Configurez et appliquez des règles d'audit aux fichiers et dossiers NTFS à l'aide de l'interface de ligne de commande

ONTAP 9

NetApp
September 12, 2024

Sommaire

Configurez et appliquez des règles d'audit aux fichiers et dossiers NTFS à l'aide de la vue d'ensemble de l'interface de ligne de commande

Lorsque vous utilisez l'interface de ligne de commande ONTAP, vous devez effectuer plusieurs étapes pour appliquer des règles d'audit aux fichiers et dossiers NTFS. Tout d'abord, vous créez un descripteur de sécurité NTFS et ajoutez des CLS au descripteur de sécurité. Ensuite, vous créez une stratégie de sécurité et ajoutez des tâches de stratégie. Vous appliquez ensuite la politique de sécurité sur une machine virtuelle de stockage (SVM).

Description de la tâche

Après avoir appliqué la stratégie de sécurité, vous pouvez surveiller la tâche de stratégie de sécurité, puis vérifier les paramètres de la stratégie d'audit appliquée.

> Lorsqu'une stratégie d'audit et des CLS associées sont appliquées, les CLS existantes sont écrasées. Il est recommandé de passer en revue les stratégies de sécurité existantes avant d'en créer et d'en appliquer de nouvelles.

Informations associées

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

Limites lors de l'utilisation de l'interface de ligne de commande pour définir la sécurité des fichiers et des dossiers

Comment les descripteurs de sécurité sont utilisés pour appliquer la sécurité des fichiers et des dossiers

"Audit et suivi de sécurité SMB et NFS"

Configurez et appliquez la sécurité des fichiers sur les fichiers et dossiers NTFS à l'aide de l'interface de ligne de commande

Créez un descripteur de sécurité NTFS

La création d'une règle d'audit NTFS est la première étape de la configuration et de l'application des listes de contrôle d'accès (ACL) NTFS aux fichiers et dossiers qui résident au sein des SVM. Vous associerez le descripteur de sécurité au chemin du fichier ou du dossier dans une tâche de stratégie.

Description de la tâche

Vous pouvez créer des descripteurs de sécurité NTFS pour les fichiers et les dossiers résidant dans des volumes de style de sécurité NTFS ou pour les fichiers et dossiers résidant sur des volumes de type sécurité mixtes.

Par défaut, lorsqu'un descripteur de sécurité est créé, quatre entrées de contrôle d'accès (ACE) de liste de contrôle d'accès discrétionnaire (DACL) sont ajoutées à ce descripteur de sécurité. Les quatre ACE par défaut sont les suivants :

Objet	Type d'accès	Droits d'accès	Où appliquer les autorisations
INTÉGRÉ\administrateurs	Autoriser	Contrôle total	ce dossier, sous-dossiers, fichiers
INTÉGRÉ\utilisateurs	Autoriser	Contrôle total	ce dossier, sous-dossiers, fichiers
PROPRIÉTAIRE DU CRÉATEUR	Autoriser	Contrôle total	ce dossier, sous-dossiers, fichiers
AUTORITÉ NT\SYSTÈME	Autoriser	Contrôle total	ce dossier, sous-dossiers, fichiers

Vous pouvez personnaliser la configuration du descripteur de sécurité à l'aide des paramètres facultatifs suivants :

- Propriétaire du Security Descriptor
- Groupe principal du propriétaire
- Indicateurs de contrôle bruts

La valeur de n'importe quel paramètre facultatif est ignorée pour Storage-Level Access Guard. Consultez les pages de manuels pour plus d'informations.

Étapes

1. Si vous souhaitez utiliser les paramètres avancés, définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Créez un Security Descriptor: `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. Vérifiez que la configuration du descripteur de sécurité est correcte : `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 vous êtes au niveau de privilège avancé, revenez au niveau de privilège admin : `set -privilege admin`

Ajoutez des entrées de contrôle d'accès NTFS SACL au descripteur de sécurité NTFS

L'ajout d'entrées de contrôle d'accès (ACE) SACL (System Access Control list) au descripteur de sécurité NTFS est la deuxième étape de création des politiques d'audit NTFS pour les fichiers ou les dossiers des SVM. Chaque entrée identifie l'utilisateur ou le groupe que vous souhaitez auditer. L'entrée SACL définit si vous souhaitez auditer les tentatives d'accès réussies ou échouées.

Description de la tâche

Vous pouvez ajouter un ou plusieurs ACE au SACL du descripteur de sécurité.

Si le descripteur de sécurité contient une SACL comportant des ACE existants, la commande ajoute la nouvelle ACE à la SACL. Si le descripteur de sécurité ne contient pas de SACL, la commande crée la SACL et y ajoute la nouvelle ACE.

Vous pouvez configurer les entrées SACL en spécifiant les droits que vous souhaitez auditer pour les événements de réussite ou d'échec du compte spécifié dans `-account` paramètre. Il existe trois méthodes mutuellement exclusives de définition des droits :

- Droits
- Droits avancés
- Droits bruts (privilège avancé)

> Si vous ne spécifiez pas de droits pour l'entrée SACL, le paramètre par défaut est `Full Control`.

Vous pouvez personnaliser des entrées SACL en spécifiant la façon d'appliquer l'héritage à l' `apply to` paramètre. Si vous ne spécifiez pas ce paramètre, la valeur par défaut est d'appliquer cette entrée SACL à ce dossier, sous-dossiers et fichiers.

Étapes

1. Ajoutez une entrée SACL à un descripteur de sécurité : `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. Vérifiez que l'entrée SACL est correcte : `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
```

Créer des stratégies de sécurité

La création d'une policy d'audit pour les SVM (Storage Virtual machines) constitue la troisième étape de la configuration et de l'application de ces ACL à un fichier ou à un dossier. Une règle agit comme un conteneur pour différentes tâches, où chaque tâche est une entrée unique qui peut être appliquée à des fichiers ou des dossiers. Vous pouvez ajouter des tâches à la stratégie de sécurité ultérieurement.

Description de la tâche

Les tâches que vous ajoutez à une stratégie de sécurité contiennent des associations entre le descripteur de sécurité NTFS et les chemins de fichier ou de dossier. Par conséquent, vous devez associer la stratégie de sécurité à chaque SVM (Storage Virtual machine) (contenant des volumes de style de sécurité NTFS ou des volumes de type sécurité mixtes).

Étapes

1. Création d'une stratégie de sécurité : `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. Vérifiez la stratégie de sécurité : `vserver security file-directory policy show`

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

Ajoutez une tâche à la stratégie de sécurité

La création et l'ajout d'une tâche policy à une policy de sécurité constitue la quatrième étape de la configuration et de l'application de ACL à des fichiers ou dossiers des SVM. Lorsque vous créez la tâche de stratégie, vous associez la tâche à une stratégie de sécurité. Vous pouvez ajouter une ou plusieurs entrées de tâche à une stratégie de

sécurité.

Description de la tâche

La stratégie de sécurité est un conteneur pour une tâche. Une tâche fait référence à une opération unique qui peut être effectuée par une stratégie de sécurité pour les fichiers ou dossiers avec NTFS ou la sécurité mixte (ou à un objet de volume si vous configurez Storage-Level Access Guard).

Il existe deux types de tâches :

- Tâches de fichier et de répertoire

  Permet de spécifier les tâches qui appliquent des descripteurs de sécurité aux fichiers et dossiers spécifiés. Les ACL appliquées via les tâches de fichier et de répertoire peuvent être gérées avec les clients SMB ou l'interface de ligne de commande ONTAP.

- Tâches de Storage-Level Access Guard

  Permet de spécifier les tâches qui appliquent des descripteurs de sécurité Storage-Level Access Guard à un volume spécifié. Les listes de contrôle d'accès appliquées via les tâches Storage-Level Access Guard peuvent être gérées uniquement via l'interface de ligne de commande ONTAP.

Une tâche contient des définitions pour la configuration de sécurité d'un fichier (ou d'un dossier) ou d'un ensemble de fichiers (ou de dossiers). Chaque tâche d'une stratégie est identifiée de manière unique par le chemin. Il ne peut y avoir qu'une seule tâche par chemin au sein d'une même stratégie. Une stratégie ne peut pas avoir d'entrées de tâche en double.

Instructions pour l'ajout d'une tâche à une stratégie :

- Il peut y avoir un maximum de 10,000 entrées de tâches par stratégie.
- Une stratégie peut contenir une ou plusieurs tâches.

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

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

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

Vous pouvez personnaliser la configuration du descripteur de sécurité à l'aide des paramètres facultatifs suivants :

- Type de sécurité
- Mode de propagation
- Position de l'index
- Type de contrôle d'accès

La valeur de n'importe quel paramètre facultatif est ignorée pour Storage-Level Access Guard. Consultez les pages de manuels pour plus d'informations.

Étapes

1. Ajoutez une tâche avec un descripteur de sécurité associé à la stratégie de sécurité : `vserver`

```
security file-directory policy task add -vserver vserver_name -policy-name
policy_name -path path -ntfs-sd SD_nameoptional_parameters
```

`file-directory` est la valeur par défaut de l' `-access-control` paramètre. La définition du type de contrôle d'accès lors de la configuration des tâches d'accès aux fichiers et aux répertoires est facultative.

```
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. Vérifiez la configuration de la tâche de stratégie : `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
```

Appliquez des règles de sécurité

L'application d'une règle d'audit aux SVM constitue la dernière étape de création et d'application des listes de contrôle d'accès NTFS aux fichiers ou dossiers.

Description de la tâche

Vous pouvez appliquer les paramètres de sécurité définis dans la stratégie de sécurité aux fichiers et dossiers NTFS résidant au sein de volumes FlexVol (NTFS ou style de sécurité mixte).

> Lorsqu'une stratégie d'audit et des CLS associées sont appliquées, les CLS existantes sont écrasées. Lorsqu'une stratégie de sécurité et les listes de contrôle d'accès discrétionnaire associées sont appliquées, toutes les listes de contrôle d'accès discrétionnaire existantes sont écrasées. Il est recommandé de passer en revue les stratégies de sécurité existantes avant d'en créer et d'en appliquer de nouvelles.

Étape

1. Appliquer une politique de sécurité : `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

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

La tâche d'application de la politique est planifiée et l'ID de la tâche est renvoyé.

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

Surveillez la tâche de stratégie de sécurité

Lorsque vous appliquez la stratégie de sécurité aux serveurs virtuels de stockage (SVM), vous pouvez surveiller la progression de la tâche en surveillant la tâche de stratégie de sécurité. Ceci est utile si vous voulez vérifier que l'application de la politique de sécurité a réussi. Ceci est également utile si vous avez un travail de longue durée où vous appliquez la sécurité en bloc à un grand nombre de fichiers et de dossiers.

Description de la tâche

Pour afficher des informations détaillées sur une tâche de stratégie de sécurité, vous devez utiliser le `-instance` paramètre.

Étape

1. Surveillez la tâche de stratégie de sécurité : `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
   ```

Vérifiez la règle d'audit appliquée

Vous pouvez vérifier la stratégie d'audit pour confirmer que les fichiers ou les dossiers de la machine virtuelle de stockage (SVM) à laquelle vous avez appliqué la stratégie de sécurité disposent des paramètres de sécurité d'audit souhaités.

Description de la tâche

Vous utilisez le `vserver security file-directory show` commande permettant d'afficher les informations relatives aux règles d'audit. Vous devez fournir le nom de la SVM qui contient les données et le chemin d'accès aux données dont vous souhaitez afficher les informations de la politique d'audit de fichier ou de dossier.

Étape

1. Afficher les paramètres de stratégie d'audit : `vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*

Exemple

La commande suivante affiche les informations de la politique d'audit appliquées au chemin "/corp" du SVM

vs1. Le chemin a à la fois UN SUCCÈS et une entrée SACL SUCCÈS/ÉCHEC qui lui est appliquée :

```
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
```