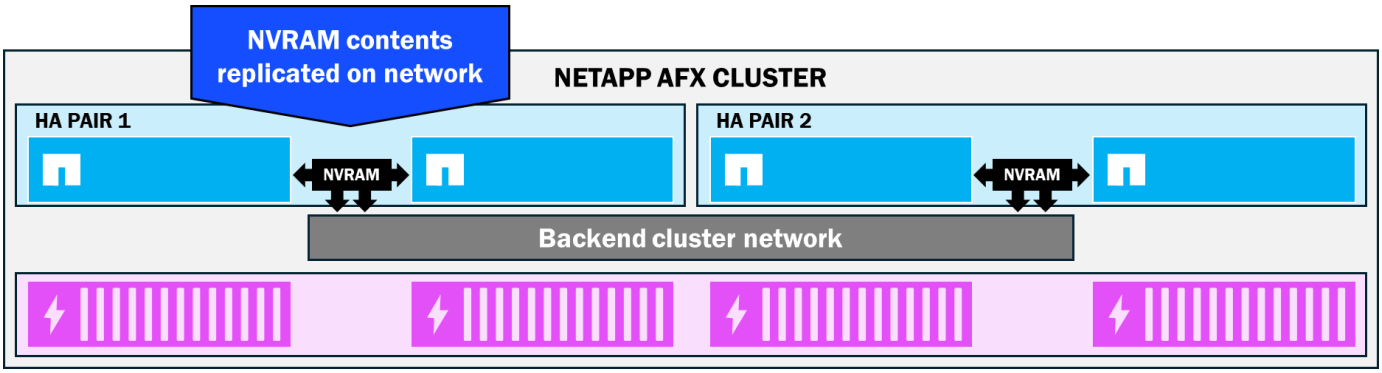
La NVRAM pasa de la conexión directa a la replicación conmutada

ONTAP utiliza NVRAM como una etapa intermedia para proteger las escrituras entrantes en un clúster. Cada nodo en un clúster ONTAP tiene una tarjeta NVRAM respaldada por batería. Cuando se envía una escritura a un volumen desde un cliente, primero se almacena en NVRAM. Luego, el contenido de la NVRAM se vuelca al disco cuando la NVRAM se llena o cuando expira un temporizador de 10s (lo que ocurra primero). Esto se conoce como punto de coherencia.

El contenido de la NVRAM también se replica constantemente entre los pares de HA, lo que ayuda aún más a proteger la coherencia de los datos, porque en caso de fallo de un nodo, el contenido de la NVRAM se conservará en el nodo superviviente y se comprometerá al disco.

En los clústeres ONTAP unificados, las tarjetas NVRAM entre pares de HA están conectadas directamente entre sí. NetApp AFX traslada la replicación de NVRAM a la red backend del clúster. Como resultado, los nodos asociados de HA no tienen un requisito de distancia entre nodos tan estricto. En su lugar, los pares de HA pueden separarse hasta la distancia máxima de ethernet.

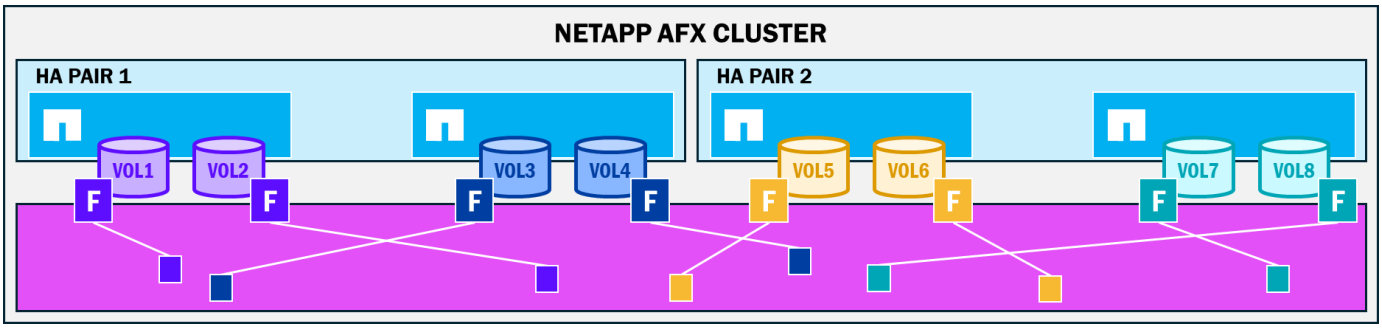
NetApp AFX NVRAM replicación



Datos escritos en cualquiera (y todos) los discos de la zona de disponibilidad

NetApp AFX elimina el concepto de propiedad del disco y traslada la construcción física agregada a un enfoque virtualizado gestionado por ONTAP, donde la capacidad adquirida para el clúster está disponible para todos los nodos conectados al clúster. Con AFX, todos los nodos tienen la capacidad de escribir en todos y cada uno de los discos de la zona de disponibilidad de almacenamiento, independientemente de cuál sea la propiedad del nodo:volumen. Los nodos siguen teniendo un concepto de propiedad de volumen, ya que las escrituras siguen teniendo una ruta a través de la NVRAM, pero esos datos pueden aterrizar en cualquier lugar de la capacidad disponible. Esto significa que un mayor número de discos puede participar en una sola carga de trabajo, lo que proporciona beneficios de rendimiento.

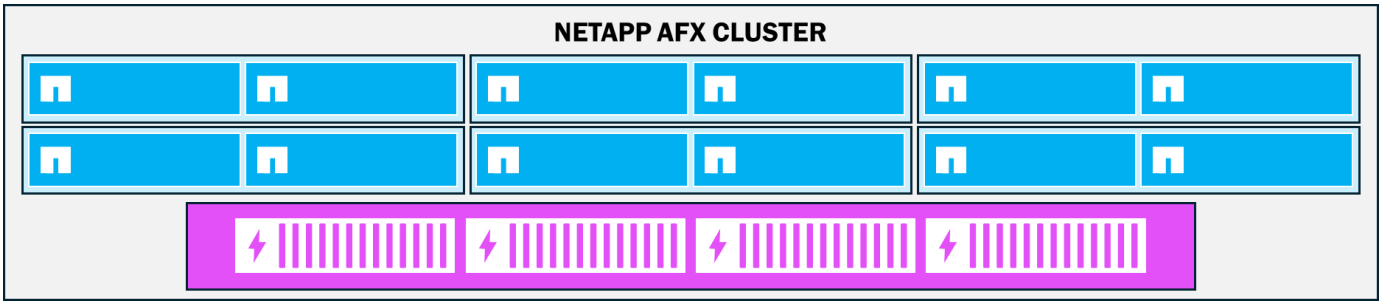
Cómo se ubican los datos en una Storage Availability Zone



Escalado independiente de capacidad y nodos de cómputo

Con los recursos de hardware desacoplados en la arquitectura NetApp AFX, los nodos ya no necesitan que se añadan discos asociados unos junto a otros. Cuando un clúster se está quedando sin recursos relacionados con el rendimiento, como RAM, CPU o el rendimiento de red, solo es necesario añadir nodos de almacenamiento al clúster y se puede aprovechar la Storage Availability Zone existente. Por el contrario, si lo que se necesita es capacidad, solo habría que añadir shelves a la mezcla. Esta flexibilidad asegura que solo compres los recursos que vas a necesitar, evitando así el sobreaprovisionamiento.

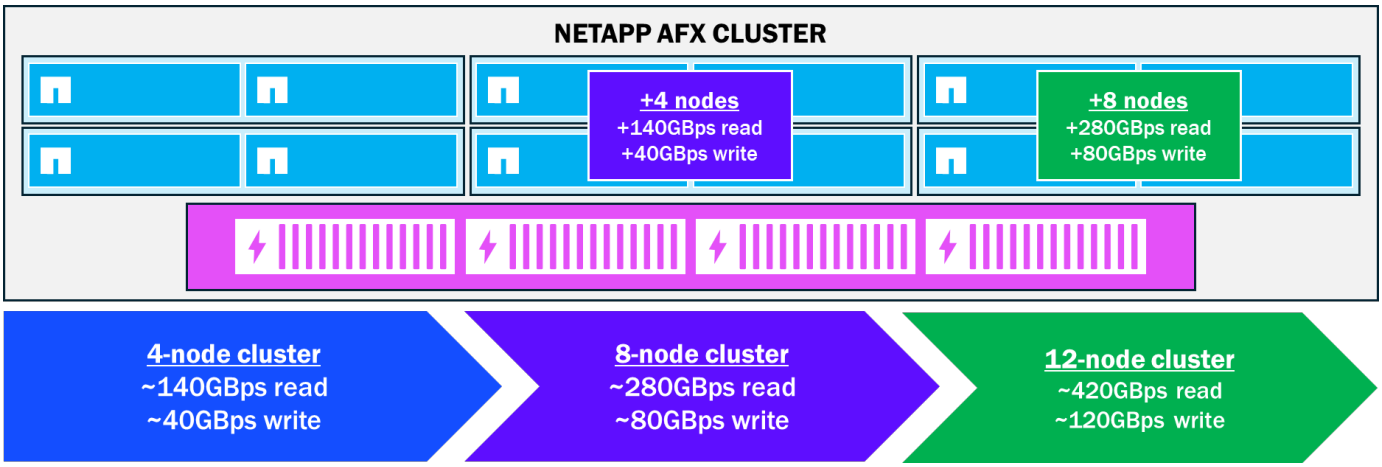
NetApp AFX – escala independiente



Escalado lineal del rendimiento de los nodos

A medida que se añaden nodos a un clúster AFX, se introducen más CPU, RAM y recursos de red en la carga de trabajo. A medida que estos recursos se incorporan al entorno, los aumentos de rendimiento son lineales por naturaleza. El gráfico siguiente muestra cómo aumentaría ese rendimiento a medida que se añaden nodos.

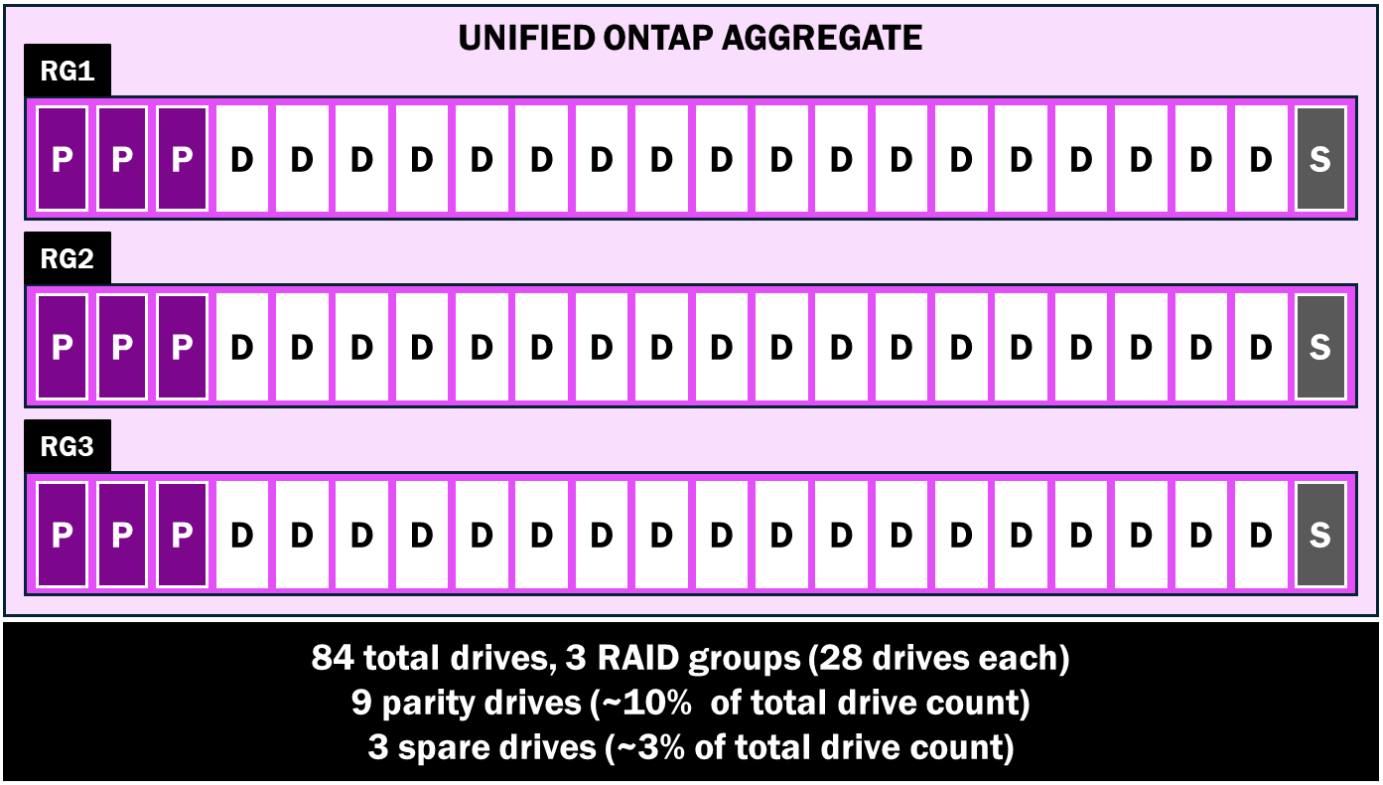
Aumento lineal del rendimiento al añadir nodos AFX a NetApp



Grupos RAID más grandes, menos unidades de paridad

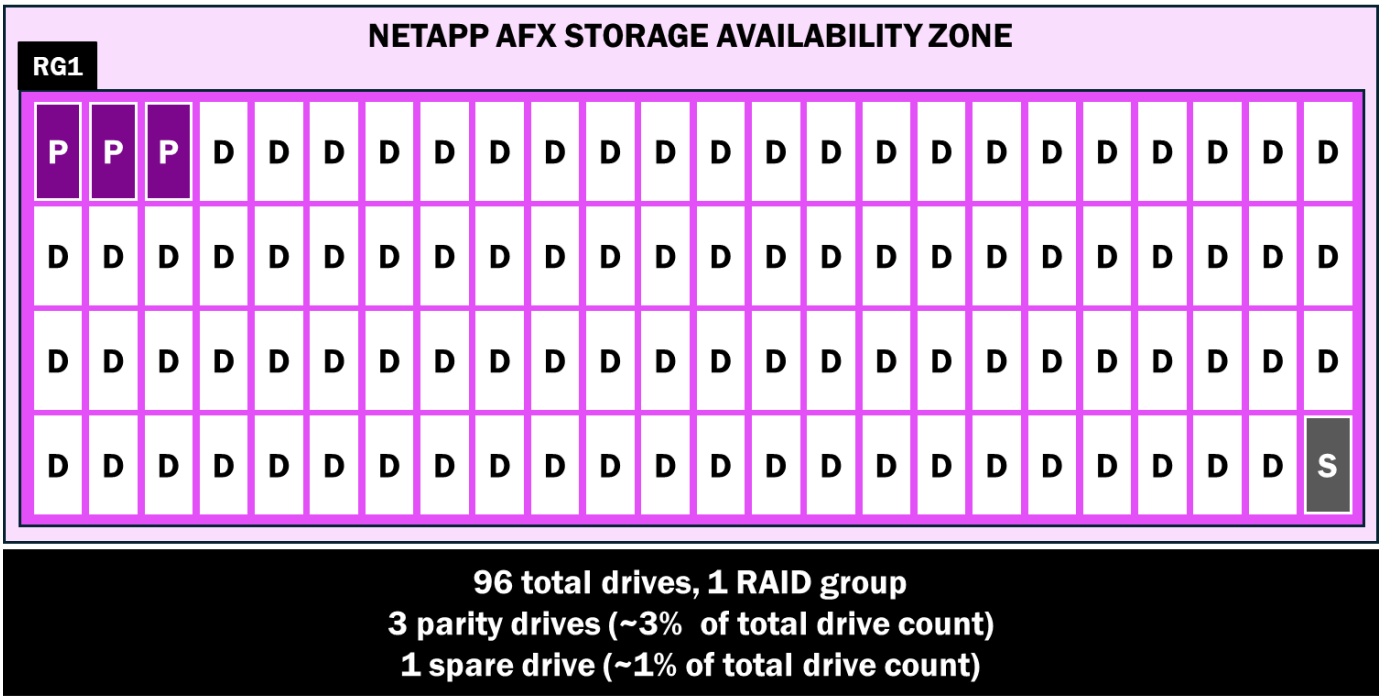
ONTAP ofrece una combinación de protección de datos y rendimiento para discos a través de grupos RAID, en concreto RAID-TEC, que ofrece protección de triple paridad en caso de fallos de disco. RAID-TEC puede sobrevivir hasta a tres fallos de disco simultáneos en un grupo RAID. En ONTAP unificado, los grupos RAID tienen un número máximo de discos de 28, donde 3 unidades se gastan en paridad y 1 unidad se reserva como repuesto. Como resultado, 24 de las 28 unidades se utilizan para operaciones de datos/RAID stripes.

Grupos RAID unificados de ONTAP



NetApp AFX sigue aprovechando RAID-TEC, pero aumenta el tamaño del grupo RAID a 96 unidades y solo requiere 3 unidades de paridad y 1 de repuesto. Los grupos RAID más grandes ofrecen un mayor rendimiento general, mientras que la exposición a fallo de unidad se minimiza gracias a una combinación de bajas tasas de fallo de las SSD, una distribución más uniforme de las operaciones entre un conjunto más grande de unidades, así como mejoras en las reconstrucciones de las unidades de datos a partir de la paridad en NetApp AFX.

Grupo RAID de zona de disponibilidad de almacenamiento AFX de NetApp



La siguiente tabla aproxima la cantidad de capacidad utilizable en bruto para 84 discos en ONTAP unificado y NetApp AFX con distintos tamaños de unidad.

Comparación aproximada de capacidad bruta, 84 unidades – Unified ONTAP y NetApp AFX

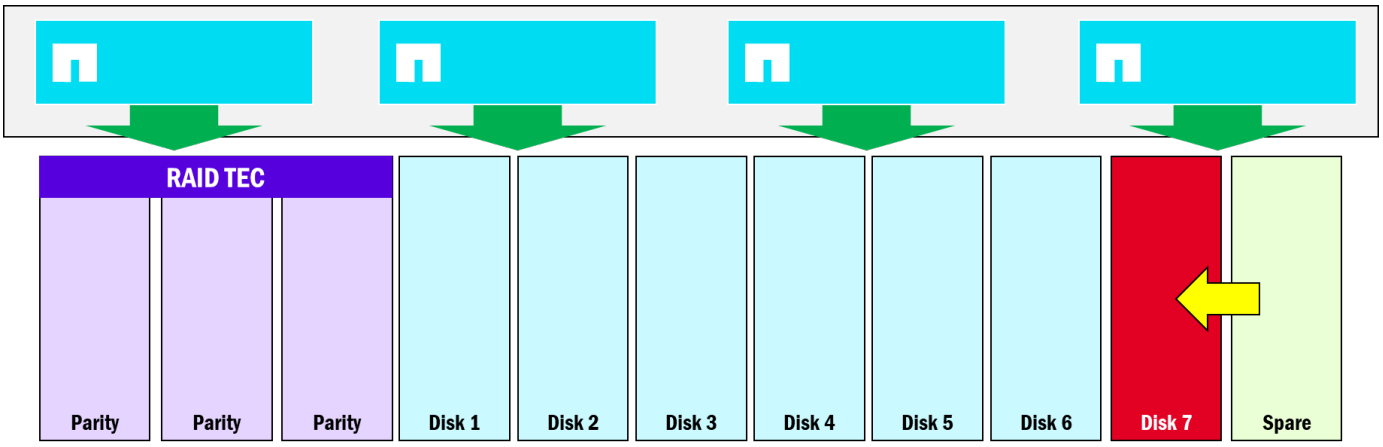
Tamaño de la unidad	Capacidad bruta aproximada (Unificada)	Capacidad bruta aproximada (AFX)
7,6 TB	~547,2TB	~608TB (+60,8TB)
15,3 TB	~1101,6TB	~1224TB (+122.4TB)
30,6 TB	~2203,2TB	~2448TB (+244,7TB)
60,1 TB	~4327,2TB	~4808TB (+480.8TB)

Tiempos de reconstrucción de fallos de disco más rápidos

En ONTAP unificado, cada nodo es propietario de un subconjunto de discos de la pila de almacenamiento. Esto significa que ese nodo solo escribe en esos discos, pero también que las reconstrucciones de disco solo las gestiona un único nodo en caso de fallo de unidad.

NetApp AFX evita la necesidad de la propiedad del disco. Como resultado, todas las unidades se pueden escribir desde un solo nodo si es necesario. Eso también significa que cuando una unidad necesita ser reconstruida a partir de la paridad, todos los nodos en el clúster participan, así que las reconstrucciones de unidades pueden ocurrir más rápido que si un solo nodo tuviera que hacerlo solo.

Reconstrucción de discos en NetApp AFX

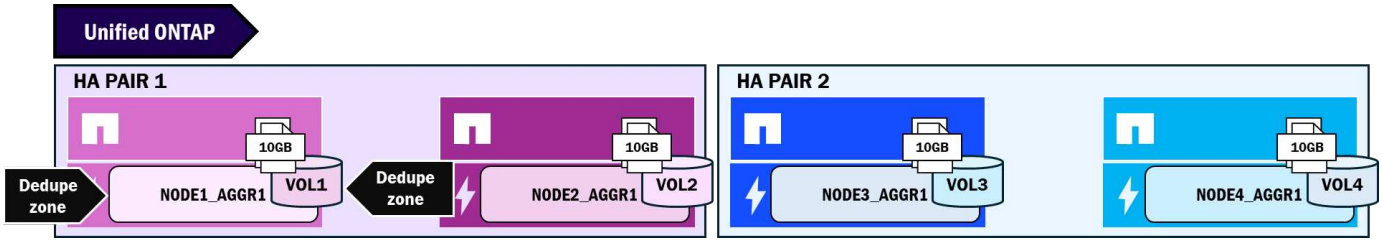


Dominios de deduplicación

La deduplicación permite a un sistema de almacenamiento encontrar bloques duplicados en su sistema de archivos y luego crear punteros a un único bloque para reducir la cantidad total de capacidad utilizada. En unified ONTAP, la deduplicación sigue un límite específico para los bloques que se pueden reducir. Esos límites dependen del tipo de deduplicación en uso. En general:

- Deduplicación basada en volumen → Límite de volumen
- Deduplicación cruzada de volúmenes → Límite de agregado

Dominios de deduplicación unificados de ONTAP



La siguiente tabla muestra los comportamientos de capacidad para datos duplicados en diferentes escenarios en ONTAP unificado. A medida que las copias de archivos abarcan nodos y agregados (y, por tanto, dominios de deduplicación), el ahorro de espacio se reduce.

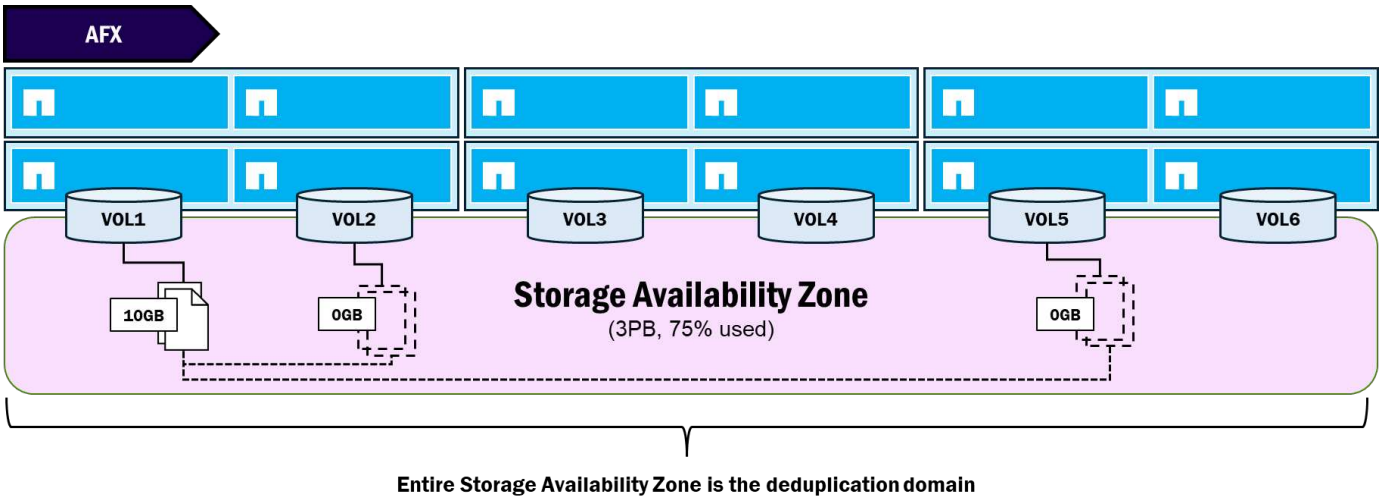
Comportamientos de deduplicación en diferentes escenarios para archivos idénticos de 10GB – ONTAP unificado

Escenario	Espacio utilizado
Cuatro copias del mismo archivo de 10GB, mismo volumen (deduplicación de volumen)	10 GB
Cuatro copias del mismo archivo de 10 GB, volúmenes diferentes, mismo agregado (deduplicación entre volúmenes activada)	10 GB
Cuatro copias del mismo archivo de 10GB, 4 volúmenes diferentes, 4 agregados diferentes (deduplicación entre volúmenes activada)	40 GB

Dado que NetApp AFX elimina los agregados físicos y traslada la gestión de la capacidad a la nueva Storage Availability Zone, los límites del dominio de deduplicación también cambian. En AFX, el dominio de deduplicación se encuentra en el nivel de volumen (como ONTAP unificado) y en el nodo (en lugar del agregado) antes de 9.19.1.

A partir de ONTAP 9.19.1, AFX admite un dominio de deduplicación global a nivel de Storage Availability Zone, por lo que todos los bloques duplicados del storage pool del clúster reciben el mismo tratamiento.

NetApp AFX – Dominio de deduplicación global (ONTAP 9.19.1)



La siguiente tabla muestra los comportamientos de capacidad para datos duplicados en diferentes escenarios en NetApp AFX.

Comportamiento de la deduplicación en distintos escenarios para archivos idénticos de 10 GB – NetApp AFX

Escenario	Espacio utilizado
Cuatro copias del mismo archivo de 10GB, mismo volumen (deduplicación de volumen)	10GB (9.18.1) 10GB (9.19.1)
Cuatro copias del mismo archivo de 10GB, volúmenes diferentes, mismo nodo (deduplicación entre volúmenes activada)	10GB (9.18.1) 10GB (9.19.1)
Cuatro copias del mismo archivo de 10 GB, 4 volúmenes diferentes, 4 nodos diferentes (deduplicación entre volúmenes activada)	40GB (9.18.1) 10GB (9.19.1)

Funciones eliminadas/no compatibles

NetApp AFX está diseñado para cargas de trabajo NAS y de objetos de alto rendimiento, en particular (pero no exclusivamente) las del espacio de entrenamiento e inferencia de IA. Con el diseño de NetApp AFX, se tomaron algunas decisiones para desactivar algunas de las funciones de ONTAP.

- Debido al enfoque en NAS de alto rendimiento y objetos, las cargas de trabajo de bloque se han eliminado de la solución NetApp AFX. No hay soporte para protocolos de datos FCP, iSCSI o NVMe y no hay planes para añadir protocolos de bloque.
- Disaggregated es sinónimo de de-aggregated, lo que significa que se han eliminado los agregados (al menos como concepto de administración de almacenamiento físico). La eliminación del agregado físico no solo simplifica la gestión de la capacidad en ONTAP, sino que también proporciona el mecanismo que permite disponer de un único pool de capacidad.
- La eliminación de los agregados significa que también se eliminan las funciones específicas de los agregados. Metrocluster, por ejemplo, aprovecha la duplicación a nivel de agregado para sus funciones de conmutación por error de sitio. Por lo tanto, Metrocluster también se elimina de NetApp AFX. En su lugar, la funcionalidad de conmutación por error de sitio será proporcionada por la nueva función SnapMirror Active-Sync para NAS ofrecida en ONTAP 9.19.1GA.
- La función de jerarquización de datos en frío denominada FabricPool tampoco está disponible actualmente para NetApp AFX, ya que también es específica de cada agregado.
- Los movimientos de volumen basados en copias ya no son necesarios en NetApp AFX, debido a la nueva arquitectura de capacidad. Para obtener más información, consulta Movimientos de volúmenes con copia cero.
- La eliminación de funciones también implica algunos cambios en la CLI/GUI/API de REST, por lo que también se eliminarán los comandos o las llamadas a la API de las funciones que ya no sean compatibles.
- ZAPI no está disponible actualmente para NetApp AFX.
- Descarga de copia de datos NFS para virtualización (volúmenes FlexGroup con distribución granular de datos solamente)

Cambios en la gestión de ONTAP

En general, la gestión de NetApp AFX no cambia los mecanismos utilizados para gestionar un clúster. Los administradores pueden seguir utilizando la CLI, la GUI y las API de REST para iniciar sesión y configurar un clúster. Pero NetApp AFX sí presentó una oportunidad para mejorar algunos aspectos de cómo se llevan a cabo las operaciones de gestión del almacenamiento.

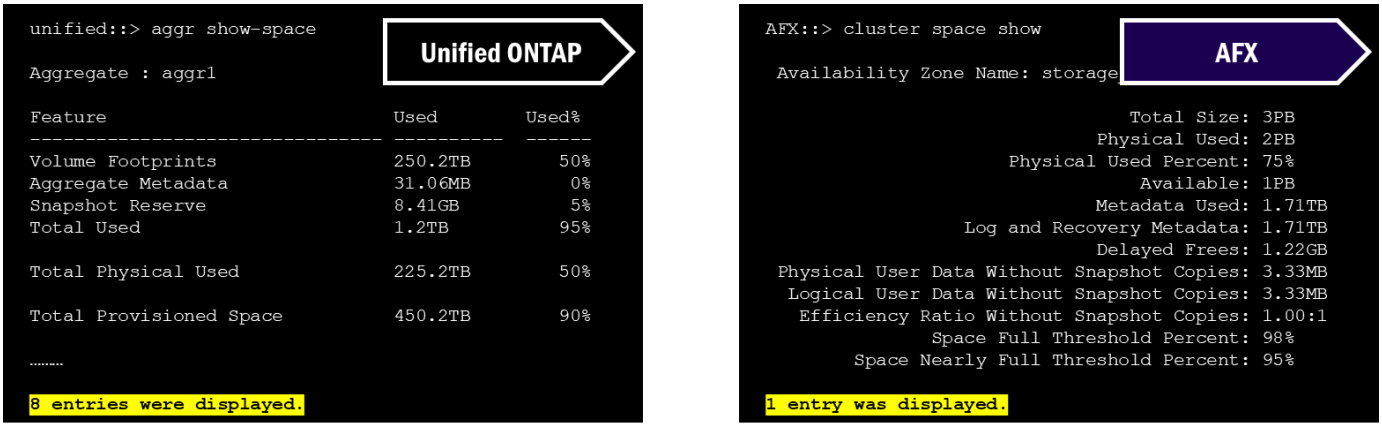
Gestión más sencilla de la capacidad

La NetApp AFX Storage Availability Zone reduce los puntos finales de gestión de un enfoque basado en nodos y agregados a un único pool de capacidad disponible para todo el clúster. A medida que los volúmenes crecen y se reducen, ONTAP toma y devuelve capacidad automáticamente a y desde la Storage Availability Zone.

Gracias a ello, los administradores de almacenamiento ya no tienen que preocuparse de localizar y gestionar el espacio libre disponible en hasta 24 nodos y, potencialmente, cientos de agregados. En su lugar, solo hay un lugar donde se gestiona y visualiza la capacidad.

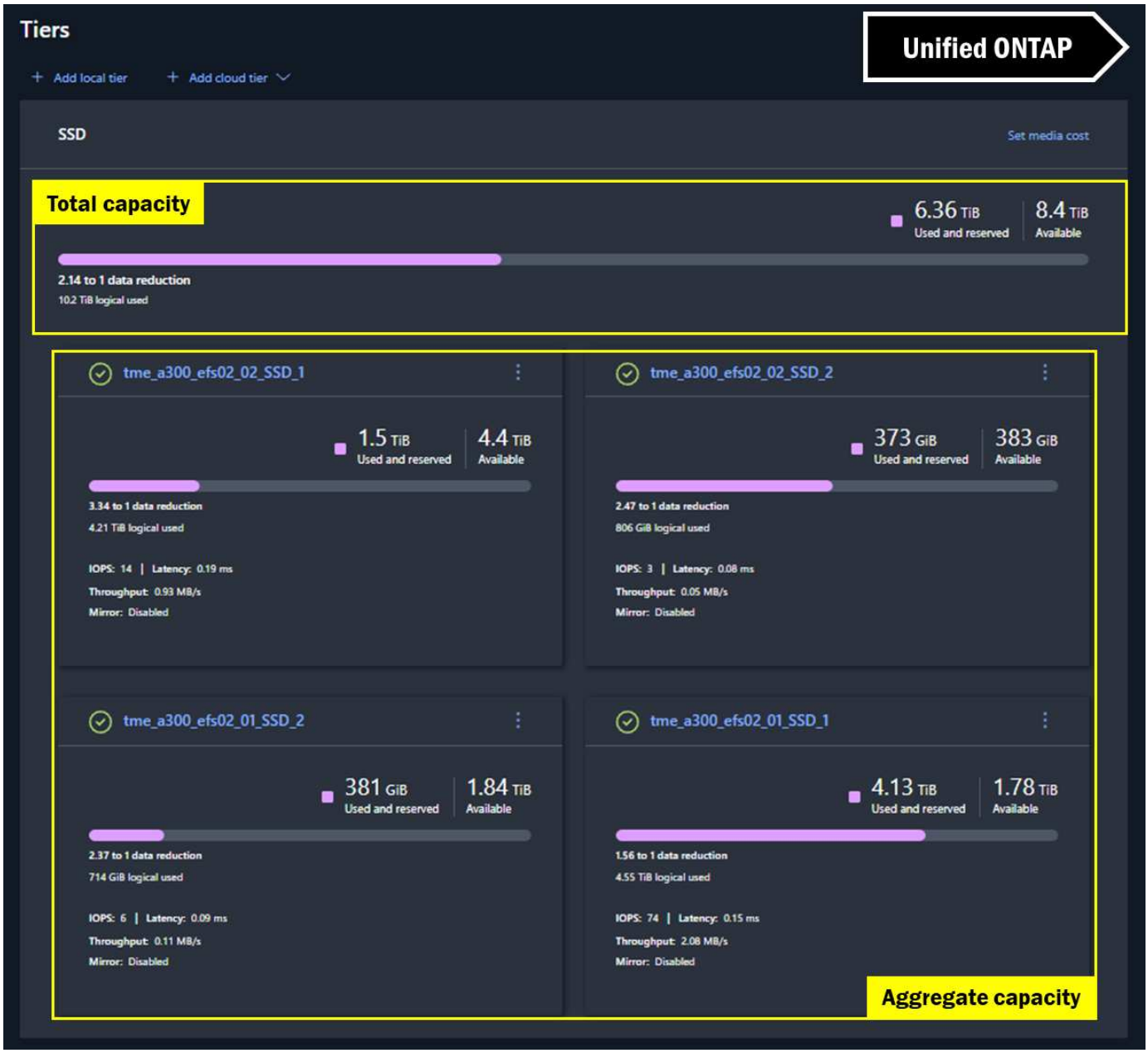
Por ejemplo, en la CLI de ONTAP unificado, si quieres ver la información sobre la capacidad física total de un clúster, usarías “aggregate show-space”, que luego mostraría cada entrada de aggregate. En NetApp AFX, tienes “cluster space show”, que mostrará solo la Storage Availability Zone.

Comparación lado a lado de los comandos CLI de capacidad en ONTAP unificado y NetApp AFX



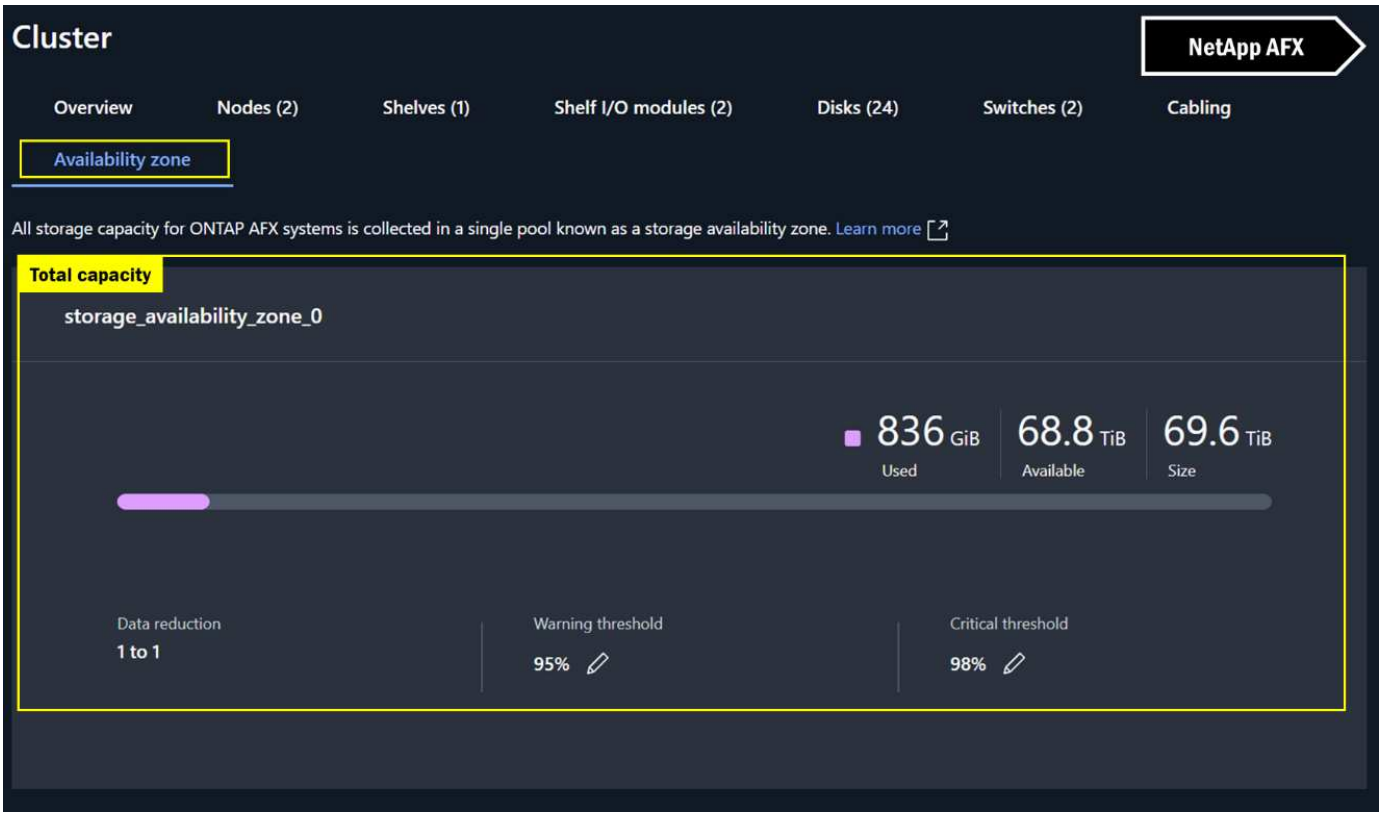
En la interfaz gráfica de usuario de Unified ONTAP System Manager, los niveles se utilizan para mostrar la capacidad. De hecho, la interfaz gráfica de usuario intenta mostrar la capacidad global del clúster sumando los totales, pero sigue mostrando el uso general por agregado.

Vistas de capacidad de System Manager – Unified ONTAP



En NetApp AFX System Manager, la vista es prácticamente la misma para el espacio de clúster, pero como no hay agregados, no hay que hacer cálculos adicionales. La capacidad que ves es la capacidad que obtienes.

Vistas de capacidad de System Manager – NetApp AFX

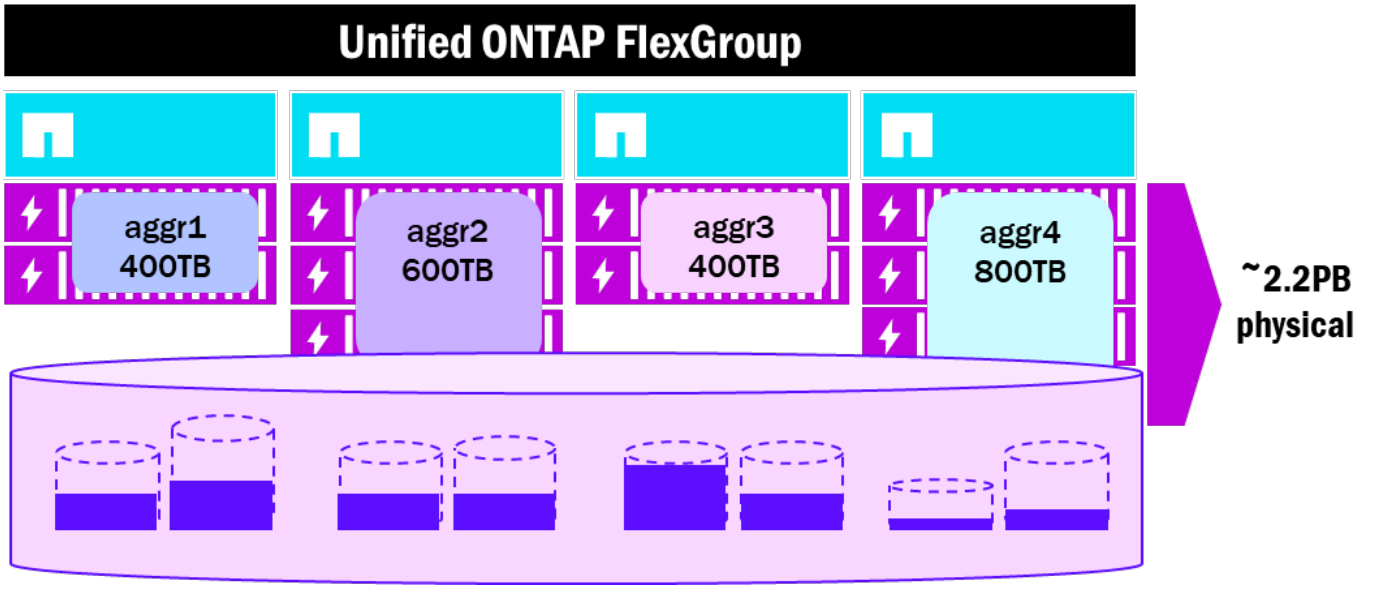


FlexGroup mejoras en la gestión de volúmenes

Un volumen FlexGroup consta de varios volúmenes constituyentes subyacentes FlexVol creados a través de varios nodos y agregados en el clúster y presentados como un único espacio de nombres grande a los clientes NAS. Los volúmenes FlexGroup proporcionan ventajas de rendimiento, escala, equilibrio de carga y recuento de archivos a las cargas de trabajo de alto rendimiento. Sin embargo, debido a que se coordinan a través de nodos y agregados, ocasionalmente se encuentran con algunas limitaciones físicas cuando la capacidad comienza a llenarse, ya que los sistemas de archivos independientes proporcionados por los agregados también tienen un uso y límites de capacidad independientes. Por ejemplo, si un agregado con volúmenes constituyentes FlexGroup comienza a llenarse antes que otros agregados en el clúster, entonces todo el FlexGroup podría estar sujeto a problemas de capacidad o rendimiento.

Como resultado, los administradores de almacenamiento pueden preocuparse demasiado por la infraestructura subyacente de FlexGroup y centrarse menos en el mantenimiento de otros aspectos del entorno.

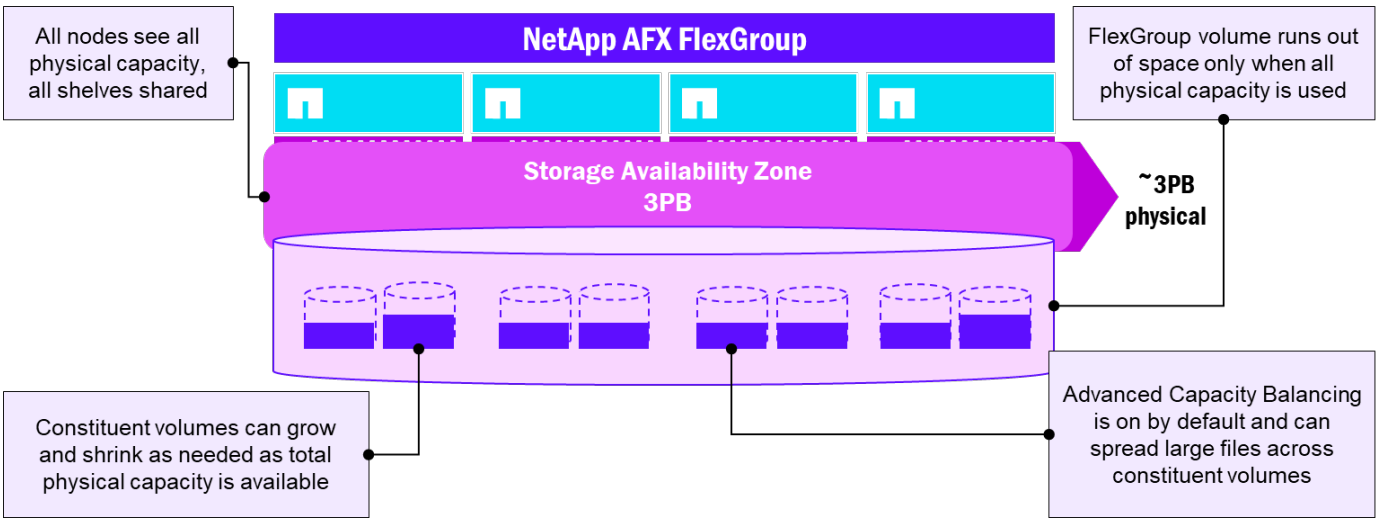
FlexGroup distribución de volúmenes - agregados unificados de ONTAP



NetApp AFX presenta la capacidad en una única Storage Availability Zone, lo que refleja más fielmente la forma en que se pretende que funcionen los volúmenes FlexGroup. En lugar de múltiples volúmenes constituyentes a través de múltiples agregados dispares de tamaños potencialmente variables, todos los volúmenes residen en el mismo pool de capacidad, lo que simplifica en gran medida la sobrecarga de gestión global al usar un volumen FlexGroup.

Además, AFX habilita por defecto Advanced Capacity Balancing para los volúmenes de FlexGroup, lo que ayuda a distribuir mejor los archivos de mayor tamaño en el volumen. Ahora, los constituyentes del volumen de FlexGroup pasan a ser menos un concepto de gestión y, en su lugar, hacen su trabajo silenciosamente en segundo plano.

Disposición del volumen FlexGroup - NetApp AFX



Tareas automatizadas de administración del almacenamiento

Con la zona de disponibilidad de almacenamiento en NetApp AFX, toda la capacidad se comparte entre todos los nodos. Aunque los nodos siguen siendo propietarios de los volúmenes, ONTAP gestiona el uso de la capacidad de cada nodo automáticamente tomando prestada y liberando capacidad en función de lo que cada nodo necesite en cada momento. Esto significa que los administradores de almacenamiento ya no tienen que preocuparse de cómo equilibrar mejor el espacio utilizable.

Además, ONTAP automatiza la gestión de los grupos RAID, donde los nuevos discos se añaden a los grupos RAID existentes o nuevos sin intervención del administrador. ONTAP también gestiona los movimientos de volúmenes entre nodos sin necesidad de copia de datos.

Movimientos de volúmenes con copia cero

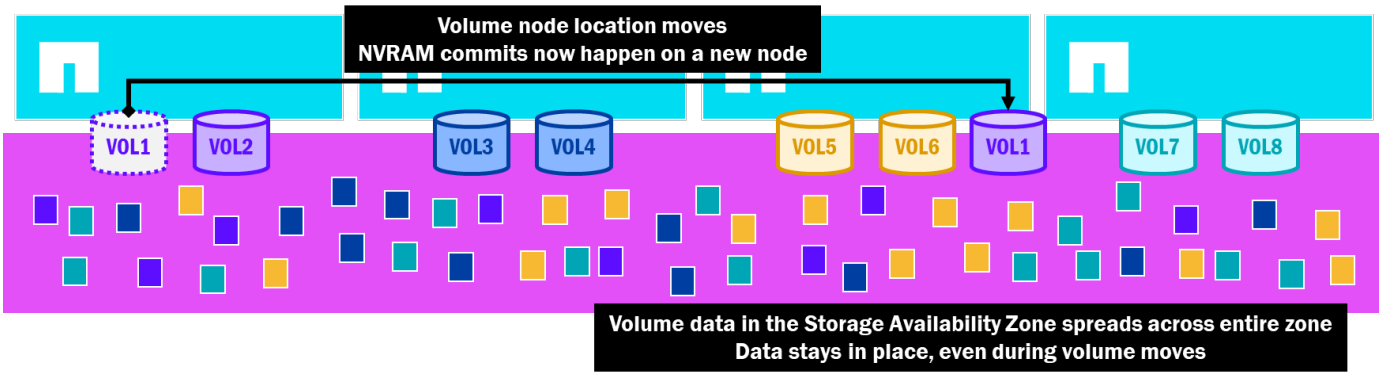
Unified ONTAP proporciona una forma de mover volúmenes de forma no disruptiva entre nodos o agregados como forma de gestionar el rendimiento y el uso de la capacidad en todo el clúster.

Cuando se inicia un movimiento de volumen, ocurre lo siguiente:

- Se crea un nuevo volumen vacío en el agregado de destino especificado
- Los metadatos del volumen (como la información sobre la eficiencia del almacenamiento, los identificadores de archivos, etc.) se replican en el nuevo volumen de destino
- Los datos de volumen se replican en el volumen de destino a través de la red de clústeres de backend mediante la tecnología SnapMirror: el agregado de destino debe disponer de espacio libre para la transición o el trabajo de transición fallará
- La replicación de volúmenes se realiza de nuevo para garantizar que ambos volúmenes son coherentes con cualquier cambio en los datos
- Se inicia un proceso de transición para desconectar el volumen de origen y promover el volumen de destino como nuevo volumen de origen para los clientes
- La E/S del cliente experimenta una breve pausa durante la transición, pero no se requieren remontajes

En NetApp AFX, la zona de disponibilidad de almacenamiento presenta toda la capacidad a todos los nodos, y todos los nodos pueden escribir en cualquier disco de ese pool. Una vez colocados los datos, permanecen donde están, incluso si se mueve el volumen. Esto significa que no es necesario copiar los datos. El proceso de movimiento del volumen es idéntico al de ONTAP unificado, menos la necesidad de replicar los datos a través de SnapMirror. No se requiere capacidad adicional.

Movimientos de volúmenes de copia cero en NetApp AFX



Disponer de una movilidad de volúmenes ligera permite a AFX automatizar muchas de las tareas de administración sin las limitaciones de rendimiento o capacidad, y estos movimientos de volúmenes se utilizan en algunas funciones nuevas que ofrece NetApp AFX, como se describe en los temas que se ven a continuación.

Comportamiento de conmutación por error en HA

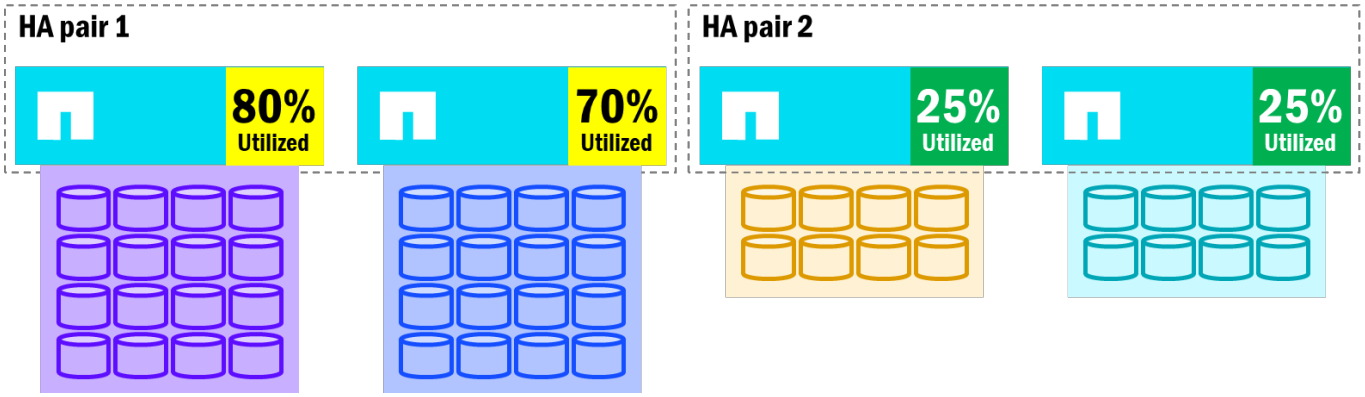
En ONTAP unificado, los nodos son propietarios de discos y agregados, donde los datos se sirven a través de volúmenes. Las escrituras se realizan utilizando la NVRAM de un nodo local para volcarse a los discos que posee el nodo. Cuando un nodo se reinicia o falla, ONTAP activará una toma de control de los recursos del

nodo fallido, donde la propiedad del disco y del agregado se transfiere al nodo asociado. Las interfaces de red también se transfieren a los puertos del espacio IP y, dado que el contenido de la NVRAM se replica constantemente en el par de HA, el nodo vaciará el contenido de la NVRAM para transferir las escrituras del nodo que ha fallado a los discos. Después de eso, el nodo superviviente será el propietario de los agregados y volúmenes del nodo fallido hasta que se produzca la recuperación del nodo. Esto significa que todo el tráfico de esos volúmenes, así como los volúmenes que ya son propiedad del nodo superviviente, se procesarán en un único nodo hasta que se resuelva el problema de la recuperación.

Como parte del despliegue inicial del clúster ONTAP unificado, se recomienda planificar con antelación las conmutaciones por error para evitar que un solo nodo sobrecargue a su compañero. Eso en sí mismo supone un reto, ya que es difícil predecir qué volúmenes pueden ser los agresores del rendimiento, pero funciones como el movimiento de volumen no disruptivo y las políticas de calidad de servicio de volumen pueden ayudar a mitigarlo.

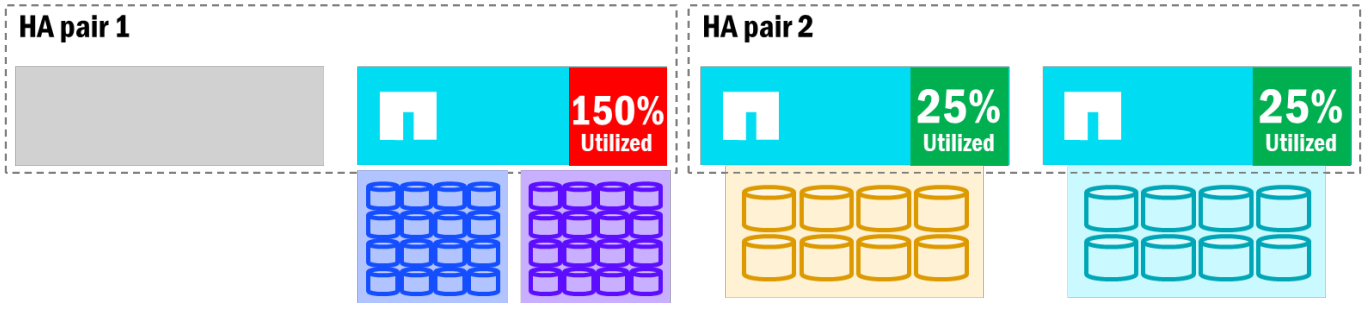
Las siguientes imágenes muestran cómo los clusters ONTAP unificados pueden incurrir en un balance de rendimiento desigual entre nodos, así como cómo un failover puede crear una degradación del rendimiento en algunos casos.

ONTAP unificado: posibles desequilibrios en la utilización de nodos



Cuando los nodos de un par de HA se desequilibran con el recuento de volúmenes y la utilización del rendimiento, los fallos de los nodos afectarán el rendimiento general, ya que el nodo superviviente ahora será propietario de todos los volúmenes del nodo que ha fallado. Mientras tanto, otros nodos del clúster pueden tener espacio para asumir trabajo adicional.

ONTAP unificado – Impacto de la conmutación por error en la utilización de nodos



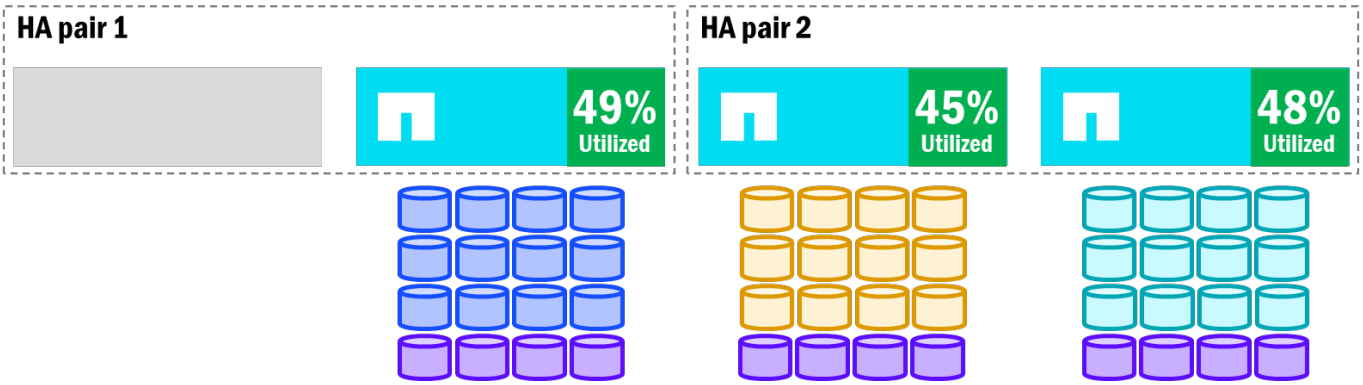
En el caso anterior, cuando un socio de HA tiene que asumir trabajo adicional, puede potencialmente sobrecargarse y afectar al rendimiento de todos los volúmenes en ese nodo. Los movimientos de volumen pueden ayudar a aliviar la situación, pero esos requieren copias entre nodos (lo que requiere espacio libre disponible), y el tiempo que lleva puede exceder el tiempo que tardan los nodos en recuperarse. Además, si reubicas un volumen, no volverá al nodo original. En su lugar, permanecerá en el nodo al que lo moviste.

Con NetApp AFX, las conmutaciones por error de los nodos adoptan algunos comportamientos diferentes.

- Dado que los nodos no poseen discos y no hay agregados físicos, la conmutación por error de un nodo no requerirá la transferencia de esos recursos. En su lugar, solo se transfieren a otros nodos las interfaces de red y la propiedad de los volúmenes.
- Los commits de NVRAM siguen produciéndose, pero a través de la red de HA en lugar de una conexión directa.
- Una vez que los volúmenes realizan la conmutación por error inicial al nodo asociado, AFX redistribuirá los volúmenes entre otros nodos supervivientes del clúster. Esto es posible gracias a los movimientos de volúmenes de copia cero.
- Cuando se recupere el nodo, los volúmenes volverán al nodo original.

NetApp AFX ya mantiene un equilibrio de rendimiento entre los nodos del clúster para mantener una utilización relativamente uniforme, así que cuando ocurre un failover y se reequilibran los volúmenes, la utilización de los nodos debería ser aproximadamente la misma en todo el clúster.

NetApp AFX - Reequilibrio de volúmenes tras la conmutación por error



Adiciones y eliminaciones de nodos

Tanto ONTAP unificado como NetApp AFX permiten añadir y eliminar nodos del clúster. Sin embargo, debido a algunas de las diferencias arquitectónicas, el proceso para añadir y eliminar nodos difiere un poco.

Adición/eliminación de nodos en ONTAP unificado

Ya hemos aprendido que ONTAP unificado tiene una propiedad directa de nodo a disco y que todos los nodos deben tener algunos discos y al menos un agregado conectado a ellos. Teniendo esto en cuenta, lo siguiente es válido para adiciones y eliminaciones.

- Las adiciones de nodos en ONTAP unificado no requieren ningún paso adicional, pero para proporcionar un rendimiento equilibrado en todos los nodos (incluidos los nuevos nodos), sería necesario mover los volúmenes a los nuevos nodos. Esto requiere un análisis previo de los volúmenes existentes y sus cargas de trabajo, decisiones sobre qué volúmenes mover y luego los movimientos de volumen reales, que, de nuevo, requerirían una copia de esos datos a través de la red de clúster backend.
- Las eliminaciones de nodos en ONTAP unificado requerirían una evacuación manual de los volúmenes existentes en el nodo, lo que significa que tienes que identificar qué nodos pueden alojar qué volúmenes para mantener un rendimiento uniforme, y debes tener suficiente capacidad libre para proporcionar un lugar a donde mover esos volúmenes. Si la capacidad libre es un reto, puede que sea necesario mover volúmenes adicionales para reorganizar un poco las cargas de trabajo en el clúster. Las eliminaciones de nodos también implican eliminaciones de pares de HA, así que el trabajo se duplica. Como los nodos son

dueños de los discos, también sería necesaria una reinicialización completa de los discos para esos nodos. Cada una de estas cosas añade tiempo y esfuerzo a lo que debería ser una tarea relativamente sencilla.

Adición/eliminación de nodos en NetApp AFX

También hemos aprendido que NetApp AFX no aprovecha la propiedad estándar de nodo a disco y no utiliza agregados físicos para presentar capacidad al clúster. Por eso, las incorporaciones y eliminaciones de nodos se comportan de manera un poco diferente.

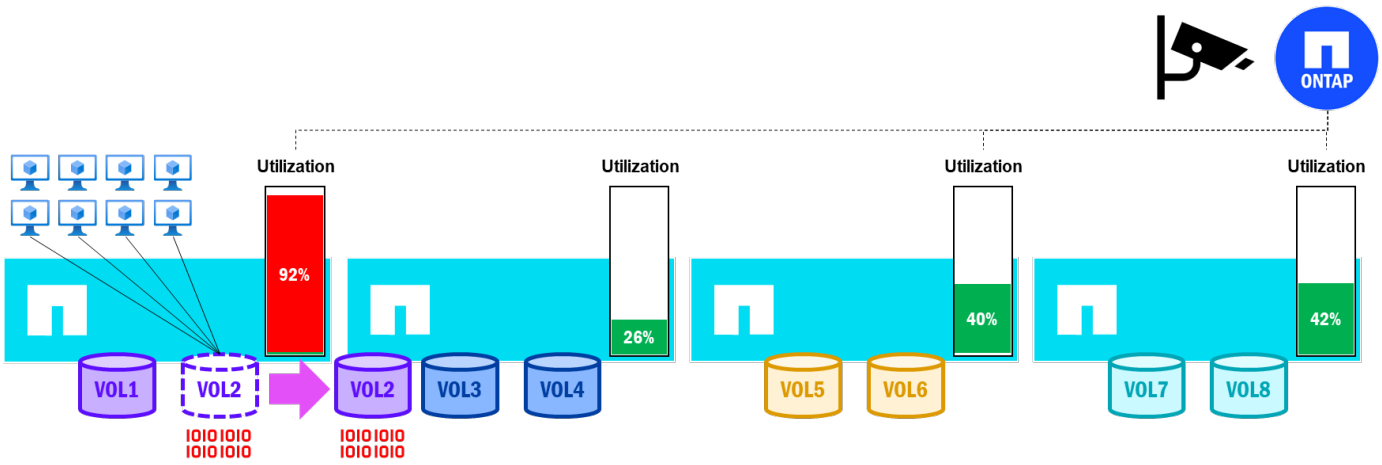
- Las adiciones de nodos en NetApp AFX no requerirán el mismo análisis previo de volúmenes ni la intervención administrativa para garantizar que cada nodo tenga un equilibrio uniforme de volúmenes. En su lugar, ONTAP equilibra automáticamente los recuentos de volúmenes entre los nodos recién añadidos para mantener perfiles de rendimiento relativamente uniformes. ONTAP moverá automáticamente los volúmenes entre los nodos sin copiar nada, lo que reduce el tiempo, la capacidad y el esfuerzo necesarios para añadir nodos a un clúster.
- La eliminación de nodos en NetApp AFX tampoco requiere mucha, si es que alguna, intervención manual. Cuando se marca un nodo para eliminación, ONTAP mueve automáticamente los volúmenes entre los nodos (de nuevo, sin copiar) para evacuar los nodos que se eliminan. Y como no hay discos propiedad de los nodos, no es necesario reinicializar los discos después de eliminar nodos. Esto hace que los nodos en AFX sean modulares por naturaleza y fáciles de escalar hacia arriba o hacia abajo.

Movimientos de volumen condicionados por el rendimiento

NetApp La funcionalidad de movimiento de volumen de copia cero de AFX significa que puede reequilibrar volúmenes según sea necesario sin copiar datos, lo que le permite actuar con rapidez y sin necesidad de capacidad adicional. Esto significa que los movimientos de volumen pueden convertirse en una mayor parte del equilibrio de carga automatizado disponible para los clusters ONTAP. Ahora que mover un volumen no cuesta relativamente nada, ONTAP puede aprovechar esta valiosa herramienta para incorporar funciones como el equilibrio de carga de volúmenes condicionado por el rendimiento.

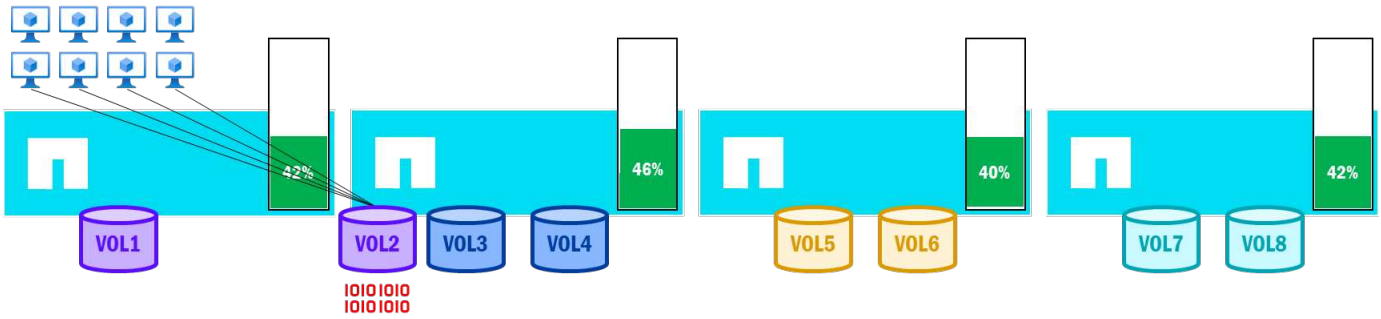
En NetApp AFX con ONTAP 9.18.1 y versiones posteriores, la utilización de nodos, pares de HA y volúmenes se supervisa constantemente, mientras se recopilan y analizan los datos de rendimiento. Si la utilización de un nodo cae fuera de los umbrales definidos, ONTAP seleccionará automáticamente un volumen para moverlo a un nodo menos utilizado en un esfuerzo por mantener un rendimiento equilibrado en todo el clúster.

Movimientos de volumen condicionados por el rendimiento en NetApp AFX – una alta utilización desencadena un movimiento de volumen



Movimientos de volumen condicionados por el rendimiento en NetApp AFX – Utilización equilibrada de

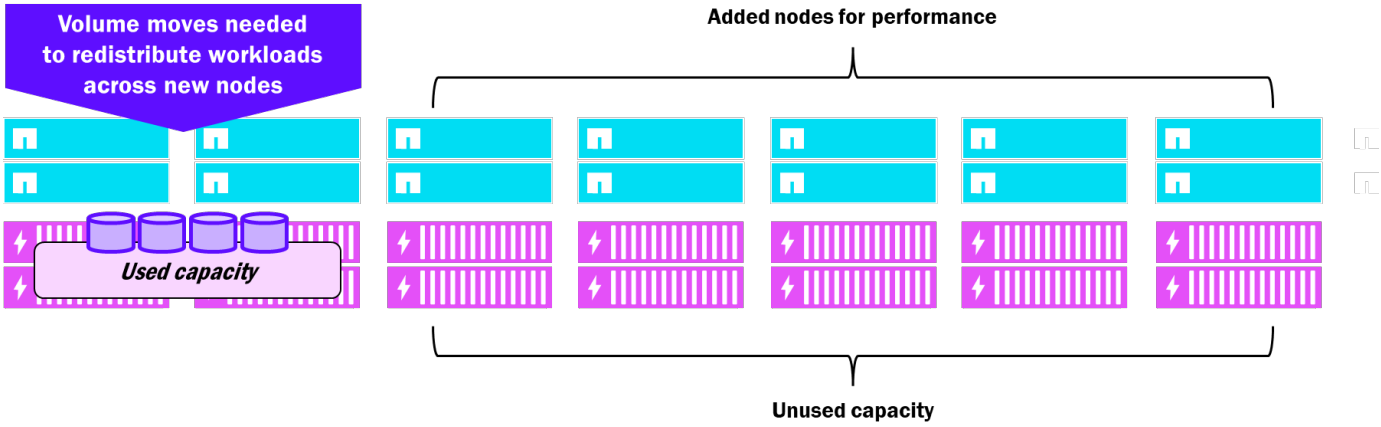
nodos tras el movimiento de volumen



Escala y expansión de clústeres

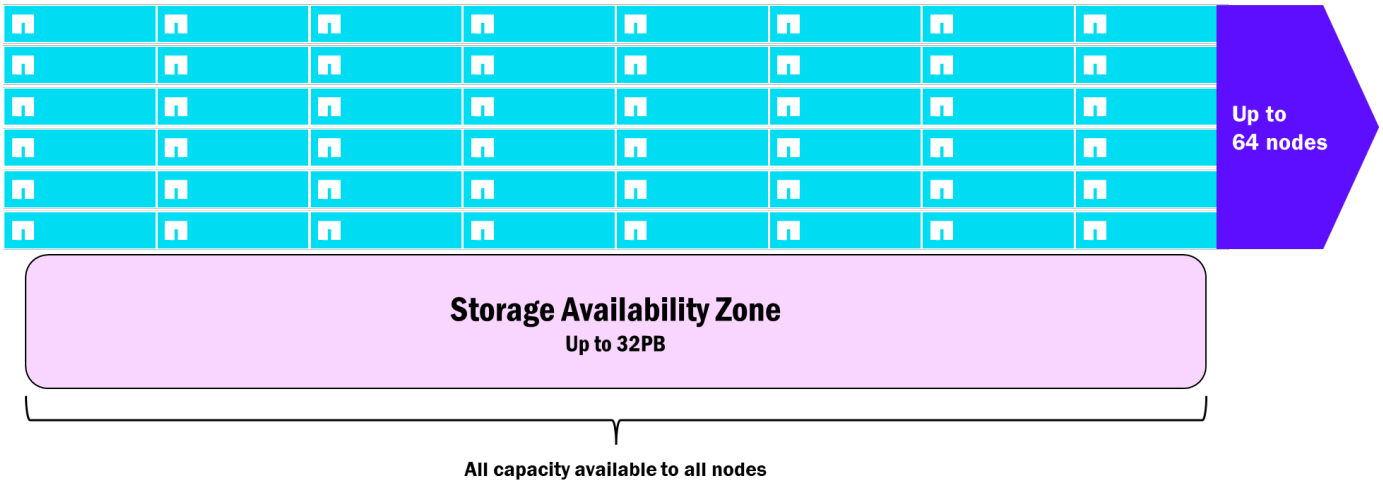
Los clústeres Unified ONTAP admiten hasta 24 nodos y cada nodo que se añada también debe añadirse con discos (tanto para la funcionalidad del sistema como para los servicios de datos). Se pueden añadir estantes de discos al clúster, pero siempre están conectados a un único par de alta disponibilidad y son propiedad de un solo nodo, incluso si el clúster tiene 24 nodos. Esto significa que se añade capacidad a un clúster incluso cuando solo se necesita rendimiento, y ese aumento de rendimiento queda relegado en su mayor parte a un conjunto específico de discos propiedad de los nuevos nodos. Como resultado, es posible que termines con una capacidad extra que no necesitas necesariamente.

Unified ONTAP – consideraciones de escala añadidas



NetApp AFX es compatible con clústeres a mayor escala. A partir de la versión 9.19.1, los clústeres AFX pueden alcanzar los 32 nodos en un único clúster. Y como todos los nodos pueden ver y acceder a todos los discos, todos pueden compartir el rendimiento y la capacidad (hasta 32PB a partir de ONTAP 9.19.1) de esos discos para que nunca haya ningún recurso varado. Los movimientos de volúmenes no requieren copias, por lo que ONTAP es capaz de mover automáticamente los volúmenes a los nodos recién añadidos para garantizar una utilización uniforme de los nodos, mientras que la capacidad se distribuye uniformemente a través de la Storage Availability Zone.

NetApp AFX – consideraciones de escala añadidas



Cambios en el volumen raíz

En NetApp ONTAP, a cada nodo se le asigna un volumen raíz, que se utiliza para archivos y funciones específicos del sistema, como archivos de registro, imágenes de arranque, archivos de núcleo, bases de datos de clúster y más.

En ONTAP unificado, esos volúmenes raíz vivían en agregados raíz físicos. Para reducir la cantidad de capacidad que utilizaban los agregados raíz, se crearon a través de particiones de unidades de datos mediante Advanced Disk Partitioning (ADP).

NetApp AFX elimina los agregados físicos de la ecuación y, como resultado, elimina la necesidad de utilizar agregados raíz y ADP. Los volúmenes raíz siguen siendo un concepto, pero ahora viven en áreas virtualizadas del pool de capacidad y no requieren configuración adicional. Además, la funcionalidad del volumen raíz cambia. Las imágenes de arranque y las bases de datos de clúster replicadas se trasladan de la pila de almacenamiento a un medio de arranque integrado que se encuentra en cada nodo AFX. Ahora, si se pierde el acceso a la pila de almacenamiento, los nodos pueden seguir arrancando y mantener la elegibilidad del clúster, lo que reduce la complejidad de la resolución de problemas.

Medios de arranque a bordo

NetApp Los nodos AFX utilizan un medio de arranque integrado, que es un dispositivo M.2 conectado a NVMe de aproximadamente 3,8 TB. Estos dispositivos de arranque contienen archivos de imagen de arranque y bases de datos replicadas que están separadas de las cabinas de almacenamiento, lo que proporciona redundancia adicional en caso de problemas de acceso al disco. Si el medio de arranque falla, el nodo será asumido por su socio de HA y el medio de arranque puede ser reemplazado. Una vez reemplazado, un administrador de almacenamiento cargará una nueva imagen de ONTAP en el dispositivo y ONTAP reconstruirá automáticamente la base de datos del clúster para restaurar la funcionalidad completa.

Rendimiento

NetApp AFX se creó pensando en el rendimiento y la escalabilidad, específicamente orientado a cargas de trabajo que requieren un alto rendimiento de lectura y escritura y pueden ofrecer una escalabilidad simple y lineal.

Rendimiento por nodo

Cada nodo de almacenamiento NetApp AFX proporciona una cantidad específica de rendimiento para lecturas y escrituras. A medida que se añaden nodos al clúster, aumentan linealmente ese rendimiento, como se

explica en la sección "Escalado lineal del rendimiento de los nodos" de este documento.

Actualmente, los tipos de nodo son "AFX 1K" y proporcionan un rendimiento para lecturas y escrituras de aproximadamente las cantidades indicadas a continuación. A medida que se disponga de hardware más nuevo para NetApp AFX, estos límites pueden cambiar. NOTA: El rendimiento máximo se alcanzó utilizando varios clientes que leían y escribían varios archivos, como se muestra en la sección "Benchmark results" a continuación.

Estimaciones de rendimiento por nodo

Tipo de nodo	Rendimiento máximo de lectura	Rendimiento máximo de escritura
AFX 1K	~35GB/s	~10GB/s

Para conocer las estimaciones de rendimiento más actualizadas, consulta a tu equipo de ventas de NetApp.

Rendimiento por estante

Cada estantería contiene módulos de estantería de alto rendimiento con 16 puertos Ethernet de 100 GB que aprovechan la comunicación RoCEv2 para una interacción de almacenamiento de ancho de banda elevado con los nodos de computación del clúster. Al igual que cualquier recurso físico, estas estanterías tienen máximos que se pueden alcanzar, especialmente porque NetApp AFX puede presentar múltiples nodos apuntando al mismo conjunto de discos. La siguiente tabla muestra el rendimiento máximo estimado de lectura y escritura para una sola estantería con unidades TLC y QLC. Para obtener más información sobre las diferencias entre TLC y QLC, consulta "TLC frente a QLC".

Estimaciones de rendimiento por estantería

Tipo de módulo de estantería	Rendimiento máximo de lectura	Rendimiento máximo de escritura
NSM 140	140GB/s (TLC y QLC)	70GB/s TLC 35GB/s QLC

Para conocer las estimaciones de rendimiento más actualizadas, consulta a tu equipo de ventas de NetApp.

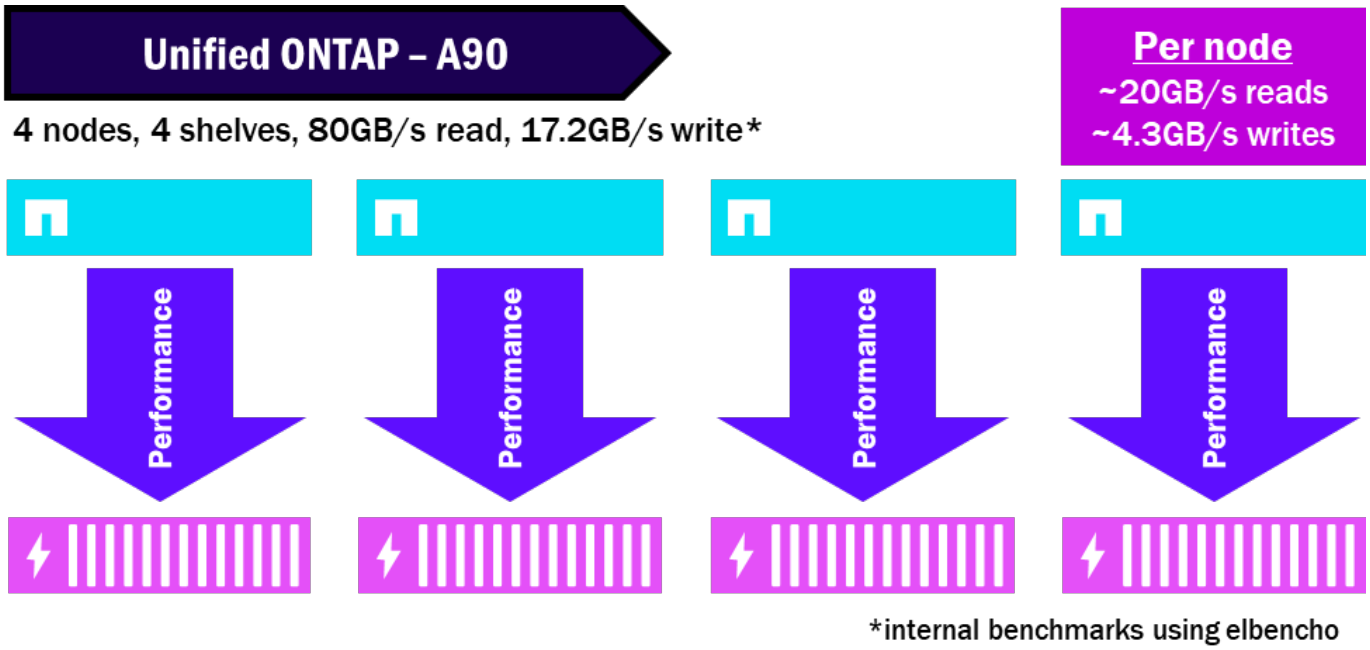
Densidad de rendimiento

La desvinculación de los nodos de almacenamiento de las estanterías en la arquitectura desagregada de ONTAP permite que más nodos dirijan el tráfico a menos estanterías, lo que ayuda a reducir la huella total del centro de datos necesaria para obtener el máximo rendimiento con solo la capacidad que necesitas.

Este concepto de "densidad de rendimiento" permite a los administradores de almacenamiento aprovechar al máximo el hardware que tienen sin tener que sobreaprovisionar nunca su entorno de almacenamiento.

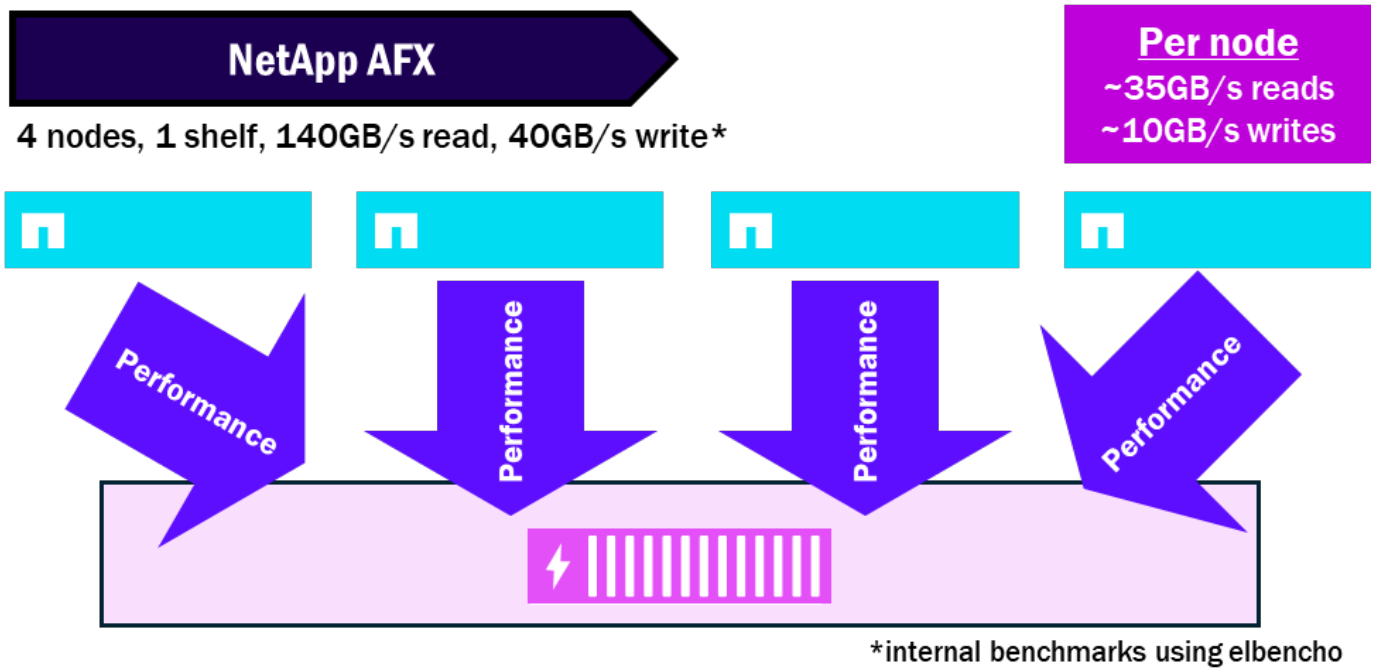
Por ejemplo, en un clúster ONTAP unificado, como cada nodo tiene su propio conjunto de discos, el rendimiento se dirige solo a los discos propiedad del nodo, y como solo un nodo puede acceder a un conjunto de discos, no necesariamente puede saturar los discos disponibles y alcanzar su máximo rendimiento.

ONTAP unificado – cómo se divide el rendimiento



NetApp AFX agrupa todos los discos en una única Zona de Disponibilidad de Almacenamiento, así que todos los nodos pueden aprovechar todos los discos. Y como los discos y los nodos están desacoplados, no necesitarás tantas estanterías para obtener el mismo rendimiento. Esto condensa el rendimiento y maximiza el potencial de rendimiento máximo de la estantería.

NetApp AFX – Densidad de rendimiento



Relación entre nodos y estantes

Los nodos de Unified ONTAP requieren al menos un conjunto de discos por nodo y pueden tener varias estanterías conectadas a un único nodo. Como resultado, puede haber cuellos de botella de rendimiento en el único nodo que puede no ser capaz de saturar sus propios discos.

NetApp AFX presenta todos los estantes de discos a todos los nodos. Cada estante contiene módulos con 16 x 100GB interfaces compatibles con RoCE para aumentar la cantidad total de rendimiento permitido por estante. Por esto, puedes saturar un solo estante con varios nodos que estarán leyendo y escribiendo en el mismo conjunto de discos.

A partir de ONTAP 9.19.1, el ratio de saturación nodo:estantería es de aproximadamente 4:1.

Resultados de las pruebas de rendimiento

La siguiente sección cubre los resultados de las pruebas de rendimiento utilizando un cluster NetApp AFX con los siguientes parámetros de configuración.

- 4 nodos, 4 interfaces de datos
- 2 estantes (unidades de 7,6 TB)
- ONTAP 9.19.1
- NFSv4.2 (pNFS, trunking de sesiones)
- FlexGroup volumen
- "ElBencho" referencia
- Escrituras: elbencho --hosts=x.x.x.[y-z] -d -w -b 1M -t 80 --iodepth 1 --direct -s 600g /fio_vol1/
- Lecturas: elbencho --hosts=x.x.x.[y-z] -r -b 256k -t 80 --lat --iodepth 2 --direct -s 600g --infloop /fio_vol1/
- 4 servidores Cisco C240 M8, tarjetas CX-7 de 2 puertos * 200GbE, 80 hilos
- Opciones de montaje NFS: rw,vers=4.2,rsize=1048576,wsize=1048576,trunkdiscovery,proto=tcp

La configuración anterior alcanzó casi el máximo de lecturas disponible para el clúster de 4 nodos (~134GB/s) y se situó justo en el máximo de escrituras permitido por nodo (40GB/s).

NetApp AFX – ElBencho rendimiento de lectura, 4 nodos

NetApp AFX – ElBencho rendimiento de escritura, 4 nodos

Lectura anticipada agresiva

En las cargas de trabajo de streaming multimedia, una película 4K suele dividirse en decenas de miles de archivos, cada uno de los cuales suele tener un tamaño de entre 50 MB y 250 MB. Cada archivo representa un fotograma, y la aplicación lee un fotograma completo en una única solicitud. Para mantener un flujo fluido e ininterrumpido sin búferes visibles, estas lecturas de fotogramas deben completarse sin caídas.

ONTAP proporciona una opción a nivel de volumen (`-aggressive-readahead-mode` para optimizar estas cargas de trabajo. A partir de ONTAP 9.19.1, se ha introducido un nuevo modo `cross_file_sequential_read` para readahead agresivo en AFX para acelerar las cargas de trabajo con patrones de E/S predecibles a través de tipos de archivo similares (por ejemplo, renderización multimedia y streaming).

cross_file_sequential_read predice el siguiente archivo que se va a leer basándose en su nombre y comienza la lectura anticipada de esos archivos antes de que el cliente emita la llamada de lectura. La lógica de predicción asume que todos los archivos de un directorio siguen un patrón de nomenclatura con un sufijo numérico monotónicamente creciente (por ejemplo, archivo1, archivo2, archivo3). Todos los archivos del directorio deben seguir este patrón, utilizando numeración decimal o hexadecimal. Los nombres de archivo pueden tener hasta 255 caracteres. La lógica es independiente de la extensión y genera el siguiente conjunto de nombres de archivo en el directorio actual basándose únicamente en el nombre de archivo actual. Si un nombre de archivo generado previamente utilizando numeración base10 no existe en el directorio, los nombres se vuelven a generar utilizando numeración hexadecimal. Si no existe ninguno de los nombres de archivo generados, no se emite ninguna precarga para ese conjunto. La precarga se reanuda cuando se emite la siguiente lectura del cliente.

Con estas opciones activadas, las pruebas de rendimiento de "frametest" pudieron leer 30,000 fotogramas 4K a 30 fotogramas por segundo con 30 clientes (NFSv3 y SMB3) y 34 clientes (NFSv4.1), sin que se perdiera ni un solo fotograma.

Aunque la lectura secuencial de archivos cruzados está diseñada principalmente para cargas de trabajo multimedia, también pueden beneficiarse otras cargas de trabajo de lectura intensiva con patrones de acceso y nombres de archivos predecibles, como el entrenamiento y la inferencia de IA.

Consideraciones y advertencias

- Caché de búfer compartida: la lectura anticipada agresiva utiliza la misma caché de búfer que otros volúmenes en el nodo. Activarla puede afectar el rendimiento de lectura de otros volúmenes en ese nodo.
- Rendimiento del almacenamiento subyacente: si los archivos no pueden leerse con la suficiente rapidez (por ejemplo, en sistemas FAS basados en HDD), los datos almacenados en caché pueden desalojarse antes de que se produzca la lectura del cliente, lo que anula las ventajas de la lectura anticipada.
- Requisitos de patrón de acceso: si el patrón de lectura de la carga de trabajo no es secuencial, o si los archivos de un directorio no se nombran en un orden secuencial creciente, el modo de lectura por adelantado agresivo cross_file_sequential_read no proporcionará beneficios significativos.

Mejoras del rendimiento de NFSv4.x

La versión de NFS 3 ha sido el estándar de oro para las aplicaciones NFS durante décadas, desde 1995, cuando se lanzó oficialmente por primera vez. Su combinación de rendimiento y resiliencia ha hecho que sea difícil considerar un cambio a versiones de NFS más recientes, y con razón.

Sin embargo, NFSv3 no está exento de limitaciones. La falta de estado del protocolo, aunque es genial para el rendimiento y para minimizar las interrupciones en la conmutación por error de almacenamiento, no lo es tanto para la coherencia de los datos y la gestión de bloqueos. Un servidor NFS no realiza un seguimiento real de los estados de bloqueo, así que si ocurre una falla, el servidor NFS puede o no liberar los bloqueos, y el cliente de NFS puede que no sepa si un archivo está bloqueado o no.

```
 Security for NFSv3 is also a bit lacking. The protocol requires multiple
open firewall ports to function properly and numeric IDs are sent in
plaintext over the wire. Furthermore, NFS does not have robust ACL
support, and does not include native file and folder auditing. As a result
of these limitations, NFSv4 was created in 2003 via
link:https://datatracker.ietf.org/doc/html/rfc3530[RFC-3530^] (obsoleted
in 2015 by link:https://datatracker.ietf.org/doc/html/rfc7530[RFC-7530^]).
Aunque NFSv4.x existe desde hace más de 20 años, aún no se ha generalizado
su adopción por varias razones.
```

- Complejidad de la gestión de identidades: muchos entornos no disponen de una infraestructura de servicio de nombres para aprovechar adecuadamente los requisitos de cadena de nombres y de seguridad de Kerberos en NFSv4.x.
- Necesidad de clientes de NFS más recientes: esta preocupación es menos acuciante en los entornos NFS modernos de hoy en día, ya que cuanto más nos alejamos de la fecha de lanzamiento inicial de NFSv4. Casi todos los sistemas operativos utilizados actualmente incluyen clientes de NFS con compatibilidad total con NFSv4, pero todavía hay sistemas heredados que pueden no tener los paquetes NFSv4.x necesarios. De hecho, algunas aplicaciones todavía requieren el uso de versiones de NFS más antiguas.
- mentalidad de "si no está roto, no lo arregles": Las empresas de TI son notoriamente conservadoras a la hora de adoptar nuevas tecnologías, incluso las que llevan más de 20 años en el mercado. Y si la versión de NFS actual funciona bien, ¿para qué cambiar?
- Problemas de rendimiento: El rendimiento de un protocolo con estado como NFSv4.x ha sido inferior al de

NFSv3 sin estado durante gran parte de los últimos 20 años. En el pasado, el impacto en el rendimiento a menudo superaba los beneficios de NFSv4.x.

Mejoras de NFSv4.x en ONTAP 9.18.1 mediante AFX

Algunos cambios en la arquitectura de ONTAP han proporcionado un aumento de rendimiento muy necesario para NFS en general y han hecho algunos avances importantes para mejorar el rendimiento de NFSv4.x en general.

A continuación se ofrece un resumen a grandes rasgos de algunos de esos cambios.

Mejora de la lectura secuencial: NFSv4.1 un 30% mejor que NFSv3

ONTAP 9.18.1 introduce soporte para IO multivía con NFSv4.1. En lugar de procesar las lecturas del sistema de archivos WAFL, MPIO desplaza las operaciones de lectura a un dominio de red para que se sirvan de forma segura multivía. Este enfoque reduce los cambios de contexto, proporcionando un mayor paralelismo general en el tráfico de lectura secuencial, además de reducir la sobrecarga de la gestión de búferes al evitar WAFL.

Mejora de la lectura aleatoria para volúmenes FlexGroup: NFSv4.1 dentro del 7% de NFSv3

Los volúmenes FlexGroup son volúmenes que toman muchos volúmenes constituyentes subyacentes y los presentan como un único espacio de nombres unificado. En AFX, los volúmenes FlexGroup tienen activado por defecto el equilibrio de capacidad avanzado, que escribirá archivos de más de 10GB en varios volúmenes constituyentes como archivos multiparte. Debido a la ubicación remota de estas partes de archivos, las lecturas aleatorias tradicionalmente han tenido una desventaja de rendimiento modesta con NFSv4.x (alrededor del 18% menos que NFSv3). ONTAP 9.18.1 introduce soporte para IO en caché para lecturas multiparte con NFSv4.x para ayudar a solucionar esto. NOTA: este cambio no se aplica a los volúmenes FlexVol.

Escrituras secuenciales: +10% de mejora respecto a versiones anteriores

Una mejora de la forma en que replicamos los datos NVLOG utilizados para la funcionalidad de conmutación por error en HA aumentó el rendimiento general de escritura secuencial para los sistemas NetApp AFX.

Operaciones de metadatos: dentro del 15% del rendimiento de NFSv3 para los benchmarks de EDA

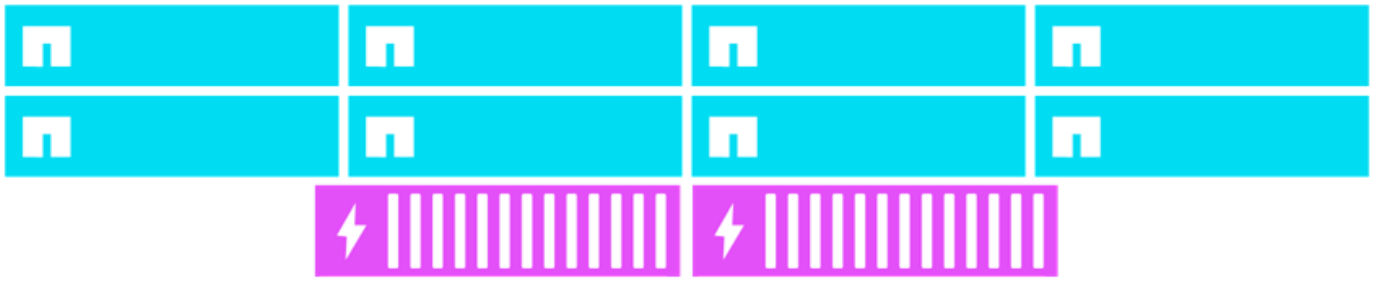
NFSv4.1 tradicionalmente serializa todas las operaciones OPEN y CLOSE, con un nodo del clúster que las procesa de una en una antes de que puedan ser enviadas desde la red a WAFL. ONTAP 9.18.1 introduce Concurrent Open Close (COC), que elimina la serialización de la red cambiando cómo se resuelven las condiciones de carrera, lo que elimina los cuellos de botella OPEN/CLOSE vistos en versiones anteriores.

Todos estos cambios, junto con los cambios de arquitectura introducidos en AFX, han permitido mejorar el rendimiento general de NFSv4.1 en ONTAP 9.18.1.

Resultados de IO secuenciales

Una de las áreas en las que se observaron algunas modestas mejoras de rendimiento fue con la IO secuencial (es decir, IO que es predecible y se emite de forma consecutiva). En las pruebas de rendimiento estándar utilizando fio, AFX ejecutando ONTAP 9.18.1 mejoró el rendimiento de lectura secuencial en casi un 30% y el rendimiento de escritura secuencial en un 10%.

NetApp AFX – rendimiento de IO secuencial NFSv4.1 en ONTAP 9.18.1



	AFX 9.17.1	AFX 9.18.1
Seq. reads	220GB/s	**283GB/s**
Seq. writes	70.6GB/s	**77.7GB/s**

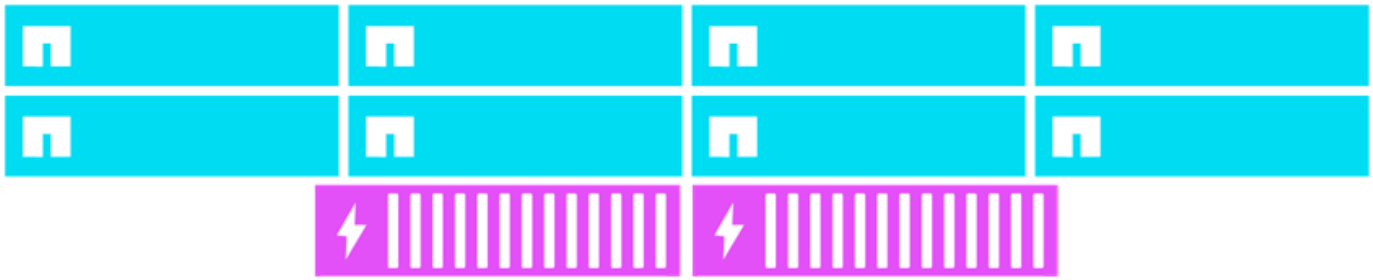
Resultados de cargas de trabajo con muchos metadatos

Aún más impresionantes son las mejoras en uno de los principales problemas de rendimiento de NFSv4.x: los metadatos. Se trata de IO aleatorias, normalmente del orden de 4K, que se utilizan para gestionar los propietarios y atributos de los archivos, crear y listar archivos, y así sucesivamente. Debido al carácter de estado de NFSv4.x, este tipo de operaciones tienden a costar más en CPU y latencia, lo que a su vez reduce el rendimiento general posible.

Con los cambios introducidos en AFX ONTAP 9.18.1, el rendimiento de NFSv4.x para este tipo de cargas de trabajo ha mejorado sustancialmente y ha cerrado la brecha con el rendimiento de NFSv3 (dentro del 15%).

Nuestros equipos de ingeniería de rendimiento compararon el rendimiento de las imágenes de IA estándar, EDA y los puntos de referencia de creación de software y descubrieron enormes mejoras con respecto a la versión anterior de ONTAP.

NetApp AFX – rendimiento de IO de metadatos NFSv4.1 en ONTAP 9.18.1



	9.17.1	9.18.1	Delta
AI Image processing	209 KIOPS	**239 KIOPS**	**+16%**
Software dev	600 KIOPS	**950 KIOPS**	**+58%**
EDA	480 KIOPS	**881 KIOPS**	**+84%**

Herramientas de gestión

Aunque hay algunas diferencias arquitectónicas bastante grandes en la forma en que se presenta el almacenamiento en NetApp AFX, el conjunto de funciones y la forma en que se gestiona ONTAP prácticamente no ha cambiado. Esto es totalmente por diseño. ONTAP es ONTAP y debe haber poca o ninguna curva de aprendizaje cuando sea posible. Y en este caso, NetApp AFX sigue ejecutando ONTAP.

Gestión – CLI

En NetApp AFX, la CLI es casi idéntica a lo que ofrece la CLI de ONTAP unificada. Los comandos se siguen ejecutando a nivel de clúster en su mayor parte, aunque todavía se pueden emitir comandos a nivel de nodo. Sigue habiendo directorios de comandos de nivel superior y subcomandos, así como completado de comandos mediante tabulación. Además, funcionan todos los mismos accesos directos de la CLI (por ejemplo, filtrado de contenido mediante `-fields`).

Las únicas diferencias reales en la CLI de NetApp AFX tienen que ver con lo que se ha añadido y lo que se ha eliminado (como se explica en la sección "" de este documento). Si se ha eliminado una función (como los agregados o Metrocluster), el comando CLI correspondiente ya no estará disponible.

Además, cuando se hayan añadido nuevas características y funcionalidades a NetApp AFX, también estarán disponibles nuevos comandos. Por ejemplo, el nuevo "NetApp AI Data Engine (AIDE)" complemento interactúa directamente con un clúster NetApp AFX a través de la red de clústeres backend. Como resultado, los directorios de comandos `dcn` y `data-engine` se añaden a la CLI de NetApp AFX.

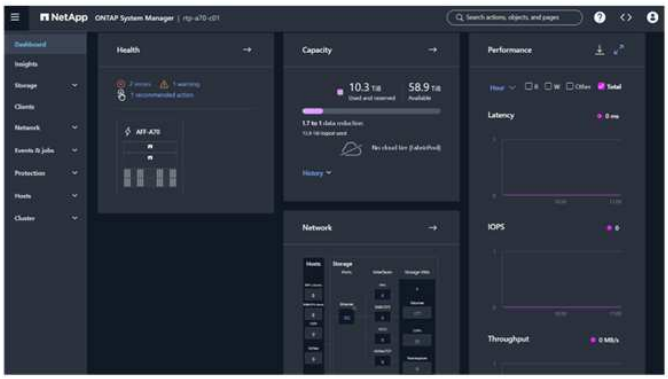
A continuación se muestran los directorios de comandos de nivel superior disponibles con privilegios de administrador en un clúster NetApp AFX. Los comandos añadidos recientemente aparecen en negrita.

```
AFX::>
    cluster         data-engine    dcn            event          exit
    history         job            man            metrocluster   network
    qos             redo           rows           run            security
    set             snaplock       snapmirror     statistics     statistics-v1
    storage         system         top            up             volume
    vserver
```

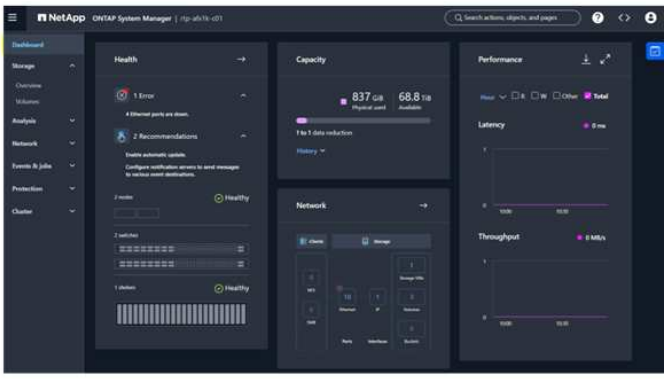
Gestión – GUI

System Manager sigue siendo la interfaz GUI para interactuar con los clústeres AFX de NetApp para la gestión de recursos, y cuando inicies sesión en él por primera vez, probablemente no podrás decir a primera vista que no sigues conectado a un sistema ONTAP unificado.

Comparación entre las páginas de inicio de ONTAP unificado y NetApp AFX System Manager



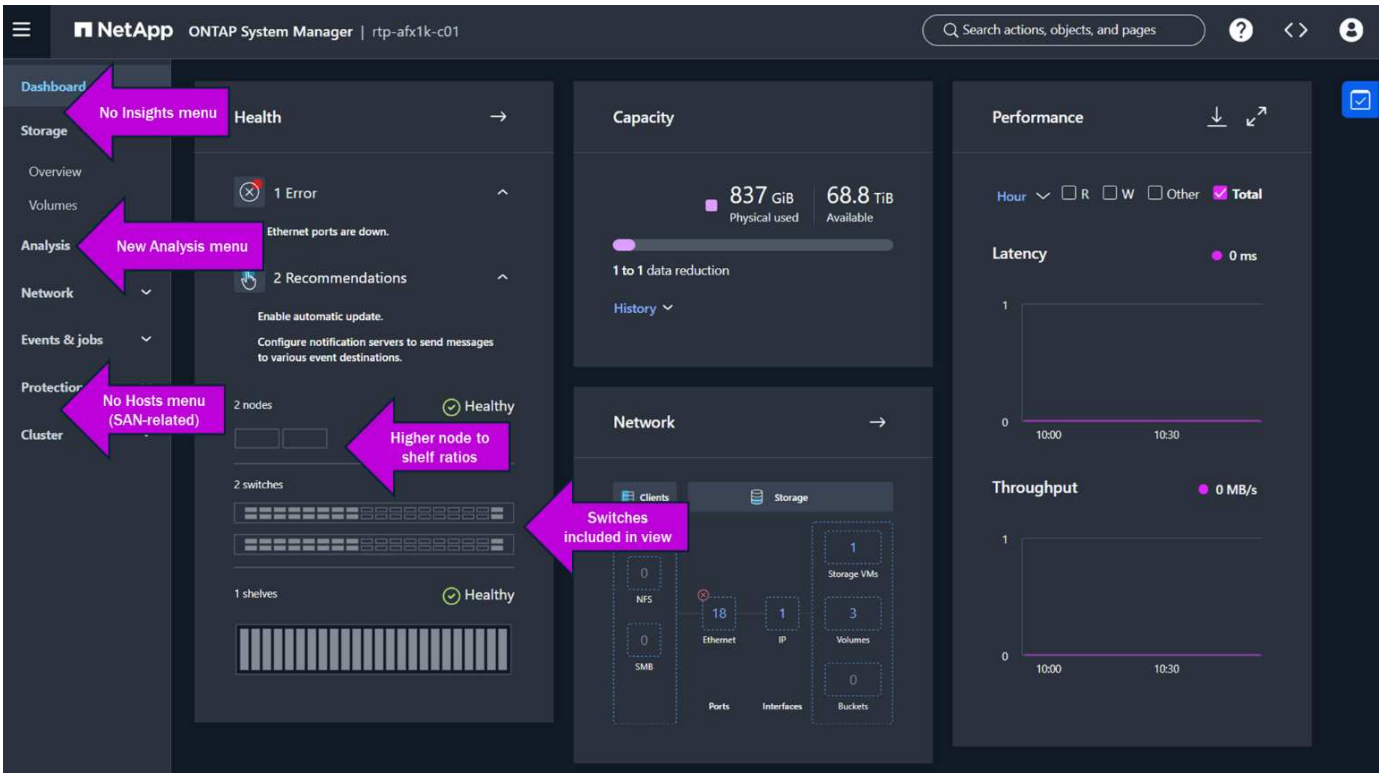
System Manager Dashboard view
Unified ONTAP



System Manager Dashboard view
NetApp AFX

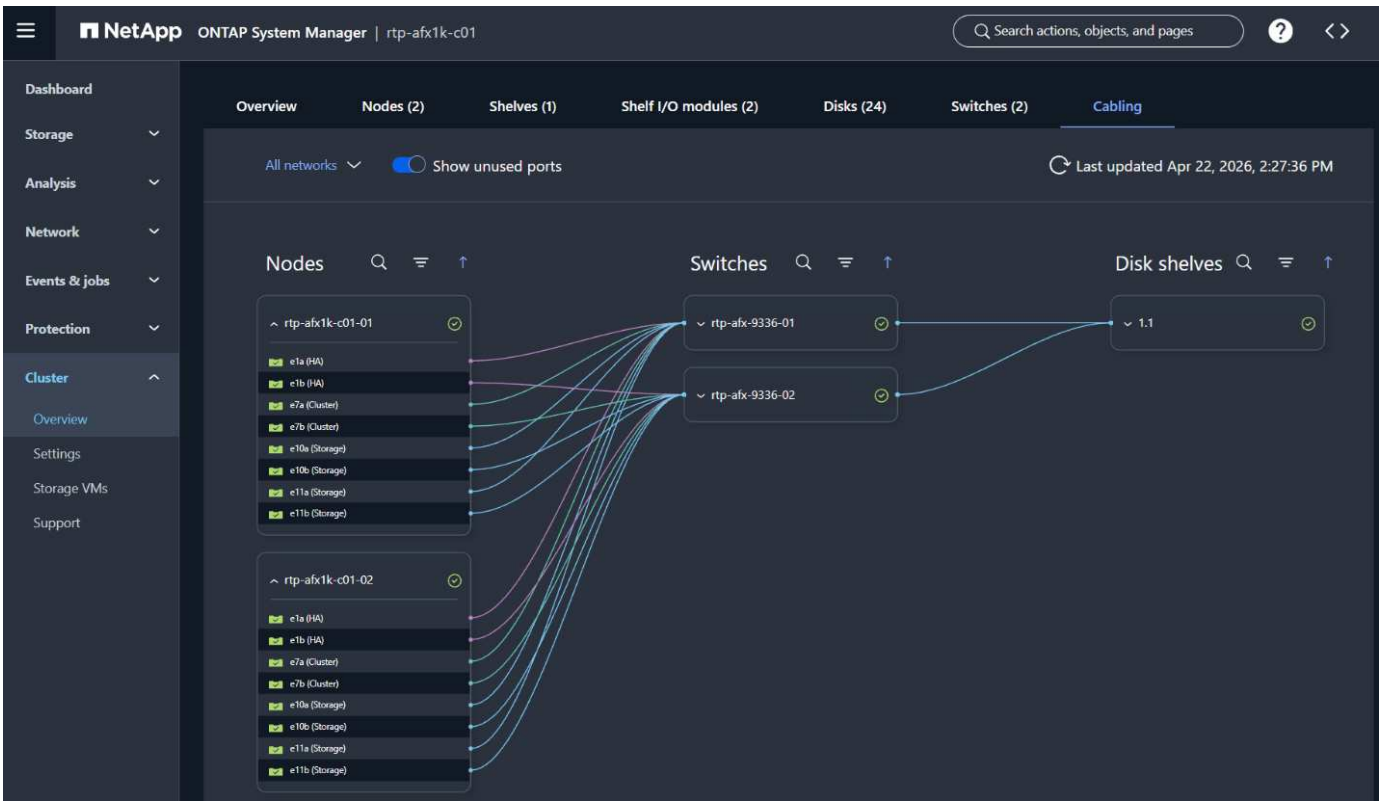
Como puedes ver en lo anterior, no hay muchas diferencias obvias en System Manager para ONTAP unificado y NetApp AFX. Sin embargo, hay algunas que lo indican.

Cómo NetApp AFX es diferente en System Manager



Al profundizar en los menús y cuadros de mando, casi todo sigue igual. Los volúmenes siguen mostrando la capacidad utilizada y total. Las interfaces de red siguen mostrando puertos y direcciones IP. Todavía puedes configurar políticas de protección para SnapMirror. Las vistas de hardware siguen estando disponibles. Pero NetApp AFX también mejora un poco las vistas al ofrecer una nueva vista de cableado, donde puedes profundizar y ver dónde están conectados todos los cables en toda la pila de almacenamiento.

NetApp vista del cableado AFX



API de REST

NetApp AFX también hace un esfuerzo concertado para conservar la mayoría de las llamadas a la API de REST de ONTAP, lo que significa que si has creado un conjunto de herramientas de automatización basadas en la API de REST, deberían poder seguir utilizándose en la mayoría de los casos. Las principales excepciones incluyen agregados, Metrocluster, SAN y algunos contadores de rendimiento. La documentación completa de la API de REST puede encontrarse en el System Manager del clúster NetApp AFX navegando a https://clus_mgmt_ip/docs/api.

Herramientas de gestión off-box de ONTAP

NetApp AFX proporciona cierto soporte para herramientas de gestión de ONTAP fuera de la caja, como:

- System Manager de NetApp
- NetApp Console
- Grafana Harvest (25.11.0 y posterior)
- NetApp Trident (25.10 y posteriores)

NetApp AFX no admite actualmente:

- NetApp ActiveIQ Unified Manager

Redes, seguridad y operaciones

NetApp AFX admite la misma pila de red, funciones de seguridad, tecnologías de protección de datos, operaciones no disruptivas y tipos de volumen que ONTAP unificado, con algunos ajustes exclusivos de la arquitectura desagregada.

Redes

La pila de red en NetApp AFX es idéntica a la de ONTAP unificado.

- Las LIF de datos se siguen utilizando para presentar direcciones de red a servicios internos y externos.
- Cada nodo tiene su propio conjunto de puertos físicos y virtuales.
- VLANs, ifgroups y BGP siguen siendo compatibles.
- Los LIF pueden seguir conmutando por error entre nodos físicos y puertos del clúster.
- Los IPspaces/dominios de difusión siguen estando configurados igual.
- Cada SVM puede tener su propia red de datos dedicada.
- Las redes de gestión pueden segmentarse de las redes de datos.
- Las redes de datos de los clientes no cambian fuera de la nueva incorporación de la compatibilidad con redes de 400GB.
- Los conmutadores de clúster del backend se siguen configurando a través de un archivo de "golden configuration" proporcionado por NetApp.

Algunas diferencias clave de la red son:

- Los puertos de red del clúster backend ahora solo admiten conexiones de 100GB a los conmutadores del clúster.

- Dado que los conmutadores del clúster tienen una capacidad de 400GB, las conexiones del nodo backend utilizan 4 cables breakout de 100GB para reducir el número de puertos usados en los conmutadores.
- La NVRAM ahora se refleja entre pares de HA a través de la red de clúster de backend mediante una nueva configuración de VLAN de HA en los switches.
- Se añade por defecto una nueva red DCN para el AI Data Engine. Estas direcciones IP se generan automáticamente y pueden cambiarse según sea necesario.

Seguridad

NetApp AFX ejecuta ONTAP, lo que significa que utiliza la misma seguridad que ONTAP. Todos los criptomódulos son idénticos, lo que significa que las certificaciones de seguridad serán idénticas una vez que se completen los procesos de certificación. NetApp AFX también aprovecha el mismo soporte para cifrados de seguridad que ONTAP unificado.

Además, NetApp AFX es compatible con muchas de las funciones de seguridad proporcionadas por unified ONTAP, incluidas (entre otras):

- Protección autónoma de ransomware
- Multi-tenancy seguro
- Cifrado en reposo (cifrado de volumen) y en vuelo (TLS 1.3)
- Unidades de autocifrado (SED)
- Autenticación y cifrado Kerberos para NFS y SMB
- Verificación de varios administradores
- SnapLock

Para obtener información sobre las certificaciones que ha recibido ONTAP unificado (así como otra información sobre el refuerzo de la seguridad), consulta:

- "NetApp Seguridad de productos"
- "Información general sobre el refuerzo de la seguridad de ONTAP"

Instantáneas y protección de datos

NetApp AFX aprovecha las mismas tecnologías de instantáneas y replicación que ONTAP unificado, sin grandes cambios en el funcionamiento de estas funciones. De hecho, AFX puede replicar desde y hacia sistemas ONTAP unificado con el mismo "reglas y configuraciones" con el que ya estás familiarizado.

La única excepción en AFX para la replicación tiene que ver con los volúmenes de FlexGroup que se replican en un sistema ONTAP unificado. En ese caso, el sistema ONTAP unificado de destino debe ejecutar ONTAP 9.16.1 o posterior para proporcionar soporte de Advanced Capacity Balancing.

Operaciones no disruptivas

ONTAP proporciona operaciones no disruptivas, como movimientos de volúmenes, actualizaciones, mantenimiento de clústeres, conmutaciones por error de almacenamiento y más. NetApp AFX ofrece las mismas operaciones no disruptivas, con algunos ajustes.

- Los movimientos de volumen siguen siendo no disruptivos, pero ya no requieren una copia.
- Las conmutaciones por error de almacenamiento siguen siendo no disruptivas, pero tras la conmutación por error inicial, los volúmenes se reequilibran en todos los nodos supervivientes del clúster.

- Las migraciones de LIF son idénticas.
- El mantenimiento y las actualizaciones del hardware son idénticos.

Tipos de volumen

Unified ONTAP admite varios tipos de volumen diferentes, como:

- FlexVols
- Volúmenes de FlexGroup
- FlexCache
- FlexClone
- Cubos de objetos

NetApp AFX proporciona compatibilidad total para cada uno de estos tipos de volumen, así como interoperabilidad total para volúmenes FlexCache con sistemas ONTAP unificados.

Para más información sobre cómo los volúmenes de FlexGroup se benefician de la arquitectura AFX, consulta "FlexGroup mejoras en la gestión de volúmenes".

Detalles del hardware

La siguiente sección cubre detalles sobre el hardware del clúster NetApp AFX. Para obtener la información más reciente sobre el hardware NetApp AFX, consulta "https://hwu.netapp.com".

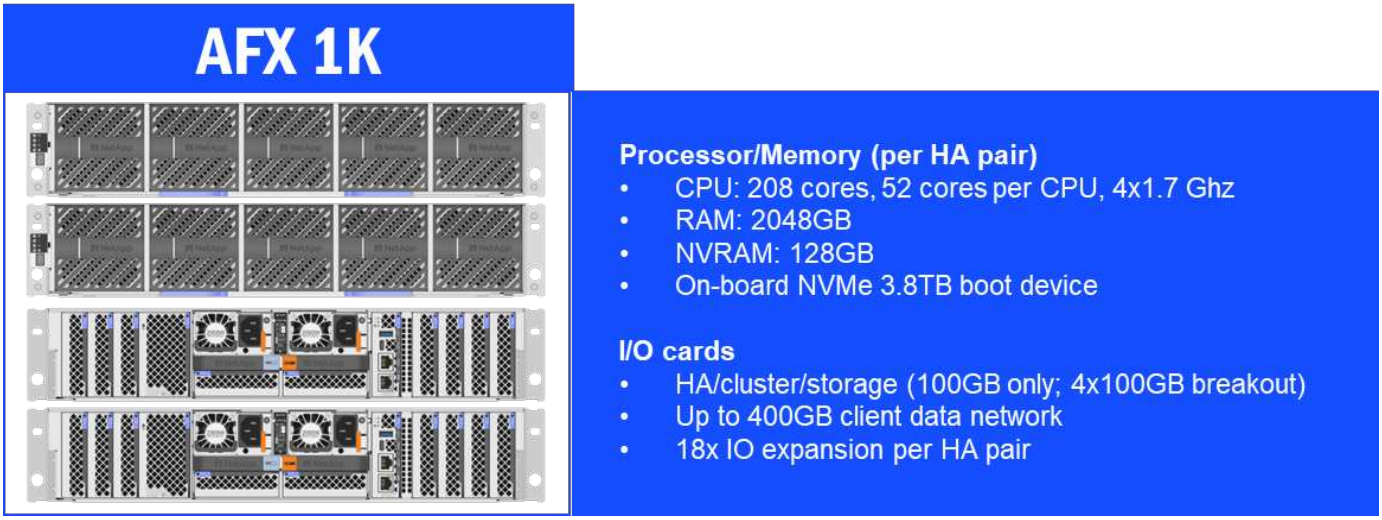
Hardware compatible

Para obtener la información más reciente sobre el hardware compatible con NetApp AFX, consulta "https://hwu.netapp.com".

Nodos

NetApp AFX se basan en el modelo de nodos AFF A1K proporcionado para clústeres ONTAP unificados. Estos nodos no tienen disco integrado para almacenamiento y están pensados para ser modulares, para que puedas añadir y quitar nodos fácilmente según los requisitos de rendimiento. Cada nodo utiliza 2U de espacio en rack y aumenta el rendimiento de forma lineal a medida que se añaden a un clúster AFX.

NetApp detalles del nodo AFX 1K



Ranuras de hardware

NetApp Los nodos AFX 1K utilizan las siguientes asignaciones de ranura.

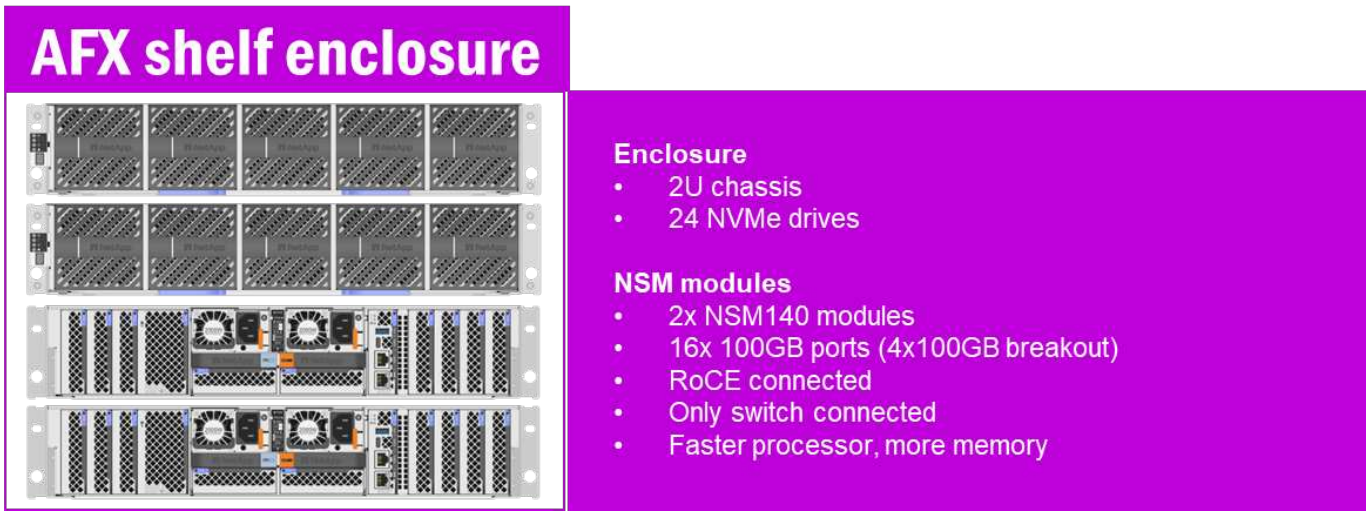
- La ranura 1 está dedicada a la replicación de HA
- La ranura 7 está dedicada a la replicación del clúster
- Las ranuras 10 y 11 están dedicadas a la comunicación del estante de almacenamiento

Bandejas

NetApp Las estanterías AFX utilizan los mismos armarios que los sistemas AFF. La principal diferencia entre las estanterías AFX radica en el módulo utilizado. Los módulos NSM140 proporcionan capacidades de rendimiento mejoradas y ayudan a hacer posible ONTAP desagregado. Algunas consideraciones clave:

- Solo se admiten estanterías completamente llenas.
- Las estanterías son detectadas automáticamente por NetApp AFX cuando se conectan.
- Actualmente no hay soporte para retirar estantes.

NetApp detalles de la caja de la estantería AFX

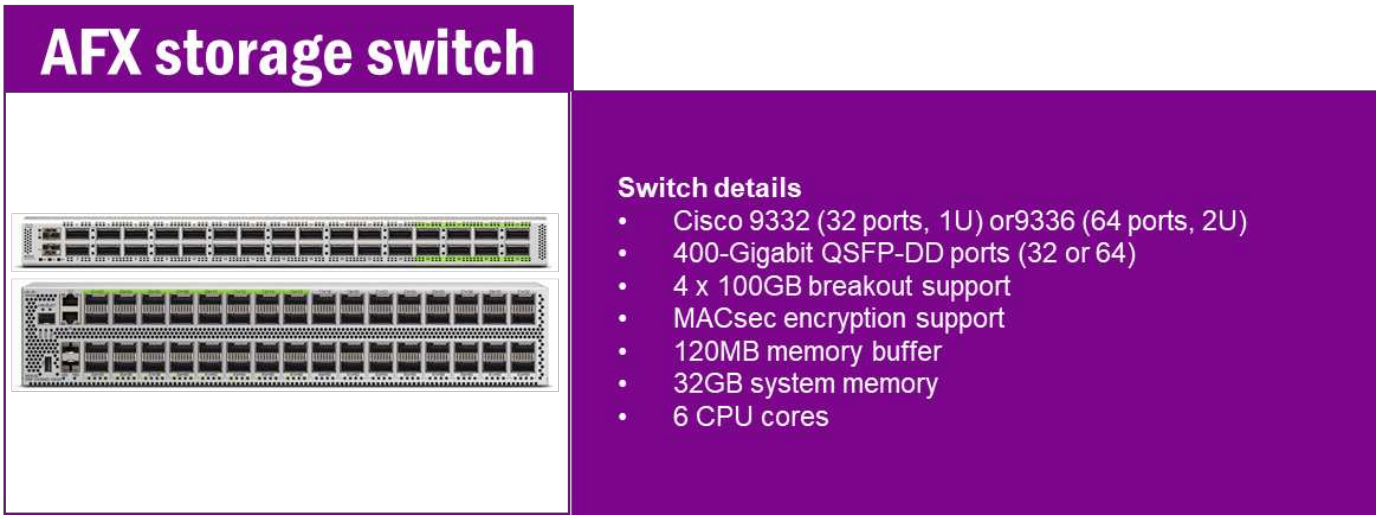


Switches

NetApp AFX sigue haciendo uso de los conmutadores de clúster backend para la comunicación intracluster, como la replicación de bases de datos de clúster, las operaciones de datos remotas, las operaciones de almacenamiento y la duplicación de NVRAM. Funcionalmente, las únicas diferencias entre los conmutadores de clúster unificados de ONTAP y NetApp AFX son:

- Compatibilidad con 400GbE
- Nueva HA VLAN
- Para más información, consulta la "Ficha técnica de los switches Cisco".

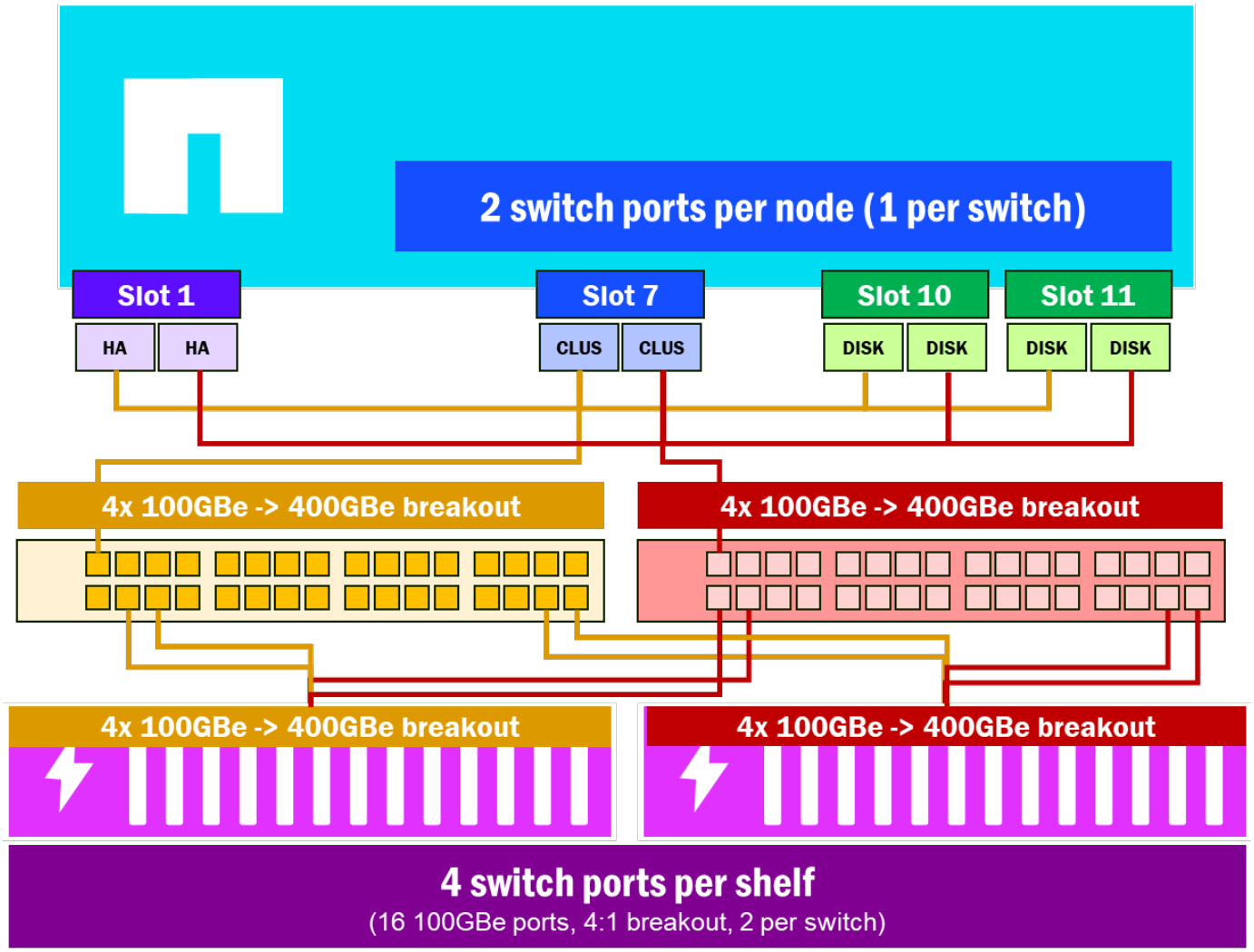
NetApp switches de clúster AFX



Conectividad del conmutador de clúster

NetApp AFX aprovecha en gran medida los conmutadores de clúster backend para muchos de sus principales conceptos arquitectónicos. Por ejemplo, las interfaces de clúster, los adaptadores de almacenamiento, los estantes de almacenamiento y las tarjetas NVRAM se conectan a los conmutadores de clúster. Actualmente, todas estas interfaces solo admiten comunicación de 100GB, mientras que los conmutadores admiten 400GB. Como resultado, las interfaces de 100GB se conectan a las interfaces de 400GB en el switch mediante cables breakout de 4 x 100GB. Este enfoque reduce el número de puertos utilizados en los switches. Por ejemplo, 16 puertos de módulo de estante de almacenamiento de 100GB usarán solo 4 puertos en los switches, mientras que los 8 puertos totales en los nodos usan 2 puertos del switch.

NetApp cableado del conmutador AFX



Tipos y tamaños de disco

NetApp AFX actualmente solo admite unidades SSD conectadas NVMe de los siguientes tamaños:

- 7,6 TB
- 15,3 TB
- 30,1 TB
- 60,6 TB

TLC frente a QLC

NetApp AFX puede aprovechar tanto los tipos de flash TLC como QLC. Las unidades de 7,6 y 15,3 TB son modelos TLC, mientras que las unidades de más de 30,1 TB serán QLC. Independientemente del tipo de soporte, se pueden cumplir los estándares de rendimiento de la certificación NVIDIA SuperPod.

Todas las unidades que se utilizan con NetApp AFX son unidades calificadas por su rendimiento, y tanto QLC como TLC tendrán un rendimiento casi idéntico para el tráfico de lectura. QLC se queda un poco atrás en el rendimiento de escritura en comparación con TLC y puede experimentar un poco más de nivelación de desgaste con cargas de trabajo con muchas escrituras.

Para conocer las cifras de rendimiento, consulta "Rendimiento por estante".

A la hora de elegir el tipo de unidad que se va a utilizar, ten en cuenta las cargas de trabajo que albergará el almacenamiento y las compensaciones entre rendimiento y densidad de capacidad.

Máximos y límites

La siguiente sección cubre los máximos y mínimos de un clúster NetApp AFX en comparación con unified ONTAP.

Para conocer los límites más recientes, consulta "Hardware Universe".

NetApp máximos y mínimos de AFX

Límite	ONTAP unificado	NetApp AFX
Recuento de volúmenes (cluster)	• 30.000 (en función de la plataforma)	• 30.000
Tamaño del agregado	• 800 TB	• N/A
Recuento de nodos	• 24	• 8 (9.17.1) • 32 (9.19.1RC1)
Capacidad total	• Depende del nodo y de la unidad. Consulta "hwu.netapp.com" para más detalles.	• 2PB (9.17.1) • 3PB (9.18.1RC1) • 16PB (versión 9.18.1GA) • 20PB (9.19.1RC0) • 32PB (9.19.1RC1)
Número de estantes compatibles	• 8 por par de HA • 192 por clúster	• 12 por clúster (9.18.1GA) • 17 por clúster (9.19.1RC0) • 25 por clúster (9.19.1RC1) (sin limitación de pares de HA)
Recuento total de unidades compatibles	• 240 por par de HA • 2880 (24 nodos)	• 288 por clúster (basado en los límites de recuento de estantes; sin limitación de pares de HA) • 408 por clúster (9.19.1RC0) • 600 por clúster (9.19.1RC1)
Tamaño del volumen	• 300 TB (FlexVol) • 60PB (FlexGroup)	• 300 TB (FlexVol) • 60 PB (FlexGroup)*
Máximo de archivos por volumen	• 2 mil millones (FlexVol) • 400 mil millones (FlexGroup)	• 2 mil millones (FlexVol) • 400 mil millones (FlexGroup)

Límite	ONTAP unificado	NetApp AFX
Máximo de archivos por directorio (valor por defecto 320MB maxdirsize)	• ~4 millones (FlexVol) • ~2 millones (FlexGroup)	• ~4 millones (FlexVol) • ~2 millones (FlexGroup)
SnapMirror transferencias simultáneas	• 250	• 250
Número de qtrees	• 4096	• 4096
Máximo de conexiones TCP por nodo	• 100.000	• 100.000
Número máximo de bloqueos por nodo	• 3 millones	• 3 millones
Número máximo de interfaces de datos (clúster)	• 4096	• 4096
Recuento máximo de constituyentes – FlexGroup	• 200	• 200 • 512 en 9.19.1 RC1
Número máximo de LIF intercluster	• 8	• 8
Número máximo de espacios IP	• 512	• 512
Número máximo de FlexCache por origen	• 100	• 100
Número máximo de FlexCache (nodo)	• 400	• 400

Dónde encontrar información adicional

Para saber más sobre la información que se describe en este documento, consulta los siguientes documentos y/o sitios web:

- Hardware universe "https://hwu.netapp.com/"
- NetApp página de producto AFX https://www.netapp.com/afx/
- NetApp AFX: infraestructura de datos de IA escalable y segura "https://www.netapp.com/blog/afx-scalable-secure-ai-data-infrastructure/"
- ¿Decidirse entre NFSv3 o NFSv4.x? La elección está cada vez más clara… "https://community.netapp.com/t5/Tech-ONTAP-Blogs/Deciding-between-NFSv3-or-NFSv4-x-The-choice-is-getting-clearer"
- NetApp Hoja de datos AFX "https://www.netapp.com/media/142853-ds-3466-netapp-afx-datasheet.pdf"

Informes técnicos de ONTAP SnapCenter

SnapCenter proporciona una plataforma unificada para la protección de datos y la gestión de clones de manera coherente con las aplicaciones. SnapCenter simplifica los procesos de backup y restauración y la gestión del ciclo de vida de los clones con flujos de trabajo integrados en las aplicaciones. Al aprovechar la gestión de datos basada en el almacenamiento, SnapCenter permite un aumento del rendimiento y la disponibilidad, y reduce los tiempos de pruebas y desarrollo.

Estos informes técnicos se amplían en "SnapCenter"la documentación del producto.

SnapCenter para Oracle

"TR-4700: Complemento de SnapCenter para prácticas recomendadas de base de datos de Oracle"
NetApp SnapCenter es una plataforma escalable y unificada para la protección de datos coherente con Oracle que automatiza las operaciones complejas con control y supervisión centralizados. Obtenga más información sobre las prácticas recomendadas para implementar bases de datos de Oracle con SnapCenter.

"TR-4964: Backup, restauración y clonación de bases de datos de Oracle con servicios de SnapCenter"
Descubre cómo configurar servicios de SnapCenter para realizar tareas de backup, restauración y clonado de bases de datos de Oracle implementadas en Amazon FSx para el almacenamiento de ONTAP y las instancias de computación EC2. Aunque es mucho más fácil de configurar y utilizar, los servicios de SnapCenter ofrecen funcionalidades clave disponibles a través de la interfaz de SnapCenter.

SnapCenter para Microsoft SQL Server

"TR-4714: Prácticas recomendadas para Microsoft SQL Server con NetApp SnapCenter"
Aprenda a implementar con éxito Microsoft SQL Server en almacenamiento de NetApp utilizando SnapCenter para la protección de datos.

SnapCenter para Microsoft Exchange Server

"TR-4681: Mejores prácticas para Microsoft Exchange Server con NetApp SnapCenter"
Aprenda a implementar con éxito Microsoft Exchange Server en un almacenamiento NetApp usando SnapCenter para la protección de datos.

SnapCenter para SAP HANA

"TR-4614: Backup y recuperación de datos de SAP HANA con SnapCenter" SnapCenter es una plataforma escalable y unificada destinada a la protección de datos de manera coherente con las aplicaciones para SAP HANA y otras bases de datos. SnapCenter proporciona control y supervisión centralizados, a la vez que delega la capacidad para que los usuarios gestionen trabajos de backup, restauración y clonado específicos de aplicaciones. Con SnapCenter, los administradores de bases de datos y almacenamiento conocen una única herramienta para gestionar los backups, las restauraciones de datos y las operaciones de clonado para diferentes aplicaciones y bases de datos.

"TR-4926: SAP HANA en Amazon FSX para ONTAP de NetApp: Backup y recuperación de datos con SnapCenter" Obtén más información sobre las prácticas recomendadas para la protección de datos de SAP HANA en Amazon FSx para NetApp ONTAP y SnapCenter. Los temas incluyen conceptos de SnapCenter,

recomendaciones de configuración y flujos de trabajo de operaciones, incluidas la configuración, las operaciones de backup, y las operaciones de restauración y recuperación.

"TR-4667: Automatización de las operaciones de clonado y copia del sistema SAP HANA con SnapCenter" La clonación del almacenamiento de SnapCenter y la opción de definir de manera flexible las operaciones previas y posteriores a la clonación permiten a los administradores de SAP Basis acelerar y automatizar las operaciones de copia, clonación o actualización del sistema SAP. Descubra ahora la opción de elegir cualquier backup Snapshot de SnapCenter en cualquier sistema de almacenamiento primario o secundario le permite abordar sus casos prácticos más importantes, como daños lógicos, pruebas de recuperación ante desastres, o la actualización de un sistema de control de calidad SAP.

"TR-4719: Backup y recuperación de datos de replicación de sistemas SAP HANA con SnapCenter" Descubra cómo la tecnología de SnapCenter y el complemento SAP HANA se pueden utilizar para realizar backups y recuperación de datos en un entorno de replicación de sistemas SAP HANA.

"TR-4667: Automatización de las operaciones de clonado y copia del sistema SAP HANA con SnapCenter" La capacidad de crear backups de Snapshot de NetApp consistentes con las aplicaciones en la capa de almacenamiento es la base para las operaciones de clonado del sistema y copia del sistema. Los backups de Snapshot basados en el almacenamiento se crean mediante el plugin de SnapCenter de NetApp para SAP HANA y las interfaces que proporciona la base de datos SAP HANA. SnapCenter registra los backups de Snapshot en el catálogo de backup de SAP HANA, de manera que estos backups se puedan usar para operaciones de restauración y recuperación, así como para operaciones de clonado.

Guía de endurecimiento de SnapCenter

"TR-4957: Guía de refuerzo de la seguridad para NetApp SnapCenter" Aprenda a configurar SnapCenter para ayudar a las organizaciones a cumplir los objetivos de seguridad prescritos para la confidencialidad, la integridad y la disponibilidad de los sistemas de información.

Informes técnicos de organización en niveles de ONTAP

Con la solución de organización en niveles de datos de FabricPool, la experiencia general de las empresas con los sistemas flash mejora y evita los inconvenientes de volver a diseñar aplicaciones para mejorar la eficiencia del almacenamiento. FabricPool reduce el espacio de almacenamiento y los costes asociados de un entorno de sistema. Los datos activos permanecen en SSD de alto rendimiento. Los datos inactivos se organizan en niveles en un almacenamiento de objetos de bajo coste y conservan las eficiencias del almacenamiento.

Estos informes técnicos se amplían en "ONTAP FabricPool"la documentación del producto.

"TR-4598: Prácticas recomendadas de FabricPool"
Conozca las funcionalidades, los requisitos, la implementación y las prácticas recomendadas para FabricPool.

"TR-4826: Guía de recomendaciones de NetApp FabricPool con StorageGRID"
Obtenga más información sobre las prácticas recomendadas para poner en marcha y ajustar el tamaño de StorageGRID como nivel de capacidad para la FabricPool del componente de ONTAP. En este documento también se tratan funcionalidades básicas, requisitos, implementación y prácticas recomendadas al utilizar StorageGRID.

"TR-4695: Organización en niveles de almacenamiento de base de datos con NetApp FabricPool"
Obtenga información sobre las ventajas y las opciones de configuración de FabricPool con varias bases de datos, incluido el sistema de gestión de bases de datos relacionales de Oracle (RDBMS).

Informes técnicos sobre virtualización de ONTAP

Las soluciones de virtualización de NetApp ayudan a sacar el máximo valor de sus servidores. Con una infraestructura de servidores virtuales con gran capacidad de respuesta basada en los pioneros sistemas flash ONTAP de alto rendimiento, podrá acceder a sus datos mucho más rápido. Su infraestructura virtual granular puede escalar sin provocar interrupciones del servicio hasta alcanzar varios petabytes de datos y ofrecer el rendimiento que necesita para garantizar el acceso compartido a varias cargas de trabajo. ONTAP ayuda a optimizar y reducir la complejidad de la puesta en marcha de su infraestructura de servidores virtuales con colaboraciones clave, indicaciones para la implementación, integración de aplicaciones y un diseño superior. ONTAP ofrece muchas prácticas y soluciones recomendadas para un entorno de virtualización sólido tanto en las instalaciones como en el cloud.

Estos informes técnicos se amplían en "Herramientas de ONTAP para VMware vSphere"la documentación del producto.

"TR-4597: VMware vSphere para ONTAP" ONTAP ha sido una solución de almacenamiento líder para entornos de VMware vSphere durante casi dos décadas y continúa añadiendo funcionalidades innovadoras para simplificar la gestión al tiempo que reduce los costes. Este documento presenta la solución ONTAP para vSphere, incluyendo la información más reciente sobre el producto y las prácticas recomendadas para simplificar la puesta en marcha, reducir el riesgo y simplificar la gestión.

"TR-4400: VMware vSphere Virtual Volumes (vVols) con ONTAP de NetApp" ONTAP ha sido una solución de almacenamiento líder para entornos VMware vSphere durante más de dos décadas y continúa añadiendo funcionalidades innovadoras para simplificar la gestión al tiempo que reduce los costes. Este documento trata las funcionalidades de ONTAP para VMware vSphere Virtual Volumes (vVols), incluida la información más reciente sobre el producto y los casos de uso, junto con las prácticas recomendadas y otra información para optimizar la puesta en marcha y reducir los errores.

"TR-4900: VMware Site Recovery Manager con NetApp ONTAP" ONTAP ha sido una solución de almacenamiento líder para entornos VMware vSphere desde su introducción en el centro de datos moderno en 2002, y continúa añadiendo funcionalidades innovadoras para simplificar la gestión y reducir los costes. Este documento presenta la solución ONTAP para VMware Site Recovery Manager (SRM), el software de recuperación ante desastres (DR) líder del sector de VMware, que incluye la información de producto más reciente y las prácticas recomendadas para simplificar la puesta en marcha, reducir el riesgo y simplificar la gestión continua.

"Introducción a la automatización para ONTAP y vSphere" La automatización ha sido una parte integral de la gestión de entornos VMware desde los primeros días de VMware ESX. La capacidad de poner en marcha infraestructura como código y ampliar las prácticas en operaciones de cloud privado ayuda a paliar las cuestiones relacionadas con el escalado, la flexibilidad, el aprovisionamiento automático y la eficiencia. Este documento presenta la solución de ONTAP para automatizar el entorno de ONTAP y VMware vSphere.

"Artículo técnico WP-7353: Herramientas de ONTAP para VMware vSphere - Seguridad del producto" Este documento describe las técnicas y la tecnología empleadas para proteger las herramientas de ONTAP para VMware vSphere 9.X de las amenazas existentes y emergentes en entornos de productos.

"WP-7355: Complemento SnapCenter Vmware vSphere - Seguridad del producto" Este documento describe las técnicas y la tecnología utilizadas para proteger el complemento NetApp SnapCenter para VMware vSphere 4.X de las amenazas existentes y emergentes en entornos de productos.

"TR-4568: Directrices de puesta en marcha de NetApp y prácticas recomendadas de almacenamiento para Windows Server" Microsoft Windows Server es un sistema operativo de clase empresarial que cubre redes, seguridad, virtualización, nube, infraestructura de escritorio virtual, protección de acceso, protección de información, servicios web, infraestructura de plataforma de aplicaciones y mucho más. Este documento se centra en Microsoft Windows, donde se presta un especial énfasis en la tecnología de virtualización de Hyper-V, incluida la información de producto más reciente y las prácticas recomendadas para simplificar la puesta en marcha, reducir los riesgos y simplificar la gestión.

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/"

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/"

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/"

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 9.16.1" "Aviso para ONTAP 9.16.0" "Aviso para ONTAP 9.15.1" "Aviso para ONTAP 9.15.0" "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 de ONTAP para configuraciones IP de MetroCluster

"9.9.1 Aviso para Mediador ONTAP para configuraciones IP de MetroCluster" "9,8 Aviso para Mediador ONTAP para configuraciones IP de MetroCluster" "9,7 Aviso para Mediador ONTAP para configuraciones IP de MetroCluster"