Sécurisez l'accès aux fichiers à l'aide de Storage-Level Access Guard

ONTAP 9

NetApp
April 24, 2024

Sommaire

Sécurisez l’accès aux fichiers à l’aide de Storage-Level Access Guard

Sécurisez l’accès aux fichiers à l’aide de Storage-Level Access Guard

Outre la sécurisation de l’accès à l’aide de la sécurité native au niveau des fichiers et de l’exportation et du partage, vous pouvez configurer Storage-Level Access Guard, une troisième couche de sécurité appliquée par ONTAP au niveau du volume. Storage-Level Access Guard s’applique à l’accès à partir de tous les protocoles NAS vers l’objet de stockage auquel il est appliqué.

Seules les autorisations d’accès NTFS sont prises en charge. Pour que ONTAP puisse effectuer des vérifications de sécurité sur les utilisateurs UNIX afin d’accéder aux données sur les volumes pour lesquels Storage-Level Access Guard a été appliqué, l’utilisateur UNIX doit mapper un utilisateur Windows sur le SVM propriétaire du volume.

Comportement de la protection d’accès au niveau du stockage

- Storage-Level Access Guard s’applique à tous les fichiers ou tous les répertoires d’un objet de stockage.

  Comme tous les fichiers ou répertoires d’un volume sont soumis aux paramètres Storage-Level Access Guard, l’héritage par propagation n’est pas requis.

- Vous pouvez configurer Storage-Level Access Guard pour qu’il s’applique aux fichiers uniquement, aux répertoires uniquement ou aux fichiers et répertoires d’un volume.
  - Sécurité des fichiers et des répertoires

    S’applique à chaque répertoire et fichier de l’objet de stockage. Il s’agit du paramètre par défaut.

  - Sécurité des fichiers

    S’applique à chaque fichier de l’objet de stockage. L’application de cette sécurité n’affecte pas l’accès aux répertoires ou leur audit.

  - Sécurité de l’annuaire

    S’applique à chaque répertoire de l’objet de stockage. L’application de cette sécurité n’affecte pas l’accès aux fichiers ou leur audit.

- Storage-Level Access Guard est utilisé pour restreindre les autorisations.

  Il ne vous donnera jamais d’autorisations d’accès supplémentaires.

- Si vous affichez les paramètres de sécurité d’un fichier ou d’un répertoire à partir d’un client NFS ou SMB, vous ne voyez pas la sécurité Storage-Level Access Guard.

  Elle est appliquée au niveau de l’objet de stockage et stockée dans les métadonnées utilisées afin de déterminer les autorisations efficaces.

- La sécurité au niveau du stockage ne peut pas être révoquée d'un client, même par un administrateur système (Windows ou UNIX).

  Il est conçu pour être modifié par les administrateurs de stockage uniquement.

- Vous pouvez appliquer Storage-Level Access Guard aux volumes dotés de NTFS ou d'un style de sécurité mixte.
- Vous pouvez appliquer Storage-Level Access Guard aux volumes de style de sécurité UNIX, tant que le SVM contenant le volume a un serveur CIFS configuré.
- Lorsque les volumes sont montés sous un chemin de jonction de volume et que Storage-Level Access Guard est présent sur ce chemin, il ne sera pas propagé aux volumes montés sous celui-ci.
- Le descripteur de sécurité Storage-Level Access Guard est répliqué avec la réplication des données SnapMirror et avec la réplication SVM.
- Il existe une dispensation spéciale pour les scanners de virus.

  Un accès exceptionnel est autorisé à ces serveurs pour afficher des fichiers et des répertoires, même si Storage-Level Access Guard refuse l'accès à l'objet.

- Les notifications FPolicy ne sont pas envoyées si l'accès est refusé car la protection d'accès du niveau de stockage est disponible.

Ordre des contrôles d'accès

L'accès à un fichier ou à un répertoire est déterminé par l'effet combiné des autorisations d'exportation ou de partage, des autorisations Storage-Level Access Guard définies sur les volumes et des autorisations de fichier natif appliquées aux fichiers et/ou répertoires. Tous les niveaux de sécurité sont évalués pour déterminer les autorisations efficaces qu'un fichier ou un répertoire possède. Les contrôles d'accès de sécurité sont effectués dans l'ordre suivant :

1. Partage SMB ou autorisations au niveau des exportations NFS
2. Protection d'accès au niveau du stockage
3. Listes de contrôle d'accès aux fichiers/dossiers NTFS (ACL), listes de contrôle d'accès NFSv4 ou bits en mode UNIX

Cas d'utilisation de Storage-Level Access Guard

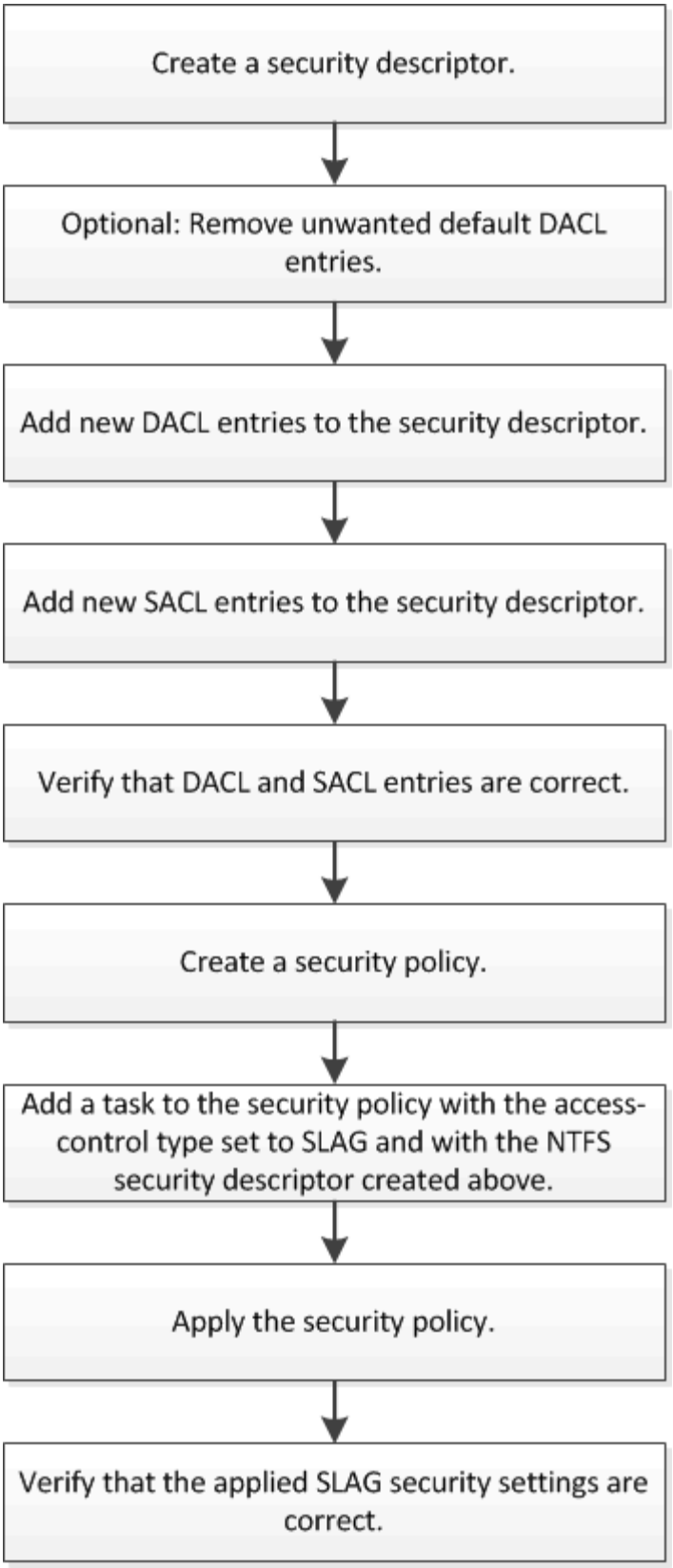
Storage-Level Access Guard fournit une sécurité supplémentaire au niveau du stockage, qui n'est pas visible du côté client. Par conséquent, il ne peut être révoqué par aucun des utilisateurs ou administrateurs de leur poste de travail. Dans certains cas, il est préférable de pouvoir contrôler l'accès au niveau de stockage.

Les cas d'utilisation typiques de cette fonctionnalité sont les suivants :

- Protection de la propriété intellectuelle par l'audit et le contrôle de l'accès de tous les utilisateurs au niveau du stockage
- Stockage pour les entreprises de services financiers, y compris les services bancaires et les groupes de transactions
- Services publics avec stockage de fichiers distinct dans les différents départements
- Universités protégeant tous les fichiers des étudiants

Workflow de configuration de Storage-Level Access Guard

Le workflow de configuration de Storage-Level Access Guard (SLAG) utilise les mêmes commandes CLI de ONTAP que celles que vous utilisez pour configurer les autorisations d'accès aux fichiers NTFS et les stratégies d'audit. Au lieu de configurer l'accès aux fichiers et aux répertoires sur une cible désignée, vous configurez LE SLAG sur le volume SVM (Storage Virtual machine) désigné.



Informations associées

Configuration de Storage-Level Access Guard

Configurer Storage-Level Access Guard

Plusieurs étapes sont nécessaires pour configurer Storage-Level Access Guard sur un volume ou un qtree. Storage-Level Access Guard fournit un niveau de sécurité d'accès défini au niveau du stockage. Elle fournit une sécurité qui s'applique à tous les accès à partir de tous les protocoles NAS vers l'objet de stockage auquel il a été appliqué.

Étapes

1. Créez un descripteur de sécurité à l'aide du `vserver security file-directory ntfs create` commande.

   `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              -
   ```

   Un descripteur de sécurité est créé avec les quatre entrées de contrôle d'accès DACL (ACE) suivantes :

   ```
   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 vous ne souhaitez pas utiliser les entrées par défaut lors de la configuration de Storage-Level Access Guard, vous pouvez les supprimer avant de créer et d'ajouter vos propres ACE au descripteur de sécurité.

2. Supprimez l'un des ACE DACL par défaut du descripteur de sécurité que vous ne souhaitez pas configurer avec la sécurité Storage-Level Access Guard :

a. Supprimez les ACE DACL indésirables à l'aide du `vserver security file-directory ntfs dacl remove` commande.

   Dans cet exemple, trois ACE DACL par défaut sont supprimés du descripteur de sécurité : BUILTIN\Administrators, BULTIN\Users et CRÉATEUR 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. Vérifiez que les ACE DACL que vous ne souhaitez pas utiliser pour la sécurité Storage-Level Access Guard sont supprimés du descripteur de sécurité à l'aide de `vserver security file-directory ntfs dacl show` commande.

   Dans cet exemple, la sortie de la commande vérifie que trois ACE DACL par défaut ont été supprimés du descripteur de sécurité, ne laissant que l'entrée ACE DACL par défaut du SYSTÈME/AUTORITÉ NT :

   ```
   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. Ajoutez une ou plusieurs entrées DACL à un descripteur de sécurité en utilisant le `vserver security file-directory ntfs dacl add` commande.

   Dans cet exemple, deux ACE DACL sont ajoutés au descripteur de sécurité :

   ```
   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. Ajoutez une ou plusieurs entrées SACL à un descripteur de sécurité à l'aide du `vserver security file-directory ntfs sacl add` commande.

   Dans cet exemple, deux ACE SACL sont ajoutés au descripteur de sécurité :

   ```
   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. Vérifier que les ACE DACL et SACL sont correctement configurés à l'aide du `vserver security file-directory ntfs dacl show` et `vserver security file-directory ntfs sacl show` respectivement.

   Dans cet exemple, la commande suivante affiche des informations sur les entrées DACL pour le descripteur de sécurité "sd1":

   ```
   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
   ```

   Dans cet exemple, la commande suivante affiche des informations sur les entrées SACL pour le descripteur de sécurité « `sd1' » :

   ```
   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. Créez une stratégie de sécurité à l'aide de `vserver security file-directory policy create` commande.

   L'exemple suivant crée une politique nommée « politique 1 » :

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

7. Vérifiez que la stratégie est correctement configurée à l'aide du `vserver security file-directory policy show` commande.

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

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

8. Ajoutez une tâche avec un descripteur de sécurité associé à la stratégie de sécurité en utilisant le `vserver security file-directory policy task add` commande avec `-access-control` paramètre défini sur `slag`.

   Même si une stratégie peut contenir plusieurs tâches Storage-Level Access Guard, vous ne pouvez pas configurer une stratégie pour contenir à la fois des tâches file-Directory et Storage-Level Access Guard. Une stratégie doit contenir soit toutes les tâches Storage-Level Access Guard, soit toutes les tâches du répertoire de fichiers.

   Dans cet exemple, une tâche est ajoutée à la politique nommée ""politie1"", qui est affectée au descripteur de sécurité "s1'". Il est affecté à l' `/datavol1` chemin avec le type de contrôle d'accès défini sur "`stable".

   ```
   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. Vérifiez que la tâche est correctement configurée à l'aide de l' `vserver security file-directory policy task show` commande.

   ```
   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. Appliquez la stratégie de sécurité de Storage-Level Access Guard à l'aide du `vserver security file-directory apply` commande.

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

    La tâche d'application de la stratégie de sécurité est planifiée.

11. Vérifiez que les paramètres de sécurité de Storage-Level Access Guard sont corrects à l'aide de l' `vserver security file-directory show` commande.

    Dans cet exemple, le résultat de la commande indique que la sécurité Storage-Level Access Guard a été appliquée au volume NTFS `/datavol1`. Bien que la DACL par défaut permettant un contrôle total à tout le monde reste, la sécurité de Storage-Level Access Guard limite (et vérifie) l'accès aux groupes définis dans les paramètres 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
```

Informations associées

Gestion de la sécurité des fichiers NTFS, des règles d'audit NTFS et Storage-Level Access Guard sur les SVM via l'interface de ligne de commande

Workflow de configuration de Storage-Level Access Guard

Affichage d'informations sur Storage-Level Access Guard

Retrait de Storage-Level Access Guard

Matrice de SCORIES efficace

Vous pouvez configurer LE SCORIES sur un volume, un qtree ou les deux. La matrice DE SCORIES définit le volume ou qtree en tant que configuration SLAG applicable dans les différents scénarios répertoriés dans le tableau.

	SCORIES de volume dans un système AFS	**FIGURE de volume dans une copie Snapshot**	**Qtree SCORIES dans un système AFS**	**Qtree LAG dans une copie Snapshot**
Accès au volume dans un système de fichiers d'accès (AFS)	OUI	NON	S/O	S/O
Accès de volume dans une copie Snapshot	OUI	NON	S/O	S/O
Accès au qtree dans un AFS (lorsque LE SCORIES est présent dans le qtree)	NON	NON	OUI	NON
Accès au qtree dans un AFS (lorsque LE SCORIES n'est pas présente dans le qtree)	OUI	NON	NON	NON
Accès qtree dans la copie Snapshot (lorsque LE SCORIES est présente dans le qtree AFS)	NON	NON	OUI	NON
Accès qtree dans la copie Snapshot (si SLAG n'est pas présent dans le qtree AFS)	OUI	NON	NON	NON

Afficher des informations sur Storage-Level Access Guard

La protection d'accès au niveau du stockage est une troisième couche de sécurité appliquée à un volume ou à un qtree. Les paramètres de Storage-Level Access Guard ne peuvent pas être affichés à l'aide de la fenêtre Propriétés de Windows. Vous devez

utiliser l'interface de ligne de commande ONTAP pour afficher des informations sur la sécurité de Storage-Level Access Guard, que vous pouvez utiliser pour valider votre configuration ou pour résoudre les problèmes d'accès aux fichiers.

Description de la tâche

Vous devez fournir le nom de la machine virtuelle de stockage (SVM) et le chemin d'accès au volume ou qtree dont vous souhaitez afficher les informations de sécurité Storage-Level Access Guard. Vous pouvez afficher les valeurs de sortie sous forme de récapitulatif ou sous forme de liste détaillée.

Étape

1. Afficher les paramètres de sécurité de Access Guard au niveau du stockage avec le niveau de détail souhaité :

Pour afficher les informations…	Saisissez la commande suivante…
Sous forme récapitulative	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
Avec détails étendus	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

Exemples

L'exemple suivant présente les informations de sécurité Storage-Level Access Guard pour le volume de style de sécurité NTFS avec le chemin d'accès `/datavol1` Au 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
```

L'exemple suivant affiche les informations Storage-Level Access Guard sur le volume de style de sécurité mixte au niveau du chemin `/datavol5` Au SVM vs1. Le niveau supérieur de ce volume dispose d'une sécurité effective UNIX. Le volume est doté de la sécurité Storage-Level Access Guard.

```
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
```

Retirez la protection d’accès au niveau du stockage

Vous pouvez supprimer Storage-Level Access Guard sur un volume ou qtree si vous ne souhaitez plus définir de sécurité d’accès au niveau du stockage. La suppression de Storage-Level Access Guard ne modifie pas ou ne supprime pas la sécurité des fichiers et répertoires NTFS standard.

Étapes

1. Vérifier que la protection d’accès au niveau du stockage est configurée à l’aide du volume ou qtree `vserver security file-directory show` commande.

   ```
   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. Retirez le protecteur d'accès au niveau du stockage à l'aide du `vserver security file-directory remove-slag` commande.

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

3. Vérifiez que Storage-Level Access Guard a été supprimé du volume ou qtree en utilisant le `vserver security file-directory show` commande.

   ```
   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
```