Affiche des informations sur les stratégies d'audit appliquées aux fichiers et aux répertoires

ONTAP 9

NetApp
April 24, 2024

Sommaire

Affiche des informations sur les stratégies d'audit appliquées aux fichiers et aux répertoires

Affiche des informations sur les stratégies d'audit à l'aide de l'onglet sécurité Windows

Vous pouvez afficher des informations sur les stratégies d'audit qui ont été appliquées aux fichiers et aux répertoires à l'aide de l'onglet sécurité de la fenêtre Propriétés de Windows. Cette méthode est identique à celle utilisée pour les données résidant sur un serveur Windows. Elle permet aux clients d'utiliser la même interface graphique qu'ils sont habitués.

Description de la tâche

L'affichage des informations sur les stratégies d'audit appliquées aux fichiers et aux répertoires vous permet de vérifier que les listes de contrôle d'accès système (SACL) appropriées sont définies sur les fichiers et dossiers spécifiés.

Pour afficher des informations sur les listes de contrôle d'application qui ont été appliquées aux fichiers et dossiers NTFS, procédez comme suit sur un hôte Windows.

Étapes

1. Dans le menu **Tools** de l'Explorateur Windows, sélectionnez **Map network drive**.
2. Renseignez la boîte de dialogue **Map Network Drive** :
   a. Sélectionnez une lettre **lecteur**.
   b. Dans la zone **Folder**, saisissez l'adresse IP ou le nom du serveur SMB de la machine virtuelle de stockage (SVM) contenant le partage contenant à la fois les données que vous souhaitez auditer et le nom du partage.

      Si votre nom de serveur SMB est "SMB_SERVER" et que votre partage est nommé "share1", vous devez entrer `\\SMB_SERVER\share1`.

      > Vous pouvez indiquer l'adresse IP de l'interface de données du serveur SMB au lieu du nom du serveur SMB.

   c. Cliquez sur **Terminer**.

   Le lecteur sélectionné est monté et prêt avec la fenêtre de l'Explorateur Windows affichant les fichiers et dossiers contenus dans le partage.
3. Sélectionnez le fichier ou le répertoire pour lequel vous affichez les informations d'audit.
4. Cliquez avec le bouton droit de la souris sur le fichier ou le répertoire et sélectionnez **Propriétés**.
5. Sélectionnez l'onglet **sécurité**.
6. Cliquez sur **Avancé**.
7. Sélectionnez l'onglet **Audit**.
8. Cliquez sur **Continuer**.

La boîte de dialogue Audit s'ouvre. La boîte de dialogue **Auditing Entries** affiche un récapitulatif des utilisateurs et des groupes auxquels des SACL sont appliquées.

9. Dans la zone **Auditing Entries**, sélectionnez l'utilisateur ou le groupe dont vous souhaitez afficher les entrées SACL.
10. Cliquez sur **Modifier**.

    L'entrée Audit pour <Object> s'ouvre.

11. Dans la zone **Access**, affichez les CLS actuelles appliquées à l'objet sélectionné.
12. Cliquez sur **Annuler** pour fermer l'entrée **Audit pour <objet>**.
13. Cliquez sur **Annuler** pour fermer la case **Audit**.

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 ces informations pour valider votre configuration de sécurité ou résoudre les problèmes d'audit.

Description de la tâche

L'affichage des informations sur les stratégies d'audit appliquées aux fichiers et aux répertoires vous permet de vérifier que les listes de contrôle d'accès système (SACL) appropriées sont définies sur les fichiers et dossiers spécifiés.

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	`vserver security file-directory show -vserver vserver_name -path path`
En tant que liste détaillée	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

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
```

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 particulier nommé "*", vous devez fournir le chemin complet à l’intérieur des 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
```