Seguridad

ONTAP Technical Reports

NetApp
January 23, 2026

Tabla de contenidos

Seguridad . . . 1
- Informes técnicos de seguridad de ONTAP . . . 1
  - Ciberalmacén de ONTAP . . . 1
  - Ransomware . . . 1
  - Confianza cero . . . 1
  - Autenticación multifactor . . . 1
  - Multi-tenancy . . . 2
  - Estándares . . . 2
  - Control de acceso basado en atributos . . . 2
- Solución de NetApp para ransomware . . . 2
  - La cartera de protección de NetApp y ransomware . . . 2
  - SnapLock y snapshots a prueba de manipulaciones para la protección contra el ransomware . . . 5
  - Bloqueo de archivos FPolicy . . . 6
  - Data Infrastructure Insights Almacenamiento Carga de trabajo Seguridad . . . 7
  - Detección y respuesta integradas de NetApp ONTAP basadas en IA . . . 8
  - Protección WORM aislada con copia digital en ONTAP . . . 9
  - Protección frente al ransomware del asesor digital . . . 11
  - Resiliencia integral con protección contra ransomware de NetApp . . . 11
- NetApp y Zero Trust . . . 12
  - NetApp y Zero Trust . . . 12
  - Diseñe un enfoque de Zero Trust centrado en los datos con ONTAP . . . 14
  - Controles de orquestación y automatización de la seguridad de NetApp externos a ONTAP . . . 19
  - Puesta en marcha de cloud híbrido y confianza cero . . . 19
- Control de acceso basado en atributos . . . 20
  - Control de acceso basado en atributos con ONTAP . . . 20
  - Enfoques para el control de acceso basado en atributos (ABAC) en ONTAP . . . 20

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.

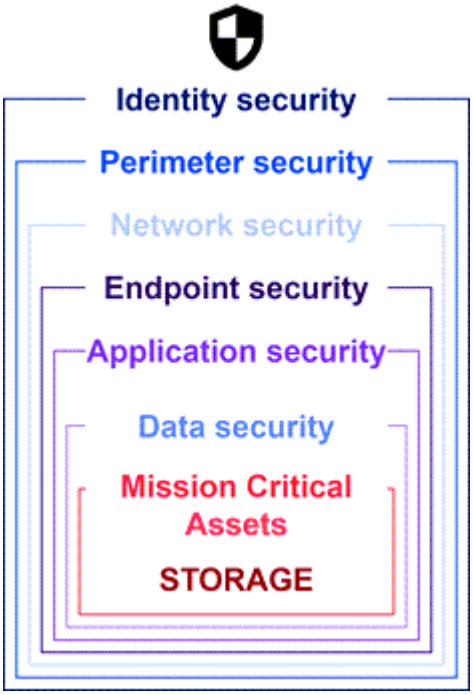
El Gama de productos de NetApp ofrece varias herramientas eficaces para la visibilidad, detección y corrección que ayudan a detectar el ransomware de manera temprana, prevenir la propagación y recuperarse rápidamente, si es necesario, para evitar costosos tiempos de inactividad. Las soluciones tradicionales 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.

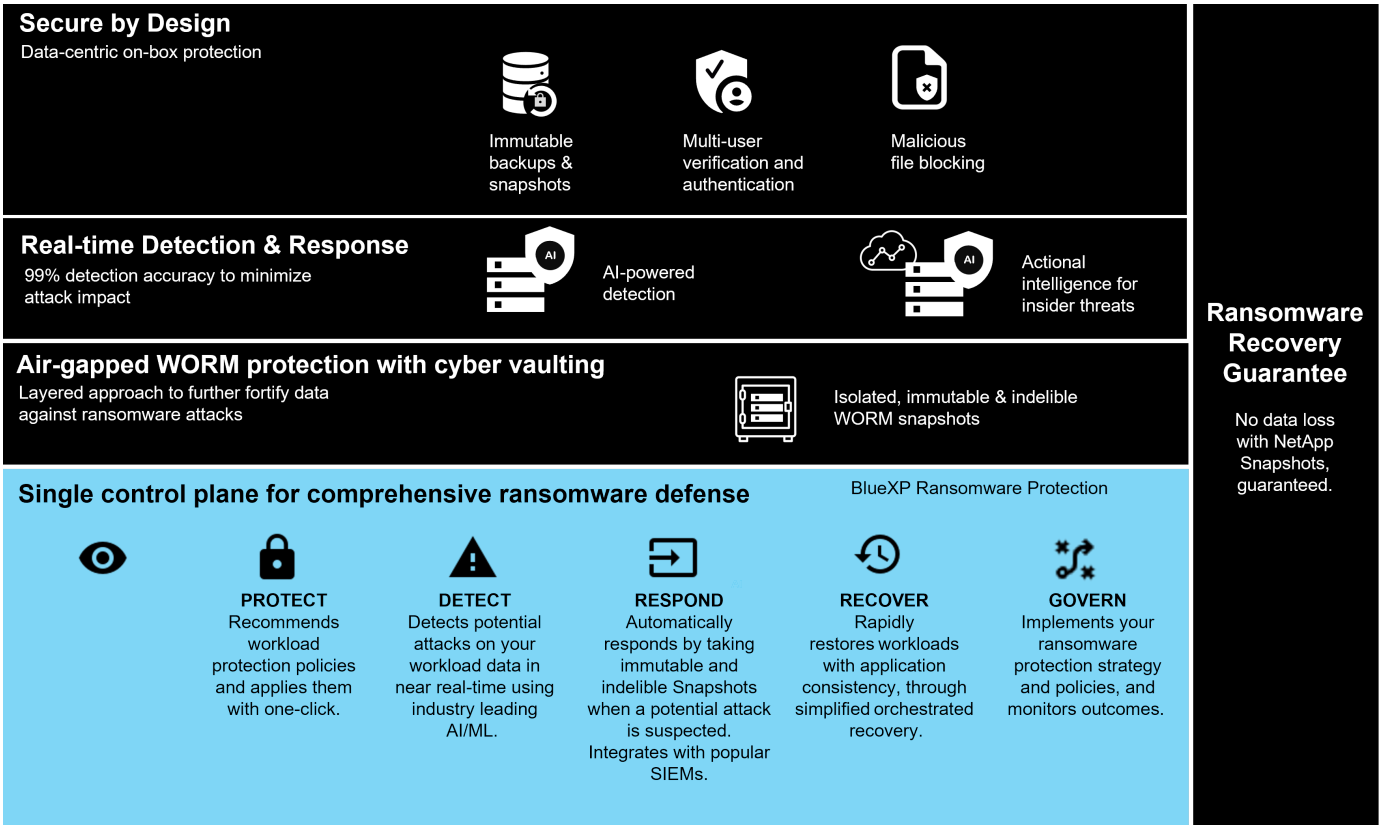
Protección frente a ransomware en la capa de datos

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

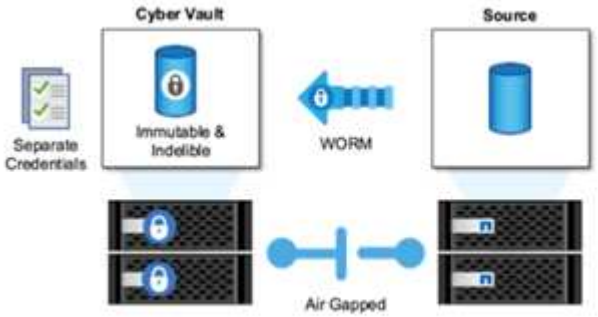
El enfoque de NetApp de un ciberalmacén es una arquitectura de referencia creada específicamente para un ciberalmacén con brecha lógica. Este enfoque aprovecha las tecnologías de refuerzo de la seguridad y cumplimiento de normativas, como SnapLock, para permitir copias Snapshot inalterables e indelebles.

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".

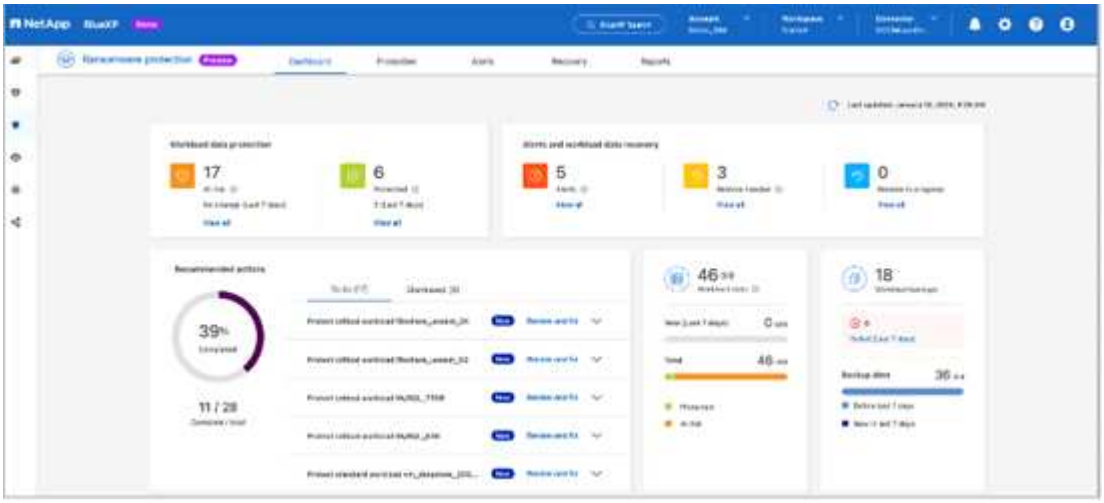
Resiliencia integral con protección contra ransomware de NetApp

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.

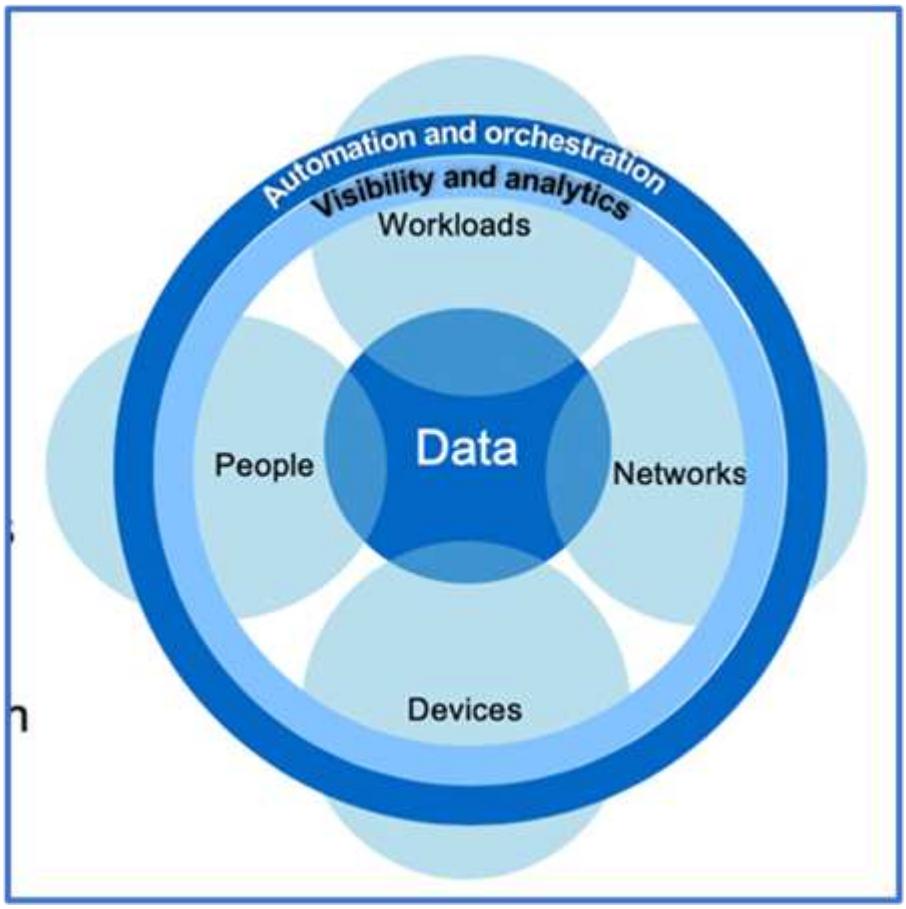
Recursos de seguridad

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

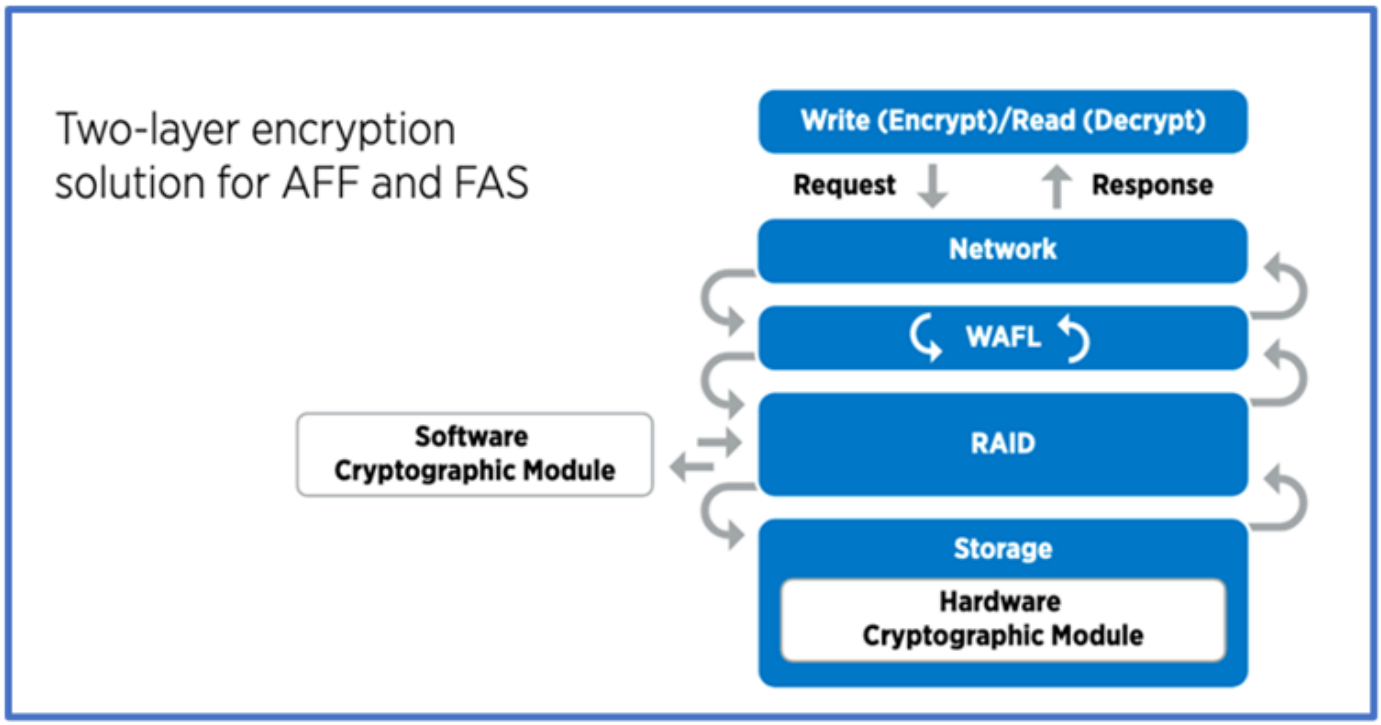
Cifrado de los datos en reposo

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

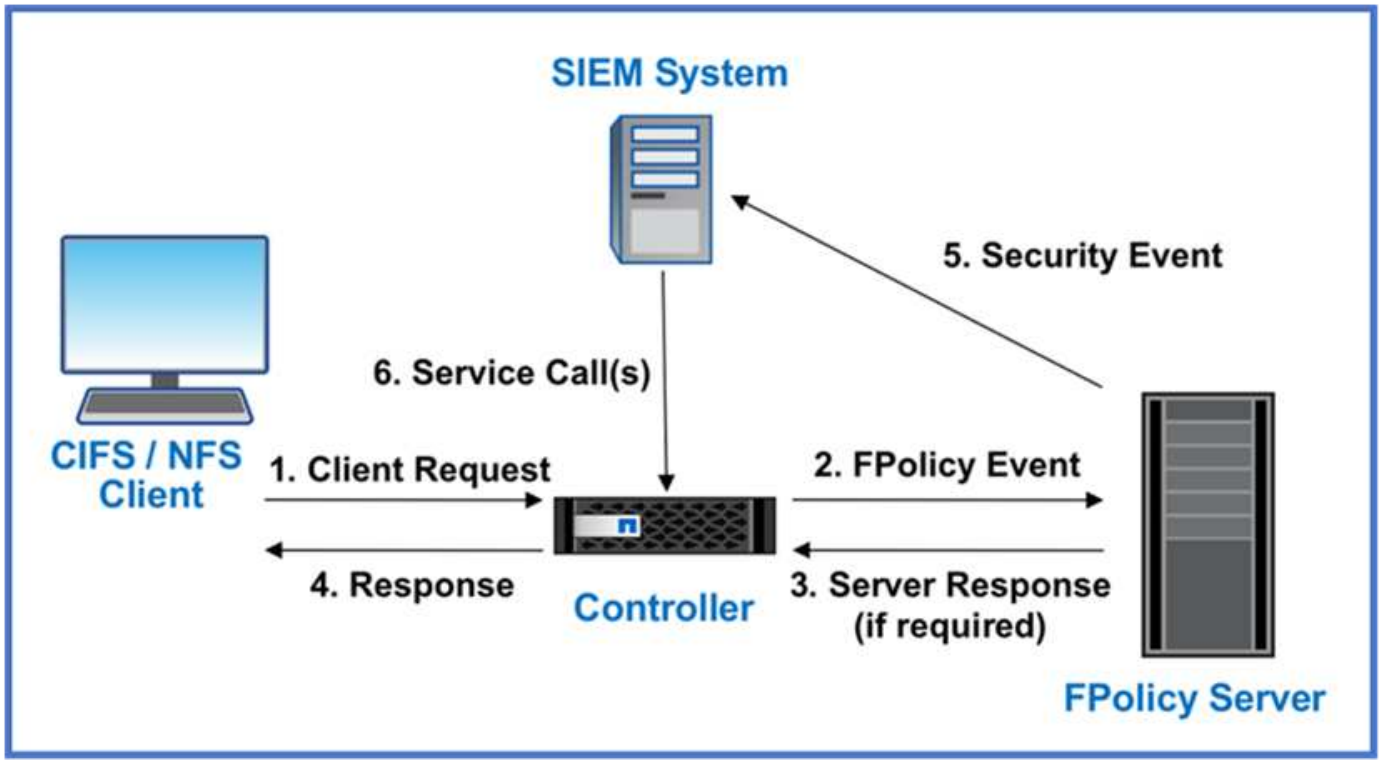
El cifrado de datos en tiempo real de ONTAP protege el acceso a los datos de usuario y el acceso al plano de control. El acceso a los datos del usuario puede cifrarse mediante el cifrado SMB 3,0 para el acceso a recursos compartidos de Microsoft CIFS o por krb5P para Kerberos 5 NFS. El acceso a los datos 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.

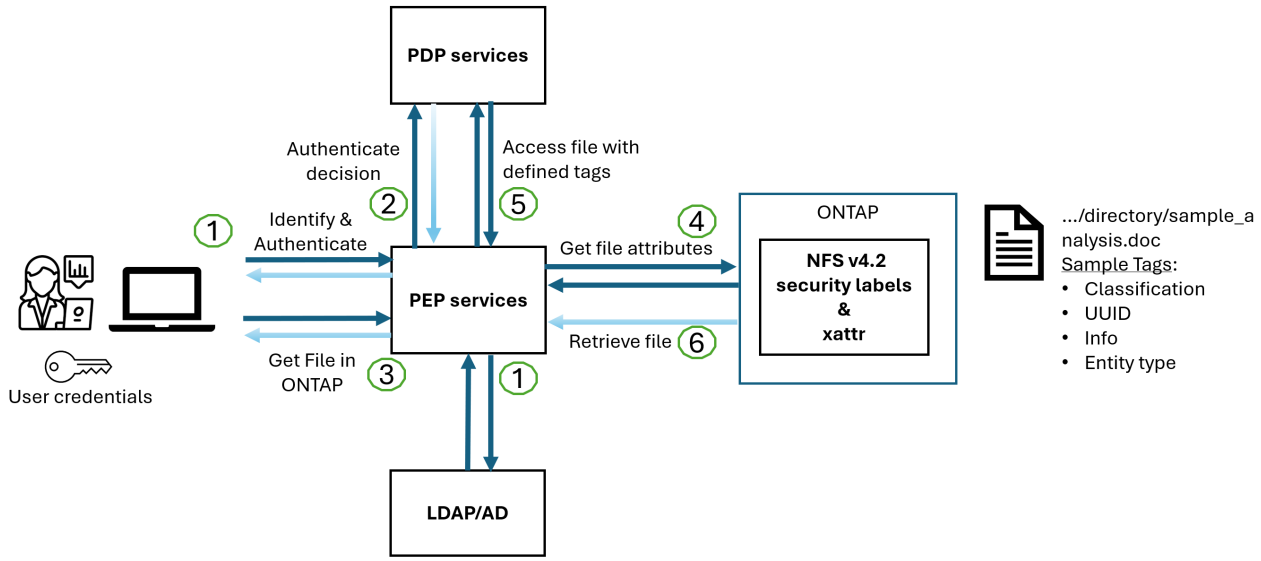
   Estas políticas tienen en cuenta varios atributos relacionados con el usuario, el recurso en cuestión y el entorno circundante. Basándose en estas políticas, el PDP toma una decisión de acceso para permitir o denegar y luego comunica esta decisión al PEP.

   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"

Información de copyright

Información de la marca comercial