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

ONTAP 9

NetApp
September 12, 2024

Sommaire

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

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

Vous pouvez gérer la sécurité des fichiers NTFS, les règles d'audit NTFS et Storage-Level Access Guard sur les SVM de stockage virtuels à l'aide de l'interface de ligne de commande.

Vous pouvez gérer les règles de sécurité et d'audit des fichiers NTFS des clients SMB ou à l'aide de l'interface de ligne de commande. Toutefois, l'utilisation de la CLI pour configurer les stratégies de sécurité des fichiers et d'audit supprime la nécessité d'utiliser un client distant pour gérer la sécurité des fichiers. L'utilisation de l'interface de ligne de commande permet de réduire considérablement le temps nécessaire à l'application de la sécurité sur de nombreux fichiers et dossiers à l'aide d'une seule commande.

Vous pouvez configurer Storage-Level Access Guard, qui est une autre couche de sécurité appliquée par ONTAP aux volumes de SVM. Storage-Level Access Guard s'applique aux accès de tous les protocoles NAS à l'objet de stockage auquel Storage-Level Access Guard est appliqué.

Storage-Level Access Guard peut être configuré et géré uniquement à partir de l'interface de ligne de commande ONTAP. Vous ne pouvez pas gérer les paramètres Storage-Level Access Guard à partir des clients SMB. De plus, si vous affichez les paramètres de sécurité d'un fichier ou d'un répertoire à partir d'un client NFS ou SMB, vous ne verrez pas la sécurité Storage-Level Access Guard. La sécurité Access Guard au niveau du stockage ne peut pas être révoquée d'un client, même par un administrateur système (Windows ou UNIX). Par conséquent, Storage-Level Access Guard offre une couche supplémentaire de sécurité pour l'accès aux données, qui est défini et géré de façon indépendante par l'administrateur du stockage.

> Bien que seules les autorisations d'accès NTFS soient prises en charge pour Storage-Level Access Guard, ONTAP peut effectuer des vérifications de sécurité pour l'accès via NFS aux données sur les volumes où Storage-Level Access Guard est appliqué si l'utilisateur UNIX mappe avec un utilisateur Windows sur le SVM propriétaire du volume.

Volumes de sécurité NTFS

Tous les fichiers et dossiers contenus dans des volumes et qtrees de style de sécurité NTFS bénéficient d'une sécurité efficace. Vous pouvez utiliser le `vserver security file-directory` Famille de commandes permettant d'implémenter les types de sécurité suivants sur les volumes de style de sécurité NTFS :

- Autorisations liées aux fichiers et stratégies d'audit pour les fichiers et les dossiers contenus dans le volume
- Sécurité Access Guard du niveau de stockage sur les volumes

Volumes de sécurité mixtes

Les qtrees et volumes de style de sécurité mixtes peuvent contenir certains fichiers et dossiers disposant d'une sécurité effective UNIX et utiliser des autorisations de fichiers UNIX, soit les bits de mode, soit les listes de contrôle d'accès NFSv4.x et les règles d'audit NFSv4.x, ainsi que certains fichiers et dossiers disposant d'une sécurité efficace NTFS, et utilisant les autorisations d'accès aux fichiers NTFS et les règles d'audit. Vous pouvez utiliser le `vserver security file-directory` famille de commandes pour appliquer les types de sécurité suivants aux données de style de sécurité mixte :

- Autorisations liées aux fichiers et règles d'audit sur les fichiers et les dossiers avec le style de sécurité effectif NTFS dans le volume mixte ou le qtree
- Access Guard au niveau du stockage pour les volumes NTFS et UNIX

Volumes de style de sécurité UNIX

Les volumes et les qtrees de style de sécurité UNIX contiennent des fichiers et des dossiers qui disposent d'une sécurité effective UNIX (soit les bits de mode, soit les ACL NFSv4.x). Si vous souhaitez utiliser le, vous devez garder à l'esprit les éléments suivants `vserver security file-directory` Famille de commandes pour implémenter la sécurité sur des volumes de type sécurité UNIX :

- Le `vserver security file-directory` Les familles de commandes ne peuvent pas être utilisées pour gérer la sécurité des fichiers UNIX et les règles d'audit sur les volumes et les qtrees de style de sécurité UNIX.
- Vous pouvez utiliser le `vserver security file-directory` Gamme de commandes permettant de configurer Storage-Level Access Guard sur des volumes de style de sécurité UNIX, à condition que le SVM avec le volume cible contienne un serveur CIFS.

Informations associées

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

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

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

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

Utilisez les cas d'utilisation de l'interface de ligne de commande pour définir la sécurité des fichiers et des dossiers

Puisque vous pouvez appliquer et gérer la sécurité des fichiers et des dossiers localement sans l'intervention d'un client distant, vous pouvez réduire considérablement le temps nécessaire pour définir la sécurité en bloc sur un grand nombre de fichiers ou de dossiers.

Vous pouvez utiliser l'interface de ligne de commande pour définir la sécurité des fichiers et des dossiers dans les cas d'utilisation suivants :

- Stockage de fichiers dans les grands environnements d'entreprise, tels que le stockage de fichiers dans les répertoires locaux
- Migration des données
- Changement de domaine Windows
- Standardisation des règles de sécurité des fichiers et d'audit sur l'ensemble des systèmes de fichiers NTFS

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

Vous devez connaître certaines limites lorsque vous utilisez l'interface de ligne de commande pour définir la sécurité des fichiers et des dossiers.

- Le `vserver security file-directory` La famille de commandes ne prend pas en charge la configuration des listes de contrôle d'accès NFSv4.

  Vous pouvez uniquement appliquer des descripteurs de sécurité NTFS aux fichiers et dossiers NTFS.

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

Les descripteurs de sécurité contiennent les listes de contrôle d'accès qui déterminent les actions qu'un utilisateur peut effectuer sur les fichiers et les dossiers, et ce qui est vérifié lorsqu'un utilisateur accède à des fichiers et à des dossiers.

- **Autorisations**

  Les autorisations sont autorisées ou refusées par le propriétaire d'un objet et déterminent les actions qu'un objet (utilisateurs, groupes ou objets informatiques) peut exécuter sur des fichiers ou dossiers spécifiés.

- **Descripteurs de sécurité**

  Les descripteurs de sécurité sont des structures de données contenant des informations de sécurité qui définissent les autorisations associées à un fichier ou à un dossier.

- **Listes de contrôle d'accès (ACL)**

  Les listes de contrôle d'accès sont les listes contenues dans un descripteur de sécurité qui contiennent des informations sur les actions que les utilisateurs, les groupes ou les objets informatiques peuvent exécuter sur le fichier ou le dossier auquel le descripteur de sécurité est appliqué. Le Security Descriptor peut contenir les deux types de listes de contrôle d'accès suivants :

  - Listes de contrôle d'accès discrétionnaire (DACL)
  - Listes de contrôle d'accès au système (SACL)
- * Listes de contrôle d'accès discrétionnaire (listes DACL)*

  Les DACL contiennent la liste des SID pour les utilisateurs, les groupes et les objets d'ordinateur qui sont

autorisés ou refusés à effectuer des actions sur des fichiers ou des dossiers. Les listes DALC contiennent au moins zéro entrée de contrôle d'accès (ACE).

- **Listes de contrôle d'accès au système (SACL)**

  Les SACL contiennent la liste des PEID pour les utilisateurs, les groupes et les objets d'ordinateur pour lesquels des événements d'audit réussis ou échoués sont consignés. Les SACL contiennent au moins zéro entrée de contrôle d'accès (ACE).

- **Entrées de contrôle d'accès (ACE)**

  Ces sont des entrées individuelles dans DACL ou SACL :

  - Une entrée de contrôle d'accès DACL spécifie les droits d'accès autorisés ou refusés pour certains utilisateurs, groupes ou objets d'ordinateur.
  - Une entrée de contrôle d'accès SACL spécifie les événements succès ou échec à consigner lors de l'audit des actions spécifiées effectuées par des utilisateurs, des groupes ou des objets d'ordinateur particuliers.

- **Héritage des autorisations**

  L'héritage des autorisations décrit comment les autorisations définies dans les descripteurs de sécurité sont propagées à un objet à partir d'un objet parent. Seules les autorisations héritables sont héritées par des objets enfants. Lorsque vous définissez des autorisations sur l'objet parent, vous pouvez décider si les dossiers, sous-dossiers et fichiers peuvent les hériter avec "'appliquer à `this-folder`, `sub-folders`, et `fichierss".

Informations associées

"Audit et suivi de sécurité SMB et NFS"

Configuration et application de règles d'audit aux fichiers et dossiers NTFS à l'aide de l'interface de ligne de commande

Consignes d'application des stratégies de répertoires de fichiers utilisant des utilisateurs ou des groupes locaux sur la destination de reprise après incident du SVM

Si la configuration de votre politique de répertoire de fichiers utilise des utilisateurs ou des groupes locaux dans le Security Descriptor ou les entrées DACL ou SACL, vous devez garder à l'esprit avant d'appliquer les stratégies de répertoires de fichiers sur la destination de reprise après incident SVM (Storage Virtual machine) en configuration de suppression d'ID.

Il est possible de configurer une configuration de reprise sur incident pour un SVM où le SVM source sur le cluster source réplique les données et la configuration depuis le SVM source vers un SVM destination sur un cluster de destination.

Vous pouvez configurer l'un des deux types de reprise après incident des SVM :

- Identité préservée

  Avec cette configuration, l'identité du SVM et du serveur CIFS est préservée.

- Identité rejetée

  Avec cette configuration, l'identité du SVM et du serveur CIFS n'est pas conservée Dans ce scénario, le nom du SVM et du serveur CIFS sur le SVM de destination est différent de celui du SVM et du nom du serveur CIFS sur le SVM source.

Instructions pour les configurations éliminées par identité

Dans une configuration définie par l'identité, pour une source SVM qui contient des configurations utilisateur, groupe et privilège local, le nom du domaine local (nom du serveur CIFS local) doit être modifié afin de correspondre au nom du serveur CIFS sur la destination du SVM. Par exemple, si le nom du SVM source est « vs1 » et que le nom du serveur CIFS est « CIFS1 », et que le nom du SVM de destination est « vs1_dst » et que le nom du serveur CIFS est « CIFS1_DST », le nom de domaine local d'un utilisateur local nommé « DST CI1\user1 » est automatiquement modifié sur la SVM « destination » :

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

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

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

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

Même si les noms d'utilisateur et de groupe locaux sont automatiquement modifiés dans les bases de données des utilisateurs et des groupes locaux, les noms d'utilisateurs ou de groupes locaux ne sont pas automatiquement modifiés dans les configurations des stratégies de répertoires de fichiers (règles configurées sur la CLI à l'aide de l' `vserver security file-directory` famille de commande).

Par exemple, pour « vs1 », si vous avez configuré une entrée DACL où le `-account` Le paramètre est défini sur « CIFS1\user1 », le paramètre n'est pas automatiquement modifié sur le SVM de destination pour refléter le nom du serveur CIFS de destination.

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

Vserver: vs1
  NTFS Security Descriptor Name: sd1

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

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

Vserver: vs1_dst
  NTFS Security Descriptor Name: sd1

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

Vous devez utiliser le `vserver security file-directory modify` Commandes permettant de modifier manuellement le nom du serveur CIFS sur le nom du serveur CIFS de destination.

Composants de configuration de la stratégie de répertoire de fichiers contenant des paramètres de compte

Il existe trois composants de configuration de stratégie de répertoire de fichiers qui peuvent utiliser des paramètres pouvant contenir des utilisateurs ou des groupes locaux :

- Descripteur de sécurité

  Vous pouvez éventuellement spécifier le propriétaire du descripteur de sécurité et le groupe principal du propriétaire du descripteur de sécurité. Si le Security Descriptor utilise un utilisateur ou groupe local pour les entrées propriétaire et groupe principal, vous devez modifier le Security Descriptor afin d'utiliser le SVM destination dans le nom du compte. Vous pouvez utiliser le `vserver security file-directory ntfs modify` commande permettant de modifier les noms de compte si nécessaire.

- Entrées DACL

  Chaque entrée DACL doit être associée à un compte. Vous devez modifier tout DACL qui utilisent des comptes utilisateur ou groupe locaux pour utiliser le nom de SVM de destination. Étant donné que vous ne pouvez pas modifier le nom du compte pour les entrées DACL existantes, vous devez supprimer toutes les entrées DACL avec des utilisateurs ou des groupes locaux des descripteurs de sécurité, créer de nouvelles entrées DACL avec les noms de compte de destination corrigés et associer ces nouvelles entrées DACL aux descripteurs de sécurité appropriés.

- Entrées SACL

Chaque entrée SACL doit être associée à un compte. Vous devez modifier les CLS qui utilisent des comptes utilisateur ou groupe locaux pour utiliser le nom de SVM de destination. Comme vous ne pouvez pas modifier le nom du compte pour les entrées SACL existantes, vous devez supprimer les entrées SACL avec des utilisateurs ou des groupes locaux des descripteurs de sécurité, créer de nouvelles entrées SACL avec les noms de compte de destination corrigés et associer ces nouvelles entrées SACL aux descripteurs de sécurité appropriés.

Vous devez apporter les modifications nécessaires aux utilisateurs ou groupes locaux utilisés dans la configuration de la stratégie de répertoire de fichiers avant d'appliquer la stratégie. Sinon, la tâche d'application échoue.

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'un Security Descriptor (politique de sécurité des fichiers) NTFS constitue la première étape de configuration et d'application des listes de contrôle d'accès (ACL) NTFS aux fichiers et dossiers résidant sur les SVM (Storage Virtual machines). Vous pouvez associer 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.

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

L'ajout d'entrées de contrôle d'accès (ACE) DACL (liste de contrôle d'accès discrétionnaire) au descripteur de sécurité NTFS est la deuxième étape de la configuration et de l'application des listes de contrôle d'accès NTFS à un fichier ou à un dossier. Chaque entrée identifie quel objet est autorisé ou refusé à accéder et définit ce que l'objet peut ou ne peut pas faire pour les fichiers ou dossiers définis dans ACE.

Description de la tâche

Vous pouvez ajouter un ou plusieurs ACE au DACL du Security Descriptor.

Si le descripteur de sécurité contient un DACL contenant des ACE existants, la commande ajoute le nouveau ACE au DACL. Si le descripteur de sécurité ne contient pas de DACL, la commande crée le DACL et y ajoute le nouveau ACE.

Vous pouvez éventuellement personnaliser les entrées DACL en spécifiant les droits que vous souhaitez autoriser ou refuser pour le 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 DACL, la valeur par défaut est de définir les droits sur `Full Control`.

Vous pouvez personnaliser les entrées DACL en spécifiant la manière d'appliquer l'héritage.

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. Ajouter une entrée DACL à un descripteur de sécurité : `vserver security file-directory ntfs dacl add -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SIDoptional_parameters`

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

2. Vérifier que l'entrée DACL est correcte : `vserver security file-directory ntfs dacl show -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SID`

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

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

Créer des stratégies de sécurité

La création d'une politique de sécurité des fichiers pour les SVM représente la troisième étape de la configuration et de l'application de ces ACL à un fichier ou 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. Vous devez donc associer la politique de sécurité à chaque SVM (qui contient 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.

Lorsque vous ajoutez des tâches aux stratégies de sécurité, vous devez spécifier les quatre paramètres requis suivants :

- Nom du SVM
- Nom de la règle
- Chemin
- Descripteur de sécurité à associer au chemin d'accès

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 politique de sécurité des fichiers aux SVM est la dernière étape de la création et de l'application de ces ACL NTFS aux fichiers ou aux 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 sécurité appliquée des fichiers

Vous pouvez vérifier les paramètres de sécurité des fichiers 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 souhaités.

Description de la tâche

Vous devez fournir le nom de la SVM qui contient les données et le chemin d'accès au fichier et aux dossiers sur lesquels vous souhaitez vérifier les paramètres de sécurité. Vous pouvez utiliser l'option `-expand-mask` paramètre pour afficher des informations détaillées sur les paramètres de sécurité.

Étape

1. Afficher les paramètres de sécurité des fichiers et dossiers : `vserver security file-directory show -vserver vserver_name -path path [-expand-mask true]`

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

```
         Vserver: vs1
              File Path: /data/engineering
      File Inode Number: 5544
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

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

```
                            .... .... .... ..0. = Group Defaulted
                            .... .... .... ...0 = Owner Defaulted

                          Owner:BUILTIN\Administrators
                          Group:BUILTIN\Administrators
                          DACL - ACEs
                            ALLOW-Everyone-0x1f01ff
                            0... .... .... .... .... .... .... .... =
Generic Read
                            .0.. .... .... .... .... .... .... .... =
Generic Write
                            ..0. .... .... .... .... .... .... .... =
Generic Execute
                            ...0 .... .... .... .... .... .... .... =
Generic All
                            .... ...0 .... .... .... .... .... .... =
System Security
                            .... .... ...1 .... .... .... .... .... =
Synchronize
                            .... .... .... 1... .... .... .... .... =
Write Owner
                            .... .... .... .1.. .... .... .... .... =
Write DAC
                            .... .... .... ..1. .... .... .... .... =
Read Control
                            .... .... .... ...1 .... .... .... .... =
Delete
                            .... .... .... .... .... ...1 .... .... =
Write Attributes
                            .... .... .... .... .... .... 1... .... =
Read Attributes
                            .... .... .... .... .... .... .1.. .... =
Delete Child
                            .... .... .... .... .... .... ..1. .... =
Execute
                            .... .... .... .... .... .... ...1 .... =
Write EA
                            .... .... .... .... .... .... .... 1... =
Read EA
                            .... .... .... .... .... .... .... .1.. =
Append
                            .... .... .... .... .... .... .... ..1. =
Write
                            .... .... .... .... .... .... .... ...1 =
Read
```

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

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
```

Considérations relatives à la gestion des tâches de stratégie de sécurité

Si une tâche de stratégie de sécurité existe, dans certaines circonstances, vous ne pouvez pas modifier cette stratégie de sécurité ou les tâches affectées à cette stratégie. Vous devez comprendre dans quelles conditions vous pouvez ou ne pouvez pas modifier les stratégies de sécurité pour que toute tentative de modification de la stratégie soit réussie. Les modifications apportées à la stratégie comprennent l'ajout, la suppression ou la modification de tâches affectées à la stratégie et la suppression ou la modification de celle-ci.

Vous ne pouvez pas modifier une stratégie de sécurité ou une tâche affectée à cette stratégie si un travail existe pour cette stratégie et que ce travail se trouve dans les États suivants :

- Le travail est en cours d'exécution ou en cours d'exécution.
- Le travail est suspendu.
- Le travail reprend et est en cours d'exécution.
- Si le travail attend le basculement vers un autre nœud.

Dans les circonstances suivantes, si une tâche existe pour une stratégie de sécurité, vous pouvez modifier avec succès cette stratégie de sécurité ou une tâche affectée à cette stratégie :

- La tâche de stratégie est arrêtée.
- La tâche de stratégie s'est terminée avec succès.

Commandes de gestion des descripteurs de sécurité NTFS

Il existe des commandes ONTAP spécifiques pour gérer les descripteurs de sécurité. Vous pouvez créer, modifier, supprimer et afficher des informations sur les descripteurs de sécurité.

Les fonctions que vous recherchez…	Utilisez cette commande…
Créer des descripteurs de sécurité NTFS	`vserver security file-directory ntfs create`
Modifiez les descripteurs de sécurité NTFS existants	`vserver security file-directory ntfs modify`
Affiche des informations sur les descripteurs de sécurité NTFS existants	`vserver security file-directory ntfs show`
Supprimez les descripteurs de sécurité NTFS	`vserver security file-directory ntfs delete`

Consultez les pages de manuel pour le `vserver security file-directory ntfs` commandes pour plus d'informations.

Commandes de gestion des entrées de contrôle d'accès NTFS DACL

Il existe des commandes ONTAP spécifiques pour la gestion des entrées de contrôle d'accès DACL (ACE). Vous pouvez ajouter des ACE aux listes de contrôle d'accès NTFS à tout moment. Vous pouvez également gérer les listes de contrôle d'accès NTFS existantes en modifiant, supprimant et affichant des informations sur les ACE dans les listes de contrôle d'accès.

Les fonctions que vous recherchez…	Utilisez cette commande…
Créez des ACE et ajoutez-les dans les listes de contrôle d'accès NTFS	`vserver security file-directory ntfs dacl add`
Modifier les ACE existants dans les listes de contrôle d'accès NTFS	`vserver security file-directory ntfs dacl modify`

Les fonctions que vous recherchez…	Utilisez cette commande…
Affiche des informations sur les ACE existants dans les DACL NTFS	`vserver security file-directory ntfs dacl show`
Supprimez les ACE existants des listes de contrôle d'accès NTFS	`vserver security file-directory ntfs dacl remove`

Consultez les pages de manuel pour le `vserver security file-directory ntfs dacl` commandes pour plus d'informations.

Commandes de gestion des entrées de contrôle d'accès NTFS SACL

Il existe des commandes ONTAP spécifiques pour gérer les entrées de contrôle d'accès SACL (ACE). Vous pouvez ajouter des ACE aux CLS NTFS à tout moment. Vous pouvez également gérer les SALC NTFS existants en modifiant, supprimant et affichant des informations sur les ACE dans les SACL.

Les fonctions que vous recherchez…	Utilisez cette commande…
Créez des ACE et ajoutez-les aux CLS NTFS	`vserver security file-directory ntfs sacl add`
Modifier les ACE existants dans les SACL NTFS	`vserver security file-directory ntfs sacl modify`
Affiche des informations sur les ACE existants dans les CLS NTFS	`vserver security file-directory ntfs sacl show`
Supprimez les ACE existants des SACL NTFS	`vserver security file-directory ntfs sacl remove`

Consultez les pages de manuel pour le `vserver security file-directory ntfs sacl` commandes pour plus d'informations.

Commandes permettant de gérer les stratégies de sécurité

Il existe des commandes ONTAP spécifiques pour gérer les stratégies de sécurité. Vous pouvez afficher des informations sur les règles et supprimer les règles. Vous ne pouvez pas modifier une stratégie de sécurité.

Les fonctions que vous recherchez…	Utilisez cette commande…
Créer des stratégies de sécurité	`vserver security file-directory policy create`
Affiche des informations sur les stratégies de sécurité	`vserver security file-directory policy show`
Supprimer des stratégies de sécurité	`vserver security file-directory policy delete`

Consultez les pages de manuel pour le `vserver security file-directory policy` commandes pour plus d'informations.

Commandes permettant de gérer les tâches de stratégie de sécurité

Il existe des commandes ONTAP permettant d'ajouter, de modifier, de supprimer et d'afficher des informations relatives aux tâches de la stratégie de sécurité.

Les fonctions que vous recherchez…	Utilisez cette commande…
Ajouter des tâches de stratégie de sécurité	`vserver security file-directory policy task add`
Modifier les tâches de stratégie de sécurité	`vserver security file-directory policy task modify`
Afficher des informations sur les tâches de stratégie de sécurité	`vserver security file-directory policy task show`
Supprimer les tâches de stratégie de sécurité	`vserver security file-directory policy task remove`

Consultez les pages de manuel pour le `vserver security file-directory policy task` commandes pour plus d'informations.

Commandes permettant de gérer les tâches de stratégie de sécurité

Des commandes ONTAP permettent d'interrompre, de reprendre, d'arrêter et d'afficher des informations sur les tâches de stratégie de sécurité.

Les fonctions que vous recherchez…	Utilisez cette commande…
Interrompre les tâches de stratégie de sécurité	`vserver security file-directory job pause -vserver vserver_name -id integer`
Reprendre les tâches de stratégie de sécurité	`vserver security file-directory job resume -vserver vserver_name -id integer`
Affiche des informations sur les tâches de stratégie de sécurité	`vserver security file-directory job show -vserver vserver_name` Vous pouvez déterminer l'ID d'un travail à l'aide de cette commande.
Arrêtez les tâches de stratégie de sécurité	`vserver security file-directory job stop -vserver vserver_name -id integer`

Consultez les pages de manuel pour le `vserver security file-directory job` commandes pour plus d'informations.