



Affiche des informations sur la sécurité des fichiers et les stratégies d'audit

ONTAP 9

NetApp
April 24, 2024

Sommaire

Affiche des informations sur la sécurité des fichiers et les stratégies d'audit	1
Affiche des informations sur la sécurité des fichiers et l'aperçu des stratégies d'audit	1
Affiche des informations sur la sécurité des fichiers sur les volumes de style de sécurité NTFS	2
Affiche des informations sur la sécurité des fichiers sur des volumes de style de sécurité mixtes	8
Affiche des informations sur la sécurité des fichiers sur des volumes de type sécurité UNIX	11
Affiche des informations sur les règles d'audit NTFS sur les volumes FlexVol à l'aide de l'interface de ligne de commande	14
Affiche des informations sur les règles d'audit NFSv4 sur les volumes FlexVol à l'aide de l'interface de ligne de commandes	17
Moyens d'afficher des informations sur la sécurité des fichiers et les stratégies d'audit	18

Affiche des informations sur la sécurité des fichiers et les stratégies d'audit

Affiche des informations sur la sécurité des fichiers et l'aperçu des stratégies d'audit

Vous pouvez afficher des informations sur la sécurité des fichiers dans les fichiers et les répertoires contenus dans les volumes des SVM (Storage Virtual machine). Vous pouvez afficher des informations sur les règles d'audit sur les volumes FlexVol. Si configuré, vous pouvez afficher des informations sur les paramètres de sécurité Storage-Level Access Guard et Dynamic Access Control sur les volumes FlexVol.

Affichage des informations relatives à la sécurité des fichiers

Vous pouvez afficher les informations relatives à la sécurité des fichiers appliquées aux données contenues dans des volumes et des qtrees (pour les volumes FlexVol) avec les styles de sécurité suivants :

- NTFS
- UNIX
- Mixte

Affichage des informations relatives aux stratégies d'audit

Vous pouvez afficher des informations sur les règles d'audit pour l'audit des événements d'accès sur les volumes FlexVol sur les protocoles NAS suivants :

- SMB (toutes les versions)
- NFSv4.x

Affichage d'informations sur la sécurité de Storage-Level Access Guard (SLAG)

La sécurité de la protection d'accès au niveau du stockage peut être appliquée sur des volumes FlexVol et des objets qtree avec les styles de sécurité suivants :

- NTFS
- Mixte
- UNIX (si un serveur CIFS est configuré sur le SVM qui contient le volume)

Affichage d'informations sur la sécurité du contrôle d'accès dynamique (DAC)

La sécurité du contrôle d'accès dynamique peut être appliquée à un objet au sein d'un volume FlexVol avec les styles de sécurité suivants :

- NTFS
- Mixte (si l'objet dispose d'une sécurité NTFS effective)

Informations associées

Affiche des informations sur la sécurité des fichiers sur les volumes de style de sécurité NTFS

Vous pouvez afficher des informations sur la sécurité des fichiers et des répertoires sur les volumes de style de sécurité NTFS, notamment le style de sécurité et les styles de sécurité efficaces, les autorisations appliquées et les informations sur les attributs DOS. Les résultats vous permettent de valider votre configuration de sécurité ou de 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 aux données dont vous souhaitez afficher les informations de sécurité des fichiers ou des dossiers. Vous pouvez afficher les valeurs de sortie sous forme de récapitulatif ou sous forme de liste détaillée.

- Étant donné que les volumes et les qtrees de style de sécurité NTFS utilisent uniquement les autorisations de fichier NTFS et les utilisateurs et groupes Windows lors de la détermination des droits d'accès aux fichiers, les champs de sortie liés à UNIX contiennent des informations d'autorisation de fichier UNIX en affichage uniquement.
- Les valeurs de sortie ACL sont affichées pour les fichiers et les dossiers avec la sécurité NTFS.
- Étant donné que la sécurité Storage-Level Access Guard peut être configurée sur le volume racine ou qtree, le résultat d'un chemin de volume ou qtree dans lequel Storage-Level Access Guard est configuré peut afficher à la fois les listes de contrôle d'accès standard des fichiers et les listes de contrôle d'accès Storage-Level Access Guard.
- La sortie affiche également des informations sur les ACE de contrôle d'accès dynamique si le contrôle d'accès dynamique est configuré pour le chemin de fichier ou de répertoire donné.

Étape

1. Afficher les paramètres de sécurité des fichiers et des répertoires avec le niveau de détail souhaité :

Pour afficher les informations...	Saisissez la commande suivante...
Sous forme récapitulative	<pre>vserver security file-directory show -vserver vserver_name -path path</pre>
Avec détails étendus	<pre>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</pre>

Exemples

L'exemple suivant affiche les informations de sécurité relatives au chemin d'accès /vol14 Au SVM vs1 :

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

```

        Vserver: vs1
        File Path: /vol4
    File Inode Number: 64
        Security Style: ntfs
        Effective Style: ntfs
        DOS Attributes: 10
    DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
        Unix User Id: 0
        Unix Group Id: 0
        Unix Mode Bits: 777
    Unix Mode Bits in Text: rwxrwxrwx
        ACLs: NTFS Security Descriptor
            Control:0x8004
            Owner:BUILTIN\Administrators
            Group:BUILTIN\Administrators
            DACL - ACEs
            ALLOW-Everyone-0x1f01ff
            ALLOW-Everyone-0x10000000-
```

OI|CI|IO

L'exemple suivant affiche les informations de sécurité avec des masques étendus sur le chemin /data/engineering Au SVM vs1 :

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

```

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

```

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

```

```

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

```

```

Owner:BUILTIN\Administrators
Group:BUILTIN\Administrators
DACL - ACEs

```

```

    ALLOW-Everyone-0x1f01ff

```

	0... .. =
Generic Read	
	.0.. .. =
Generic Write	
	..0. =
Generic Execute	
	...0 =
Generic All	
0 =
System Security	
 1 =
Synchronize	
 1... .. =
Write Owner	
1. =
Write DAC	
1. =
Read Control	
1 =
Delete	

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

Execute0..... =
Write EA0..... =
Read EA0..... =
Append0..... =
Write0..... =
Read0..... =

L'exemple suivant affiche des informations de sécurité, y compris des informations de sécurité Storage-Level Access Guard, pour le volume 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
```

Informations associées

[Affichage d'informations sur la sécurité des fichiers sur des volumes de style de sécurité mixtes](#)

[Affichage d'informations sur la sécurité des fichiers sur des volumes de style de sécurité UNIX](#)

Affiche des informations sur la sécurité des fichiers sur des volumes de style de sécurité mixtes

Vous pouvez afficher des informations sur la sécurité des fichiers et des répertoires sur des volumes de style de sécurité mixtes, y compris le style de sécurité et les styles de sécurité efficaces, les autorisations appliquées et les informations sur les propriétaires et groupes UNIX. Les résultats vous permettent de valider votre configuration de sécurité ou de 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 aux données dont vous souhaitez afficher les informations de sécurité des fichiers ou des dossiers. Vous pouvez afficher les valeurs de sortie sous forme de récapitulatif ou sous forme de liste détaillée.

- Les qtrees et volumes de style de sécurité mixtes peuvent contenir certains fichiers et dossiers qui utilisent des autorisations de fichier UNIX, soit les bits de mode ou les ACL NFSv4, ainsi que certains fichiers et répertoires utilisant les autorisations de fichier NTFS.
- Le niveau supérieur d'un volume de type sécurité mixte peut avoir une sécurité efficace UNIX ou NTFS.
- Les valeurs de sortie ACL s'affichent uniquement pour les fichiers et les dossiers avec sécurité NTFS ou NFSv4.

Ce champ est vide pour les fichiers et les répertoires utilisant la sécurité UNIX qui n'ont que des autorisations de bit de mode appliquées (pas de listes de contrôle d'accès NFSv4).

- Les champs de sortie propriétaire et groupe de la sortie ACL ne s'appliquent que dans le cas des descripteurs de sécurité NTFS.
- Étant donné que la sécurité de Storage-Level Access Guard peut être configurée sur un volume mixte de style de sécurité, même si le style de sécurité efficace de la racine du volume ou de qtree est UNIX, La sortie d'un chemin de volume ou qtree dans lequel Storage-Level Access Guard est configuré peut afficher à la fois les autorisations de fichiers UNIX et les listes de contrôle d'accès Storage-Level Access Guard.
- Si le chemin entré dans la commande est de données avec la sécurité effective NTFS, la sortie affiche également des informations sur les ACE de contrôle d'accès dynamique si le contrôle d'accès dynamique est configuré pour le chemin de fichier ou de répertoire donné.

Étape

1. Afficher les paramètres de sécurité des fichiers et des répertoires avec le niveau de détail souhaité :

Pour afficher les informations...	Saisissez la commande suivante...
Sous forme récapitulative	<code>vserver security file-directory show -vserver vserver_name -path path</code>
Avec détails étendus	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>

Exemples

L'exemple suivant affiche les informations de sécurité relatives au chemin d'accès `/projects` Dans le SVM

vs1 sous forme de masque étendu. Ce chemin de sécurité mixte possède une sécurité efficace UNIX.

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

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

L'exemple suivant affiche les informations de sécurité relatives au chemin d'accès /data Au SVM vs1. Ce chemin de sécurité mixte dispose d'une sécurité NTFS efficace.

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

```

        Vserver: vs1
        File Path: /data
    File Inode Number: 544
        Security Style: mixed
        Effective Style: ntfs
        DOS Attributes: 10
    DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
        Unix User Id: 0
        Unix Group Id: 0
        Unix Mode Bits: 777
    Unix Mode Bits in Text: rwxrwxrwx
        ACLs: NTFS Security Descriptor
            Control:0x8004
            Owner:BUILTIN\Administrators
            Group:BUILTIN\Administrators
            DACL - ACEs
                ALLOW-Everyone-0x1f01ff
                ALLOW-Everyone-0x10000000-
```

OI|CI|IO

L'exemple suivant affiche les informations de sécurité relatives au volume sur le chemin d'accès /datavol5 Au SVM vs1. Le niveau supérieur de ce volume de type sécurité mixte 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
          AUDIT-EXAMPLE\market-0x1f01ff-SA
      DACL (Applies to Directories):
          ALLOW-BUILTIN\Administrators-0x1f01ff
          ALLOW-CREATOR OWNER-0x1f01ff
          ALLOW-EXAMPLE\Domain Users-0x120089
          ALLOW-EXAMPLE\engineering-0x1f01ff
          ALLOW-EXAMPLE\market-0x1f01ff
      SACL (Applies to Files):
          AUDIT-EXAMPLE\Domain Users-0x120089-FA
          AUDIT-EXAMPLE\engineering-0x1f01ff-SA
          AUDIT-EXAMPLE\market-0x1f01ff-SA
      DACL (Applies to Files):
          ALLOW-BUILTIN\Administrators-0x1f01ff
          ALLOW-CREATOR OWNER-0x1f01ff
          ALLOW-EXAMPLE\Domain Users-0x120089
          ALLOW-EXAMPLE\engineering-0x1f01ff
          ALLOW-EXAMPLE\market-0x1f01ff
```

Informations associées

[Affichage d'informations sur la sécurité des fichiers sur les volumes de style de sécurité NTFS](#)

[Affichage d'informations sur la sécurité des fichiers sur des volumes de style de sécurité UNIX](#)

Affiche des informations sur la sécurité des fichiers sur des volumes de type sécurité UNIX

Vous pouvez afficher des informations sur la sécurité des fichiers et des répertoires sur

les volumes de style de sécurité UNIX, notamment les styles de sécurité et les styles de sécurité efficaces, les autorisations appliquées et les informations sur les propriétaires et groupes UNIX. Les résultats vous permettent de valider votre configuration de sécurité ou de 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 aux données dont vous souhaitez afficher les informations de sécurité de fichier ou de répertoire. Vous pouvez afficher les valeurs de sortie sous forme de récapitulatif ou sous forme de liste détaillée.

- Les volumes et les qtrees de style de sécurité UNIX n'utilisent que les autorisations de fichier UNIX, soit les bits de mode, soit les listes de contrôle d'accès NFSv4 lors de la détermination des droits d'accès aux fichiers.
- Les valeurs de sortie ACL s'affichent uniquement pour les fichiers et les dossiers avec la sécurité NFSv4.

Ce champ est vide pour les fichiers et les répertoires utilisant la sécurité UNIX qui n'ont que des autorisations de bit de mode appliquées (pas de listes de contrôle d'accès NFSv4).

- Les champs de sortie propriétaire et groupe de la sortie ACL ne s'appliquent pas dans le cas des descripteurs de sécurité NFSv4.

Ils ne sont utiles que pour les descripteurs de sécurité NTFS.

- Étant donné que la sécurité Storage-Level Access Guard est prise en charge sur un volume UNIX ou qtree si un serveur CIFS est configuré sur le SVM, le résultat peut contenir des informations relatives à la sécurité Storage-Level Access Guard appliquée au volume ou au qtree spécifié dans le `-path` paramètre.

Étape

1. Afficher les paramètres de sécurité des fichiers et des répertoires avec le niveau de détail souhaité :

Pour afficher les informations...	Saisissez la commande suivante...
Sous forme récapitulative	<pre>vserver security file-directory show -vserver vserver_name -path path</pre>
Avec détails étendus	<pre>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</pre>

Exemples

L'exemple suivant affiche les informations de sécurité relatives au chemin d'accès `/home` Au SVM `vs1` :

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

```

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

L'exemple suivant affiche les informations de sécurité relatives au chemin d'accès /home Au SVM vs1 sous forme de masque étendu :

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

```

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

Informations associées

[Affichage d'informations sur la sécurité des fichiers sur les volumes de style de sécurité NTFS](#)

[Affichage d'informations sur la sécurité des fichiers sur des volumes de style de sécurité mixtes](#)

Affiche des informations sur les règles d'audit NTFS sur les volumes FlexVol à l'aide de l'interface de ligne de commande

Vous pouvez afficher des informations sur les stratégies d'audit NTFS sur les volumes FlexVol, notamment les styles de sécurité et les styles de sécurité efficaces, les autorisations appliquées et les informations sur les listes de contrôle d'accès système. Vous pouvez utiliser les résultats pour valider votre configuration de sécurité ou pour résoudre les problèmes d'audit.

Description de la tâche

Vous devez fournir le nom de la machine virtuelle de stockage (SVM) et le chemin d'accès aux fichiers ou dossiers dont vous souhaitez afficher les informations d'audit. Vous pouvez afficher les valeurs de sortie sous forme de récapitulatif ou sous forme de liste détaillée.

- Les volumes et les qtrees de style de sécurité NTFS utilisent uniquement des listes de contrôle d'accès au système NTFS pour les stratégies d'audit.
- Les règles d'audit NTFS peuvent être appliquées aux fichiers et dossiers d'un volume de style de sécurité mixte avec la sécurité efficace NTFS.

Les volumes et qtrees de style de sécurité mixtes peuvent contenir certains fichiers et répertoires qui utilisent des autorisations de fichier UNIX, soit les bits de mode, soit les ACL NFSv4, ainsi que certains fichiers et répertoires utilisant les autorisations de fichier NTFS.

- Le niveau supérieur d'un volume de style de sécurité mixte peut avoir une sécurité efficace sous UNIX ou NTFS et peut-être ne pas contenir des CLS NTFS.
- Étant donné que la sécurité de Storage-Level Access Guard peut être configurée sur un volume mixte de style de sécurité, même si le style de sécurité efficace de la racine du volume ou de qtree est UNIX, La sortie d'un chemin de volume ou qtree dans lequel Storage-Level Access Guard est configuré peut afficher à la fois le fichier régulier et le dossier SACLs NFSv4 et les SACLs NTFS Storage-Level Access Guard.
- Si le chemin entré dans la commande est celui des données avec la sécurité effective NTFS, la sortie affiche également des informations sur les ACE de contrôle d'accès dynamique si le contrôle d'accès dynamique est configuré pour le chemin d'accès au fichier ou au répertoire donné.
- Lorsque vous affichez des informations de sécurité sur les fichiers et les dossiers avec la sécurité efficace NTFS, les champs de sortie liés à UNIX contiennent des informations d'autorisation de fichier UNIX en affichage uniquement.

Les fichiers et dossiers de style de sécurité NTFS utilisent uniquement les autorisations de fichier NTFS et les utilisateurs et groupes Windows lors de la détermination des droits d'accès aux fichiers.

- Les valeurs de sortie ACL s'affichent uniquement pour les fichiers et les dossiers disposant de la sécurité NTFS ou NFSv4.

Ce champ est vide pour les fichiers et les dossiers utilisant la sécurité UNIX qui n'ont que des autorisations de bit de mode appliquées (pas de listes de contrôle d'accès NFSv4).

- Les champs de sortie propriétaire et groupe de la sortie ACL ne s'appliquent que dans le cas des descripteurs de sécurité NTFS.

Étape

1. Afficher les paramètres de stratégie d'audit de fichier et de répertoire avec le niveau de détail souhaité :

Pour afficher les informations...	Saisissez la commande suivante...
Sous forme récapitulative	<code>vserver security file-directory show -vserver vserver_name -path path</code>
En tant que liste détaillée	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>

Exemples

L'exemple suivant affiche les informations de la stratégie d'audit pour le chemin `/corp` Au SVM `vs1`. Le chemin dispose d'une sécurité NTFS efficace. Le descripteur de sécurité NTFS contient à la fois une entrée RACL RÉUSSIE/ÉCHEC.

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

L'exemple suivant affiche les informations de la stratégie d'audit pour le chemin /datavol1 Au SVM vs1. Le chemin contient à la fois des fichiers standard et des SACL de dossier et des SALC de Storage-Level Access Guard.

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

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

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

Affiche des informations sur les règles d'audit NFSv4 sur les volumes FlexVol à l'aide de l'interface de ligne de commandes

Vous pouvez afficher des informations sur les stratégies d'audit NFSv4 sur les volumes FlexVol à l'aide de l'interface de ligne de commande ONTAP, notamment les styles de sécurité et les styles de sécurité efficaces, les autorisations appliquées, ainsi que les informations sur les listes de contrôle d'accès système (SACL). Vous pouvez utiliser les résultats pour valider votre configuration de sécurité ou pour résoudre les problèmes d'audit.

Description de la tâche

Vous devez fournir le nom de la machine virtuelle de stockage (SVM) et le chemin d'accès aux fichiers ou aux répertoires dont vous souhaitez afficher les informations d'audit. Vous pouvez afficher les valeurs de sortie sous forme de récapitulatif ou sous forme de liste détaillée.

- Les volumes et les qtrees de style de sécurité UNIX n'utilisent que les règles d'audit NFSv4.
- Les fichiers et les répertoires d'un volume mixte de style de sécurité UNIX peuvent appliquer des règles d'audit NFSv4.

Les volumes et qtrees de style de sécurité mixtes peuvent contenir certains fichiers et répertoires qui utilisent des autorisations de fichier UNIX, soit les bits de mode, soit les ACL NFSv4, ainsi que certains fichiers et répertoires utilisant les autorisations de fichier NTFS.

- Le niveau supérieur d'un volume de type sécurité mixte peut présenter une sécurité efficace sous UNIX ou NTFS et peut-être ne pas contenir des CLS NFSv4.
- Les valeurs de sortie ACL s'affichent uniquement pour les fichiers et les dossiers avec sécurité NTFS ou NFSv4.

Ce champ est vide pour les fichiers et les dossiers utilisant la sécurité UNIX qui n'ont que des autorisations de bit de mode appliquées (pas de listes de contrôle d'accès NFSv4).

- Les champs de sortie propriétaire et groupe de la sortie ACL ne s'appliquent que dans le cas des descripteurs de sécurité NTFS.
- Étant donné que la sécurité de Storage-Level Access Guard peut être configurée sur un volume mixte de style de sécurité, même si le style de sécurité efficace de la racine du volume ou de qtree est UNIX, La sortie d'un chemin de volume ou qtree dans lequel Storage-Level Access Guard est configuré peut afficher à la fois le fichier NFSv4 régulier et le répertoire SACLs et les SACLs NTFS Storage-Level Access Guard.
- Étant donné que la sécurité Storage-Level Access Guard est prise en charge sur un volume UNIX ou qtree si un serveur CIFS est configuré sur le SVM, le résultat peut contenir des informations relatives à la sécurité Storage-Level Access Guard appliquée au volume ou au qtree spécifié dans le `-path` paramètre.

Étapes

1. Afficher les paramètres de sécurité des fichiers et des répertoires avec le niveau de détail souhaité :

Pour afficher les informations...	Saisissez la commande suivante...
Sous forme récapitulative	<code>vserver security file-directory show -vserver vserver_name -path path</code>
Avec détails étendus	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>

Exemples

L'exemple suivant affiche les informations de sécurité relatives au chemin d'accès /lab Au SVM vs1. Ce chemin de style de sécurité UNIX dispose d'un SACL NFSv4.

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

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

Moyens d'afficher des informations sur la sécurité des fichiers et les stratégies d'audit

Vous pouvez utiliser le caractère générique (*) pour afficher des informations sur la sécurité des fichiers et les stratégies d'audit de tous les fichiers et répertoires sous un chemin donné ou un volume racine.

Le caractère générique () peut être utilisé comme dernier sous-composant d'un chemin d'accès de répertoire donné, sous lequel vous souhaitez afficher les informations de tous les fichiers et répertoires. Si vous souhaitez afficher les informations d'un fichier ou d'un répertoire donné nommé "",

vous devez alors indiquer le chemin complet à l'intérieur de guillemets doubles ("").

Exemple

La commande suivante avec le caractère générique affiche les informations relatives à tous les fichiers et répertoires sous le chemin d'accès /1/ Du SVM vs1 :

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

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

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

La commande suivante affiche les informations d'un fichier nommé "" sous le chemin d'accès /vol1/a Du SVM vs1. Le chemin est entouré de guillemets doubles ("").

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

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

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.