Gestione cómo se presenta la seguridad de archivos a los clientes SMB para los datos de estilo de seguridad UNIX

ONTAP 9

NetApp
September 12, 2024

This PDF was generated from https://docs.netapp.com/es-es/ontap/smb-admin/manage-file-security-clients-unix-style-concept.html on September 12, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

Gestione cómo se presenta la seguridad de archivos a los clientes SMB para los datos de estilo de seguridad UNIX . . . 1
Gestione cómo se presenta la seguridad de archivos a los clientes SMB para una visión general de los datos de estilo de seguridad UNIX . . . 1
Habilitar o deshabilitar la presentación de ACL NTFS para datos de estilo de seguridad de UNIX . . . 2
Cómo ONTAP conserva los permisos de UNIX . . . 2
Administre los permisos de UNIX mediante la ficha Seguridad de Windows . . . 2

Gestione cómo se presenta la seguridad de archivos a los clientes SMB para los datos de estilo de seguridad UNIX

Gestione cómo se presenta la seguridad de archivos a los clientes SMB para una visión general de los datos de estilo de seguridad UNIX

Puede elegir cómo desea presentar la seguridad de archivos a los clientes de SMB para los datos de estilo de seguridad de UNIX habilitando o deshabilitando la presentación de ACL NTFS a clientes SMB. Existen ventajas en cada entorno, que debe entender para elegir el ajuste que mejor se ajuste a los requisitos de su negocio.

De forma predeterminada, ONTAP presenta los permisos de UNIX sobre volúmenes de estilo de seguridad de UNIX a clientes de SMB como ACL de NTFS. Hay escenarios en los que esto es deseable, incluyendo los siguientes:

- Desea ver y editar los permisos de UNIX mediante la ficha **Seguridad** del cuadro Propiedades de Windows.

  No puede modificar los permisos de un cliente Windows si el sistema UNIX no permite la operación. Por ejemplo, no puede cambiar la propiedad de un archivo que no posee, ya que el sistema UNIX no permite esta operación. Esta restricción impide a los clientes SMB omitir los permisos de UNIX establecidos en los archivos y carpetas.

- Los usuarios están editando y guardando archivos en el volumen de estilo de seguridad de UNIX utilizando ciertas aplicaciones de Windows, por ejemplo, Microsoft Office, donde ONTAP debe conservar los permisos de UNIX durante las operaciones de guardado.
- Hay ciertas aplicaciones de Windows en su entorno que esperan leer ACL NTFS en los archivos que utilizan.

En determinadas circunstancias, es posible que desee deshabilitar la presentación de permisos UNIX como ACL NTFS. Si esta funcionalidad está deshabilitada, ONTAP presenta volúmenes de estilo de seguridad UNIX como volúmenes FAT a clientes SMB. Hay motivos específicos por los que puede que desee presentar volúmenes de estilo de seguridad de UNIX como volúmenes FAT a clientes SMB:

- Sólo se pueden cambiar los permisos de UNIX mediante montajes en clientes UNIX.

  La pestaña Seguridad no está disponible cuando se asigna un volumen de estilo de seguridad UNIX en un cliente SMB. La unidad asignada parece formatearse con el sistema de archivos FAT, que no tiene permisos de archivo.

- Está utilizando aplicaciones a través de SMB que establecen ACL NTFS en archivos y carpetas a los que se tiene acceso, lo cual puede fallar si los datos residen en volúmenes de estilo de seguridad de UNIX.

  Si ONTAP informa del volumen como FAT, la aplicación no intenta cambiar una ACL.

Información relacionada

Configuración de estilos de seguridad en volúmenes FlexVol

Habilitar o deshabilitar la presentación de ACL NTFS para datos de estilo de seguridad de UNIX

Puede habilitar o deshabilitar la presentación de ACL NTFS a clientes SMB para datos de estilo de seguridad de UNIX (volúmenes de estilo de seguridad de UNIX y volúmenes mixtos de estilo de seguridad con seguridad efectiva de UNIX).

Acerca de esta tarea

Si habilita esta opción, ONTAP presenta archivos y carpetas en volúmenes con un estilo de seguridad UNIX efectivo para los clientes de SMB como si tuviera ACL NTFS. Si deshabilita esta opción, los volúmenes se presentan como volúmenes FAT a los clientes de SMB. El valor predeterminado es presentar ACL de NTFS a los clientes de SMB.

Pasos

1. Configure el nivel de privilegio en Advanced: `set -privilege advanced`
2. Configure el valor de opción de ACL de UNIX NTFS: `vserver cifs options modify -vserver` *`vserver_name`* `-is-unix-nt-acl-enabled {true|false}`
3. Compruebe que la opción está establecida en el valor deseado: `vserver cifs options show -vserver` *`vserver_name`*
4. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

Cómo ONTAP conserva los permisos de UNIX

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

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

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

Administre los permisos de UNIX mediante la ficha Seguridad de Windows

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

- Modificación de permisos de UNIX

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

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

- Cambiar los permisos de UNIX a los permisos NTFS

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

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

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

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

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

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

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

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

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

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

Información de la marca comercial

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