Cómo ONTAP controla el acceso a los archivos

ONTAP 9

NetApp
April 20, 2024

This PDF was generated from https://docs.netapp.com/es-es/ontap/nfs-admin/ontap-controls-access-files-concept.html on April 20, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

Cómo ONTAP controla el acceso a los archivos 1
Información general sobre cómo ONTAP controla el acceso a los archivos 1
Restricciones basadas en autenticación 1
Restricciones basadas en archivos 1

Cómo ONTAP controla el acceso a los archivos

Información general sobre cómo ONTAP controla el acceso a los archivos

ONTAP controla el acceso a los archivos de acuerdo con las restricciones basadas en archivos y en autenticación que especifique.

Cuando un cliente se conecta al sistema de almacenamiento para acceder a los archivos, ONTAP debe realizar dos tareas:

- Autenticación

  ONTAP debe autenticar el cliente verificando la identidad con un origen de confianza. Además, el tipo de autenticación del cliente es un método que puede utilizarse para determinar si un cliente puede acceder a los datos al configurar políticas de exportación (opcional para CIFS).

- Autorización

  ONTAP tiene que autorizar al usuario comparando las credenciales del usuario con los permisos configurados en el archivo o directorio y determinando qué tipo de acceso, si hubiera, proporcionar.

Para administrar correctamente el control de acceso a archivos, ONTAP debe comunicarse con servicios externos como servidores NIS, LDAP y Active Directory. La configuración de un sistema de almacenamiento para el acceso a archivos mediante CIFS o NFS requiere configurar los servicios adecuados en función de su entorno en ONTAP.

Restricciones basadas en autenticación

Con las restricciones basadas en la autenticación, puede especificar qué máquinas cliente y qué usuarios se pueden conectar a la máquina virtual de almacenamiento (SVM).

ONTAP es compatible con la autenticación Kerberos desde servidores UNIX y Windows.

Restricciones basadas en archivos

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 está determinado por los permisos efectivos después de la evaluación de los tres niveles de seguridad.

Cualquier objeto de almacenamiento puede contener hasta tres tipos de capas 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.

  > Si ve la configuración de seguridad en un archivo o un directorio desde un cliente NFS o SMB, no verá la seguridad de Access Guard a nivel de almacenamiento. La seguridad de protección de acceso a nivel de almacenamiento no se puede revocar de un cliente, ni siquiera por un administrador de sistema (Windows o UNIX).

- 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.

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.