Seguridad

ONTAP 9

NetApp
January 08, 2026

Tabla de contenidos

Seguridad

Autenticación y autorización de clientes

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

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

Autenticación

Es posible crear cuentas de usuario locales o remotas:

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

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

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

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

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

Autorización

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

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

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

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

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

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

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

Autenticación con SAML

ONTAP admite el lenguaje de marcado de aserción de seguridad (SAML) para la autenticación de usuarios remotos. Se admiten varios proveedores de identidad (IDPs) populares. Para obtener más información sobre los IDPs soportados e instrucciones para habilitar la autenticación SAML, consulte "Configurar la autenticación SAML".

OAuth 2,0 con clientes API REST DE ONTAP

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

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

Autenticación de administrador y RBAC

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

Autenticación

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

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

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

utiliza para autenticar clientes.

RBAC

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

Detección de virus

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

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

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

  El análisis durante el acceso no es compatible con NFS.

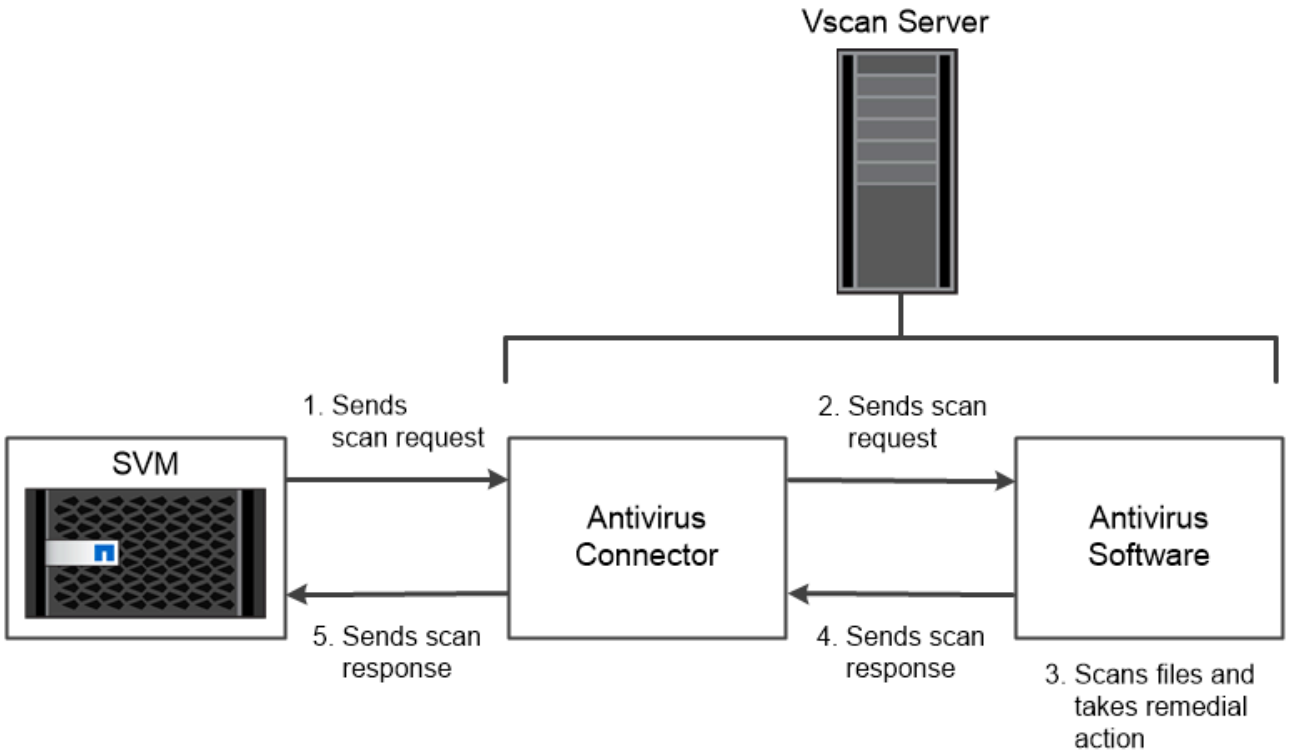
- Puede utilizar *análisis bajo demanda* para comprobar los archivos en busca de virus inmediatamente o en una programación. Por ejemplo, es posible que desee ejecutar análisis sólo en horas de menor actividad. El servidor externo actualiza el estado de análisis de los archivos comprobados, de modo que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

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

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

detección de virus en recuperación de desastres y configuraciones de MetroCluster

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



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

Cifrado

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

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

- Soluciones de hardware:
  - Cifrado en almacenamiento de NetApp (NSE)

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

  - SED de NVMe

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

- Soluciones de software:
  - Cifrado de agregados de NetApp (NAE)

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

  - Cifrado de volúmenes de NetApp (NVE)

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

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

Cifrado del almacenamiento de NetApp

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

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

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

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

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

Unidades de autocifrado NVMe

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

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

Cifrado de agregados de NetApp

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

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

A partir de ONTAP 9.7, los agregados y los volúmenes recién creados se cifran de forma predeterminada cuando dispone de "Licencia de NVE"la gestión de claves externa o incorporada.

Cifrado de volúmenes de NetApp

El cifrado de volúmenes de NetApp (NVE) es una tecnología basada en software para cifrar datos en reposo un volumen por vez. Una clave de cifrado que solo puede acceder el sistema de almacenamiento garantiza

que los datos de volumen no se puedan leer si el dispositivo subyacente está separado del sistema.

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

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

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

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

  Los servidores KMIP admiten múltiples clústeres con una gestión centralizada de las claves de cifrado.
- Su empresa requiere una seguridad añadida para almacenar claves de autenticación en un sistema o en una ubicación distinta de los datos.

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

Información relacionada

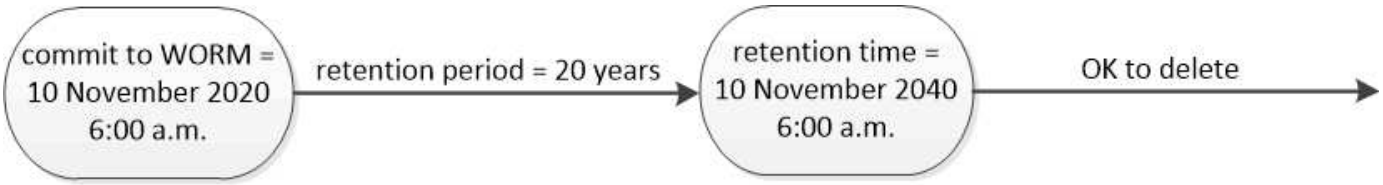
"Preguntas más frecuentes: Cifrado de volúmenes de NetApp y cifrado de agregados de NetApp"

Almacenamiento de WORM

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

Una sola licencia le da derecho a usar SnapLock en el modo estricto *Cumplimiento* para cumplir con los mandatos externos como la Regla SEC 17a-4(f) y un modo más suelto *Empresa,* para cumplir con las regulaciones internas para la protección de activos digitales. SnapLock utiliza un *ComplianceClock_prueba de manipulación* para determinar cuándo ha transcurrido el período de retención de un archivo WORM.

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



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