Gestione la seguridad de archivos NTFS, políticas de auditoría NTFS y Storage-Level Access Guard mediante la CLI

ONTAP 9

NetApp
April 16, 2024

Tabla de contenidos

Gestione la seguridad de archivos NTFS, políticas de auditoría NTFS y Storage-Level Access Guard mediante la CLI

Gestione la seguridad de archivos NTFS, políticas de auditoría NTFS y Storage-Level Access Guard mediante la información general de la CLI

Puede gestionar la seguridad de archivos NTFS, políticas de auditoría de NTFS y Storage-Level Access Guard en máquinas virtuales de almacenamiento (SVM) mediante la interfaz de línea de comandos.

Puede gestionar las políticas de auditoría y seguridad de archivos NTFS desde clientes SMB o mediante la CLI. Sin embargo, al utilizar la interfaz de línea de comandos para configurar las políticas de seguridad de los archivos y de auditoría, no es necesario utilizar un cliente remoto para gestionar la seguridad de los archivos. El uso de la CLI puede reducir significativamente el tiempo que lleva aplicar la seguridad en muchos archivos y carpetas mediante un único comando.

Puede configurar la protección de acceso al nivel de almacenamiento, que es otra capa de seguridad aplicada por ONTAP a los volúmenes de SVM. Storage-Level Access Guard se aplica a los accesos desde todos los protocolos NAS al objeto de almacenamiento al que se aplica la protección de acceso a nivel de almacenamiento.

El protector de acceso a nivel de almacenamiento se puede configurar y gestionar solo desde la interfaz de línea de comandos de ONTAP. No se puede gestionar la configuración de Access Guard en el nivel de almacenamiento desde clientes SMB. Además, si ve la configuración de seguridad en un archivo o un directorio desde un cliente NFS o SMB, no verá la seguridad Storage-Level Access Guard. 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). Por lo tanto, Storage-Level Access Guard ofrece una capa adicional de seguridad para el acceso a los datos que el administrador de almacenamiento establece y gestiona independientemente.

> Aunque solo se admiten permisos de acceso NTFS para Storage-Level Access Guard, ONTAP puede realizar comprobaciones de seguridad para acceder a través de NFS a datos en volúmenes donde se aplica Storage-Level Access Guard si el usuario UNIX se asigna a un usuario de Windows en la SVM propietaria del volumen.

Volúmenes de estilo de seguridad NTFS

Todos los archivos y carpetas contenidos en qtrees y volúmenes de estilo de seguridad NTFS tienen una seguridad efectiva de NTFS. Puede utilizar el `vserver security file-directory` Familia de comandos para implementar los siguientes tipos de seguridad en volúmenes de estilo de seguridad NTFS:

- Los permisos de archivo y las políticas de auditoría a los archivos y las carpetas que contiene el volumen
- Seguridad para proteger el acceso al nivel de almacenamiento en los volúmenes

Volúmenes mixtos de estilo de seguridad

Los volúmenes y qtrees de estilo de seguridad mixtos pueden contener algunos archivos y carpetas con seguridad efectiva de UNIX y usar permisos de archivos de UNIX, bits de modo o ACL de NFSv4.x y políticas de auditoría de NFSv4.x, y algunos archivos y carpetas que tengan seguridad efectiva de NTFS y usen permisos de archivos NTFS y políticas de auditoría. Puede utilizar el `vserver security file-directory` familia de comandos para aplicar los siguientes tipos de seguridad a los datos mixtos de estilo de seguridad:

- Permisos de archivo y políticas de auditoría para archivos y carpetas con un estilo de seguridad NTFS efectivo en el volumen o qtree mixtos
- Protección del acceso a nivel de almacenamiento para volúmenes con seguridad efectiva de NTFS y UNIX

Volúmenes de estilo de seguridad de UNIX

Los volúmenes y qtrees de estilo de seguridad de UNIX contienen archivos y carpetas que tienen una seguridad efectiva de UNIX (bits de modo o ACL de NFSv4.x). Si desea utilizar el, debe tener en cuenta los siguientes aspectos `vserver security file-directory` Familia de comandos para implementar la seguridad en volúmenes de estilo de seguridad UNIX:

- La `vserver security file-directory` No se puede utilizar la familia de comandos para gestionar las políticas de auditoría y seguridad de archivos UNIX en volúmenes y qtrees de estilo de seguridad de UNIX.
- Puede utilizar el `vserver security file-directory` Familia de comandos para configurar Storage-Level Access Guard en volúmenes de estilo de seguridad UNIX, siempre que la SVM con el volumen de destino contenga un servidor CIFS.

Información relacionada

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

Configurar y aplicar la seguridad de archivos en archivos y carpetas NTFS mediante la CLI

Configurar y aplicar directivas de auditoría a archivos y carpetas NTFS mediante la interfaz de línea de comandos

Acceso seguro a archivos mediante Storage-Level Access Guard

Utilice casos para utilizar la CLI para establecer la seguridad de archivos y carpetas

Dado que puede aplicar y administrar la seguridad de archivos y carpetas localmente sin la participación de un cliente remoto, puede reducir significativamente el tiempo que tarda en establecer la seguridad masiva en un gran número de archivos o carpetas.

Puede beneficiarse del uso de la CLI para establecer la seguridad de archivos y carpetas en los siguientes casos de uso:

- Almacenamiento de ficheros en entornos empresariales de gran tamaño, como el almacenamiento de ficheros en directorios iniciales
- Migración de datos

- Cambio de dominio de Windows
- Estandarización de las políticas de auditoría y seguridad de archivos en sistemas de archivos NTFS

Limita el uso de la CLI para establecer la seguridad de archivos y carpetas

Debe estar al tanto de determinados límites cuando utilice la CLI para establecer la seguridad de archivos y carpetas.

- La `vserver security file-directory` La familia de comandos no admite la configuración de ACL de NFSv4.

  Sólo puede aplicar descriptores de seguridad NTFS a archivos y carpetas NTFS.

Cómo se utilizan los descriptores de seguridad para aplicar la seguridad de archivos y carpetas

Los descriptores de seguridad contienen las listas de control de acceso que determinan qué acciones puede realizar un usuario en archivos y carpetas, y qué se audita cuando un usuario accede a archivos y carpetas.

- **Permisos**

  El propietario de un objeto permite o deniega los permisos y determina qué acciones puede realizar un objeto (usuarios, grupos u objetos de equipo) en archivos o carpetas especificados.

- **Descriptores de seguridad**

  Los descriptores de seguridad son estructuras de datos que contienen información de seguridad que definen los permisos asociados a un archivo o carpeta.

- **Listas de control de acceso (ACL)**

  Las listas de control de acceso son las listas contenidas en un descriptor de seguridad que contienen información sobre las acciones que los usuarios, grupos o objetos de equipo pueden realizar en el archivo o la carpeta a la que se aplica el descriptor de seguridad. El descriptor de seguridad puede contener los siguientes dos tipos de ACL:

  - Listas de control de acceso discrecional (DACL)
  - Listas de control de acceso del sistema (SACL)

- **Listas de control de acceso discrecional (DACL)**

  Las DACL contienen la lista de SIDS para los usuarios, grupos y objetos de equipo a los que se permite o deniega el acceso para realizar acciones en archivos o carpetas. Las DACL contienen entradas de control de acceso cero o más (ACE).

- **Listas de control de acceso al sistema (SACL)**

  SACL contiene la lista de SID para los usuarios, grupos y objetos de equipo para los que se registran eventos de auditoría correctos o fallidos. Las SACL contienen entradas de control de acceso cero o más

(ACE).

- **Entradas de control de acceso (ACE)**

  Las ACE son entradas individuales en DACL o SACL:

  - Una entrada de control de acceso DACL especifica los derechos de acceso que se permiten o deniegan para determinados usuarios, grupos o objetos de equipo.
  - Una entrada de control de acceso SACL especifica los eventos de éxito o de error que se deben registrar al auditar acciones especificadas realizadas por usuarios, grupos o objetos de equipo específicos.

- **Herencia de permisos**

  La herencia de permisos describe cómo los permisos definidos en los descriptores de seguridad se propagan a un objeto de un objeto primario. Sólo los objetos secundarios heredan los permisos heredables. Al establecer permisos en el objeto primario, puede decidir si las carpetas, subcarpetas y archivos pueden heredarlos con "'aplicar a. `this-folder`, `sub-folders`, y «ficheros».

Información relacionada

"Seguimiento de seguridad y auditoría de SMB y NFS"

Configurar y aplicar directivas de auditoría a archivos y carpetas NTFS mediante la CLI

Directrices para aplicar políticas de directorio de archivos que utilizan usuarios o grupos locales en el destino de recuperación ante desastres de SVM

Hay ciertas directrices que debe tener en cuenta antes de aplicar políticas de directorio de archivos en el destino de recuperación ante desastres de la máquina virtual de almacenamiento (SVM) en una configuración de descarte de ID si la configuración de la política de directorio de archivos usa usuarios o grupos locales en el descriptor de seguridad, o en las entradas DACL o SACL.

Puede configurar una configuración de recuperación ante desastres para una SVM donde la SVM de origen en el clúster de origen replica los datos y la configuración desde la SVM de origen a una SVM de destino en un clúster de destino.

Puede configurar uno de los dos tipos de recuperación ante desastres de SVM:

- Se conserva la identidad

  Con esta configuración se conserva la identidad de la SVM y el servidor CIFS.

- Identidad descartada

  Con esta configuración, no se conserva la identidad de la SVM y el servidor CIFS. En esta situación, el nombre de la SVM y el servidor CIFS en la SVM de destino es diferente de la SVM y del nombre del servidor CIFS en la SVM de origen.

Directrices para configuraciones de identidad descartadas

En una configuración de identidad descartada, en el caso de un origen de SVM que contenga configuraciones de usuarios locales, grupos y privilegios, se debe cambiar el nombre del dominio local (nombre del servidor CIFS local) para que coincida con el nombre del servidor CIFS en el destino de SVM. Por ejemplo, si el nombre de la SVM de origen es «'vs1'» y el nombre del servidor CIFS es «'CIFS1'» y el nombre de la SVM de destino es «'vs1_dst'» y el nombre del servidor CIFS es «'CIFS1_DST», el nombre de dominio local de un usuario local denominado «'CIFS1\user1' se cambia automáticamente a «CIFS1» en el destino».

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1          CIFS1\Administrator                     Built-in
administrator account
vs1          CIFS1\user1              -              -

cluster1dst::> vserver cifs users-and-groups local-user show -vserver
vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1_dst      CIFS1_DST\Administrator                 Built-in
administrator account
vs1_dst      CIFS1_DST\user1          -              -
```

Aunque los nombres de usuario local y de grupo se cambian automáticamente en las bases de datos de usuario local y de grupo, los usuarios locales o los nombres de grupo no se cambian automáticamente en las configuraciones de políticas de directorio de archivos (las políticas configuradas en la CLI mediante el `vserver security file-directory` familia de comandos).

Por ejemplo, para "'vs1'", si ha configurado una entrada DACL en la `-account` El parámetro se establece en "'CIFS1\user1'", la configuración no se cambia automáticamente en la SVM de destino para reflejar el nombre del servidor CIFS del destino.

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1

Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    CIFS1\user1      allow    full-control      this-folder

cluster1::> vserver security file-directory ntfs dacl show -vserver
vs1_dst

Vserver: vs1_dst
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    **CIFS1**\user1          allow    full-control      this-folder
```

Debe utilizar el `vserver security file-directory modify` Comandos para cambiar manualmente el nombre del servidor CIFS en el nombre del servidor CIFS de destino.

Componentes de configuración de directivas de directorio de archivos que contienen parámetros de cuenta

Existen tres componentes de configuración de directivas de directorio de archivos que pueden utilizar parámetros que pueden contener usuarios o grupos locales:

- Descriptor de seguridad

  Opcionalmente, puede especificar el propietario del descriptor de seguridad y el grupo primario del propietario del descriptor de seguridad. Si el descriptor de seguridad utiliza un usuario o grupo local para las entradas del propietario y del grupo primario, debe modificar el descriptor de seguridad para utilizar la SVM de destino en el nombre de cuenta. Puede utilizar el `vserver security file-directory ntfs modify` para realizar los cambios necesarios en los nombres de cuentas.

- Entradas DACL

  Cada entrada DACL debe estar asociada con una cuenta. Debe modificar todas las DACL que utilicen cuentas de usuario local o de grupo para usar el nombre de la SVM de destino. Debido a que no puede modificar el nombre de cuenta para las entradas DACL existentes, debe eliminar todas las entradas DACL con usuarios o grupos locales de los descriptores de seguridad, crear nuevas entradas DACL con los nombres de cuenta de destino corregidos y asociar estas entradas DACL nuevas con los descriptores de seguridad adecuados.

- Entradas de SACL

Cada entrada de SACL debe estar asociada a una cuenta. Debe modificar todas las SACL que utilicen cuentas de usuario o de grupo local para utilizar el nombre de la SVM de destino. Debido a que no puede modificar el nombre de cuenta para las entradas SACL existentes, debe eliminar todas las entradas SACL con usuarios o grupos locales de los descriptores de seguridad, crear nuevas entradas SACL con los nombres de cuenta de destino corregidos y asociar estas nuevas entradas SACL con los descriptores de seguridad adecuados.

Debe realizar los cambios necesarios en los usuarios o grupos locales utilizados en la configuración de la directiva de directorio de archivos antes de aplicar la directiva; de lo contrario, el trabajo de aplicación fallará.

Configurar y aplicar la seguridad de archivos en archivos y carpetas NTFS mediante la CLI

Cree un descriptor de seguridad NTFS

Crear un descriptor de seguridad NTFS (política de seguridad de archivos) es el primer paso para configurar y aplicar listas de control de acceso NTFS (ACL) a archivos y carpetas que residen en máquinas virtuales de almacenamiento (SVM). Puede asociar el descriptor de seguridad a la ruta de archivo o carpeta en una tarea de directiva.

Acerca de esta tarea

Puede crear descriptores de seguridad NTFS para archivos y carpetas que residen dentro de volúmenes de estilo de seguridad NTFS o para archivos y carpetas que residen en volúmenes de estilo de seguridad mixtos.

De forma predeterminada, cuando se crea un descriptor de seguridad, se agregan cuatro entradas de control de acceso de lista de control de acceso discrecional (DACL) a ese descriptor de seguridad. Los cuatro ACE predeterminados son los siguientes:

Objeto	Tipo de acceso	Derechos de acceso	Dónde aplicar los permisos
BUILTIN\Administrators	Permita	Control total	esta carpeta, subcarpetas, archivos
BUILTIN\Users	Permita	Control total	esta carpeta, subcarpetas, archivos
PROPIETARIO DEL CREADOR	Permita	Control total	esta carpeta, subcarpetas, archivos
NT AUTHORITY\SYSTEM	Permita	Control total	esta carpeta, subcarpetas, archivos

Es posible personalizar la configuración del descriptor de seguridad mediante los siguientes parámetros opcionales:

- Propietario del descriptor de seguridad
- Grupo principal del propietario

- Indicadores de control RAW

Se ignora el valor de cualquier parámetro opcional para Storage-Level Access Guard. Consulte las páginas de manual para obtener más información.

Añada entradas de control de acceso DACL de NTFS al descriptor de seguridad de NTFS

La adición de entradas de control de acceso (ACE) de DACL (lista de control de acceso discrecional) al descriptor de seguridad de NTFS es el segundo paso para configurar y aplicar ACL de NTFS a un archivo o carpeta. Cada entrada identifica qué objeto tiene permiso o acceso denegado, y define lo que el objeto puede o no puede hacer con los archivos o carpetas definidos en ACE.

Acerca de esta tarea

Puede añadir una o varias ACE a la DACL del descriptor de seguridad.

Si el descriptor de seguridad contiene una DACL que tiene ACE existentes, el comando agrega la nueva ACE a la DACL. Si el descriptor de seguridad no contiene una DACL, el comando crea la DACL y le agrega la nueva ACE.

Opcionalmente, puede personalizar las entradas DACL especificando los derechos que desea permitir o denegar para la cuenta especificada en `-account` parámetro. Hay tres métodos mutuamente exclusivos para especificar los derechos:

- Derechos
- Derechos avanzados
- Derechos RAW (privilegio avanzado)

> Si no especifica derechos para la entrada DACL, el valor predeterminado es establecer los derechos `Full Control`.

Opcionalmente, puede personalizar las entradas DACL especificando cómo aplicar herencia.

Se ignora el valor de cualquier parámetro opcional para Storage-Level Access Guard. Consulte las páginas de manual para obtener más información.

Pasos

1. Agregue una entrada DACL a un descriptor de seguridad: `vserver security file-directory ntfs dacl add -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SIDoptional_parameters`

   ```
   vserver security file-directory ntfs dacl add -ntfs-sd sd1 -access-type deny
   -account domain\joe -rights full-control -apply-to this-folder -vserver vs1
   ```

2. Compruebe que la entrada DACL es correcta: `vserver security file-directory ntfs dacl show -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SID`

   ```
   vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
   -access-type deny -account domain\joe
   ```

```
                    Vserver: vs1
     Security Descriptor Name: sd1
                Allow or Deny: deny
          Account Name or SID: DOMAIN\joe
                Access Rights: full-control
       Advanced Access Rights: -
                     Apply To: this-folder
                Access Rights: full-control
```

Cree políticas de seguridad

Crear una política de seguridad de archivos para SVM es el tercer paso a la hora de configurar y aplicar ACL a un archivo o carpeta. Una directiva actúa como contenedor para varias tareas, donde cada tarea es una entrada única que se puede aplicar a archivos o carpetas. Posteriormente, puede agregar tareas a la directiva de seguridad.

Acerca de esta tarea

Las tareas que agrega a una directiva de seguridad contienen asociaciones entre el descriptor de seguridad NTFS y las rutas de acceso de archivos o carpetas. Por lo tanto, debe asociar la política de seguridad con cada SVM (que contenga volúmenes de estilo de seguridad NTFS o volúmenes mixtos de estilo de seguridad).

Pasos

1. Cree una política de seguridad: `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

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

2. Compruebe la directiva de seguridad: `vserver security file-directory policy show`

```
vserver security file-directory policy show
   Vserver          Policy Name
 ------------     --------------
     vs1              policy1
```

Agregar una tarea a la directiva de seguridad

Crear y añadir una tarea de política a una política de seguridad es el cuarto paso para configurar y aplicar ACL a archivos o carpetas en SVM. Al crear la tarea de directiva, asocie la tarea a una directiva de seguridad. Puede agregar una o más entradas de tareas a una directiva de seguridad.

Acerca de esta tarea

La política de seguridad es un contenedor para una tarea. Una tarea hace referencia a una única operación

que puede realizar una directiva de seguridad para archivos o carpetas con seguridad NTFS o mixta (o a un objeto de volumen si se configura Storage-Level Access Guard).

Existen dos tipos de tareas:

- Tareas de archivo y directorio

  Se utiliza para especificar tareas que aplican descriptores de seguridad a archivos y carpetas especificados. Las ACL aplicadas mediante tareas de archivo y directorio se pueden gestionar con clientes de SMB o con la interfaz de línea de comandos de ONTAP.

- Tareas de protección de acceso al nivel de almacenamiento

  Se utiliza para especificar tareas que aplican descriptores de seguridad de Access Guard de nivel de almacenamiento a un volumen especificado. Las ACL aplicadas mediante tareas de protección de acceso al nivel de almacenamiento solo se pueden gestionar a través de la interfaz de línea de comandos de ONTAP.

Una tarea contiene definiciones para la configuración de seguridad de un archivo (o carpeta) o un conjunto de archivos (o carpetas). Cada tarea de una política se identifica de forma única por la ruta. Sólo puede haber una tarea por ruta dentro de una única política. Una directiva no puede tener entradas de tareas duplicadas.

Directrices para agregar una tarea a una directiva:

- Puede haber un máximo de 10,000 entradas de tareas por directiva.
- Una política puede contener una o más tareas.

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

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

  Nunca dará permisos de acceso adicionales.

Al agregar tareas a las directivas de seguridad, debe especificar los siguientes cuatro parámetros necesarios:

- Nombre de SVM
- Nombre de la política
- Ruta
- Descriptor de seguridad que se asociará a la ruta de acceso

Es posible personalizar la configuración del descriptor de seguridad mediante los siguientes parámetros opcionales:

- Tipo de seguridad
- Modo de propagación
- Posición de índice
- Tipo de control de acceso

Se ignora el valor de cualquier parámetro opcional para Storage-Level Access Guard. Consulte las páginas de manual para obtener más información.

Pasos

1. Añada una tarea con un descriptor de seguridad asociado a la directiva de seguridad: `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory` es el valor predeterminado para `-access-control` parámetro. Es opcional especificar el tipo de control de acceso cuando se configuran las tareas de acceso a archivos y directorios.

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name
   policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2
   -index-num 1 -access-control file-directory
   ```

2. Compruebe la configuración de la tarea de directiva: `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

   `vserver security file-directory policy task show`

   ```
   Vserver: vs1
   Policy: policy1

   Index    File/Folder    Access           Security   NTFS       NTFS
   Security
            Path           Control          Type       Mode
   Descriptor Name
   -----    --------       -----------      --------   ------
   ----------------
   1        /home/dir1     file-directory   ntfs       propagate  sd2
   ```

Aplicación de las políticas de seguridad

Aplicar una política de seguridad de archivos a las SVM es el último paso a la hora de crear y aplicar ACL de NTFS a archivos o carpetas.

Acerca de esta tarea

Puede aplicar la configuración de seguridad definida en la política de seguridad a archivos y carpetas NTFS que residen en volúmenes FlexVol (estilo de seguridad NTFS o mixto).

> Cuando se aplican una directiva de auditoría y SACL asociadas, se sobrescriben todas las DACL existentes. Cuando se aplica una directiva de seguridad y sus DACL asociados, se sobrescriben todas las DACL existentes. Debe revisar las directivas de seguridad existentes antes de crear y aplicar otras nuevas.

Paso

1. Aplicar una política de seguridad: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

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

El trabajo de aplicación de política está programado y se devuelve el ID de trabajo.

```
[Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
53322" command to view the status of the operation
```

Supervise el trabajo de política de seguridad

Al aplicar la política de seguridad a máquinas virtuales de almacenamiento (SVM), puede supervisar el progreso de la tarea supervisando el trabajo de la política de seguridad. Esto es útil si desea comprobar que la aplicación de la política de seguridad ha sido satisfactoria. Esto también resulta útil si tiene un trabajo de larga ejecución en el que está aplicando seguridad masiva a un gran número de archivos y carpetas.

Acerca de esta tarea

Para mostrar información detallada sobre un trabajo de política de seguridad, debe usar `-instance` parámetro.

Paso

1. Supervise el trabajo de la política de seguridad: `vserver security file-directory job show -vserver vserver_name`

   `vserver security file-directory job show -vserver vs1`

   ```
   Job ID Name                 Vserver    Node           State
   ------ -------------------- ---------- -------------- ----------
   53322  Fsecurity Apply      vs1        node1          Success
          Description: File Directory Security Apply Job
   ```

Compruebe la seguridad del archivo aplicado

Es posible verificar la configuración de seguridad de archivos para confirmar que los archivos o las carpetas de la máquina virtual de almacenamiento (SVM) a la que aplicó la política de seguridad tienen la configuración deseada.

Acerca de esta tarea

Debe suministrar el nombre de la SVM que contenga los datos y la ruta de acceso al archivo y las carpetas en los que desea verificar la configuración de seguridad. Puede usar el opcional `-expand-mask` parámetro para mostrar información detallada acerca de la configuración de seguridad.

Paso

1. Mostrar la configuración de seguridad de archivos y carpetas: `vserver security file-directory show -vserver vserver_name -path path [-expand-mask true]`

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

Configure y aplique políticas de auditoría a archivos y carpetas NTFS usando la información general de la CLI

Hay varios pasos que debe realizar para aplicar políticas de auditoría a archivos y carpetas NTFS cuando use la CLI de ONTAP. En primer lugar, debe crear un descriptor de seguridad NTFS y agregar SACL al descriptor de seguridad. A continuación, cree una directiva de seguridad y agregue tareas de directiva. Luego, debe aplicar la política de seguridad a una SVM.

Acerca de esta tarea

Después de aplicar la directiva de seguridad, puede supervisar el trabajo de directiva de seguridad y, a continuación, verificar la configuración de la directiva de auditoría aplicada.

Cuando se aplican una directiva de auditoría y SACL asociadas, se sobrescriben todas las DACL existentes. Debe revisar las directivas de seguridad existentes antes de crear y aplicar otras nuevas.

Información relacionada

Protección del acceso a archivos mediante Storage-Level Access Guard

Limita el uso de la CLI para establecer la seguridad de archivos y carpetas

Cómo se utilizan los descriptores de seguridad para aplicar la seguridad de archivos y carpetas

"Seguimiento de seguridad y auditoría de SMB y NFS"

Configurar y aplicar la seguridad de archivos en archivos y carpetas NTFS mediante la CLI

Cree un descriptor de seguridad NTFS

Crear una política de auditoría de descriptor de seguridad NTFS es el primer paso para configurar y aplicar listas de control de acceso NTFS (ACL) a archivos y carpetas que residen en SVM. Asociará el descriptor de seguridad a la ruta de archivo o carpeta en una tarea de directiva.

Acerca de esta tarea

Puede crear descriptores de seguridad NTFS para archivos y carpetas que residen dentro de volúmenes de estilo de seguridad NTFS o para archivos y carpetas que residen en volúmenes de estilo de seguridad mixtos.

De forma predeterminada, cuando se crea un descriptor de seguridad, se agregan cuatro entradas de control de acceso de lista de control de acceso discrecional (DACL) a ese descriptor de seguridad. Los cuatro ACE predeterminados son los siguientes:

Objeto	Tipo de acceso	Derechos de acceso	Dónde aplicar los permisos
BUILTIN\Administrators	Permita	Control total	esta carpeta, subcarpetas, archivos
BUILTIN\Users	Permita	Control total	esta carpeta, subcarpetas, archivos
PROPIETARIO DEL CREADOR	Permita	Control total	esta carpeta, subcarpetas, archivos
NT AUTHORITY\SYSTEM	Permita	Control total	esta carpeta, subcarpetas, archivos

Es posible personalizar la configuración del descriptor de seguridad mediante los siguientes parámetros opcionales:

- Propietario del descriptor de seguridad
- Grupo principal del propietario

- Indicadores de control RAW

Se ignora el valor de cualquier parámetro opcional para Storage-Level Access Guard. Consulte las páginas de manual para obtener más información.

Pasos

1. Si desea usar los parámetros avanzados, configure el nivel de privilegio en Advanced: `set -privilege advanced`
2. Cree un descriptor de seguridad: `vserver security file-directory ntfs create -vserver vserver_name -ntfs-sd SD_nameoptional_parameters`

   `vserver security file-directory ntfs create -ntfs-sd sd1 -vserver vs1 -owner DOMAIN\joe`

3. Compruebe que la configuración del descriptor de seguridad sea correcta: `vserver security file-directory ntfs show -vserver vserver_name -ntfs-sd SD_name`

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

   ```
                                       Vserver: vs1
                               Security Descriptor Name: sd1
                        Owner of the Security Descriptor: DOMAIN\joe
   ```

4. Si se encuentra en el nivel de privilegio avanzado, regrese al nivel de privilegio de administrador: `set -privilege admin`

Añada entradas de control de acceso SACL a NTFS al descriptor de seguridad de NTFS

Añadir entradas de control de acceso (ACE) SACL (lista de control de acceso del sistema) al descriptor de seguridad NTFS es el segundo paso a la hora de crear directivas de auditoría NTFS para archivos o carpetas en SVM. Cada entrada identifica el usuario o grupo que desea auditar. La entrada SACL define si desea auditar los intentos de acceso fallidos o correctos.

Acerca de esta tarea

Puede agregar uno o varios ACE al SACL del descriptor de seguridad.

Si el descriptor de seguridad contiene un SACL que tiene ACE existentes, el comando agrega el nuevo ACE al SACL. Si el descriptor de seguridad no contiene un SACL, el comando crea el SACL y le agrega el nuevo ACE.

Puede configurar las entradas SACL especificando los derechos que desea auditar para los eventos de éxito o error de la cuenta especificada en `-account` parámetro. Hay tres métodos mutuamente exclusivos para especificar los derechos:

- Derechos

- Derechos avanzados
- Derechos RAW (privilegio avanzado)

> Si no especifica derechos para la entrada SACL, la configuración predeterminada es `Full Control`.

Opcionalmente, puede personalizar las entradas SACL especificando cómo aplicar herencia con `apply to` parámetro. Si no especifica este parámetro, el valor predeterminado es aplicar esta entrada SACL a esta carpeta, subcarpetas y archivos.

Pasos

1. Añada una entrada SACL a un descriptor de seguridad: `vserver security file-directory ntfs sacl add -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SIDoptional_parameters`

   ```
   vserver security file-directory ntfs sacl add -ntfs-sd sd1 -access-type
   failure -account domain\joe -rights full-control -apply-to this-folder
   -vserver vs1
   ```

2. Compruebe que la entrada de SACL es correcta: `vserver security file-directory ntfs sacl show -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SID`

   ```
   vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
   -access-type deny -account domain\joe
   ```

   ```
                                  Vserver: vs1
                   Security Descriptor Name: sd1
   Access type for Specified Access Rights: failure
                       Account Name or SID: DOMAIN\joe
                             Access Rights: full-control
                     Advanced Access Rights: -
                                  Apply To: this-folder
                             Access Rights: full-control
   ```

Cree políticas de seguridad

Crear una política de auditoría para máquinas virtuales de almacenamiento (SVM) es el tercer paso a la hora de configurar y aplicar ACL a un archivo o una carpeta. Una directiva actúa como contenedor para varias tareas, donde cada tarea es una entrada única que se puede aplicar a archivos o carpetas. Posteriormente, puede agregar tareas a la directiva de seguridad.

Acerca de esta tarea

Las tareas que agrega a una directiva de seguridad contienen asociaciones entre el descriptor de seguridad NTFS y las rutas de acceso de archivos o carpetas. Por lo tanto, debe asociar la política de seguridad con cada máquina virtual de almacenamiento (SVM) (que contenga volúmenes de estilo de seguridad NTFS o

volúmenes mixtos de estilo de seguridad).

Pasos

1. Cree una política de seguridad: `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

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

2. Compruebe la directiva de seguridad: `vserver security file-directory policy show`

```
vserver security file-directory policy show
   Vserver          Policy Name
 ------------     --------------
     vs1              policy1
```

Agregar una tarea a la directiva de seguridad

Crear y añadir una tarea de política a una política de seguridad es el cuarto paso para configurar y aplicar ACL a archivos o carpetas en SVM. Al crear la tarea de directiva, asocie la tarea a una directiva de seguridad. Puede agregar una o más entradas de tareas a una directiva de seguridad.

Acerca de esta tarea

La política de seguridad es un contenedor para una tarea. Una tarea hace referencia a una única operación que puede realizar una directiva de seguridad para archivos o carpetas con seguridad NTFS o mixta (o a un objeto de volumen si se configura Storage-Level Access Guard).

Existen dos tipos de tareas:

- Tareas de archivo y directorio

  Se utiliza para especificar tareas que aplican descriptores de seguridad a archivos y carpetas especificados. Las ACL aplicadas mediante tareas de archivo y directorio se pueden gestionar con clientes de SMB o con la interfaz de línea de comandos de ONTAP.

- Tareas de protección de acceso al nivel de almacenamiento

  Se utiliza para especificar tareas que aplican descriptores de seguridad de Access Guard de nivel de almacenamiento a un volumen especificado. Las ACL aplicadas mediante tareas de protección de acceso al nivel de almacenamiento solo se pueden gestionar a través de la interfaz de línea de comandos de ONTAP.

Una tarea contiene definiciones para la configuración de seguridad de un archivo (o carpeta) o un conjunto de archivos (o carpetas). Cada tarea de una política se identifica de forma única por la ruta. Sólo puede haber una tarea por ruta dentro de una única política. Una directiva no puede tener entradas de tareas duplicadas.

Directrices para agregar una tarea a una directiva:

- Puede haber un máximo de 10,000 entradas de tareas por directiva.

- Una política puede contener una o más tareas.

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

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

  Nunca dará permisos de acceso adicionales.

Es posible personalizar la configuración del descriptor de seguridad mediante los siguientes parámetros opcionales:

- Tipo de seguridad
- Modo de propagación
- Posición de índice
- Tipo de control de acceso

Se ignora el valor de cualquier parámetro opcional para Storage-Level Access Guard. Consulte las páginas de manual para obtener más información.

Pasos

1. Añada una tarea con un descriptor de seguridad asociado a la directiva de seguridad: `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory` es el valor predeterminado para `-access-control` parámetro. Es opcional especificar el tipo de control de acceso cuando se configuran las tareas de acceso a archivos y directorios.

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name
   policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2
   -index-num 1 -access-control file-directory
   ```

2. Compruebe la configuración de la tarea de directiva: `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

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

   ```
   Vserver: vs1
   Policy: policy1

   Index    File/Folder    Access           Security   NTFS       NTFS
   Security
            Path           Control          Type       Mode
   Descriptor Name
   -----    --------       -----------      --------   ------
   ----------------
   1        /home/dir1     file-directory   ntfs       propagate  sd2
   ```

Aplicación de las políticas de seguridad

Aplicar una política de auditoría a las SVM es el último paso a la hora de crear y aplicar ACL de NTFS a archivos o carpetas.

Acerca de esta tarea

Puede aplicar la configuración de seguridad definida en la política de seguridad a archivos y carpetas NTFS que residen en volúmenes FlexVol (estilo de seguridad NTFS o mixto).

> Cuando se aplican una directiva de auditoría y SACL asociadas, se sobrescriben todas las DACL existentes. Cuando se aplica una directiva de seguridad y sus DACL asociados, se sobrescriben todas las DACL existentes. Debe revisar las directivas de seguridad existentes antes de crear y aplicar otras nuevas.

Paso

1. Aplicar una política de seguridad: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

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

   El trabajo de aplicación de política está programado y se devuelve el ID de trabajo.

   ```
   [Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 –id
   53322" command to view the status of the operation
   ```

Supervise el trabajo de política de seguridad

Al aplicar la política de seguridad a máquinas virtuales de almacenamiento (SVM), puede supervisar el progreso de la tarea supervisando el trabajo de la política de seguridad. Esto es útil si desea comprobar que la aplicación de la política de seguridad ha sido satisfactoria. Esto también resulta útil si tiene un trabajo de larga ejecución en el que está aplicando seguridad masiva a un gran número de archivos y carpetas.

Acerca de esta tarea

Para mostrar información detallada sobre un trabajo de política de seguridad, debe usar `-instance` parámetro.

Paso

1. Supervise el trabajo de la política de seguridad: `vserver security file-directory job show -vserver vserver_name`

   `vserver security file-directory job show -vserver vs1`

```
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
53322  Fsecurity Apply      vs1        node1          Success
       Description: File Directory Security Apply Job
```

Compruebe la política de auditoría aplicada

Puede verificar la política de auditoría para confirmar que los archivos o las carpetas de la máquina virtual de almacenamiento (SVM) a la que aplicó la política de seguridad tienen la configuración de seguridad de auditoría deseada.

Acerca de esta tarea

Utilice la `vserver security file-directory show` comando para mostrar información de la política de auditoría. Debe proporcionar el nombre de la SVM que contiene los datos y la ruta a los datos cuyo archivo o carpeta de información de la política de auditoría que desea mostrar.

Paso

1. Mostrar la configuración de directivas de auditoría: `vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*

Ejemplo

El siguiente comando muestra la información de la directiva de auditoría aplicada a la ruta "'/corp" en SVM vs1. La ruta de acceso tiene aplicada UNA entrada SACL DE ÉXITO y DE FALLO:

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

                Vserver: vs1
              File Path: /corp
         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
```

Consideraciones que tener en cuenta al administrar trabajos de directiva de seguridad

Si existe un trabajo de política de seguridad, en determinadas circunstancias, no puede modificar dicha política de seguridad ni las tareas asignadas a dicha política. Debe entender en qué condiciones puede o no puede modificar las directivas de seguridad para que cualquier intento que realice para modificar la directiva se realice correctamente. Las modificaciones de la directiva incluyen agregar, eliminar o modificar tareas asignadas a la directiva y eliminar o modificar la directiva.

No puede modificar una política de seguridad ni una tarea asignada a esa política si existe un trabajo para esa política y ese trabajo está en los estados siguientes:

- El trabajo está en ejecución o en curso.
- El trabajo está en pausa.
- El trabajo se reanuda y se encuentra en estado en ejecución.
- Si el trabajo está esperando a conmutar al respaldo a otro nodo.

En las siguientes circunstancias, si existe un trabajo para una política de seguridad, puede modificar correctamente dicha política de seguridad o una tarea asignada a dicha directiva:

- El trabajo de política se ha detenido.
- El trabajo de directiva ha finalizado correctamente.

Comandos para administrar descriptores de seguridad NTFS

Existen comandos ONTAP específicos para administrar descriptores de seguridad. Puede crear, modificar, eliminar y mostrar información acerca de los descriptores de seguridad.

Si desea…	Se usa este comando…
Crear descriptores de seguridad NTFS	`vserver security file-directory ntfs create`
Modifique los descriptores de seguridad NTFS existentes	`vserver security file-directory ntfs modify`
Mostrar información acerca de los descriptores de seguridad NTFS existentes	`vserver security file-directory ntfs show`
Eliminar descriptores de seguridad NTFS	`vserver security file-directory ntfs delete`

Vea las páginas de manual para el `vserver security file-directory ntfs` comandos para obtener más información.

Comandos para administrar entradas de control de acceso DACL de NTFS

Hay comandos ONTAP específicos para administrar entradas de control de acceso de DACL (ACE). Puede agregar ACE a DACL NTFS en cualquier momento. También puede administrar las DACL de NTFS existentes modificando, eliminando y mostrando información acerca de las ACE en las DACL.

Si desea…	Se usa este comando…
Cree ACE y agréguelos a DACL NTFS	`vserver security file-directory ntfs dacl add`
Modifique los ACE existentes en las DACL NTFS	`vserver security file-directory ntfs dacl modify`

Si desea…	Se usa este comando…
Mostrar información acerca de los ACE existentes en las DACL NTFS	`vserver security file-directory ntfs dacl show`
Elimine los ACE existentes de las DACL NTFS	`vserver security file-directory ntfs dacl remove`

Vea las páginas de manual para el `vserver security file-directory ntfs dacl` comandos para obtener más información.

Comandos para gestionar entradas de control de acceso SACL de NTFS

Hay comandos ONTAP específicos para administrar entradas de control de acceso SACL (ACE). Puede agregar ACE a SACL NTFS en cualquier momento. También puede administrar SACL NTFS existentes modificando, eliminando y mostrando información acerca de ACE en SACL.

Si desea…	Se usa este comando…
Cree ACE y agréguelos a SACL NTFS	`vserver security file-directory ntfs sacl add`
Modifique los ACE existentes en SACL NTFS	`vserver security file-directory ntfs sacl modify`
Muestra información acerca de los ACE existentes en SACL NTFS	`vserver security file-directory ntfs sacl show`
Elimine los ACE existentes de SACL NTFS	`vserver security file-directory ntfs sacl remove`

Vea las páginas de manual para el `vserver security file-directory ntfs sacl` comandos para obtener más información.

Comandos para gestionar políticas de seguridad

Existen comandos ONTAP específicos para administrar las políticas de seguridad. Puede mostrar información acerca de las políticas y eliminarla. No puede modificar una política de seguridad.

Si desea…	Se usa este comando…
Cree políticas de seguridad	`vserver security file-directory policy create`
Mostrar información acerca de las directivas de seguridad	`vserver security file-directory policy show`
Eliminar políticas de seguridad	`vserver security file-directory policy delete`

Vea las páginas de manual para el `vserver security file-directory policy` comandos para obtener más información.

Comandos para administrar tareas de políticas de seguridad

Hay comandos de ONTAP para añadir, modificar, quitar y mostrar información acerca de tareas de políticas de seguridad.

Si desea…	Se usa este comando…
Agregar tareas de directiva de seguridad	`vserver security file-directory policy task add`
Modifique las tareas de las políticas de seguridad	`vserver security file-directory policy task modify`
Muestra información acerca de las tareas de directiva de seguridad	`vserver security file-directory policy task show`
Quitar tareas de directiva de seguridad	`vserver security file-directory policy task remove`

Vea las páginas de manual para el `vserver security file-directory policy task` comandos para obtener más información.

Comandos para gestionar trabajos de políticas de seguridad

Hay comandos de la ONTAP para pausar, reanudar, detener y mostrar información acerca de los trabajos de políticas de seguridad.

Si desea…	Se usa este comando…
Pausar trabajos de directiva de seguridad	`vserver security file-directory job pause -vserver vserver_name -id integer`
Reanudar trabajos de directiva de seguridad	`vserver security file-directory job resume -vserver vserver_name -id integer`
Mostrar información sobre trabajos de directivas de seguridad	`vserver security file-directory job show -vserver vserver_name` Es posible determinar el ID de trabajo de un trabajo con este comando.
Detener trabajos de directiva de seguridad	`vserver security file-directory job stop -vserver vserver_name -id integer`

Vea las páginas de manual para el `vserver security file-directory job` comandos para obtener más información.