Acceso seguro a archivos mediante Storage-Level Access Guard

ONTAP 9

NetApp
February 12, 2026

Tabla de contenidos

Acceso seguro a archivos mediante Storage-Level Access Guard

Obtenga información sobre el acceso seguro a archivos SMB de ONTAP mediante Storage-Level Access Guard

Además de proteger el acceso mediante el uso nativo a nivel de archivo y la seguridad de exportación y uso compartido, puede configurar la protección de acceso a nivel de almacenamiento, una tercera capa de seguridad aplicada por ONTAP a nivel de volumen. El servicio de protección de acceso a nivel de almacenamiento se aplica para acceder desde todos los protocolos NAS al objeto de almacenamiento al que se aplica.

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.

Comportamiento de protección del acceso al nivel de almacenamiento

- Storage-Level Access Guard se aplica a todos los archivos o todos los directorios de un objeto de almacenamiento.

  Puesto que todos los archivos o directorios de un volumen están sujetos a la configuración de Storage-Level Access Guard, no se requiere la herencia a través de la propagación.

- Puede configurar Storage-Level Access Guard para que se aplique sólo a archivos, sólo a directorios o a los archivos y directorios de un volumen.
  - Seguridad de archivos y directorios

    Se aplica a todos los directorios y archivos del objeto de almacenamiento. Esta es la configuración predeterminada.

  - Seguridad de archivos

    Se aplica a cada archivo dentro del objeto de almacenamiento. Aplicar esta seguridad no afecta al acceso a los directorios o a la auditoría de ellos.

  - Seguridad del directorio

    Se aplica a cada directorio dentro del objeto de almacenamiento. Aplicar esta seguridad no afecta al acceso a los archivos ni a la auditoría de ellos.

- Se utiliza Storage-Level Access Guard para restringir los permisos.

  Nunca dará permisos de acceso adicionales.

- 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.

  Se aplica en el nivel de objeto de almacenamiento y se almacena en los metadatos que se usan para determinar la efectividad de los permisos.

- La seguridad a nivel de almacenamiento no puede ser revocada desde un cliente, incluso por un administrador de sistema (Windows o UNIX)

  Está diseñado para que lo modifiquen únicamente administradores del almacenamiento.

- Se puede aplicar Access Guard en el nivel de almacenamiento a volúmenes con un estilo de seguridad NTFS o mixto.
- Es posible aplicar una protección de acceso al nivel de almacenamiento a los volúmenes con estilo de seguridad UNIX siempre que la SVM que contiene el volumen tenga configurado un servidor CIFS.
- Cuando los volúmenes se montan en una ruta de unión de volúmenes y, si existe la función Storage-Level Access Guard en esa ruta, no se propagará a los volúmenes montados bajo ella.
- El descriptor de seguridad de Storage-Level Access Guard se replica con la replicación de datos de SnapMirror y con la replicación de SVM.
- Hay una dispensación especial para los escáneres de virus.

  Estos servidores pueden acceder de forma excepcional a los archivos y directorios de pantalla, incluso si Storage-Level Access Guard deniega el acceso al objeto.

- Las notificaciones de FPolicy no se envían si se deniega el acceso debido a la protección de acceso al nivel de almacenamiento.

Orden de las comprobaciones de acceso

El acceso a un archivo o directorio se determina por el efecto combinado de los permisos de exportación o uso compartido, los permisos de Storage-Level Access Guard configurados en volúmenes y los permisos de archivo nativos aplicados a archivos y/o directorios. Se evalúan todos los niveles de seguridad para determinar los permisos efectivos que tiene un archivo o directorio. Las comprobaciones de acceso de seguridad se realizan en el siguiente orden:

1. Permisos a nivel de exportación de SMB o NFS
2. Protección de acceso al nivel de almacenamiento
3. Listas de control de acceso a carpetas/archivos NTFS (ACL), ACL de NFSv4 o bits de modo UNIX

Casos de uso para usar Storage-Level Access Guard

El servicio de protección de acceso a nivel de almacenamiento proporciona una seguridad adicional a nivel de almacenamiento, que no puede verse en el lado del cliente; por lo tanto, no puede ser revocado por ninguno de los usuarios o administradores de sus escritorios. Existen determinados casos de uso en los que es conveniente la capacidad de controlar el acceso en el nivel de almacenamiento.

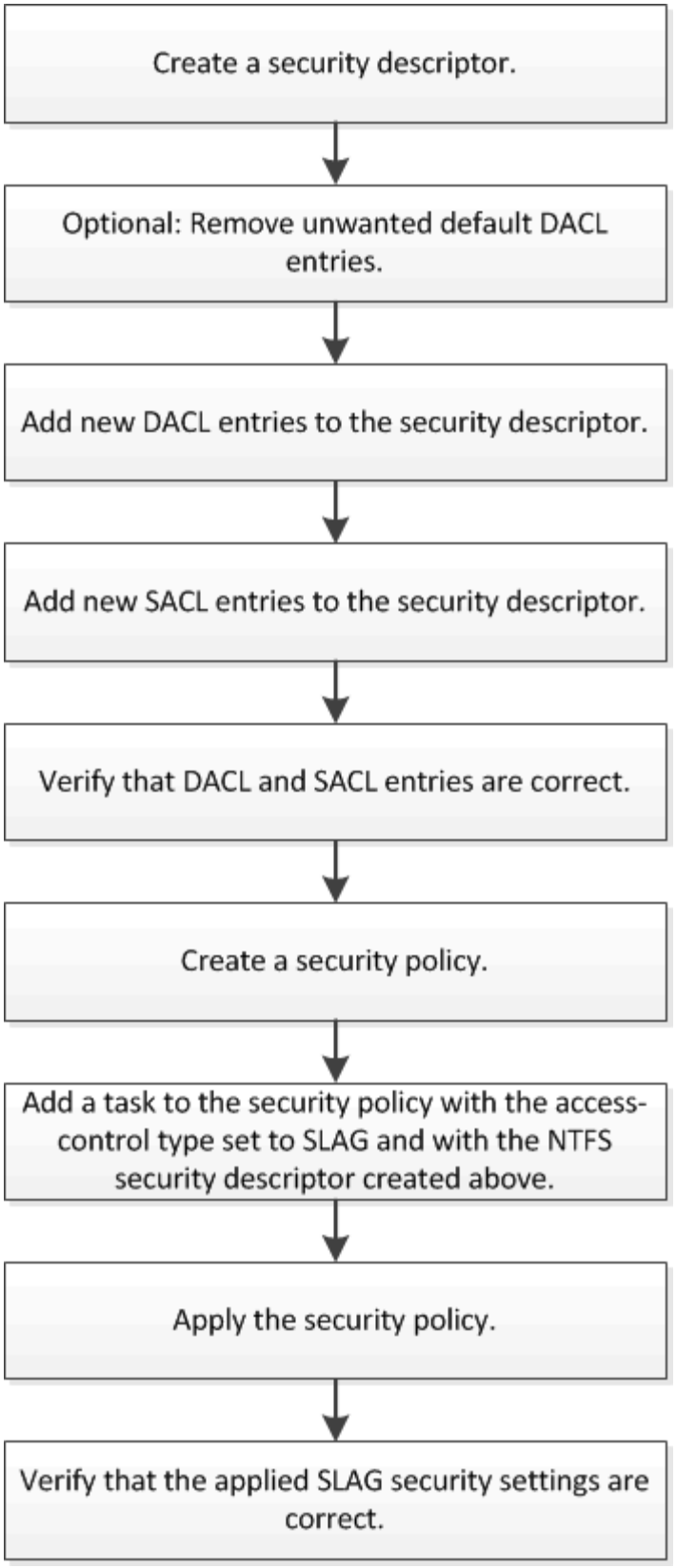
Los casos de uso típicos de esta función incluyen las siguientes situaciones:

- Protección de la propiedad intelectual mediante la auditoría y el control del acceso de todos los usuarios a nivel de almacenamiento
- Almacenamiento para empresas de servicios financieros, incluidos grupos bancarios y comerciales
- Servicios gubernamentales con almacenamiento de ficheros independiente para departamentos individuales

- Universidades que protegen todos los archivos de los estudiantes

Flujo de trabajo de configuración para Storage-Level Access Guard en servidores SMB de ONTAP

El flujo de trabajo para configurar la protección de acceso al nivel de almacenamiento (SSLAG) utiliza los mismos comandos de la CLI de ONTAP que utiliza para configurar permisos de archivos NTFS y directivas de auditoría. En lugar de configurar el acceso a archivos y directorios en un destino designado, debe configurar SLAG en el volumen de máquina virtual de almacenamiento designado.



Información relacionada

Configurar la protección de acceso a nivel de almacenamiento en los servidores

Configurar Storage-Level Access Guard en servidores SMB de ONTAP

Hay una serie de pasos que se deben seguir para configurar la protección del acceso al nivel de almacenamiento en un volumen o un qtree. El protector de acceso al nivel de almacenamiento ofrece un nivel de seguridad de acceso que se establece en el nivel de almacenamiento. Proporciona seguridad que se aplica a todos los accesos desde todos los protocolos NAS al objeto de almacenamiento al que se ha aplicado.

Pasos

1. Cree un descriptor de seguridad con `vserver security file-directory ntfs create` el comando.

   `vserver security file-directory ntfs create -vserver vs1 -ntfs-sd sd1 vserver security file-directory ntfs show -vserver vs1`

   ```
   Vserver: vs1

      NTFS Security    Owner Name
      Descriptor Name
      ------------     --------------
      sd1              -
   ```

   Se crea un descriptor de seguridad con las siguientes cuatro entradas predeterminadas de control de acceso de DACL (ACE):

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       BUILTIN\Administrators
                        allow    full-control   this-folder, sub-folders,
   files
       BUILTIN\Users    allow    full-control   this-folder, sub-folders,
   files
       CREATOR OWNER    allow    full-control   this-folder, sub-folders,
   files
       NT AUTHORITY\SYSTEM
                        allow    full-control   this-folder, sub-folders,
   files
   ```

   Si no desea utilizar las entradas predeterminadas al configurar Storage-Level Access Guard, puede eliminarlas antes de crear y agregar sus propias ACE al descriptor de seguridad.

2. Quite cualquiera de los ACE de DACL predeterminados del descriptor de seguridad que no desea configurar con la seguridad Storage-Level Access Guard:

   a. Elimine todas las ACE DACL no deseadas con el `vserver security file-directory ntfs dacl remove` comando.

      En este ejemplo, se quitan tres ACE de DACL predeterminados del descriptor de seguridad: BUILTIN\Administrators, BUILTIN\Users y CREATOR OWNER.

      ```
      vserver security file-directory ntfs dacl remove -vserver vs1 -ntfs-sd sd1
      -access-type allow -account builtin\users vserver security file-directory
      ntfs dacl remove -vserver vs1 -ntfs-sd sd1 -access-type allow -account
      builtin\administrators vserver security file-directory ntfs dacl remove
      -vserver vs1 -ntfs-sd sd1 -access-type allow -account "creator owner"
      ```

   b. Compruebe que las ACL DACL que no desea utilizar para la seguridad de Access Guard de nivel de almacenamiento se hayan eliminado del descriptor de seguridad mediante `vserver security file-directory ntfs dacl show` el comando.

      En este ejemplo, la salida del comando verifica que se han eliminado tres ACE de DACL predeterminados del descriptor de seguridad, dejando sólo la entrada de ACE de DACL predeterminada de NT AUTHORITY\SYSTEM:

      ```
      vserver security file-directory ntfs dacl show -vserver vs1
      ```

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    NT AUTHORITY\SYSTEM
                     allow    full-control   this-folder, sub-folders,
files
```

3. Añada una o varias entradas DACL a un descriptor de seguridad mediante `vserver security file-directory ntfs dacl add` el comando.

   En este ejemplo, se agregan dos ACE de DACL al descriptor de seguridad:

   ```
   vserver security file-directory ntfs dacl add -vserver vs1 -ntfs-sd sd1
   -access-type allow -account example\engineering -rights full-control -apply-to
   this-folder,sub-folders,files vserver security file-directory ntfs dacl add
   -vserver vs1 -ntfs-sd sd1 -access-type allow -account "example\Domain Users"
   -rights read -apply-to this-folder,sub-folders,files
   ```

4. Añada una o varias entradas de SACL a un descriptor de seguridad mediante `vserver security file-directory ntfs sacl add` el comando.

   En este ejemplo, se agregan dos ACE de SACL al descriptor de seguridad:

```
vserver security file-directory ntfs sacl add -vserver vs1 -ntfs-sd sd1
-access-type failure -account "example\Domain Users" -rights read -apply-to
this-folder,sub-folders,files vserver security file-directory ntfs sacl add
-vserver vs1 -ntfs-sd sd1 -access-type success -account example\engineering
-rights full-control -apply-to this-folder,sub-folders,files
```

5. Verifique que las ACE DACL y SACL estén configuradas correctamente mediante los `vserver security file-directory ntfs dacl show` `vserver security file-directory ntfs sacl show` comandos y, respectivamente.

   En este ejemplo, el siguiente comando muestra información sobre las entradas de DACL para el descriptor de seguridad “D1”:

   ```
   vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
   ```

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       EXAMPLE\Domain Users
                        allow    read           this-folder, sub-folders,
   files
       EXAMPLE\engineering
                        allow    full-control   this-folder, sub-folders,
   files
       NT AUTHORITY\SYSTEM
                        allow    full-control   this-folder, sub-folders,
   files
   ```

   En este ejemplo, el siguiente comando muestra información sobre las entradas de SACL para el descriptor de seguridad “D1”:

   ```
   vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
   ```

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    EXAMPLE\Domain Users
                     failure  read           this-folder, sub-folders,
files
    EXAMPLE\engineering
                     success  full-control   this-folder, sub-folders,
files
```

6. Cree una política de seguridad mediante `vserver security file-directory policy create` el comando.

   En el siguiente ejemplo se crea una directiva denominada «'póliza 1'»:

   ```
   vserver security file-directory policy create -vserver vs1 -policy-name
   policy1
   ```

7. Compruebe que la política se ha configurado correctamente mediante `vserver security file-directory policy show` el comando.

   ```
   vserver security file-directory policy show
   ```

   ```
   Vserver          Policy Name
   ------------     --------------
   vs1              policy1
   ```

8. Agregue una tarea con un descriptor de seguridad asociado a la política de seguridad mediante el `vserver security file-directory policy task add` comando con el `-access-control` parámetro definido en `slag`.

   Aunque una directiva puede contener más de una tarea de Storage-Level Access Guard, no puede configurar una directiva para que contenga tareas de directorio de archivos y de Storage-Level Access Guard. Una política debe contener todas las tareas de Storage-Level Access Guard o todas las tareas de directorio de archivos.

   En este ejemplo, se agrega una tarea a la política denominada "'poly1'", que se asigna al descriptor de seguridad "sD1". Se asigna a la `/datavol1` ruta con el tipo de control de acceso establecido en “Slag”.

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name
   policy1 -path /datavol1 -access-control slag -security-type ntfs -ntfs-mode
   propagate -ntfs-sd sd1
   ```

9. Compruebe que la tarea está configurada correctamente mediante `vserver security file-directory policy task show` el comando.

```
vserver security file-directory policy task show -vserver vs1 -policy-name
policy1
```

```
 Vserver: vs1
  Policy: policy1

   Index  File/Folder  Access           Security  NTFS       NTFS
Security
          Path         Control          Type      Mode       Descriptor
Name
   -----  -----------  ---------------  --------  ----------
---------------
   1      /datavol1    slag             ntfs      propagate  sd1
```

10. Aplique la política de seguridad Access Guard de nivel de almacenamiento mediante `vserver security file-directory apply` el comando.

    ```
    vserver security file-directory apply -vserver vs1 -policy-name policy1
    ```

    El trabajo que se va a aplicar la directiva de seguridad está programado.

11. Verifique que la configuración de seguridad de Access Guard de nivel de almacenamiento aplicada sea correcta mediante el `vserver security file-directory show` comando.

    En este ejemplo, la salida del comando muestra que la seguridad de Storage-Level Access Guard se ha aplicado al volumen NTFS `/datavol1` . Aunque el DACL predeterminado que permite el control total para todos permanece, la seguridad de Storage-Level Access Guard restringe (y audita) el acceso a los grupos definidos en la configuración de Storage-Level Access Guard.

    ```
    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

- Comandos para administrar la seguridad de archivos NTFS, las políticas de auditoría de NTFS y la protección de acceso a nivel de almacenamiento
- Flujo de trabajo de configuración para Storage-Level Access Guard en servidores
- Mostrar información sobre la protección de acceso a nivel de almacenamiento en los servidores
- Eliminar la protección de acceso a nivel de almacenamiento en los servidores

Matriz SLAG eficaz en servidores SMB de ONTAP

Puede configurar SLAG en un volumen, un qtree o ambos. La matriz SLAG define en qué volumen o qtree se aplica la configuración SLAG en los distintos escenarios que se indican en la tabla.

	Volumen SLAG en un AFS	**ASIGNACIÓN DE volumen en una instantánea**	**Qtree SLAG en un AFS**	**ELIMINACIÓN DE qtree en una copia snapshot**
Acceso de volumen en un sistema de archivos de acceso (AFS)	SÍ	NO	N / A	N / A
Acceso del volumen en una copia de Snapshot	SÍ	NO	N / A	N / A
Acceso a Qtree en un AFS (cuando SLAG está presente en el qtree)	NO	NO	SÍ	NO
Acceso a Qtree en un AFS (cuando SLAG no está presente en qtree)	SÍ	NO	NO	NO
Acceso a Qtree en una copia de Snapshot (cuando hay UN SUFIJO en el AFS para qtree)	NO	NO	SÍ	NO
Acceso a Qtree en una copia de Snapshot (cuando no está presente LA función SLAG en el AFS para qtree)	SÍ	NO	NO	NO

Mostrar información sobre Storage-Level Access Guard en servidores SMB de ONTAP

El servicio de protección del acceso a nivel de almacenamiento es una tercera capa de seguridad aplicada en un volumen o un qtree. La configuración de Storage-Level Access Guard no se puede ver mediante la ventana Propiedades de Windows. Es necesario

usar la interfaz de línea de comandos de ONTAP para ver información sobre la seguridad de protección del acceso a nivel de almacenamiento, que se puede utilizar para validar la configuración o solucionar problemas de acceso a archivos.

Acerca de esta tarea

Se debe proporcionar el nombre de la máquina virtual de almacenamiento (SVM) y la ruta al volumen o qtree cuya información de seguridad de protección de acceso de nivel de almacenamiento desea mostrar. Puede mostrar el resultado en forma de resumen o como una lista detallada.

Paso

1. Mostrar la configuración de seguridad de protección de acceso a nivel de almacenamiento 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 siguiente ejemplo, se muestra información de seguridad de Access Guard de nivel de almacenamiento para el volumen de estilo de seguridad NTFS 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
```

En el siguiente ejemplo, se muestra información de Access Guard al nivel de almacenamiento acerca del volumen mixto de estilo de seguridad en la ruta de `/datavol5` SVM VS1. El nivel superior de este volumen tiene 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
                         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
```

Eliminar la protección de acceso a nivel de almacenamiento en servidores SMB de ONTAP

Puede quitar la protección de acceso al nivel de almacenamiento en un volumen o qtree si ya no desea establecer la seguridad de acceso en el nivel de almacenamiento. La eliminación de la protección de acceso a nivel de almacenamiento no modifica ni quita la seguridad normal de archivos NTFS y directorios.

Pasos

1. Compruebe que el volumen o qtree tiene la protección de acceso a nivel de almacenamiento configurada mediante `vserver security file-directory show` el comando.

   ```
   vserver security file-directory show -vserver vs1 -path /datavol2
   ```

```
                Vserver: vs1
              File Path: /datavol2
      File Inode Number: 99
         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:0xbf14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI

                         Storage-Level Access Guard security
                         DACL (Applies to Directories):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         DACL (Applies to Files):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

2. Quite la protección de acceso al nivel de almacenamiento mediante `vserver security file-directory remove-slag` el comando.

   ```
   vserver security file-directory remove-slag -vserver vs1 -path /datavol2
   ```

3. Compruebe que la protección de acceso al nivel de almacenamiento se haya eliminado del volumen o qtree mediante `vserver security file-directory show` el comando.

   ```
   vserver security file-directory show -vserver vs1 -path /datavol2
   ```

```
               Vserver: vs1
             File Path: /datavol2
      File Inode Number: 99
         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:0xbf14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI
```