Muestra información acerca de las políticas de auditoría y seguridad de archivos

ONTAP 9

NetApp
February 12, 2026

Tabla de contenidos

Muestra información acerca de las políticas de auditoría y seguridad de archivos

Obtenga información sobre cómo visualizar las políticas de seguridad y auditoría de archivos SMB de ONTAP

Puede mostrar información sobre la seguridad de los archivos y directorios contenidos en volúmenes en máquinas virtuales de almacenamiento (SVM). Puede mostrar información sobre las políticas de auditoría en los volúmenes de FlexVol. Si se configura, se puede mostrar información acerca de las opciones de seguridad Protección del acceso a nivel de almacenamiento y Control de acceso dinámico en volúmenes de FlexVol.

Mostrar información acerca de la seguridad de archivos

Puede visualizar la información sobre la seguridad de los archivos aplicada a los datos contenidos en volúmenes y qtrees (para volúmenes FlexVol) con los siguientes estilos de seguridad:

- NTFS
- UNIX
- Mixto

Visualización de información acerca de las directivas de auditoría

Puede mostrar información sobre las políticas de auditoría para auditar eventos de acceso en los volúmenes FlexVol mediante los siguientes protocolos NAS:

- SMB (todas las versiones)
- NFSv4.x

Mostrar información acerca de la seguridad de la protección de acceso a nivel de almacenamiento (SLAG)

La seguridad de protección de acceso a nivel de almacenamiento se puede aplicar en volúmenes de FlexVol y objetos de qtree con los siguientes estilos de seguridad:

- NTFS
- Mixto
- UNIX (si se configura un servidor CIFS en la SVM que contiene el volumen)

Mostrar información acerca de la seguridad del control de acceso dinámico (DAC)

La seguridad de control de acceso dinámico se puede aplicar a un objeto dentro de un volumen FlexVol con los siguientes estilos de seguridad:

- NTFS
- Mixto (si el objeto tiene seguridad efectiva NTFS)

Información relacionada

- Obtenga información sobre el acceso seguro a archivos mediante Storage-Level Access Guard
- Mostrar información sobre la protección de acceso a nivel de almacenamiento en los servidores

Mostrar información sobre la seguridad de archivos SMB de ONTAP en volúmenes de estilo de seguridad NTFS

Puede mostrar información acerca de la seguridad de archivos y directorios en volúmenes de estilo de seguridad NTFS, incluidos el estilo de seguridad y los estilos de seguridad efectivos, los permisos que se aplican e información acerca de los atributos dos. Puede utilizar los resultados para validar la configuración de seguridad o solucionar problemas de acceso a archivos.

Acerca de esta tarea

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

- Debido a que los volúmenes y qtrees 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, los campos de salida relacionados con UNIX contienen información de permisos de archivo UNIX de sólo visualización.
- Se muestra la salida de ACL para archivos y carpetas con seguridad NTFS.
- Como la seguridad de Access Guard a nivel de almacenamiento se puede configurar en el volumen raíz o en el qtree, la salida de un volumen o una ruta de qtree en la que se configure la protección de acceso a nivel de almacenamiento puede mostrar tanto ACL de archivos normales como ACL de Storage-Level Access Guard.
- El resultado también muestra información acerca de los ACE de control de acceso dinámico si el Control de acceso dinámico está configurado para la ruta de acceso de archivo o directorio indicada.

Paso

1. Mostrar la configuración de seguridad 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`*
Con detalle ampliado	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

Ejemplos

En el ejemplo siguiente se muestra información de seguridad sobre la ruta de `/vol4` SVM VS1:

```
cluster::> vserver security file-directory show -vserver vs1 -path /vol4

                                Vserver: vs1
                              File Path: /vol4
                      File Inode Number: 64
                         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:0x8004
                                          Owner:BUILTIN\Administrators
                                          Group:BUILTIN\Administrators
                                          DACL - ACEs
                                          ALLOW-Everyone-0x1f01ff
                                          ALLOW-Everyone-0x10000000-
OI|CI|IO
```

En el siguiente ejemplo, se muestra la información de seguridad con máscaras expandidas sobre la ruta de `/data/engineering` SVM VS1:

```
cluster::> vserver security file-directory show -vserver vs1 -path -path
/data/engineering -expand-mask true

               Vserver: vs1
             File Path: /data/engineering
      File Inode Number: 5544
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
```

```
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

                             1... .... .... .... = Self Relative
                             .0.. .... .... .... = RM Control Valid
                             ..0. .... .... .... = SACL Protected
                             ...0 .... .... .... = DACL Protected
                             .... 0... .... .... = SACL Inherited
                             .... .0.. .... .... = DACL Inherited
                             .... ..0. .... .... = SACL Inherit Required
                             .... ...0 .... .... = DACL Inherit Required
                             .... .... ..0. .... = SACL Defaulted
                             .... .... ...0 .... = SACL Present
                             .... .... .... 0... = DACL Defaulted
                             .... .... .... .1.. = DACL Present
                             .... .... .... ..0. = Group Defaulted
                             .... .... .... ...0 = Owner Defaulted

                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                             0... .... .... .... .... .... .... .... =
Generic Read
                             .0.. .... .... .... .... .... .... .... =
Generic Write
                             ..0. .... .... .... .... .... .... .... =
Generic Execute
                             ...0 .... .... .... .... .... .... .... =
Generic All
                             .... ...0 .... .... .... .... .... .... =
System Security
                             .... .... ...1 .... .... .... .... .... =
Synchronize
                             .... .... .... 1... .... .... .... .... =
Write Owner
                             .... .... .... .1.. .... .... .... .... =
Write DAC
                             .... .... .... ..1. .... .... .... .... =
Read Control
                             .... .... .... ...1 .... .... .... .... =
Delete
```

```
                              .... .... .... .... .... ...1 .... .... =
Write Attributes
                              .... .... .... .... .... .... 1... .... =
Read Attributes
                              .... .... .... .... .... .... .1.. .... =
Delete Child
                              .... .... .... .... .... .... ..1. .... =
Execute
                              .... .... .... .... .... .... ...1 .... =
Write EA
                              .... .... .... .... .... .... .... 1... =
Read EA
                              .... .... .... .... .... .... .... .1.. =
Append
                              .... .... .... .... .... .... .... ..1. =
Write
                              .... .... .... .... .... .... .... ...1 =
Read

                            ALLOW-Everyone-0x10000000-OI|CI|IO
                              0... .... .... .... .... .... .... .... =
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...1 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...0 .... .... .... .... .... =
Synchronize
                              .... .... .... 0... .... .... .... .... =
Write Owner
                              .... .... .... .0.. .... .... .... .... =
Write DAC
                              .... .... .... ..0. .... .... .... .... =
Read Control
                              .... .... .... ...0 .... .... .... .... =
Delete
                              .... .... .... .... .... ...0 .... .... =
Write Attributes
                              .... .... .... .... .... .... 0... .... =
Read Attributes
                              .... .... .... .... .... .... .0.. .... =
Delete Child
```

```
                                .... .... .... .... .... .... ..0. .... =
Execute
                                .... .... .... .... .... .... ...0 .... =
Write EA
                                .... .... .... .... .... .... .... 0... =
Read EA
                                .... .... .... .... .... .... .... .0.. =
Append
                                .... .... .... .... .... .... .... ..0. =
Write
                                .... .... .... .... .... .... .... ...0 =
Read
```

En el siguiente ejemplo, se muestra información de seguridad, incluida la información de seguridad de Storage-Level Access Guard, del volumen con la ruta `/datavol1` en SVM VS1:

```
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:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         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
```

Información relacionada

- Muestra información sobre la seguridad de archivos en volúmenes mixtos de estilo de seguridad
- Muestra información sobre la seguridad de archivos en volúmenes de estilo de seguridad UNIX

Mostrar información sobre la seguridad de los archivos SMB de ONTAP en volúmenes de estilo de seguridad mixto

Puede mostrar información acerca de la seguridad de archivos y directorios en volúmenes mixtos de estilo de seguridad, incluidos el estilo de seguridad y los estilos de seguridad efectivos, los permisos que se aplican y la información acerca de los propietarios y grupos de UNIX. Puede utilizar los resultados para validar la configuración de seguridad o solucionar problemas de acceso a archivos.

Acerca de esta tarea

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

- Los volúmenes y qtrees de estilo de seguridad mixtos pueden contener archivos y carpetas 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 mixto de estilo de seguridad puede tener una seguridad efectiva de UNIX o NTFS.
- La salida de ACL se muestra solo para archivos y carpetas con seguridad NTFS o NFSv4.

  Este campo está vacío para archivos y directorios 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.
- 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, La salida de un volumen o una ruta de qtree en la que se configure Storage-Level Access Guard podría mostrar tanto los permisos de archivos UNIX como las ACL de Storage-Level Access Guard.
- Si la ruta de acceso introducida en el comando es a datos con seguridad efectiva de NTFS, el resultado también muestra información acerca de ACE de Control de acceso dinámico si Control de acceso dinámico está configurado para el archivo o la ruta de acceso de directorio dada.

Paso

1. Mostrar la configuración de seguridad 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`
Con detalle ampliado	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Ejemplos

El siguiente ejemplo muestra la información de seguridad sobre la ruta de `/projects` SVM VS1 en formato

de máscara expandida. Esta ruta mixta de estilo de seguridad tiene una seguridad efectiva de UNIX.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/projects -expand-mask true

                Vserver: vs1
              File Path: /projects
      File Inode Number: 78
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 1
         Unix Mode Bits: 700
 Unix Mode Bits in Text: rwx------
                   ACLs: -
```

En el ejemplo siguiente se muestra información de seguridad sobre la ruta de `/data` SVM VS1. Esta ruta mixta de estilo de seguridad tiene una seguridad NTFS efectiva.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /data

                                Vserver: vs1
                              File Path: /data
                      File Inode Number: 544
                         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:0x8004
                                          Owner:BUILTIN\Administrators
                                          Group:BUILTIN\Administrators
                                          DACL - ACEs
                                            ALLOW-Everyone-0x1f01ff
                                            ALLOW-Everyone-0x10000000-
OI|CI|IO
```

En el ejemplo siguiente se muestra información de seguridad sobre el volumen en la ruta de `/datavol5` SVM VS1. El nivel superior de este volumen mixto de estilo de seguridad ofrece una seguridad efectiva para UNIX. El volumen tiene seguridad de protección de acceso en el nivel de almacenamiento.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5
                Vserver: vs1
              File Path: /datavol5
      File Inode Number: 3374
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
                   ACLs: Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
```

Información relacionada

- Muestra información sobre la seguridad de archivos en volúmenes de estilo de seguridad NTFS
- Muestra información sobre la seguridad de archivos en volúmenes de estilo de seguridad UNIX

Mostrar información sobre la seguridad de archivos SMB de ONTAP en volúmenes de estilo de seguridad UNIX

Puede mostrar información acerca de la seguridad de archivos y directorios en los

volúmenes de estilo de seguridad de UNIX, incluidos los estilos de seguridad y los estilos de seguridad efectivos, los permisos que se aplican y la información acerca de los propietarios y grupos de UNIX. Puede utilizar los resultados para validar la configuración de seguridad o solucionar problemas de acceso a archivos.

Acerca de esta tarea

Debe proporcionar el nombre de la máquina virtual de almacenamiento (SVM) y la ruta a los datos cuyo archivo o información de seguridad de directorio desee mostrar. Puede mostrar el resultado en forma de resumen o como una lista detallada.

- Los volúmenes y qtrees de estilo de seguridad de UNIX solo utilizan permisos de archivos UNIX, ya sea bits de modo o ACL de NFSv4 al determinar los derechos de acceso a los archivos.
- La salida de ACL se muestra solo para los archivos y las carpetas con seguridad de NFSv4.

  Este campo está vacío para archivos y directorios 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 de ACL no se aplican en el caso de los descriptores de seguridad de NFSv4.

  Sólo son significativos para los descriptores de seguridad NTFS.

- Como la seguridad de Access Guard en el nivel de almacenamiento se admite en un volumen UNIX o qtree si hay un servidor CIFS configurado en la SVM, el resultado puede contener información sobre la seguridad de Access Guard en el nivel de almacenamiento aplicada al volumen o qtree especificados en el `-path` parámetro.

Paso

1. Mostrar la configuración de seguridad 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`*
Con detalle ampliado	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

Ejemplos

En el ejemplo siguiente se muestra información de seguridad sobre la ruta de `/home` SVM VS1:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home

                                Vserver: vs1
                              File Path: /home
                      File Inode Number: 9590
                         Security Style: unix
                        Effective Style: unix
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 1
                         Unix Mode Bits: 700
                 Unix Mode Bits in Text: rwx------
                                   ACLs: -
```

El siguiente ejemplo muestra la información de seguridad sobre la ruta de `/home` SVM VS1 en formato de máscara expandida:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
-expand-mask true

                                Vserver: vs1
                              File Path: /home
                      File Inode Number: 9590
                         Security Style: unix
                        Effective Style: unix
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: 0x10
                    ...0 .... .... .... = Offline
                    .... ..0. .... .... = Sparse
                    .... .... 0... .... = Normal
                    .... .... ..0. .... = Archive
                    .... .... ...1 .... = Directory
                    .... .... .... .0.. = System
                    .... .... .... ..0. = Hidden
                    .... .... .... ...0 = Read Only
                           Unix User Id: 0
                          Unix Group Id: 1
                         Unix Mode Bits: 700
                 Unix Mode Bits in Text: rwx------
                                   ACLs: -
```

Información relacionada

- Mostrar información sobre la seguridad de los archivos en volúmenes de estilo de seguridad
- Muestra información sobre la seguridad de archivos en volúmenes mixtos de estilo de seguridad

Comandos de ONTAP para mostrar información sobre las políticas de auditoría de NTFS en volúmenes SMB FlexVol

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 los resultados para validar la configuración de seguridad o para solucionar problemas de auditoría.

Acerca de esta tarea

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 siguiente ejemplo, se muestra información de política de auditoría para la ruta `/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 siguiente ejemplo, se muestra información de política de auditoría para la ruta `/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
```

Comandos de ONTAP para mostrar información sobre las políticas de auditoría de NFSv4 en volúmenes SMB FlexVol

Puede mostrar información sobre las políticas de auditoría de NFSv4 en volúmenes de FlexVol mediante la interfaz de línea de comandos de ONTAP, incluidos los estilos de seguridad y los estilos de seguridad efectivos, qué permisos se aplican e información sobre las listas de control de acceso del sistema (SACL). Puede utilizar los resultados para validar la configuración de seguridad o para solucionar problemas de auditoría.

Acerca de esta tarea

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

- Los volúmenes y qtrees de estilo de seguridad de UNIX solo utilizan NFSv4 SACL para las políticas de auditoría.
- Los archivos y directorios de un volumen de estilo de seguridad mixto que sea de estilo de seguridad UNIX pueden hacer que se les apliquen las políticas de auditoría de NFSv4.

  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 con estilo de seguridad mixto puede tener seguridad efectiva de UNIX o NTFS y puede que contenga o no SACL de NFSv4.
- La salida de ACL se muestra solo para archivos y 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.
- 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, Los resultados de una ruta de volumen o qtree en la que se configuró Storage-Level Access Guard pueden mostrar tanto el archivo NFSv4 normal como las SACL de directorio y las SACL de Storage-Level Access Guard.
- Como la seguridad de Access Guard en el nivel de almacenamiento se admite en un volumen UNIX o qtree si hay un servidor CIFS configurado en la SVM, el resultado puede contener información sobre la seguridad de Access Guard en el nivel de almacenamiento aplicada al volumen o qtree especificados en el `-path` parámetro.

Pasos

1. Mostrar la configuración de seguridad 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`

Si desea mostrar información…	Introduzca el siguiente comando…
Con detalle ampliado	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Ejemplos

En el ejemplo siguiente se muestra información de seguridad sobre la ruta de `/lab` SVM VS1. Esta ruta de seguridad de UNIX tiene un SACL de NFSv4.

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

                Vserver: vs1
              File Path: /lab
      File Inode Number: 288
         Security Style: unix
        Effective Style: unix
         DOS Attributes: 11
 DOS Attributes in Text: ----D--R
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 0
 Unix Mode Bits in Text: ---------
                   ACLs: NFSV4 Security Descriptor
                         Control:0x8014
                         SACL - ACEs
                           SUCCESSFUL-S-1-520-0-0xf01ff-SA
                           FAILED-S-1-520-0-0xf01ff-FA
                         DACL - ACEs
                           ALLOW-S-1-520-1-0xf01ff
```

Aprenda a mostrar información sobre políticas de auditoría y seguridad de archivos SMB de ONTAP

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 concreto denominado «*»**», deberá proporcionar la ruta completa dentro de comillas dobles (»'"').

Ejemplo

El siguiente comando con carácter comodín muestra la información de todos los archivos y directorios debajo de la ruta de `/1/` 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 llamado “*” bajo la ruta de `/vol1/a` 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
```