Cómo afectan los estilos de seguridad al acceso a los datos

ONTAP 9

NetApp
February 12, 2026

This PDF was generated from https://docs.netapp.com/es-es/ontap/nfs-admin/security-styles-their-effects-concept.html on February 12, 2026. Always check docs.netapp.com for the latest.

Tabla de contenidos

Cómo afectan los estilos de seguridad al acceso a los datos 1
Conozca los estilos de seguridad de ONTAP NAS 1
Obtenga información sobre los estilos de seguridad en los volúmenes ONTAP NFS FlexVol 2
Decide qué estilo de seguridad utilizar en las SVM de ONTAP NAS 2
Obtenga más información sobre la herencia del estilo de seguridad NFS de ONTAP 3
Obtenga información sobre la conservación de permisos de ONTAP NFS UNIX 3
Administre los permisos de UNIX en las SVM NFS de ONTAP mediante la pestaña Seguridad de Windows 3

Cómo afectan los estilos de seguridad al acceso a los datos

Conozca los estilos de seguridad de ONTAP NAS

Hay cuatro estilos de seguridad diferentes: UNIX, NTFS, mixto y unificado. Cada estilo de seguridad tiene un efecto diferente sobre cómo se gestionan los permisos para los datos. Debe comprender los diferentes efectos para asegurarse de que selecciona el estilo de seguridad adecuado para sus propósitos.

Es importante entender que los estilos de seguridad no determinan qué tipos de clientes pueden o no pueden tener acceso a los datos. Los estilos de seguridad sólo determinan el tipo de permisos que ONTAP utiliza para controlar el acceso a los datos y qué tipo de cliente puede modificar estos permisos.

Por ejemplo, si un volumen utiliza el estilo de seguridad UNIX, los clientes SMB todavía pueden acceder a los datos (siempre y cuando estos se autentiquen y autoricen correctamente) debido a la naturaleza multiprotocolo de ONTAP. Sin embargo, ONTAP utiliza permisos UNIX que sólo los clientes UNIX pueden modificar mediante herramientas nativas.

Estilo de seguridad	Clientes que pueden modificar permisos	Permisos que pueden utilizar los clientes	El estilo de seguridad efectivo resultante	Clientes que pueden acceder a los ficheros
UNIX	NFS	Bits del modo NFSv3	UNIX	NFS y SMB
		ACL de NFSv4.x		
NTFS	SMB	ACL de NTFS	NTFS	
Mixto	NFS o SMB	Bits del modo NFSv3	UNIX	
		NFSv4.ACLs		
		ACL de NTFS	NTFS	
Unificado (solo para Infinite Volume, en ONTAP 9.4 y versiones anteriores).	NFS o SMB	Bits del modo NFSv3	UNIX	
		ACL de NFSv4.1		
		ACL de NTFS	NTFS	

Los volúmenes de FlexVol son compatibles con UNIX, NTFS y estilos de seguridad mixtos. Cuando el estilo de seguridad es mixto o unificado, los permisos efectivos dependen del tipo de cliente que modificó por última vez los permisos porque los usuarios establecen el estilo de seguridad de forma individual. Si el último cliente que modificó permisos era un cliente NFSv3, los permisos son bits del modo NFSv3 de UNIX. Si el último cliente era un cliente NFSv4, los permisos son ACL de NFSv4. Si el último cliente era un cliente SMB, los permisos son ACL de Windows NTFS.

El estilo de seguridad unificado solo está disponible en Infinite Volume, que ya no son compatibles con ONTAP 9.5 y versiones posteriores. Para obtener más información, consulte Información general de gestión de volúmenes de FlexGroup.

El `show-effective-permissions` parámetro con el `vserver security file-directory` El comando le permite mostrar los permisos efectivos otorgados a un usuario de Windows o UNIX en la ruta de archivo o carpeta especificada. Además, el parámetro opcional `-share-name` le permite mostrar el permiso de uso compartido efectivo. Obtenga más información sobre `vserver security file-directory show-effective-permissions` en el "Referencia de comandos del ONTAP".

> ONTAP establece inicialmente algunos permisos de archivo predeterminados. De forma predeterminada, el estilo de seguridad efectivo de todos los datos de los volúmenes de estilo de seguridad mixto y unificado es UNIX y el tipo de permisos efectivos es bits de modo UNIX (0755 a menos que se especifique lo contrario) hasta que un cliente lo configure como permite el estilo de seguridad predeterminado. De forma predeterminada, el estilo de seguridad efectivo en todos los datos de los volúmenes de estilo de seguridad NTFS es NTFS y tiene una ACL que permite un control total para todos.

Información relacionada

- "Referencia de comandos del ONTAP"

Obtenga información sobre los estilos de seguridad en los volúmenes ONTAP NFS FlexVol

Los estilos de seguridad se pueden establecer en volúmenes de FlexVol (tanto volúmenes raíz como de datos) y qtrees. Los estilos de seguridad se pueden configurar manualmente en el momento de la creación, heredados automáticamente o modificados posteriormente.

Decide qué estilo de seguridad utilizar en las SVM de ONTAP NAS

Para ayudar a decidir qué estilo de seguridad se debe usar en un volumen, se deben tener en cuenta dos factores. El factor principal es el tipo de administrador que administra el sistema de archivos. El factor secundario es el tipo de usuario o servicio que tiene acceso a los datos del volumen.

Al configurar el estilo de seguridad en un volumen, debe tener en cuenta las necesidades del entorno para garantizar que selecciona el mejor estilo de seguridad y evitar problemas con la gestión de permisos. Las siguientes consideraciones pueden ayudarle a decidir:

Estilo de seguridad	Elija si…
UNIX	• Un administrador de UNIX gestiona el sistema de ficheros. • La mayoría de los usuarios son clientes NFS. • Una aplicación que accede a los datos utiliza un usuario UNIX como cuenta de servicio.

NTFS	• Un administrador de Windows gestiona el sistema de archivos. • La mayoría de los usuarios son clientes SMB. • Una aplicación que accede a los datos utiliza un usuario de Windows como cuenta de servicio.
Mixto	• El sistema de archivos lo gestionan administradores de UNIX y Windows, y los usuarios están formados por clientes NFS y SMB.

Obtenga más información sobre la herencia del estilo de seguridad NFS de ONTAP

Si no especifica el estilo de seguridad al crear un nuevo volumen de FlexVol o un qtree, hereda su estilo de seguridad de formas diferentes.

Los estilos de seguridad se heredan de la siguiente manera:

- Un volumen FlexVol hereda el estilo de seguridad del volumen raíz de su SVM que contiene.
- Un qtree hereda el estilo de seguridad del volumen FlexVol que contiene.
- Un archivo o un directorio hereda el estilo de seguridad de su volumen o qtree de FlexVol.

Obtenga información sobre la conservación de permisos de ONTAP NFS UNIX

Cuando las aplicaciones Windows editan y guardan archivos de un volumen FlexVol que actualmente tienen permisos UNIX, ONTAP puede preservar los permisos UNIX.

Cuando las aplicaciones de clientes de Windows editan y guardan archivos, leen las propiedades de seguridad del archivo, crean un nuevo archivo temporal, aplican esas propiedades al archivo temporal y, a continuación, asignan al archivo temporal el nombre de archivo original.

Cuando los clientes de Windows realizan una consulta para las propiedades de seguridad, reciben una ACL construida que representa exactamente los permisos de UNIX. El único propósito de esta ACL construida es preservar los permisos UNIX del archivo a medida que las aplicaciones de Windows actualizan los archivos para garantizar que los archivos resultantes tengan los mismos permisos UNIX. ONTAP no establece ninguna ACL de NTFS usando la ACL construida.

Administre los permisos de UNIX en las SVM NFS de ONTAP mediante la pestaña Seguridad de Windows

Si desea manipular los permisos de UNIX de archivos o carpetas en volúmenes o qtrees de estilo de seguridad mixtos en las SVM, puede utilizar la pestaña Seguridad en clientes de Windows. También puede utilizar aplicaciones que puedan consultar y establecer ACL de Windows.

- Modificación de permisos de UNIX

Puede usar la pestaña Seguridad de Windows para ver y cambiar los permisos de UNIX para un volumen o un qtree de estilo de seguridad mixto. Si utiliza la ficha Seguridad de Windows principal para cambiar los permisos de UNIX, primero debe quitar la ACE existente que desea editar (esto establece los bits de modo en 0) antes de realizar los cambios. De forma alternativa, puede utilizar el editor avanzado para cambiar los permisos.

Si se utilizan permisos de modo, puede cambiar directamente los permisos de modo para el UID, GID y otros (todos los demás con una cuenta en el equipo) de la lista. Por ejemplo, si el UID mostrado tiene permisos r-x, puede cambiar los permisos de UID a rwx.

- Cambiar los permisos de UNIX a los permisos NTFS

  Puede usar la pestaña Seguridad de Windows para reemplazar objetos de seguridad UNIX por objetos de seguridad de Windows en un volumen o qtree de estilo de seguridad mixto donde los archivos y carpetas tienen un estilo de seguridad efectivo de UNIX.

  Primero debe quitar todas las entradas de permisos de UNIX enumeradas antes de que pueda reemplazarlas con los objetos de usuario y grupo de Windows deseados. A continuación, puede configurar ACL basados en NTFS en los objetos Usuario y Grupo de Windows. Si quita todos los objetos de seguridad de UNIX y agrega sólo usuarios y grupos de Windows a un archivo o carpeta de un volumen o qtree de estilo de seguridad mixto, cambie el estilo de seguridad efectivo del archivo o carpeta de UNIX a NTFS.

  Al cambiar los permisos de una carpeta, el comportamiento predeterminado de Windows es propagar estos cambios a todas las subcarpetas y archivos. Por lo tanto, debe cambiar la opción de propagación a la configuración deseada si no desea propagar un cambio en el estilo de seguridad a todas las carpetas secundarias, subcarpetas y archivos.

Información de copyright

Copyright © 2026 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.