Muestra información sobre las directivas de auditoría aplicadas a los archivos y directorios

ONTAP 9

NetApp
April 20, 2024

This PDF was generated from https://docs.netapp.com/es-es/ontap/nas-audit/display-audit-policies-windows-security-tab-task.html on April 20, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

Muestra información sobre las directivas de auditoría aplicadas a los archivos y directorios 1
Muestra información sobre las directivas de auditoría mediante la ficha Seguridad de Windows 1
Muestra información sobre las políticas de auditoría de NTFS en los volúmenes de FlexVol usando la interfaz de línea de comandos 2
Formas de mostrar información acerca de las políticas de auditoría y seguridad de archivos 6

Muestra información sobre las directivas de auditoría aplicadas a los archivos y directorios

Muestra información sobre las directivas de auditoría mediante la ficha Seguridad de Windows

Puede mostrar información acerca de las directivas de auditoría que se han aplicado a archivos y directorios mediante la ficha Seguridad de la ventana Propiedades de Windows. Este es el mismo método utilizado para los datos que se encuentran en un servidor de Windows, con el que los clientes pueden utilizar la misma interfaz gráfica de usuario que están acostumbrados a utilizar.

Acerca de esta tarea

La visualización de información acerca de las directivas de auditoría aplicadas a archivos y directorios permite verificar que se han establecido las listas de control de acceso del sistema (SACL) adecuadas en archivos y carpetas especificados.

Para mostrar información acerca de SACL que se han aplicado a archivos y carpetas NTFS, lleve a cabo los siguientes pasos en un host de Windows.

Pasos

1. En el menú **Herramientas** del Explorador de Windows, seleccione **asignar unidad de red**.
2. Complete el cuadro de diálogo **asignar unidad de red**:

   a. Seleccione una letra **Unidad**.

   b. En el cuadro **carpeta**, escriba la dirección IP o el nombre del servidor SMB de la máquina virtual de almacenamiento (SVM) que contiene el recurso compartido que contiene tanto los datos que desea auditar como el nombre del recurso compartido.

      Si el nombre de su servidor SMB es «MMB_SERVER» y su cuota se denomina «shara1», debe introducir `\\SMB_SERVER\share1`.

      > Puede especificar la dirección IP de la interfaz de datos para el servidor SMB en lugar del nombre del servidor SMB.

   c. Haga clic en **Finalizar**.

   La unidad seleccionada está montada y lista con la ventana del Explorador de Windows que muestra archivos y carpetas contenidos en el recurso compartido.

3. Seleccione el archivo o directorio para el que se muestra información de auditoría.
4. Haga clic con el botón derecho del ratón en el archivo o directorio y seleccione **Propiedades**.
5. Seleccione la ficha **Seguridad**.
6. Haga clic en **Avanzado**.
7. Seleccione la ficha **Auditoría**.
8. Haga clic en **continuar**.

Se abre el cuadro Auditoría. El cuadro **Entradas de auditoría** muestra un resumen de los usuarios y grupos que tienen SACL aplicados a ellos.

9. En el cuadro **Entradas de auditoría**, seleccione el usuario o grupo cuyas entradas de SACL desee mostrar.
10. Haga clic en **Editar**.

    Se abre el cuadro Entrada de auditoría para <object>.

11. En el cuadro **Access**, vea las SACL actuales que se aplican al objeto seleccionado.
12. Haga clic en **Cancelar** para cerrar el cuadro **Entrada de auditoría para <object>**.
13. Haga clic en **Cancelar** para cerrar el cuadro **Auditoría**.

Muestra información sobre las políticas de auditoría de NTFS en los volúmenes de FlexVol usando la interfaz de línea de comandos

Puede mostrar información acerca de las directivas de auditoría NTFS en los volúmenes FlexVol, incluidos los estilos de seguridad y los estilos de seguridad efectivos, los permisos que se aplican e información acerca de las listas de control de acceso al sistema. Puede utilizar la información para validar la configuración de seguridad o para solucionar problemas de auditoría.

Acerca de esta tarea

La visualización de información acerca de las directivas de auditoría aplicadas a archivos y directorios permite verificar que se han establecido las listas de control de acceso del sistema (SACL) adecuadas en archivos y carpetas especificados.

Debe proporcionar el nombre de la máquina virtual de almacenamiento (SVM) y la ruta a los archivos o carpetas cuya información de auditoría desee mostrar. Puede mostrar el resultado en forma de resumen o como una lista detallada.

- Los volúmenes y qtrees de estilo de seguridad NTFS sólo utilizan listas de control de acceso al sistema (SACL) NTFS para las directivas de auditoría.
- Los archivos y carpetas de un volumen mixto de estilo de seguridad con seguridad efectiva NTFS pueden tener directivas de auditoría NTFS aplicadas.

  Los volúmenes y qtrees de estilo de seguridad mixtos pueden contener archivos y directorios que utilizan permisos de archivo de UNIX, bits de modo o ACL de NFSv4 y algunos archivos y directorios que utilizan permisos de archivo NTFS.

- El nivel superior de un volumen de estilo de seguridad mixto puede tener seguridad efectiva de UNIX o NTFS y puede que no contenga SACL NTFS.
- Debido a que la seguridad de Access Guard a nivel de almacenamiento se puede configurar en un volumen o qtree de estilo de seguridad mixto incluso si el estilo de seguridad efectivo del volumen raíz o qtree es UNIX, El resultado de una ruta de volumen o qtree en la que se configuró Storage-Level Access Guard puede mostrar tanto el archivo normal como la carpeta NFSv4 SACL y Storage-Level Access Guard NTFS SACL.
- Si la ruta de acceso que se introduce en el comando es para los datos con seguridad efectiva NTFS, la

salida también muestra información sobre los ACE de control dinámico de acceso si el Control dinámico de acceso está configurado para la ruta de acceso del archivo o directorio dada.

- Cuando se muestra información de seguridad sobre archivos y carpetas con seguridad efectiva NTFS, los campos de salida relacionados con UNIX contienen información de permisos de archivo UNIX de sólo visualización.

  Los archivos y carpetas de estilo de seguridad NTFS utilizan sólo permisos de archivo NTFS y usuarios y grupos de Windows al determinar los derechos de acceso a archivos.

- El resultado de ACL se muestra solo para los archivos y las carpetas con seguridad NTFS o NFSv4.

  Este campo está vacío para archivos y carpetas que utilizan la seguridad de UNIX que solo tienen aplicados permisos de bit de modo (sin ACL de NFSv4).

- Los campos de salida de propietario y grupo de la salida ACL se aplican sólo en el caso de los descriptores de seguridad NTFS.

Paso

1. Mostrar la configuración de la directiva de auditoría de archivos y directorios con el nivel de detalle deseado:

Si desea mostrar información…	Introduzca el siguiente comando…
En forma de resumen	`vserver security file-directory show -vserver vserver_name -path path`
Como una lista detallada	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Ejemplos

En el ejemplo siguiente se muestra la información de la directiva de auditoría de la ruta de acceso `/corp` En SVM vs1. La ruta de acceso tiene seguridad efectiva NTFS. El descriptor de seguridad NTFS contiene UNA entrada SACL CORRECTA y UNA entrada SACL SUCCESS/FAIL.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
                Vserver: vs1
              File Path: /corp
      File Inode Number: 357
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

En el ejemplo siguiente se muestra la información de la directiva de auditoría de la ruta de acceso `/datavol1` En SVM vs1. La ruta de acceso contiene tanto SACL de archivo normal como de carpeta y SACL de Storage-Level Access Guard.

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
        File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xaa14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Formas de mostrar información acerca de las políticas de auditoría y seguridad de archivos

Puede utilizar el carácter comodín (*) para mostrar información acerca de las directivas de auditoría y seguridad de archivos de todos los archivos y directorios de una ruta de acceso determinada o de un volumen raíz.

El carácter comodín (*) se puede utilizar como último subcomponente de una ruta de directorio dada debajo de la cual se desea mostrar información de todos los archivos y directorios.

Si desea mostrar información de un archivo o directorio en particular denominado "*", entonces debe proporcionar la ruta completa dentro de comillas dobles (" ").

Ejemplo

El siguiente comando con el carácter comodín muestra la información sobre todos los archivos y directorios debajo de la ruta de acceso `/1/` De SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 –path /1/*

                   Vserver: vs1
                 File Path: /1/1
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8514
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
                   Vserver: vs1
                 File Path: /1/1/abc
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8404
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

El siguiente comando muestra la información de un archivo denominado "*" en la ruta de acceso `/vol1/a` De SVM vs1. La ruta está entre comillas dobles (" ").

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"

                 Vserver: vs1
               File Path: “/vol1/a/*”
          Security Style: mixed
         Effective Style: unix
          DOS Attributes: 10
  DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
            Unix User Id: 1002
           Unix Group Id: 65533
          Unix Mode Bits: 755
  Unix Mode Bits in Text: rwxr-xr-x
                    ACLs: NFSV4 Security Descriptor
                          Control:0x8014
                          SACL - ACEs
                            AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
                          DACL - ACEs
                            ALLOW-EVERYONE@-0x1f00a9-FI|DI
                            ALLOW-OWNER@-0x1f01ff-FI|DI
                            ALLOW-GROUP@-0x1200a9-IG
```

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.