Configurez l'accès aux fichiers à l'aide de SMB

ONTAP 9

NetApp
April 24, 2024

Sommaire

Configurez l’accès aux fichiers à l’aide de SMB

Configurer les styles de sécurité

Comment les styles de sécurité affectent l’accès aux données

Quels sont les styles de sécurité et leurs effets

Il existe quatre styles de sécurité différents : UNIX, NTFS, mixte et unifié. Chaque style de sécurité a un effet différent sur la façon dont les autorisations sont traitées pour les données. Vous devez comprendre les différents effets pour vous assurer que vous sélectionnez le style de sécurité approprié à vos fins.

Il est important de comprendre que les styles de sécurité ne déterminent pas quels types de clients peuvent ou ne peuvent pas accéder aux données. Les styles de sécurité déterminent uniquement le type d’autorisations que ONTAP utilise pour contrôler l’accès aux données et le type de client pouvant modifier ces autorisations.

Par exemple, si un volume utilise le style de sécurité UNIX, les clients SMB peuvent toujours accéder aux données (à condition qu’ils s’authentifient et autorisent correctement) en raison de la nature multiprotocole de ONTAP. Toutefois, ONTAP utilise des autorisations UNIX que seuls les clients UNIX peuvent modifier à l’aide d’outils natifs.

Style de sécurité	Clients pouvant modifier des autorisations	Autorisations que les clients peuvent utiliser	Un style de sécurité efficace	Clients pouvant accéder aux fichiers
UNIX	NFS	Bits de mode NFSv3	UNIX	NFS et SMB
Listes de contrôle d’accès NFSv4.x	UNIX	NTFS	PME	ALC NTFS
NTFS	Mixte	NFS ou SMB	Bits de mode NFSv3	UNIX
Listes de contrôle d’accès NFSv4.x	UNIX	ALC NTFS	NTFS	Unifiée
NFS ou SMB	Bits de mode NFSv3	UNIX	ACL NFSv4.1	UNIX
ALC NTFS	NTFS	Unifiée (Pour Infinite volumes uniquement, dans ONTAP 9.4 et les versions antérieures.)	NFS ou SMB	Bits de mode NFSv3
UNIX	ACL NFSv4.1			ALC NTFS

Les volumes FlexVol prennent en charge les styles de sécurité UNIX, NTFS et mixte. Lorsque le style de sécurité est mixte ou unifié, les autorisations effectives dépendent du type de client qui a modifié les autorisations pour la dernière fois, car les utilisateurs définissent le style de sécurité sur une base individuelle. Si le dernier client ayant modifié des autorisations était un client NFSv3, les autorisations sont des bits en mode UNIX NFSv3. Si le dernier client était un client NFSv4, les autorisations sont définies comme listes de contrôle d’accès NFSv4. Si le dernier client était un client SMB, les autorisations sont des listes de contrôle d’accès Windows NTFS.

La méthode de sécurité unifiée est uniquement disponible avec des volumes infinis, qui ne sont plus pris en charge dans ONTAP 9.5 et versions ultérieures. Pour plus d'informations, voir "Présentation de la gestion des volumes FlexGroup".

À partir de ONTAP 9.2, le `show-effective-permissions` paramètre au `vserver security file-directory` La commande vous permet d'afficher les autorisations effectives accordées à un utilisateur Windows ou UNIX sur le chemin d'accès au fichier ou au dossier spécifié. De plus, le paramètre facultatif `-share-name` vous permet d'afficher l'autorisation de partage effective.

> ONTAP définit au départ certaines autorisations de fichier par défaut. Par défaut, le style de sécurité effectif sur toutes les données des volumes de style de sécurité UNIX, mixte et unifié est UNIX et le type d'autorisation effectif est bits de mode UNIX (0755 sauf indication contraire) jusqu'à ce qu'un client soit configuré comme autorisé par le style de sécurité par défaut. Par défaut, le style de sécurité effectif sur toutes les données des volumes de style de sécurité NTFS est NTFS et dispose d'une liste de contrôle d'accès permettant un contrôle total à tous.

Où et quand définir les styles de sécurité

Les styles de sécurité peuvent être définis sur les volumes FlexVol (volumes root ou de données) et les qtrees. Les styles de sécurité peuvent être définis manuellement au moment de la création, hérités automatiquement ou modifiés ultérieurement.

Choisissez le style de sécurité à utiliser sur les SVM

Pour vous aider à choisir le style de sécurité à utiliser sur un volume, vous devez tenir compte de deux facteurs. Le facteur principal est le type d'administrateur qui gère le système de fichiers. Le facteur secondaire désigne le type d'utilisateur ou de service qui accède aux données du volume.

Lorsque vous configurez le style de sécurité sur un volume, vous devez tenir compte des besoins de votre environnement pour vous assurer que vous sélectionnez le meilleur style de sécurité et éviter les problèmes liés à la gestion des autorisations. Vous pouvez décider des considérations suivantes :

Style de sécurité	Choisissez si…
UNIX	• Le système de fichiers est géré par un administrateur UNIX. • La plupart des utilisateurs sont des clients NFS. • Une application accédant aux données utilise un utilisateur UNIX comme compte de service.
NTFS	• Le système de fichiers est géré par un administrateur Windows. • La majorité des utilisateurs sont des clients SMB. • Une application accédant aux données utilise un utilisateur Windows comme compte de service.

Style de sécurité	Choisissez si…
Mixte	Le système de fichiers est géré à la fois par les administrateurs et utilisateurs d'UNIX et de Windows, et il se compose de clients NFS et SMB.

Fonctionnement de l'héritage du style de sécurité

Si vous ne spécifiez pas le style de sécurité lors de la création d'un nouveau volume FlexVol ou d'un qtree, il hérite de son style de sécurité de différentes manières.

Les styles de sécurité sont hérités de la manière suivante :

- Un volume FlexVol hérite du style de sécurité du volume root de son SVM contenant.
- Un qtree hérite du style de sécurité de son volume FlexVol.
- Un fichier ou un répertoire hérite du style de sécurité de son volume FlexVol ou qtree.

Comment ONTAP préserve les autorisations UNIX

Lorsque les fichiers d'un volume FlexVol qui disposent actuellement d'autorisations UNIX sont modifiés et enregistrés par des applications Windows, ONTAP peut préserver les autorisations UNIX.

Lorsque des applications sur des clients Windows modifient et enregistrent des fichiers, elles lisent les propriétés de sécurité du fichier, créent un nouveau fichier temporaire, appliquent ces propriétés au fichier temporaire, puis donnent au fichier temporaire le nom du fichier d'origine.

Lorsque les clients Windows effectuent une requête pour les propriétés de sécurité, ils reçoivent une ACL construite qui représente exactement les autorisations UNIX. Le seul but de cette liste de contrôle d'accès construite est de préserver les autorisations UNIX du fichier lorsque les fichiers sont mis à jour par les applications Windows pour s'assurer que les fichiers résultants ont les mêmes autorisations UNIX. ONTAP ne définit pas d'ACL NTFS à l'aide de la liste de contrôle d'accès construite.

Gérez les autorisations UNIX à l'aide de l'onglet sécurité Windows

Si vous souhaitez manipuler les autorisations UNIX de fichiers ou de dossiers dans des volumes ou des qtrees de style sécurité mixtes sur des SVM, vous pouvez utiliser l'onglet sécurité sur les clients Windows. Vous pouvez également utiliser des applications qui peuvent interroger et définir des listes de contrôle d'accès Windows.

- Modification des autorisations UNIX

  Vous pouvez utiliser l'onglet sécurité Windows pour afficher et modifier les autorisations UNIX pour un volume ou qtree de style de sécurité mixte. Si vous utilisez l'onglet principal sécurité Windows pour modifier les autorisations UNIX, vous devez d'abord supprimer l'ACE que vous souhaitez modifier (ceci définit les bits de mode sur 0) avant d'effectuer vos modifications. Vous pouvez également utiliser l'éditeur avancé pour modifier les autorisations.

  Si des autorisations de mode sont utilisées, vous pouvez modifier directement les autorisations de mode pour l'UID, le GID et d'autres (tous les autres utilisateurs disposant d'un compte sur l'ordinateur). Par exemple, si l'UID affiché possède des autorisations r-x, vous pouvez modifier les autorisations UID sur rwx.

- Modification des autorisations UNIX en autorisations NTFS

  Vous pouvez utiliser l'onglet sécurité Windows pour remplacer les objets de sécurité UNIX par des objets de sécurité Windows sur un volume ou qtree de style de sécurité mixte, où les fichiers et les dossiers ont une méthode de sécurité efficace UNIX.

  Vous devez d'abord supprimer toutes les entrées d'autorisation UNIX répertoriées pour pouvoir les remplacer par les objets utilisateur et groupe Windows souhaités. Vous pouvez ensuite configurer des listes de contrôle d'accès NTFS sur les objets utilisateur et groupe Windows. En supprimant tous les objets de sécurité UNIX et en ajoutant uniquement des utilisateurs et des groupes Windows à un fichier ou à un dossier dans un volume ou qtree de style de sécurité mixte, vous modifiez le style de sécurité effectif sur le fichier ou le dossier d'UNIX à NTFS.

  Lors de la modification des autorisations sur un dossier, le comportement par défaut de Windows consiste à propager ces modifications à tous les sous-dossiers et fichiers. Par conséquent, vous devez modifier le choix de propagation sur le paramètre souhaité si vous ne souhaitez pas propager de modification du style de sécurité à tous les dossiers, sous-dossiers et fichiers enfants.

Configurer des styles de sécurité sur les volumes root SVM

Il configure la style de sécurité du volume root de la machine virtuelle de stockage (SVM) afin de déterminer le type d'autorisations utilisées pour les données sur le volume root de la SVM.

Étapes

1. Utilisez le `vserver create` commande avec `-rootvolume-security-style` paramètre pour définir le style de sécurité.

   Les options possibles pour le style de sécurité du volume racine sont `unix`, `ntfs`, ou `mixed`.

2. Afficher et vérifier la configuration, y compris le style de sécurité du volume root du SVM que vous avez créé : `vserver show -vserver` *`vserver_name`*

Configurer des styles de sécurité sur les volumes FlexVol

Configurez le style de sécurité des volumes FlexVol afin de déterminer le type d'autorisations utilisées pour les données sur des volumes FlexVol de la machine virtuelle de stockage (SVM).

Étapes

1. Effectuez l'une des opérations suivantes :

Si le volume FlexVol…	Utilisez la commande…
N'existe pas encore	`volume create` et inclure le `-security-style` paramètre pour spécifier le style de sécurité.
Existe déjà	`volume modify` et inclure le `-security-style` paramètre pour spécifier le style de sécurité.

Les options possibles pour le style de sécurité du volume FlexVol sont `unix`, `ntfs`, ou `mixed`.

Si vous ne spécifiez pas de style de sécurité lors de la création d'un volume FlexVol, le volume hérite du style de sécurité du volume racine.

Pour plus d'informations sur le `volume create` ou `volume modify` commandes, voir "Gestion du stockage logique".

2. Pour afficher la configuration, en incluant le style de sécurité du volume FlexVol que vous avez créé, entrez la commande suivante :

```
volume show -volume volume_name -instance
```

Configurer des styles de sécurité sur les qtrees

Vous configurez le style de sécurité du volume qtree afin de déterminer le type d'autorisations utilisées pour les données sur des qtrees.

Étapes

1. Effectuez l'une des opérations suivantes :

Si le qtree…	Utilisez la commande…
N'existe pas encore	`volume qtree create` et inclure le `-security -style` paramètre pour spécifier le style de sécurité.
Existe déjà	`volume qtree modify` et inclure le `-security -style` paramètre pour spécifier le style de sécurité.

Les options possibles pour la méthode de sécurité qtree sont `unix`, `ntfs`, ou `mixed`.

Si vous ne spécifiez pas de style de sécurité lors de la création d'un qtree, le style de sécurité par défaut est `mixed`.

Pour plus d'informations sur le `volume qtree create` ou `volume qtree modify` commandes, voir "Gestion du stockage logique".

2. Pour afficher la configuration, y compris le style de sécurité du qtree que vous avez créé, entrez la commande suivante : `volume qtree show -qtree qtree_name -instance`

Création et gestion des volumes de données dans les espaces de noms NAS

Créer et gérer des volumes de données dans les espaces de noms NAS

Pour gérer l'accès aux fichiers dans un environnement NAS, vous devez gérer les volumes et les points de jonction des données sur votre SVM (Storage Virtual machine).

Cela inclut la planification de votre architecture d'espace de noms, la création de volumes avec ou sans points de jonction, le montage ou le démontage de volumes, et l'affichage des informations sur les volumes de données et les serveurs NFS ou les espaces de noms de serveurs CIFS.

Créez des volumes de données avec des points de jonction spécifiés

Vous pouvez spécifier le point de jonction lorsque vous créez un volume de données. Le volume ainsi obtenu est automatiquement monté au point de jonction et est immédiatement disponible pour la configuration pour l'accès NAS.

Avant de commencer

L'agrégat dans lequel vous souhaitez créer le volume doit déjà exister.

> Les caractères suivants ne peuvent pas être utilisés dans le chemin de jonction : * # " > < | ? \
>
> De plus, la longueur du chemin de jonction ne peut pas dépasser 255 caractères.

Étapes

1. Créer le volume avec un point de jonction : `volume create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed} -junction-path` *`junction_path`*

   Le chemin de jonction doit commencer par la racine (/) et peut contenir à la fois des répertoires et des volumes reliés. Il n'est pas nécessaire que la Junction path contienne le nom du volume. Les Junction paths sont indépendants du nom du volume.

   La spécification d'un style de sécurité de volume est facultative. Si vous ne spécifiez pas de style de sécurité, ONTAP crée le volume avec le même style de sécurité que celui appliqué au volume racine de la machine virtuelle de stockage (SVM). Cependant, le style de sécurité du volume racine n'est peut-être pas celui que vous souhaitez appliquer au volume de données que vous créez. Il est recommandé de spécifier le style de sécurité lors de la création du volume afin de minimiser les problèmes d'accès aux fichiers difficiles à résoudre.

   Le chemin de jonction n'est pas sensible à la casse ; `/ENG` est identique à `/eng`. Si vous créez un partage CIFS, Windows traite le chemin de jonction comme s'il est sensible à la casse. Par exemple, si la jonction est de `/ENG`, Le chemin d'un partage CIFS doit commencer par `/ENG`pas `/eng`.

   De nombreux paramètres facultatifs peuvent être utilisés pour personnaliser un volume de données. Pour en savoir plus, consultez les pages de manuel pour le `volume create` commande.

2. Vérifier que le volume a été créé avec le point de jonction souhaité : `volume show -vserver` *`vserver_name`* `-volume` *`volume_name`* `-junction`

Exemple

L'exemple suivant crée un volume nommé « maison 4 » situé sur le SVM vs1 qui a une Junction path `/eng/home`:

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -volume home4 -junction
                  Junction                 Junction
Vserver   Volume  Active   Junction Path   Path Source
--------- ------- -------- --------------- -----------
vs1       home4   true     /eng/home       RW_volume
```

Créez des volumes de données sans spécifier de points de jonction

Vous pouvez créer un volume de données sans spécifier de point de jonction. Le volume résultant n'est pas monté automatiquement et n'est pas disponible pour configurer l'accès NAS. Vous devez monter le volume avant de configurer les partages SMB ou les exportations NFS pour ce volume.

Avant de commencer

L'agrégat dans lequel vous souhaitez créer le volume doit déjà exister.

Étapes

1. Créer le volume sans point de jonction en utilisant la commande suivante : `volume create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed}`

   La spécification d'un style de sécurité de volume est facultative. Si vous ne spécifiez pas de style de sécurité, ONTAP crée le volume avec le même style de sécurité que celui appliqué au volume racine de la machine virtuelle de stockage (SVM). Toutefois, le style de sécurité du volume racine n'est peut-être pas celui que vous souhaitez appliquer au volume de données. Il est recommandé de spécifier le style de sécurité lors de la création du volume afin de minimiser les problèmes d'accès aux fichiers difficiles à résoudre.

   De nombreux paramètres facultatifs peuvent être utilisés pour personnaliser un volume de données. Pour en savoir plus, consultez les pages de manuel pour le `volume create` commande.

2. Vérifier que le volume a été créé sans point de jonction : `volume show -vserver` *`vserver_name`* `-volume` *`volume_name`* `-junction`

Exemple

L'exemple suivant crée un volume nommé « sales » situé sur la SVM vs1 qui n'est pas monté à un point de jonction :

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -junction
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      -        -               -
```

Montez ou démontez les volumes existants dans l'espace de noms NAS

Un volume doit être monté sur le namespace NAS avant de pouvoir configurer l'accès des clients NAS aux données contenues dans les volumes SVM (Storage Virtual machine). Vous pouvez monter un volume sur un point de jonction s'il n'est pas actuellement monté. Vous pouvez également démonter des volumes.

Description de la tâche

Si vous démontez et mettez un volume hors ligne, toutes les données du point de jonction, y compris les données des volumes dont les points de jonction se trouvent dans l'espace de noms du volume non monté, sont inaccessibles aux clients NAS.

> Pour interrompre l'accès client NAS à un volume, il ne suffit pas de démonter le volume. Vous devez mettre le volume hors ligne ou prendre d'autres mesures pour vous assurer que les caches de descripteur de fichier côté client sont invalidés. Pour plus d'informations, consultez l'article suivant de la base de connaissances : "Les clients NFSv3 ont toujours accès à un volume après avoir été supprimés du namespace dans ONTAP"

Lorsque vous démontez et mettez un volume hors ligne, les données du volume ne sont pas perdues. En outre, les règles d'exportation de volume et les partages SMB créés sur le volume ou sur des répertoires et des points de jonction au sein du volume démonté sont conservés. Si vous remontez le volume démonté, les clients NAS peuvent accéder aux données contenues dans le volume à l'aide des règles d'exportation et des partages SMB existants.

Étapes

1. Effectuez l'action souhaitée :

Les fonctions que vous recherchez…	Entrez les commandes…
Montez un volume	`volume mount -vserver` *`svm_name`* `-volume` *`volume_name`* `-junction-path` *`junction_path`*

Les fonctions que vous recherchez…	Entrez les commandes…
Démonter un volume	`volume unmount -vserver` *`svm_name`* `-volume` *`volume_name`* `volume offline -vserver` *`svm_name`* `-volume` *`volume_name`*

2. Vérifiez que le volume est dans l'état de montage souhaité :

   `volume show -vserver` *`svm_name`* `-volume` *`volume_name`* `-fields state,junction-path,junction-active`

Exemples

L'exemple suivant monte un volume nommé « ventes » situé sur la SVM « vs1 » au point de jonction « /ventes » :

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active

vserver   volume     state     junction-path   junction-active
--------- ---------- -------- --------------- ----------------
vs1       data       online    /data           true
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

L'exemple suivant démonte et met hors ligne un volume nommé « `data' situé sur le SVM « vs1` » :

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active

vserver   volume     state     junction-path   junction-active
--------- ---------- --------- --------------- ---------------
vs1       data       offline   -               -
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

Affiche les informations sur le montage du volume et le point de jonction

Vous pouvez afficher des informations sur les volumes montés pour les SVM et les points de jonction auxquels les volumes sont montés. Vous pouvez également déterminer quels

volumes ne sont pas montés sur un point de jonction. Vous pouvez utiliser ces informations pour comprendre et gérer votre namespace SVM.

Étapes

1. Effectuez l'action souhaitée :

Si vous voulez afficher…	Entrez la commande…
Récapitulatif des informations sur les volumes montés et démontés sur le SVM	`volume show -vserver vserver_name -junction`
Informations détaillées sur les volumes montés et démontés sur le SVM	`volume show -vserver vserver_name -volume volume_name -instance`
Informations spécifiques sur les volumes montés et démontés sur le SVM	a. Si nécessaire, vous pouvez afficher des champs valides pour l' `-fields` paramètre via la commande suivante : `volume show -fields ?` b. Afficher les informations souhaitées à l'aide de l' `-fields` paramètre : volume show -vserver_name -champs fieldname,…

Exemples

L'exemple suivant affiche un récapitulatif des volumes montés et démontés sur le SVM vs1 :

```
cluster1::> volume show -vserver vs1 -junction
                      Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      true     /sales          RW_volume
```

L'exemple suivant affiche des informations sur les champs spécifiés pour les volumes situés sur le SVM vs2 :

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume   aggregate size state  type security-style junction-path
junction-parent node
------- ------   --------- ---- ------ ---- -------------- -------------
--------------- -----
vs2     data1    aggr3     2GB  online RW   unix           -            -
node3
vs2     data2    aggr3     1GB  online RW   ntfs           /data2
vs2_root        node3
vs2     data2_1  aggr3     8GB  online RW   ntfs           /data2/d2_1
data2           node3
vs2     data2_2  aggr3     8GB  online RW   ntfs           /data2/d2_2
data2           node3
vs2     pubs     aggr1     1GB  online RW   unix           /publications
vs2_root        node1
vs2     images   aggr3     2TB  online RW   ntfs           /images
vs2_root        node3
vs2     logs     aggr1     1GB  online RW   unix           /logs
vs2_root        node1
vs2     vs2_root aggr3     1GB  online RW   ntfs           /            -
node3
```

Configurez les mappages de noms

Présentation de la configuration des mappages de noms

ONTAP fait appel au mappage de noms pour mapper les identités CIFS aux identités UNIX, les identités Kerberos aux identités UNIX et les identités UNIX aux identités CIFS. Il a besoin de ces informations pour obtenir les informations d'identification des utilisateurs et fournir un accès approprié aux fichiers, qu'ils se connectent à partir d'un client NFS ou d'un client CIFS.

Il existe deux exceptions lorsque vous n'avez pas besoin d'utiliser le mappage de noms :

- Vous configurez un environnement UNIX pur et ne prévoyez pas d'utiliser l'accès CIFS ou le style de sécurité NTFS sur les volumes.
- Vous configurez l'utilisateur par défaut à utiliser à la place.

  Dans ce scénario, le mappage de noms n'est pas nécessaire car au lieu de mapper chaque identifiant client individuel, toutes les informations d'identification client sont mappées au même utilisateur par défaut.

Notez que vous pouvez utiliser le mappage de noms uniquement pour les utilisateurs, pas pour les groupes.

Toutefois, vous pouvez mapper un groupe d'utilisateurs individuels à un utilisateur spécifique. Par exemple,

vous pouvez mapper tous les utilisateurs AD qui commencent ou se terminent par le mot VENTES à un utilisateur UNIX spécifique et à l'UID de l'utilisateur.

Fonctionnement du mappage de noms

Lorsque ONTAP doit mapper les informations d'identification d'un utilisateur, il recherche tout d'abord un mappage existant dans la base de données de mappage de noms locaux et le serveur LDAP. Qu'elle vérifie un ou les deux et dans quel ordre est déterminé par la configuration du service de nom du SVM.

- Pour le mappage Windows à UNIX

  Si aucun mappage n'est trouvé, ONTAP vérifie si le nom d'utilisateur Windows minuscule est un nom d'utilisateur valide dans le domaine UNIX. Si cela ne fonctionne pas, il utilise l'utilisateur UNIX par défaut à condition qu'il soit configuré. Si l'utilisateur UNIX par défaut n'est pas configuré et que ONTAP ne peut pas obtenir de mappage de cette façon, le mappage échoue et une erreur est renvoyée.

- Pour le mappage d'UNIX à Windows

  Si aucun mappage n'est trouvé, ONTAP tente de trouver un compte Windows correspondant au nom UNIX dans le domaine SMB. Si cela ne fonctionne pas, il utilise l'utilisateur SMB par défaut, à condition qu'il soit configuré. Si l'utilisateur CIFS par défaut n'est pas configuré et que ONTAP ne peut pas obtenir de mappage de cette façon, le mappage échoue et une erreur est renvoyée.

Par défaut, les comptes machine sont mappés à l'utilisateur UNIX par défaut spécifié. Si aucun utilisateur UNIX par défaut n'est spécifié, les mappages de compte machine échouent.

- À partir de ONTAP 9.5, vous pouvez mapper des comptes machine à des utilisateurs autres que l'utilisateur UNIX par défaut.
- Dans ONTAP 9.4 et versions antérieures, vous ne pouvez pas mapper les comptes machine à d'autres utilisateurs.

  Même si des mappages de noms pour des comptes machine sont définis, les mappages sont ignorés.

Multidomaine recherche les mappages de noms d'utilisateur UNIX vers Windows

ONTAP prend en charge les recherches multidomaine lors du mappage d'utilisateurs UNIX aux utilisateurs Windows. Tous les domaines de confiance découverts sont recherchés pour trouver des correspondances avec le modèle de remplacement jusqu'à ce qu'un résultat correspondant soit renvoyé. Vous pouvez également configurer une liste de domaines de confiance préférés, qui est utilisée à la place de la liste de domaines de confiance découverts et est recherchée dans l'ordre jusqu'à ce qu'un résultat correspondant soit renvoyé.

La manière dont les approbations de domaine affectent les recherches de mappage de noms d'utilisateur UNIX à des noms d'utilisateur Windows

Pour comprendre le fonctionnement du mappage de noms d'utilisateur multidomaine, vous devez comprendre comment les approbations de domaine fonctionnent avec ONTAP. Les relations de confiance Active Directory avec le domaine personnel du serveur CIFS peuvent être une confiance bidirectionnelle ou l'un des deux types de fiducies unidirectionnelles, soit une confiance entrante, soit une confiance sortante. Le home domain est le

domaine auquel le serveur CIFS du SVM appartient.

- *Confiance bidirectionnelle*

  Avec des approbations bidirectionnelles, les deux domaines se font confiance. Si le domaine de base du serveur CIFS possède une confiance bidirectionnelle avec un autre domaine, le domaine de base peut authentifier et autoriser un utilisateur appartenant au domaine de confiance et vice versa.

  Les recherches de mappage de noms d'utilisateur UNIX à Windows peuvent être effectuées uniquement sur les domaines avec des approbations bidirectionnelles entre le domaine principal et l'autre domaine.

- *Confiance sortante*

  Avec une confiance sortante, le domaine d'origine approuve l'autre domaine. Dans ce cas, le domaine home peut authentifier et autoriser un utilisateur appartenant au domaine de confiance sortant.

  Un domaine avec une confiance sortante avec le domaine d'origine est *NOT* recherché lors de l'exécution de recherches de mappage entre utilisateurs UNIX et noms d'utilisateur Windows.

- *Confiance entrante*

  Avec une confiance entrante, l'autre domaine approuve le domaine personnel du serveur CIFS. Dans ce cas, le domaine personnel ne peut pas authentifier ni autoriser un utilisateur appartenant au domaine de confiance entrant.

  Un domaine avec une confiance entrante avec le domaine d'origine est *NOT* recherché lors de l'exécution de recherches de mappage entre utilisateurs UNIX et noms d'utilisateur Windows.

Comment les caractères génériques (*) sont utilisés pour configurer les recherches multidomaines pour le mappage de noms

Les recherches de mappage de noms de domaines multiples sont facilitées par l'utilisation de caractères génériques dans la section domaine du nom d'utilisateur Windows. Le tableau suivant illustre comment utiliser des caractères génériques dans la partie domaine d'une entrée de mappage de nom pour activer les recherches multidomaine :

Motif	Remplacement	Résultat
racine	*\\administrateur	L'utilisateur UNIX « root » est mappé à l'utilisateur nommé « administrateur ». Tous les domaines approuvés sont recherchés dans l'ordre jusqu'à ce que le premier utilisateur correspondant nommé « administrateur » soit trouvé.

Motif	Remplacement	Résultat
*	**	Les utilisateurs UNIX valides sont mappés aux utilisateurs Windows correspondants. Tous les domaines approuvés sont recherchés dans l'ordre jusqu'à ce que le premier utilisateur correspondant à ce nom soit trouvé. Le schéma ** n'est valide que pour le mappage de noms d'UNIX à Windows, pas l'inverse.

Mode d'exécution des recherches sur plusieurs noms de domaine

Vous pouvez choisir l'une des deux méthodes pour déterminer la liste des domaines approuvés utilisés pour les recherches de noms multidomaines :

- Utilisez la liste d'approbation bidirectionnelle automatiquement découverte compilée par ONTAP
- Utilisez la liste de domaines approuvés que vous compilez

Si un utilisateur UNIX est mappé à un utilisateur Windows avec un caractère générique utilisé pour la section domaine du nom d'utilisateur, l'utilisateur Windows est recherché dans tous les domaines approuvés comme suit :

- Si une liste de domaines de confiance est configurée, l'utilisateur Windows mappé est uniquement recherché dans cette liste de recherche, dans l'ordre.
- Si une liste préférée de domaines approuvés n'est pas configurée, l'utilisateur Windows est alors recherché dans tous les domaines de confiance bidirectionnels du domaine de départ.
- S'il n'existe pas de domaines de confiance bidirectionnellement pour le domaine personnel, l'utilisateur est recherché dans le domaine personnel.

Si un utilisateur UNIX est mappé à un utilisateur Windows sans section de domaine dans le nom d'utilisateur, l'utilisateur Windows est recherché dans le domaine personnel.

Règles de conversion du mappage de noms

Un système ONTAP conserve un ensemble de règles de conversion pour chaque SVM. Chaque règle se compose de deux éléments : un *pattern* et un *remplacement*. Les conversions commencent au début de la liste appropriée et effectuent une substitution basée sur la première règle correspondante. Le motif est une expression régulière de style UNIX. Le remplacement est une chaîne contenant des séquences d'échappement représentant des sous-expressions du motif, comme dans UNIX `sed` programme.

Créer un mappage de nom

Vous pouvez utiliser le `vserver name-mapping create` commande permettant de créer un mappage de noms. Vous utilisez les mappages de noms pour permettre aux utilisateurs Windows d'accéder aux volumes du style de sécurité UNIX et les inverser.

Description de la tâche

Par SVM, ONTAP prend en charge jusqu'à 12,500 mappages de noms dans chaque direction.

Étape

1. Créer un mappage de noms : `vserver name-mapping create -vserver` *`vserver_name`* `-direction {krb-unix|win-unix|unix-win} -position` *`integer`* `-pattern text -replacement` *`text`*

> Le `-pattern` et `-replacement` les énoncés peuvent être formulés comme des expressions régulières. Vous pouvez également utiliser le `-replacement` instruction pour refuser explicitement un mappage à l'utilisateur en utilisant la chaîne de remplacement nulle `" "` (le caractère d'espace). Voir la `vserver name-mapping create` page de manuel pour plus de détails.

Lorsque des mappages entre Windows et UNIX sont créés, tous les clients SMB disposant de connexions ouvertes au système ONTAP au moment de la création des nouveaux mappages doivent se déconnecter et se reconnecter pour voir les nouveaux mappages.

Exemples

La commande suivante crée un nom de mappage sur le SVM nommé vs1. Le mappage est un mappage d'UNIX à Windows à la position 1 dans la liste des priorités. Le mappage mappe l'utilisateur UNIX johnd à l'utilisateur Windows ENG\johndoe.

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

La commande suivante crée un autre mappage de nom sur le SVM nommé vs1. Le mappage est un mappage de Windows à UNIX à la position 1 dans la liste des priorités. Dans ce cas, le motif et le remplacement incluent des expressions régulières. Le mapping mappe chaque utilisateur CIFS du domaine ENG aux utilisateurs du domaine LDAP associé avec la SVM.

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\1"
```

La commande suivante crée un autre mappage de nom sur le SVM nommé vs1. Ici, le schéma inclut "`$'" comme élément du nom d'utilisateur Windows qui doit être échappé. Le mappage mappe l'utilisateur Windows ENG\ john$OPS à l'utilisateur UNIX john_OPS.

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

Configurez l'utilisateur par défaut

Vous pouvez configurer un utilisateur par défaut à utiliser si toutes les autres tentatives de mappage échouent pour un utilisateur, ou si vous ne souhaitez pas mapper des utilisateurs individuels entre UNIX et Windows. Si vous souhaitez que l'authentification des utilisateurs non mappés échoue, vous ne devez pas configurer un utilisateur par défaut.

Description de la tâche

Pour l'authentification CIFS, si vous ne souhaitez pas mapper chaque utilisateur Windows à un utilisateur UNIX individuel, vous pouvez spécifier un utilisateur UNIX par défaut.

Pour l'authentification NFS, si vous ne souhaitez pas mapper chaque utilisateur UNIX à un utilisateur Windows individuel, vous pouvez spécifier un utilisateur Windows par défaut.

Étapes

1. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Saisissez la commande suivante…
Configurez l'utilisateur UNIX par défaut	`vserver cifs options modify -default -unix-user` *`user_name`*
Configurez l'utilisateur Windows par défaut	`vserver nfs modify -default-win-user` *`user_name`*

Commandes permettant de gérer les mappages de noms

Il existe des commandes ONTAP spécifiques permettant de gérer les mappages de noms.

Les fonctions que vous recherchez…	Utilisez cette commande…
Créer un mappage de nom	`vserver name-mapping create`
Insérez un mappage de nom à une position spécifique	`vserver name-mapping insert`
Afficher les mappages de noms	`vserver name-mapping show`

Les fonctions que vous recherchez…	Utilisez cette commande…
Échangez la position de deux mappages de noms Un swap n'est pas autorisé lorsque le mappage-nom est configuré avec une entrée de qualificatif-ip.	`vserver name-mapping swap`
Modifier un mappage de noms	`vserver name-mapping modify`
Supprime un mappage de noms	`vserver name-mapping delete`
Valider le mappage de nom correct	`vserver security file-directory show-effective-permissions -vserver vs1 -win -user-name user1 -path / -share-name sh1`

Consultez la page man pour chaque commande pour plus d'informations.

Configurez les recherches de mappage de noms-domaines multiples

Activez ou désactivez les recherches de mappage de noms multidomaine

Avec les recherches de mappage de noms multidomaine, vous pouvez utiliser un caractère générique (*) dans la partie domaine d'un nom Windows lors de la configuration du mappage de noms d'utilisateurs UNIX vers Windows. L'utilisation d'un caractère générique (*) dans la partie domaine du nom permet à ONTAP de rechercher tous les domaines ayant une confiance bidirectionnelle avec le domaine qui contient le compte ordinateur du serveur CIFS.

Description de la tâche

Comme alternative à la recherche de tous les domaines de confiance bidirectionnels, vous pouvez configurer une liste de domaines de confiance préférés. Lorsqu'une liste de domaines de confiance privilégiés est configurée, ONTAP utilise la liste de domaines de confiance préférée au lieu des domaines de confiance bidirectionnels découverts pour effectuer des recherches de mappage de noms multiples domaines.

- Les recherches de mappage de noms de domaines multiples sont activées par défaut.
- Cette option est disponible au niveau de privilège avancé.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Effectuez l'une des opérations suivantes :

Pour effectuer des recherches sur le mappage de noms de domaines multiples…	Entrez la commande…
Activé	`vserver cifs options modify -vserver` *`vserver_name`* `-is-trusted-domain-enum -search-enabled true`
Désactivé	`vserver cifs options modify -vserver` *`vserver_name`* `-is-trusted-domain-enum -search-enabled false`

3. Retour au niveau de privilège admin : `set -privilege admin`

Informations associées

Options de serveur SMB disponibles

Réinitialiser et redécouvrir des domaines de confiance

Vous pouvez forcer la redécouverte de tous les domaines de confiance. Ceci peut être utile lorsque les serveurs de domaine approuvés ne répondent pas correctement ou que les relations de confiance ont changé. Seuls les domaines avec une confiance bidirectionnelle avec le domaine de base, qui est le domaine contenant le compte ordinateur du serveur CIFS, sont découverts.

Étape

1. Réinitialisez et redécouvrez des domaines de confiance à l'aide de `vserver cifs domain trusts rediscover` commande.

   ```
   vserver cifs domain trusts rediscover -vserver vs1
   ```

Informations associées

Affichage des informations sur les domaines de confiance découverts

Affiche des informations sur les domaines de confiance découverts

Vous pouvez afficher des informations sur les domaines approuvés découverts pour le domaine personnel du serveur CIFS, qui est le domaine contenant le compte d'ordinateur du serveur CIFS. Cela peut être utile lorsque vous voulez savoir quels domaines de confiance sont découverts et comment ils sont ordonnés dans la liste domaine de confiance découvert.

Description de la tâche

Seuls les domaines avec des approbations bidirectionnelles avec le domaine de départ sont découverts. Étant donné que le contrôleur de domaine (DC) du domaine d'origine renvoie la liste des domaines de confiance dans un ordre déterminé par le DC, l'ordre des domaines dans la liste ne peut pas être prédit. En affichant la liste des domaines de confiance, vous pouvez déterminer l'ordre de recherche des recherches de mappage de noms de domaines multiples.

Les informations des domaines de confiance affichés sont regroupées par nœud et par SVM (Storage Virtual machine).

Étape

1. Affiche des informations sur les domaines de confiance découverts à l'aide du `vserver cifs domain trusts show` commande.

   `vserver cifs domain trusts show -vserver vs1`

   ```
      Node: node1
   Vserver: vs1

   Home Domain            Trusted Domain
   ---------------------  -----------------------------------
   EXAMPLE.COM            CIFS1.EXAMPLE.COM,
                          CIFS2.EXAMPLE.COM
                          EXAMPLE.COM

      Node: node2
   Vserver: vs1

   Home Domain            Trusted Domain
   ---------------------  -----------------------------------
   EXAMPLE.COM            CIFS1.EXAMPLE.COM,
                          CIFS2.EXAMPLE.COM
                          EXAMPLE.COM
   ```

Informations associées

Réinitialisation et redécouverte des domaines de confiance

Ajoutez, supprimez ou remplacez des domaines de confiance dans les listes de domaines de confiance préférées

Vous pouvez ajouter ou supprimer des domaines approuvés de la liste des domaines approuvés préférés pour le serveur SMB ou modifier la liste actuelle. Si vous configurez une liste de domaines de confiance privilégiés, cette liste est utilisée à la place des domaines de confiance bidirectionnels découverts lors de l'exécution de recherches sur le mappage de noms multidomaines.

Description de la tâche

- Si vous ajoutez des domaines approuvés à une liste existante, la nouvelle liste est fusionnée avec la liste existante et les nouvelles entrées sont placées à la fin Les domaines de confiance sont recherchés dans l'ordre dans lequel ils apparaissent dans la liste des domaines de confiance.
- Si vous supprimez des domaines de confiance de la liste existante et ne spécifiez pas de liste, la liste de domaines de confiance complète pour la machine virtuelle de stockage (SVM) spécifiée est supprimée.
- Si vous modifiez la liste existante des domaines approuvés, la nouvelle liste remplace la liste existante.

> Vous devez entrer uniquement les domaines de confiance bidirectionnels dans la liste des domaines de confiance préférés. Même si vous pouvez entrer des domaines de confiance sortants ou entrants dans la liste de domaines préférés, ils ne sont pas utilisés lors de recherches de mappage de noms de domaines multiples. ONTAP ignore l'entrée du domaine unidirectionnel et passe au domaine de confiance bidirectionnel suivant dans la liste.

Étape

1. Effectuez l'une des opérations suivantes :

Si vous souhaitez effectuer les opérations suivantes avec la liste des domaines de confiance préférés…	Utilisez la commande…
Ajouter des domaines de confiance à la liste	`vserver cifs domain name-mapping-search add -vserver _vserver_name_ -trusted-domains FQDN, ...`
Supprimer des domaines de confiance de la liste	`vserver cifs domain name-mapping-search remove -vserver _vserver_name_ [-trusted-domains FQDN, ...]`
Modifier la liste existante	`vserver cifs domain name-mapping-search modify -vserver _vserver_name_ -trusted-domains FQDN, ...`

Exemples

La commande suivante ajoute deux domaines de confiance (cifs1.example.com et cifs2.example.com) à la liste de domaines de confiance privilégiée utilisée par le SVM vs1 :

```
cluster1::> vserver cifs domain name-mapping-search add -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

La commande suivante supprime deux domaines de confiance de la liste utilisée par le SVM vs1 :

```
cluster1::> vserver cifs domain name-mapping-search remove -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

La commande suivante modifie la liste de domaines approuvés utilisée par le SVM vs1. La nouvelle liste remplace la liste d'origine :

```
cluster1::> vserver cifs domain name-mapping-search modify -vserver vs1
-trusted-domains cifs3.example.com
```

Informations associées

Affichage d'informations sur la liste de domaines de confiance préférée

Affiche des informations sur la liste de domaines de confiance préférée

Vous pouvez afficher des informations sur les domaines de confiance dans la liste des domaines de confiance préférés et l'ordre dans lequel ils sont recherchés si les recherches de mappage de noms de domaines multiples sont activées. Vous pouvez configurer une liste de domaines de confiance préférée comme alternative à l'utilisation de la liste de domaines de confiance automatiquement découverts.

Étapes

1. Effectuez l'une des opérations suivantes :

Pour afficher des informations sur les éléments suivants…	Utilisez la commande…
Tous les domaines de confiance privilégiés dans le cluster regroupés par SVM (Storage Virtual machine)	`vserver cifs domain name-mapping-search show`
Tous les domaines fiables préférés pour un SVM spécifié	`vserver cifs domain name-mapping-search show -vserver` *`vserver_name`*

La commande suivante affiche des informations sur tous les domaines de confiance privilégiés sur le cluster :

```
cluster1::> vserver cifs domain name-mapping-search show
Vserver         Trusted Domains
--------------  ----------------------------------
vs1             CIFS1.EXAMPLE.COM
```

Informations associées

Ajout, suppression ou remplacement de domaines de confiance dans les listes de domaines de confiance préférées

Créez et configurez des partages SMB

Présentation de la création et de la configuration des partages SMB

Avant que les utilisateurs et les applications n'accèdent aux données sur le serveur CIFS via SMB, vous devez créer et configurer des partages SMB, qui est un point d'accès nommé dans un volume. Vous pouvez personnaliser les partages en spécifiant des paramètres de partage et des propriétés de partage. Vous pouvez modifier un partage existant à tout moment.

Lorsque vous créez un partage SMB, ONTAP crée une liste de contrôle d'accès par défaut pour le partage avec les autorisations de contrôle total pour tous.

Les partages SMB sont liés au serveur CIFS sur la machine virtuelle de stockage (SVM). Les partages SMB

sont supprimés si le SVM est supprimé ou si le serveur CIFS auquel il est associé est supprimé de la SVM. Si vous recréez le serveur CIFS sur le SVM, vous devez recréer les partages SMB.

Informations associées

Gérer l'accès aux fichiers via SMB

"Configuration SMB pour Microsoft Hyper-V et SQL Server"

Configurez le mappage de caractères pour la conversion de nom de fichier SMB sur des volumes

Définition des partages administratifs par défaut

Lorsque vous créez un serveur CIFS sur votre SVM (Storage Virtual machine), les partages administratifs par défaut sont automatiquement créés. Vous devez comprendre ce que sont ces partages par défaut et comment ils sont utilisés.

Lors de la création du serveur CIFS, ONTAP crée les partages administratifs par défaut suivants :

> Depuis ONTAP 9.8, le partage admin$ n'est plus créé par défaut.

- ipc$
- admin$ (ONTAP 9.7 et versions antérieures uniquement)
- c$

Les partages qui se terminent par le caractère $ étant des partages masqués, les partages administratifs par défaut ne sont pas visibles depuis mon ordinateur, mais vous pouvez les afficher à l'aide de dossiers partagés.

Utilisation des partages IPC$ et admin$ par défaut

Les partages ipc$ et admin$ sont utilisés par ONTAP et ne peuvent pas être utilisés par les administrateurs Windows pour accéder aux données résidant sur la SVM.

- part ipc$

  La part ipc$ est une ressource qui partage les canaux nommés qui sont essentiels à la communication entre les programmes. Le partage ipc$ est utilisé lors de l'administration à distance d'un ordinateur et lors de l'affichage des ressources partagées d'un ordinateur. Vous ne pouvez pas modifier les paramètres de partage, les propriétés de partage ou les listes de contrôle d'accès du partage ipc$. Vous ne pouvez pas non plus renommer ou supprimer le partage ipc$.

- Partage admin$ (ONTAP 9.7 et versions antérieures uniquement)

  > Depuis ONTAP 9.8, le partage admin$ n'est plus créé par défaut.

  Le partage admin$ est utilisé pendant l'administration à distance du SVM. Le chemin de cette ressource est toujours le chemin vers la racine SVM. Vous ne pouvez pas modifier les paramètres de partage, les propriétés de partage ou les listes de contrôle d'accès pour le partage admin$. Vous ne pouvez pas non plus renommer ou supprimer le partage admin$.

Utilisation du partage par défaut c$

Le partage c$ est un partage administratif que l'administrateur du cluster ou du SVM peut utiliser pour accéder au volume root du SVM et le gérer.

Voici les caractéristiques de la part c$:

- Le chemin pour ce partage est toujours le chemin vers le volume root du SVM et ne peut pas être modifié.
- La liste de contrôle d'accès par défaut pour le partage c$ est Administrator / Full Control.

  Cet utilisateur est le BULILTIN\Administrator. Par défaut, BUILTIN\Administrator peut mapper sur le partage et l'affichage, créer, modifier ou supprimer des fichiers et dossiers dans le répertoire racine mappé. Soyez prudent lorsque vous gérez des fichiers et des dossiers dans ce répertoire.

- Vous pouvez modifier l'ACL du partage c$.
- Vous pouvez modifier les paramètres de partage c$ et les propriétés de partage.
- Vous ne pouvez pas supprimer le partage c$.
- L'administrateur du SVM peut accéder au reste de l'espace de noms du SVM à partir du partage c$ mappé en croisant les jonctions de l'espace de noms.
- Le partage c$ est accessible à l'aide de la console de gestion Microsoft.

Informations associées

Configuration des autorisations de fichier NTFS avancées à l'aide de l'onglet sécurité de Windows

Exigences de nommage des partages SMB

Lors de la création de partages SMB sur votre serveur SMB, veillez à respecter les exigences de dénomination des partages ONTAP.

Les conventions de nom des partages pour ONTAP sont identiques à celles de Windows et doivent être respectées dans ce cas :

- Le nom de chaque partage doit être unique pour le serveur SMB.
- Les noms de partage ne sont pas sensibles à la casse.
- La longueur maximale du nom de partage est de 80 caractères.
- Les noms de partage Unicode sont pris en charge.
- Les noms de partage se terminant par le caractère $ sont des partages masqués.
- Pour ONTAP 9.7 et les versions antérieures, les partages administratifs admin$, ipc$ et c$ sont automatiquement créés sur chaque serveur CIFS et sont des noms de partage réservés. Depuis ONTAP 9.8, le partage admin$ n'est plus créé automatiquement.
- Lors de la création d'un partage, vous ne pouvez pas utiliser le nom de partage ONTAP_ADMIN$.
- Les noms de partage contenant des espaces sont pris en charge :
  - Vous ne pouvez pas utiliser un espace comme premier caractère ou comme dernier caractère dans un nom de partage.
  - Vous devez inclure des noms de partage contenant un espace entre guillemets.

> Les guillemets simples sont considérés comme faisant partie du nom du partage et ne peuvent pas être utilisés à la place des guillemets.

- Les caractères spéciaux suivants sont pris en charge lorsque vous nommez des partages SMB :

  ! @ # $ % et ' _ - . ~ ( ) { }

- Les caractères spéciaux suivants ne sont pas pris en charge lorsque vous nommez des partages SMB :
  - " / \ : ; | < > , ? * =

Exigences de sensibilité aux cas de répertoire lors de la création de partages dans un environnement multiprotocole

Si vous créez des partages dans un SVM où le schéma de nommage 8.3 est utilisé pour faire la distinction entre les noms de répertoire où il n'y a que des différences de cas entre les noms, vous devez utiliser le nom 8.3 du chemin de partage pour s'assurer que le client se connecte au chemin de répertoire souhaité.

Dans l'exemple suivant, deux répertoires nommés « testdir » et « TESTDIR » ont été créés sur un client Linux. La Junction path du volume contenant les répertoires est `/home`. La première sortie provient d'un client Linux et la seconde sortie provient d'un client SMB.

```
 ls -l
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:23 testdir
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:24 TESTDIR
```

```
dir

 Directory of Z:\

04/17/2015  11:23 AM    <DIR>          testdir
04/17/2015  11:24 AM    <DIR>          TESTDI~1
```

Lorsque vous créez un partage dans le second répertoire, vous devez utiliser le nom 8.3 dans le chemin du partage. Dans cet exemple, le chemin du partage vers le premier répertoire est `/home/testdir` et le chemin du partage vers le second répertoire est `/home/TESTDI~1`.

Utilisez les propriétés du partage SMB

Utiliser la présentation des propriétés de partage SMB

Vous pouvez personnaliser les propriétés des partages SMB.

Les propriétés de partage disponibles sont les suivantes :

Propriétés du partage	Description
`oplocks`	Cette propriété indique que le partage utilise des verrous opportunistes, également appelés mise en cache côté client.
`browsable`	Cette propriété permet aux clients Windows de parcourir le partage.
`showsnapshot`	Cette propriété spécifie que les copies Snapshot peuvent être visualisées et traversées par les clients.
`changenotify`	Cette propriété indique que le partage prend en charge les demandes de notification des modifications. Pour les partages sur un SVM, il s'agit d'une propriété initiale par défaut.
`attributecache`	Cette propriété permet la mise en cache des attributs de fichier sur le partage SMB afin d'accélérer l'accès aux attributs. La valeur par défaut est de désactiver la mise en cache des attributs. Cette propriété ne doit être activée que si des clients se connectent à des partages sur SMB 1.0. Cette propriété de partage n'est pas applicable si les clients se connectent à des partages via SMB 2.x ou SMB 3.0.
`continuously-available`	Cette propriété permet aux clients SMB qui la prennent en charge d'ouvrir des fichiers de façon persistante. Les fichiers ouverts de cette façon sont protégés contre les événements perturbateurs, tels que le basculement et le rétablissement.
`branchcache`	Cette propriété spécifie que le partage permet aux clients de demander des hachages de BranchCache sur les fichiers de ce partage. Cette option n'est utile que si vous spécifiez « par partage » en mode de fonctionnement dans la configuration de BranchCache CIFS.
`access-based-enumeration`	Cette propriété spécifie que *accès basé sur Enumeration* (ABE) est activé sur ce partage. Les dossiers partagés filtrés PAR ABE sont visibles par un utilisateur en fonction des droits d'accès de cet utilisateur, empêchant l'affichage des dossiers ou d'autres ressources partagées que l'utilisateur ne dispose pas des droits d'accès.

Propriétés du partage	Description
`namespace-caching`	Cette propriété spécifie que les clients SMB qui se connectent à ce partage peuvent mettre en cache les résultats d'énumération de répertoire renvoyés par les serveurs CIFS, ce qui peut fournir de meilleures performances. Par défaut, les clients SMB 1 ne mettent pas en cache les résultats d'énumération des répertoires. Étant donné que les clients SMB 2 et SMB 3 mettent en cache les résultats d'énumération de répertoires par défaut, la spécification de cette propriété de partage n'offre des avantages en termes de performances que pour les connexions clients SMB 1.
`encrypt-data`	Cette propriété spécifie que le chiffrement SMB doit être utilisé lors de l'accès à ce partage. Les clients SMB qui ne prennent pas en charge le chiffrement lors de l'accès aux données SMB ne pourront pas accéder à ce partage.

Ajouter ou supprimer des propriétés de partage sur un partage SMB existant

Vous pouvez personnaliser un partage SMB existant en ajoutant ou en supprimant des propriétés de partage. Cela peut être utile si vous voulez modifier la configuration du partage pour répondre aux exigences changeantes de votre environnement.

Avant de commencer

Le partage dont vous souhaitez modifier les propriétés doit exister.

Description de la tâche

Instructions pour l'ajout de propriétés de partage :

- Vous pouvez ajouter une ou plusieurs propriétés de partage à l'aide d'une liste délimitée par des virgules.
- Toutes les propriétés de partage que vous avez précédemment spécifiées restent en vigueur.

  Les nouvelles propriétés ajoutées sont ajoutées à la liste existante des propriétés de partage.

- Si vous spécifiez une nouvelle valeur pour les propriétés de partage qui sont déjà appliquées au partage, la nouvelle valeur spécifiée remplace la valeur d'origine.
- Vous ne pouvez pas supprimer les propriétés de partage à l'aide de `vserver cifs share properties add` commande.

  Vous pouvez utiliser le `vserver cifs share properties remove` commande permettant de supprimer les propriétés de partage.

Consignes de suppression des propriétés de partage :

- Vous pouvez supprimer une ou plusieurs propriétés de partage à l'aide d'une liste délimitée par des virgules.

- Toutes les propriétés de partage que vous avez précédemment spécifiées mais que vous ne les supprimez pas restent en vigueur.

Étapes

1. Saisissez la commande appropriée :

Les fonctions que vous recherchez…	Entrez la commande…
Ajouter des propriétés de partage	`vserver cifs share properties add -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...`
Supprimer les propriétés de partage	`vserver cifs share properties remove -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...`

2. Vérifiez les paramètres de propriété de partage : `vserver cifs share show -vserver vserver_name -share-name share_name`

Exemples

La commande suivante ajoute la `showsnapshot` Partagez la propriété avec une part nommée « `khare1' » sur la SVM vs1 :

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties showsnapshot

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share   Path      Properties   Comment    ACL
---------  ------  --------  ----------   --------   -----------
vs1        share1  /share1   oplocks      -          Everyone / Full
Control
                             browsable
                             changenotify
                             showsnapshot
```

La commande suivante supprime le `browsable` Partagez des biens d'une part nommée « `sune2` » sur la SVM vs1 :

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share2 -share-properties browsable

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share   Path      Properties   Comment    ACL
---------  ------  --------  ----------   --------   -----------
vs1        share2  /share2   oplocks      -          Everyone / Full
Control
                             changenotify
```

Informations associées

Commandes de gestion des partages SMB

Optimisez l'accès des utilisateurs SMB à l'aide du paramètre de partage force-groupe

Lorsque vous créez un partage à partir de la ligne de commande ONTAP vers des données avec sécurité efficace UNIX, vous pouvez spécifier que tous les fichiers créés par les utilisateurs SMB de ce partage appartiennent au même groupe, appelé *force-group*, qui doit être un groupe prédéfini dans la base de données du groupe UNIX. L'utilisation d'un groupe de force facilite l'accès aux fichiers par les utilisateurs SMB appartenant à différents groupes.

La spécification d'un groupe de force n'est pertinente que si le partage est dans un qtree UNIX ou mixte. Il n'est pas nécessaire de définir un groupe de force pour les partages d'un volume NTFS ou d'un qtree, car l'accès aux fichiers de ces partages est déterminé par les autorisations Windows, et non par des GIDS UNIX.

Si un groupe de force a été spécifié pour un partage, les valeurs suivantes deviennent vraies pour le partage :

- Les moyennes entreprises qui accèdent à ce partage sont temporairement modifiées en GID du groupe force.

  Ce GID leur permet d'accéder aux fichiers de ce partage qui ne sont pas accessibles normalement avec leur GID ou leur UID principal.

- Tous les fichiers de ce partage créés par les utilisateurs SMB appartiennent au même groupe de force, quel que soit le GID principal du propriétaire du fichier.

Lorsque les utilisateurs SMB essaient d'accéder à un fichier créé par NFS, les principaux GID des utilisateurs SMB déterminent les droits d'accès.

La force-group n'affecte pas la façon dont les utilisateurs NFS accèdent aux fichiers dans ce partage. Un fichier créé par NFS acquiert le GID du propriétaire du fichier. La détermination des autorisations d'accès est basée sur l'UID et le GID principal de l'utilisateur NFS qui tente d'accéder au fichier.

L'utilisation d'un groupe de force facilite l'accès aux fichiers par les utilisateurs SMB appartenant à différents groupes. Par exemple, si vous souhaitez créer un partage pour stocker les pages Web de l'entreprise et donner un accès en écriture aux utilisateurs des départements Ingénierie et Marketing, vous pouvez créer un partage et donner accès en écriture à un groupe de force nommé « webgroupe1 ». En raison du groupe de force, tous les fichiers créés par les utilisateurs SMB de ce partage appartiennent au groupe « webgroupe1 ».

En outre, les utilisateurs se voient automatiquement attribuer le GID du groupe « webgroupe1 » lorsqu'ils accèdent au partage. Par conséquent, tous les utilisateurs peuvent écrire sur ce partage sans avoir à gérer les droits d'accès des utilisateurs dans les services Ingénierie et Marketing.

Informations associées

Création d'un partage SMB avec le paramètre de partage force-group

Créez un partage SMB avec le paramètre de partage force-group

Vous pouvez créer un partage SMB avec le paramètre de partage force-group si vous souhaitez que les utilisateurs SMB qui accèdent aux données sur des volumes ou des qtrees avec la sécurité de fichier UNIX soient considérés par ONTAP comme appartenant au même groupe UNIX.

Étape

1. Créez le partage SMB : `vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path path -force-group-for-create` *`UNIX_group_name`*

   Si le chemin UNC (`\\servername\sharename\filepath`) du partage contient plus de 256 caractères (à l'exclusion de la première «`\\`" Dans le chemin UNC), l'onglet **sécurité** de la boîte Propriétés de Windows n'est pas disponible. Il s'agit d'un problème de client Windows plutôt que d'un problème ONTAP. Pour éviter ce problème, ne créez pas de partages avec des chemins UNC de plus de 256 caractères.

   Si vous souhaitez supprimer le groupe de force après la création du partage, vous pouvez modifier le partage à tout moment et spécifier une chaîne vide ("") comme valeur pour le `-force-group-for -create` paramètre. Si vous supprimez le groupe de force en modifiant le partage, toutes les connexions existantes à ce partage continuent d'avoir le groupe de force précédemment défini comme GID principal.

Exemple

La commande suivante crée un partage « pages Web » accessible sur le Web dans le `/corp/companyinfo` Répertoire dans lequel tous les fichiers créés par les utilisateurs SMB sont affectés au groupe webgroupe1 :

```
vserver cifs share create -vserver vs1 -share-name webpages -path
/corp/companyinfo -force-group-for-create webgroup1
```

Informations associées

Optimisez l'accès des utilisateurs SMB à l'aide du paramètre de partage force-groupe

Afficher les informations sur les partages SMB à l'aide de la console MMC

Vous pouvez afficher les informations relatives aux partages SMB sur votre SVM et effectuer certaines tâches de gestion à l'aide de la console de gestion Microsoft (MMC). Avant de pouvoir afficher les partages, vous devez connecter la MMC au SVM.

Description de la tâche

Vous pouvez effectuer les tâches suivantes sur les partages contenus dans les SVM à l'aide de MMC :

- Afficher les partages
- Afficher les sessions actives

- Afficher les fichiers ouverts
- Énumérer la liste des sessions, des fichiers et des connexions d'arborescence dans le système
- Fermez les fichiers ouverts dans le système
- Fermer les sessions ouvertes
- Création/gestion de partages

> Les vues affichées par les fonctionnalités précédentes sont propres à chaque nœud et non à chaque cluster. Par conséquent, lorsque vous utilisez le MMC pour vous connecter au nom d'hôte du serveur SMB (à savoir, cifs01.domain.local), vous êtes routé, selon la façon dont vous avez configuré DNS, vers une seule LIF au sein de votre cluster.

Les fonctions suivantes ne sont pas prises en charge dans MMC pour ONTAP :

- Création de nouveaux utilisateurs/groupes locaux
- Gestion/affichage des utilisateurs/groupes locaux existants
- Affichage des événements ou des journaux de performances
- Stockage
- Services et applications

Dans les cas où l'opération n'est pas prise en charge, vous pouvez être confrontés à une situation `remote procedure call failed` erreurs.

"FAQ : utilisation de Windows MMC avec ONTAP"

Étapes

1. Pour ouvrir Computer Management MMC sur n'importe quel serveur Windows, dans le **panneau de configuration**, sélectionnez **Outils d'administration** > **gestion de l'ordinateur**.
2. Sélectionnez **action** > **connexion à un autre ordinateur**.

   La boîte de dialogue Sélectionner un ordinateur s'affiche.

3. Tapez le nom du système de stockage ou cliquez sur **Parcourir** pour localiser le système de stockage.
4. Cliquez sur **OK**.

   La MMC se connecte à la SVM.

5. Dans le volet de navigation, cliquez sur **dossiers partagés** > **partages**.

   Une liste des partages sur le SVM est affichée dans le volet d'affichage droit.

6. Pour afficher les propriétés de partage d'un partage, double-cliquez sur le partage pour ouvrir la boîte de dialogue **Propriétés**.
7. Si vous ne pouvez pas vous connecter au système de stockage à l'aide de MMC, vous pouvez ajouter l'utilisateur au groupe BULTIN\Administrators ou BULTIN\Power Users en utilisant l'une des commandes suivantes sur le système de stockage :

```
cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name BUILTIN\Administrators -member-names <domainuser>

cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name "BUILTIN\Power Users" -member-names <domainuser>
```

Commandes de gestion des partages SMB

Vous utilisez le `vserver cifs share` et `vserver cifs share properties` Commandes pour gérer les partages SMB.

Les fonctions que vous recherchez…	Utilisez cette commande…
Créez un partage SMB	`vserver cifs share create`
Affiche les partages SMB	`vserver cifs share show`
Modifiez un partage SMB	`vserver cifs share modify`
Supprime un partage SMB	`vserver cifs share delete`
Ajouter des propriétés de partage à un partage existant	`vserver cifs share properties add`
Supprimer les propriétés de partage d'un partage existant	`vserver cifs share properties remove`
Affiche des informations sur les propriétés de partage	`vserver cifs share properties show`

Consultez la page man pour chaque commande pour plus d'informations.

Sécurisez l'accès aux fichiers à l'aide des ACL de partage SMB

Directives pour la gestion des ACL de niveau partage SMB

Vous pouvez modifier les listes de contrôle d'accès au niveau du partage pour accorder aux utilisateurs plus ou moins de droits d'accès au partage. Vous pouvez configurer les listes de contrôle d'accès au niveau du partage en utilisant soit des utilisateurs et des groupes Windows, soit des utilisateurs et des groupes UNIX.

Après avoir créé un partage, par défaut, la liste de contrôle d'accès au niveau du partage donne un accès en lecture au groupe standard nommé Everyone. L'accès en lecture dans la liste de contrôle d'accès signifie que tous les utilisateurs du domaine et tous les domaines approuvés ont un accès en lecture seule au partage.

Vous pouvez modifier une liste de contrôle d'accès au niveau du partage en utilisant la console MMC (Microsoft Management Console) sur un client Windows ou la ligne de commande ONTAP.

Les directives suivantes s'appliquent lorsque vous utilisez la console MMC :

- Les noms d'utilisateur et de groupe spécifiés doivent être des noms Windows.
- Vous ne pouvez spécifier que des autorisations Windows.

Les consignes suivantes s'appliquent lorsque vous utilisez la ligne de commande ONTAP :

- Les noms d'utilisateur et de groupe spécifiés peuvent être des noms Windows ou UNIX.

  Si un type d'utilisateur et de groupe n'est pas spécifié lors de la création ou de la modification des listes de contrôle d'accès, le type par défaut est utilisateurs et groupes Windows.

- Vous ne pouvez spécifier que des autorisations Windows.

Créer des listes de contrôle d'accès pour le partage SMB

La configuration des autorisations de partage en créant des listes de contrôle d'accès (ACL) pour les partages SMB vous permet de contrôler le niveau d'accès à un partage pour les utilisateurs et les groupes.

Description de la tâche

Vous pouvez configurer les listes de contrôle d'accès au niveau du partage à l'aide des noms d'utilisateur ou de groupe Windows locaux ou de domaine ou des noms d'utilisateur ou de groupe UNIX.

Avant de créer une nouvelle liste de contrôle d'accès, vous devez supprimer la liste de contrôle d'accès de partage par défaut `Everyone / Full Control`, qui pose un risque pour la sécurité.

En mode Workgroup, le nom de domaine local est le nom du serveur SMB.

Étapes

1. Supprimez la liste de contrôle d'accès du partage par défaut : « vserver cifs share Access-control delete -vserver *vserver_name* -share *share_name* -user-or-group everyone »
2. Configurer la nouvelle liste de contrôle d'accès :

Si vous souhaitez configurer des listes de contrôle d'accès à l'aide d'un…	Entrez la commande…
Utilisateur Windows	`vserver cifs share access-control create -vserver` *`vserver_name`* `-share` *`share_name`* `-user-group-type windows -user-or-group` *`Windows_domain_name\user_name`* `-permission` *`access_right`*

Si vous souhaitez configurer des listes de contrôle d'accès à l'aide d'un…	Entrez la commande…
Groupe Windows	`vserver cifs share access-control create -vserver` *`vserver_name`* `-share` *`share_name`* `-user-group-type windows -user-or-group` *`Windows_domain_name\group_name`* `-permission` *`access_right`*
Utilisateur UNIX	`vserver cifs share access-control create -vserver` *`vserver_name`* `-share` *`share_name`* `-user-group-type` *`unix-user`* `-user-or-group` *`UNIX_user_name`* `-permission access_right`
Groupe UNIX	`vserver cifs share access-control create -vserver` *`vserver_name`* `-share` *`share_name`* `-user-group-type` *`unix-group`* `-user-or-group` *`UNIX_group_name`* `-permission access_right`

3. Vérifiez que la liste de contrôle d'accès appliquée au partage est correcte à l'aide de la `vserver cifs share access-control show` commande.

Exemple

La commande suivante donne `Change` Autorisations au groupe Windows "sales Team" pour la part "sales" sur le SVM "vs1.example.com":

```
cluster1::> vserver cifs share access-control create -vserver
vs1.example.com -share sales -user-or-group "DOMAIN\Sales Team"
-permission Change

cluster1::> vserver cifs share access-control show -vserver
vs1.example.com
                 Share       User/Group              User/Group  Access
Vserver          Name        Name                    Type
Permission
---------------- ----------- --------------------    ---------
-----------
vs1.example.com  c$          BUILTIN\Administrators  windows
Full_Control
vs1.example.com  sales       DOMAIN\Sales Team     windows     Change
```

La commande suivante donne `Read` Autorisation au groupe UNIX « ingénierie » pour la part « eng » sur le SVM « vs2.example.com » :

```
cluster1::> vserver cifs share access-control create -vserver
vs2.example.com -share eng -user-group-type unix-group -user-or-group
engineering -permission Read

cluster1::> vserver cifs share access-control show -vserver
vs2.example.com
                 Share       User/Group                User/Group  Access
Vserver          Name        Name                      Type
Permission
---------------- ----------- -------------------       -----------
-----------
vs2.example.com  c$          BUILTIN\Administrators    windows
Full_Control
vs2.example.com  eng         engineering               unix-group  Read
```

Les commandes suivantes fournissent `Change` L'autorisation au groupe Windows local nommé « Tiger Team » et `Full_Control` Autorisation à l'utilisateur Windows local nommé "rue Chang" pour le partage "vatavol5" sur le "SVM" "vs1":

```
cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vserver cifs share access-control show -vserver vs1
               Share       User/Group                   User/Group  Access
Vserver        Name        Name                         Type
Permission
-------------- ----------- --------------------------- -----------
-----------
vs1            c$          BUILTIN\Administrators      windows
Full_Control
vs1            datavol5    Tiger Team         windows     Change
vs1            datavol5    Sue Chang          windows     Full_Control
```

Commandes de gestion des listes de contrôle d'accès au partage SMB

Vous devez connaître les commandes de gestion des listes de contrôle d'accès (ACL) SMB, notamment leur création, leur affichage, leur modification et leur suppression.

Les fonctions que vous recherchez…	Utilisez cette commande…
Créer une nouvelle liste de contrôle d'accès	`vserver cifs share access-control create`
Afficher les ACL	`vserver cifs share access-control show`
Modifier une ACL	`vserver cifs share access-control modify`
Supprimer une ACL	`vserver cifs share access-control delete`

Sécurisez l'accès aux fichiers grâce aux autorisations liées aux fichiers

Configurez les autorisations de fichier NTFS avancées à l'aide de l'onglet sécurité de Windows

Vous pouvez configurer les autorisations de fichier NTFS standard sur les fichiers et les dossiers en utilisant l'onglet **sécurité Windows** de la fenêtre Propriétés Windows.

Avant de commencer

L'administrateur effectuant cette tâche doit disposer d'autorisations NTFS suffisantes pour modifier les autorisations sur les objets sélectionnés.

Description de la tâche

La configuration des autorisations de fichiers NTFS se fait sur un hôte Windows en ajoutant des entrées aux listes de contrôle d'accès discrétionnaire NTFS (DACL) associées à un descripteur de sécurité NTFS. Le descripteur de sécurité est ensuite appliqué aux fichiers et répertoires NTFS. Ces tâches sont traitées automatiquement par l'interface graphique de 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 le nom du serveur CIFS contenant le partage contenant les données auxquelles vous souhaitez appliquer les autorisations et le nom du partage.

   Si le nom de votre serveur CIFS est ""CIFS_SERVER"" et que votre partage est nommé "`hare1"", vous devez taper `\\CIFS_SERVER\share1`.

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

   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 souhaitez définir les autorisations de fichier NTFS.
4. Cliquez avec le bouton droit de la souris sur le fichier ou le répertoire, puis sélectionnez **Propriétés**.
5. Sélectionnez l'onglet **sécurité**.

   L'onglet **sécurité** affiche la liste des utilisateurs et des groupes pour lesquels les autorisations NTFS sont définies. La zone **autorisations pour** affiche une liste des autorisations Autoriser et refuser en vigueur pour chaque utilisateur ou groupe sélectionné.

6. Cliquez sur **Avancé**.

   La fenêtre Propriétés de Windows affiche des informations sur les autorisations de fichier existantes attribuées aux utilisateurs et aux groupes.

7. Cliquez sur **Modifier les autorisations**.

   La fenêtre autorisations s'ouvre.

8. Effectuez les opérations souhaitées :

Les fonctions que vous recherchez…	Procédez comme suit…
Configurez des autorisations NTFS avancées pour un nouvel utilisateur ou un nouveau groupe	a. Cliquez sur **Ajouter**. b. Dans la zone **Entrez le nom de l'objet à sélectionner**, saisissez le nom de l'utilisateur ou du groupe que vous souhaitez ajouter. c. Cliquez sur **OK**.
Modifiez les autorisations NTFS avancées d'un utilisateur ou d'un groupe	a. Dans la zone **permissions Entries:**, sélectionnez l'utilisateur ou le groupe dont vous souhaitez modifier les autorisations avancées. b. Cliquez sur **Modifier**.
Supprimez les autorisations NTFS avancées pour un utilisateur ou un groupe	a. Dans la zone **permissions Entries:**, sélectionnez l'utilisateur ou le groupe à supprimer. b. Cliquez sur **Supprimer**. c. Passez à l'étape 13.

   Si vous ajoutez des autorisations NTFS avancées sur un nouvel utilisateur ou un nouveau groupe ou si vous modifiez les autorisations avancées NTFS sur un utilisateur ou un groupe existant, la zone entrée d'autorisation de <objet> s'ouvre.

9. Dans la zone **appliquer à**, sélectionnez la façon dont vous souhaitez appliquer cette entrée d'autorisation de fichier NTFS.

   Si vous configurez des autorisations de fichier NTFS sur un seul fichier, la case **appliquer à** n'est pas active. Le paramètre **appliquer à** est défini par défaut sur **cet objet uniquement**.

10. Dans la zone **permissions**, sélectionnez les cases **Autoriser** ou **refuser** pour les autorisations avancées que vous souhaitez définir sur cet objet.
    - Pour autoriser l'accès spécifié, cochez la case **Autoriser**.
    - Pour ne pas autoriser l'accès spécifié, cochez la case **Deny**. Vous pouvez définir des autorisations sur les droits avancés suivants :
    - **Contrôle total**

      Si vous choisissez ce droit avancé, tous les autres droits avancés sont automatiquement choisis (autoriser ou refuser des droits).
    - **Dossier traverse / fichier d'exécution**
    - **Liste de dossiers / lecture de données**
    - **Lire les attributs**
    - **Lire les attributs étendus**
    - **Créer des fichiers / écrire des données**
    - **Créer des dossiers / ajouter des données**
    - **Ecrire des attributs**
    - **Ecrire des attributs étendus**
    - **Supprimer des sous-dossiers et des fichiers**
    - **Supprimer**
    - **Autorisations de lecture**
    - **Modifier les autorisations**
    - * Prendre possession*

      Si l'une des zones d'autorisation avancée n'est pas sélectionnable, c'est parce que les autorisations sont héritées de l'objet parent.
11. Si vous souhaitez que les sous-dossiers et les fichiers de cet objet héritent de ces autorisations, cochez la case **appliquer ces autorisations aux objets et/ou aux conteneurs dans ce conteneur uniquement**.
12. Cliquez sur **OK**.
13. Une fois que vous avez terminé d'ajouter, de supprimer ou de modifier des autorisations NTFS, spécifiez le paramètre d'héritage de cet objet :
    - Sélectionnez la case **inclure les autorisations héritables dans la boîte parent** de cet objet.

      Il s'agit de la valeur par défaut.
    - Sélectionnez la case **remplacer toutes les autorisations d'objet enfant par des autorisations héritables de cet objet**.

      Ce paramètre n'est pas présent dans la zone autorisations si vous définissez des autorisations de fichier NTFS sur un seul fichier.

> Soyez prudent lorsque vous sélectionnez ce paramètre. Ce paramètre supprime toutes les autorisations existantes sur tous les objets enfants et les remplace par les paramètres d'autorisation de cet objet. Vous pourriez supprimer par inadvertance les autorisations que vous ne souhaitez pas supprimer. Il est particulièrement important lorsque vous définissez des autorisations dans un volume mixte de style de sécurité ou qtree. Si les objets enfant ont un style de sécurité UNIX effectif, la propagation des autorisations NTFS à ces objets enfant entraîne le ONTAP changement de style de sécurité UNIX au style de sécurité NTFS, et toutes les autorisations UNIX sur ces objets enfants sont remplacées par des autorisations NTFS.

- Sélectionnez les deux cases.
- Sélectionnez aucune case.

14. Cliquez sur **OK** pour fermer la case **permissions**.
15. Cliquez sur **OK** pour fermer la case **Paramètres de sécurité avancés pour <objet>**.

    Pour plus d'informations sur la définition des autorisations NTFS avancées, consultez votre documentation Windows.

Informations associées

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

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

Affichage d'informations sur la sécurité des fichiers sur des volumes de style de sécurité UNIX

Configurez les autorisations d'accès aux fichiers NTFS à l'aide de l'interface de ligne de commande ONTAP

Vous pouvez configurer les autorisations d'accès aux fichiers NTFS sur les fichiers et les répertoires à l'aide de l'interface de ligne de commande ONTAP. Cela vous permet de configurer les autorisations d'accès aux fichiers NTFS sans avoir à vous connecter aux données à l'aide d'un partage SMB sur un client Windows.

Vous pouvez configurer les autorisations d'accès aux fichiers NTFS en ajoutant des entrées aux listes de contrôle d'accès discrétionnaire NTFS (DACL) associées à un descripteur de sécurité NTFS. Le descripteur de sécurité est ensuite appliqué aux fichiers et répertoires NTFS.

Vous ne pouvez configurer les autorisations de fichier NTFS qu'à l'aide de la ligne de commande. Vous ne pouvez pas configurer les listes de contrôle d'accès NFSv4 en utilisant l'interface de ligne de commandes.

Étapes

1. Créez un descripteur de sécurité NTFS.

```
vserver security file-directory ntfs create -vserver svm_name -ntfs-sd
ntfs_security_descriptor_name -owner owner_name -group primary_group_name
-control-flags-raw raw_control_flags
```

2. Ajoutez des listes de contrôle d'accès discrétionnaire au descripteur de sécurité NTFS.

   ```
   vserver security file-directory ntfs dacl add -vserver svm_name -ntfs-sd
   ntfs_security_descriptor_name -access-type {deny|allow} -account account_name
   -rights {no-access|full-control|modify|read-and-execute|read|write} -apply-to
   {this-folder|sub-folders|files}
   ```

3. Créez une stratégie de sécurité de fichiers/répertoires.

   ```
   vserver security file-directory policy create -vserver svm_name -policy-name
   policy_name
   ```

Comment les autorisations d'accès aux fichiers UNIX permettent de contrôler l'accès aux fichiers sur SMB

Un volume FlexVol peut avoir l'un des trois types de style de sécurité suivants : NTFS, UNIX ou mixte. Vous pouvez accéder aux données via SMB quel que soit le style de sécurité. Cependant, des autorisations appropriées sur les fichiers UNIX sont nécessaires pour accéder aux données à l'aide de la sécurité effective d'UNIX.

Lorsque vous accédez aux données via SMB, plusieurs contrôles d'accès sont utilisés pour déterminer si un utilisateur est autorisé à effectuer une action demandée :

- Droits d'exportation

  La configuration des autorisations d'exportation pour l'accès SMB est facultative.

- Partager les autorisations
- Autorisations liées aux fichiers

  Les types d'autorisations de fichier suivants peuvent être appliqués aux données sur lesquelles l'utilisateur souhaite effectuer une action :

  - NTFS
  - ACL UNIX NFSv4
  - Bits mode UNIX

Pour les données avec des ACL NFSv4 ou des bits de mode UNIX définis, les autorisations de style UNIX sont utilisées afin de déterminer les droits d'accès aux fichiers aux données. L'administrateur du SVM doit définir l'autorisation appropriée pour garantir que les utilisateurs disposent des droits nécessaires pour effectuer l'action souhaitée.

> Les données d'un volume de type sécurité mixte peuvent avoir un style de sécurité NTFS ou UNIX. Si les données ont un style de sécurité UNIX effectif, les autorisations NFSv4 ou les bits du mode UNIX sont utilisés pour déterminer les droits d'accès aux fichiers aux données.

Accès sécurisé aux fichiers à l'aide du contrôle d'accès dynamique (DAC)

Sécuriser l'accès aux fichiers à l'aide de la présentation du contrôle d'accès dynamique (DAC)

Vous pouvez sécuriser l'accès à l'aide du contrôle d'accès dynamique et en créant des stratégies d'accès centrales dans Active Directory et en les appliquant aux fichiers et dossiers sur les SVM via des objets de stratégie de groupe appliqués (GPO, Applied Group Policy Objects). Vous pouvez configurer l'audit de manière à utiliser les événements d'activation de stratégie d'accès central pour voir les effets des modifications apportées aux stratégies d'accès central avant de les appliquer.

Ajouts aux informations d'identification CIFS

Avant le contrôle d'accès dynamique, un identifiant CIFS incluait une identité de sécurité (de l'utilisateur) et une appartenance au groupe Windows. Avec le contrôle d'accès dynamique, trois autres types d'informations sont ajoutés à l'identité du périphérique, aux réclamations du périphérique et aux réclamations de l'utilisateur :

- Identité du périphérique

  Analogique des informations d'identité de l'utilisateur, à l'exception de l'identité et de l'appartenance au groupe de l'appareil à partir de lequel l'utilisateur se connecte.

- Réclamations de l'appareil

  Assertions sur un principal de sécurité de périphérique. Par exemple, un sinistre de périphérique peut être qu'il est membre d'une UO spécifique.

- Réclamations de l'utilisateur

  Assertions sur un principal de sécurité utilisateur. Par exemple, une réclamation d'utilisateur peut être que son compte AD est membre d'une unité d'organisation spécifique.

Politiques d'accès centralisé

Les stratégies d'accès centrales aux fichiers permettent aux organisations de déployer et de gérer de manière centralisée des stratégies d'autorisation qui incluent des expressions conditionnelles à l'aide de groupes d'utilisateurs, de revendications d'utilisateurs, de revendications de périphériques et de propriétés de ressources.

Par exemple, pour accéder aux données à fort impact sur l'entreprise, un utilisateur doit être un employé à plein temps et n'a accès qu'aux données à partir d'un périphérique géré. Les stratégies d'accès central sont définies dans Active Directory et distribuées aux serveurs de fichiers via le mécanisme GPO.

Mise en place centralisée des stratégies d'accès avec audit avancé

Les politiques d'accès central peuvent être « mises en service », auquel cas elles sont évaluées de manière « par quoi » lors des contrôles d'accès aux fichiers. Les résultats de ce qui se serait passé si la stratégie était en vigueur et la différence par rapport à ce qui est actuellement configuré sont consignés en tant qu'événement d'audit. De cette façon, les administrateurs peuvent utiliser les journaux d'événements d'audit pour étudier l'impact d'une modification de stratégie d'accès avant de mettre la stratégie en jeu. Après avoir évalué l'impact

d'une modification de règle d'accès, la règle peut être déployée via des GPO sur les SVM souhaités.

Informations associées

Stratégies de groupe prises en charge

Application d'objets de stratégie de groupe aux serveurs CIFS

Activation ou désactivation de la prise en charge de GPO sur un serveur CIFS

Affichage des informations sur les configurations GPO

Affichage d'informations sur les règles d'accès central

Affichage d'informations sur les règles de stratégie d'accès central

Configuration des règles d'accès centrales pour sécuriser les données sur les serveurs CIFS

Affichage d'informations sur la sécurité du contrôle d'accès dynamique

"Audit et suivi de sécurité SMB et NFS"

Prise en charge de la fonctionnalité de contrôle dynamique d'accès

Si vous souhaitez utiliser le contrôle d'accès dynamique (DAC) sur votre serveur CIFS, vous devez comprendre comment ONTAP prend en charge la fonctionnalité de contrôle d'accès dynamique dans les environnements Active Directory.

Pris en charge pour le contrôle d'accès dynamique

ONTAP prend en charge la fonctionnalité suivante lorsque le contrôle d'accès dynamique est activé sur le serveur CIFS :

Fonctionnalité	Commentaires
Réclamations dans le système de fichiers	Les revendications sont des paires de nom et de valeur simples qui indiquent une certaine vérité sur un utilisateur. Les informations d'identification utilisateur contiennent des informations sur les sinistres, et les descripteurs de sécurité sur les fichiers peuvent effectuer des vérifications d'accès qui incluent des vérifications de sinistres. Les administrateurs peuvent ainsi mieux contrôler qui peut accéder aux fichiers.
Expressions conditionnelles pour les vérifications d'accès aux fichiers	Lors de la modification des paramètres de sécurité d'un fichier, les utilisateurs peuvent ajouter des expressions conditionnelles arbitrairement complexes au descripteur de sécurité du fichier. L'expression conditionnelle peut inclure des vérifications pour les sinistres.

Fonctionnalité	Commentaires
Contrôle centralisé de l'accès aux fichiers via des règles d'accès centrales	Les stratégies d'accès central sont des types de listes de contrôle d'accès stockées dans Active Directory et peuvent être balisées vers un fichier. L'accès au fichier n'est accordé que si les contrôles d'accès du Security Descriptor sur disque et de la stratégie d'accès centrale balisée permettent l'accès.cela permet aux administrateurs de contrôler l'accès aux fichiers à partir d'un emplacement central (AD) sans avoir à modifier le Security Descriptor sur disque.
Mise en place de stratégies d'accès centrales	Ajoute la capacité d'essayer des changements de sécurité sans affecter l'accès réel aux fichiers, en "mettant en place" un changement aux politiques d'accès central, et en voyant l'effet de la modification dans un rapport d'audit.
Affichage d'informations sur la sécurité des règles d'accès centrales à l'aide de l'interface de ligne de commande de ONTAP	Étend le `vserver security file-directory show` commande pour afficher les informations sur les règles d'accès central appliquées.
Suivi de la sécurité qui inclut les stratégies d'accès centralisé	Étend le `vserver security trace` famille de commandes permettant d'afficher les résultats qui incluent des informations sur les stratégies d'accès central appliquées.

Non pris en charge pour le contrôle d'accès dynamique

ONTAP ne prend pas en charge la fonctionnalité suivante lorsque le contrôle d'accès dynamique est activé sur le serveur CIFS :

Fonctionnalité	Commentaires
Classification automatique des objets du système de fichiers NTFS	Il s'agit d'une extension de l'infrastructure de classification de fichiers Windows qui n'est pas prise en charge dans ONTAP.
Audit avancé autre que la mise en place de stratégies d'accès centrales	Seul le staging de stratégie d'accès central est pris en charge pour l'audit avancé.

Considérations relatives à l'utilisation du contrôle d'accès dynamique et des règles d'accès central avec des serveurs CIFS

Vous devez garder à l'esprit certaines considérations lorsque vous utilisez le contrôle d'accès dynamique (DAC) et les règles d'accès central pour sécuriser les fichiers et dossiers sur les serveurs CIFS.

L'accès NFS peut être refusé à la racine si la règle de stratégie s'applique à l'utilisateur de domaine\administrateur

Dans certaines circonstances, l'accès NFS à la racine peut être refusé lorsque la sécurité de la stratégie d'accès centrale est appliquée aux données auxquelles l'utilisateur root tente d'accéder. Le problème se produit lorsque la stratégie d'accès central contient une règle appliquée au domaine\administrateur et que le compte racine est mappé au compte domaine\administrateur.

Au lieu d'appliquer une règle à l'utilisateur domaine/administrateur, vous devez appliquer la règle à un groupe avec des privilèges d'administration, tels que le groupe domaine/administrateurs. De cette façon, vous pouvez mapper root sur le compte domaine\administrateur sans que ce problème n'ait d'impact sur la racine.

Le groupe BUILTIN\Administrators du serveur CIFS a accès aux ressources lorsque la stratégie d'accès central appliquée n'est pas trouvée dans Active Directory

Il est possible que les ressources contenues dans le serveur CIFS aient des règles d'accès centrales qui leur sont appliquées, mais lorsque le serveur CIFS utilise le SID de la stratégie d'accès centrale pour tenter de récupérer des informations à partir d'Active Directory, le SID ne correspond à aucun SID de stratégie d'accès centrale existant dans Active Directory. Dans ces circonstances, le serveur CIFS applique la stratégie de restauration par défaut locale pour cette ressource.

La stratégie de récupération par défaut locale permet au groupe BUILTIN\Administrators du serveur CIFS d'accéder à cette ressource.

Activer ou désactiver la présentation du contrôle d'accès dynamique

L'option qui vous permet d'utiliser le contrôle d'accès dynamique (DAC) pour sécuriser les objets sur votre serveur CIFS est désactivée par défaut. Vous devez activer cette option si vous souhaitez utiliser le contrôle d'accès dynamique sur votre serveur CIFS. Si vous décidez par la suite de ne pas utiliser le contrôle d'accès dynamique pour sécuriser les objets stockés sur le serveur CIFS, vous pouvez désactiver cette option.

Description de la tâche

Une fois le contrôle d'accès dynamique activé, le système de fichiers peut contenir des listes de contrôle d'accès avec des entrées liées au contrôle d'accès dynamique. Si le contrôle d'accès dynamique est désactivé, les entrées de contrôle d'accès dynamique actuelles seront ignorées et les nouvelles ne seront pas autorisées.

Cette option n'est disponible qu'au niveau de privilège avancé.

Étape

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Effectuez l'une des opérations suivantes :

Si vous voulez que le contrôle d'accès dynamique soit…	Entrez la commande…
Activé	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled true`

Désactivé	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled false`

3. Revenir au niveau de privilège administrateur : `set -privilege admin`

Informations associées

Configuration des règles d'accès centrales pour sécuriser les données sur les serveurs CIFS

Gérer les listes de contrôle d'accès qui contiennent des ACE de contrôle d'accès dynamique lorsque le contrôle d'accès dynamique est désactivé

Si vous disposez de ressources dont les listes de contrôle d'accès sont appliquées avec les ACE de contrôle d'accès dynamique et que vous désactivez le contrôle d'accès dynamique sur la machine virtuelle de stockage (SVM), vous devez supprimer les ACE de contrôle d'accès dynamique avant de pouvoir gérer les ACE de contrôle d'accès non dynamique sur cette ressource.

Description de la tâche

Une fois le contrôle d'accès dynamique désactivé, vous ne pouvez pas supprimer les ACE existants de contrôle d'accès non dynamique ou ajouter de nouveaux ACE de contrôle d'accès non dynamique tant que vous n'avez pas supprimé les ACE de contrôle d'accès dynamique existants.

Vous pouvez utiliser n'importe quel outil que vous utilisez normalement pour gérer les listes de contrôle d'accès pour effectuer ces étapes.

Étapes

1. Déterminez quels ACE de contrôle d'accès dynamique sont appliqués à la ressource.
2. Supprimez les ACE de contrôle d'accès dynamique de la ressource.
3. Ajoutez ou supprimez des ACE de contrôle d'accès non dynamiques comme vous le souhaitez de la ressource.

Configurez les règles d'accès centrales pour sécuriser les données sur les serveurs CIFS

Il existe plusieurs étapes à suivre pour sécuriser l'accès aux données sur le serveur CIFS à l'aide de stratégies d'accès centrales, notamment l'activation du contrôle d'accès dynamique (DAC) sur le serveur CIFS, la configuration de stratégies d'accès central dans Active Directory, l'application des règles d'accès central aux conteneurs Active Directory avec des GPO, Et activation des stratégies de groupe sur le serveur CIFS.

Avant de commencer

- L'Active Directory doit être configuré pour utiliser les stratégies d'accès central.
- Vous devez disposer d'un accès suffisant sur les contrôleurs de domaine Active Directory pour créer des stratégies d'accès centrales et pour créer et appliquer des GPO aux conteneurs contenant les serveurs CIFS.
- Vous devez disposer d'un accès administratif suffisant sur le SVM (Storage Virtual machine) pour exécuter les commandes nécessaires.

Description de la tâche

Les stratégies d'accès central sont définies et appliquées aux objets de stratégie de groupe (GPO, Group Policy Objects) d'Active Directory. Vous pouvez consulter la bibliothèque Microsoft TechNet pour obtenir des instructions sur la configuration des stratégies d'accès centralisé et des GPO.

"Bibliothèque Microsoft TechNet"

Étapes

1. Activer le contrôle dynamique d'accès sur le SVM si celui-ci n'est pas déjà activé à l'aide de `vserver cifs options modify` commande.

   ```
   vserver cifs options modify -vserver vs1 -is-dac-enabled true
   ```

2. Activez les objets de stratégie de groupe (GPO, Group policy objects) sur le serveur CIFS s'ils ne sont pas déjà activés à l'aide de l' `vserver cifs group-policy modify` commande.

   ```
   vserver cifs group-policy modify -vserver vs1 -status enabled
   ```

3. Créez des règles d'accès centrales et des stratégies d'accès central sur Active Directory.
4. Créez un objet de stratégie de groupe (GPO) pour déployer les stratégies d'accès central sur Active Directory.
5. Appliquez l'objet GPO au conteneur où se trouve le compte d'ordinateur du serveur CIFS.
6. Mettre à jour manuellement les GPO appliqués au serveur CIFS à l'aide de `vserver cifs group-policy update` commande.

   ```
   vserver cifs group-policy update -vserver vs1
   ```

7. Vérifiez que la stratégie d'accès central GPO est appliquée aux ressources du serveur CIFS à l'aide de `vserver cifs group-policy show-applied` commande.

   L'exemple suivant montre que la stratégie de domaine par défaut comporte deux stratégies d'accès central appliquées au serveur CIFS :

   ```
   vserver cifs group-policy show-applied
   ```

   ```
   Vserver: vs1
   ----------------------------
       GPO Name: Default Domain Policy
          Level: Domain
         Status: enabled
     Advanced Audit Settings:
         Object Access:
             Central Access Policy Staging: failure
     Registry Settings:
         Refresh Time Interval: 22
         Refresh Random Offset: 8
         Hash Publication Mode for BranchCache: per-share
         Hash Version Support for BranchCache: all-versions
     Security Settings:
   ```

```
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2

  GPO Name: Resultant Set of Policy
     Level: RSOP
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
```

```
        File Security:
            /vol1/home
            /vol1/dir1
        Kerberos:
            Max Clock Skew: 5
            Max Ticket Age: 10
            Max Renew Age:  7
        Privilege Rights:
            Take Ownership: usr1, usr2
            Security Privilege: usr1, usr2
            Change Notify: usr1, usr2
        Registry Values:
            Signing Required: false
        Restrict Anonymous:
            No enumeration of SAM accounts: true
            No enumeration of SAM accounts and shares: false
            Restrict anonymous access to shares and named pipes: true
            Combined restriction for anonymous user: no-access
        Restricted Groups:
            gpr1
            gpr2
  Central Access Policy Settings:
        Policies: cap1
                  cap2
2 entries were displayed.
```

Informations associées

Affichage des informations sur les configurations GPO

Affichage d'informations sur les règles d'accès central

Affichage d'informations sur les règles de stratégie d'accès central

Activation ou désactivation du contrôle d'accès dynamique

Afficher des informations sur la sécurité du contrôle d'accès dynamique

Vous pouvez afficher des informations sur la sécurité DAC (Dynamic Access Control) sur des volumes NTFS et sur des données avec la sécurité efficace NTFS sur des volumes de type sécurité mixtes. Cela comprend de l'information sur les ACE conditionnels, les ACE de ressources et les ACE de politique d'accès central. 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.

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	`vserver security file-directory show -vserver vserver_name -path path`
Avec détails étendus	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`
Où la sortie est affichée avec les SID de groupe et d'utilisateur	`vserver security file-directory show -vserver vserver_name -path path -lookup-names false`
A propos de la sécurité des fichiers et des répertoires pour les fichiers et les répertoires où le masque binaire hexadécimal est traduit en format texte	`vserver security file-directory show -vserver vserver_name -path path -textual-mask true`

Exemples

L'exemple suivant affiche les informations de sécurité du contrôle d'accès dynamique sur le chemin `/vol1` Au SVM vs1 :

```
cluster1::> vserver security file-directory show -vserver vs1 -path /vol1
                           Vserver: vs1
                         File Path: /vol1
                  File Inode Number: 112
                     Security Style: mixed
                    Effective Style: ntfs
                     DOS Attributes: 10
             DOS Attributes in Text: ----D---
             Expanded Dos Attribute: -
                       Unix User Id: 0
                      Unix Group Id: 1
                     Unix Mode Bits: 777
             Unix Mode Bits in Text: rwxrwxrwx
                               ACLs: NTFS Security Descriptor
                                     Control:0xbf14
                                     Owner:CIFS1\Administrator
                                     Group:CIFS1\Domain Admins
                                     SACL - ACEs
                                        ALL-Everyone-0xf01ff-OI|CI|SA|FA
                                        RESOURCE ATTRIBUTE-Everyone-0x0

("Department_MS",TS,0x10020,"Finance")
                                        POLICY ID-All resources - No Write-
0x0-OI|CI
                                     DACL - ACEs
                                        ALLOW-CIFS1\Administrator-0x1f01ff-
OI|CI
                                        ALLOW-Everyone-0x1f01ff-OI|CI
                                        ALLOW CALLBACK-DAC\user1-0x1200a9-
OI|CI

((@User.department==@Resource.Department_MS&&@Resource.Impact_MS>1000)&&@D
evice.department==@Resource.Department_MS)
```

Informations associées

Affichage des informations sur les configurations GPO

Affichage d'informations sur les règles d'accès central

Affichage d'informations sur les règles de stratégie d'accès central

Considérations relatives au contrôle d'accès dynamique

Vous devez savoir ce qui se passe lors du retour à une version de ONTAP qui ne prend pas en charge le contrôle d'accès dynamique (DAC) et ce que vous devez faire avant et après le rétablissement.

Si vous souhaitez restaurer le cluster vers une version de ONTAP qui ne prend pas en charge le contrôle d'accès dynamique et que le contrôle d'accès dynamique est activé sur une ou plusieurs machines virtuelles de stockage (SVM), vous devez effectuer les opérations suivantes avant le rétablissement :

- Vous devez désactiver le contrôle d'accès dynamique sur tous les SVM sur lesquels il est activé sur le cluster.
- Vous devez modifier toutes les configurations d'audit sur le cluster contenant le `cap-staging` type d'événement pour utiliser uniquement le `file-op` type d'événement.

Vous devez comprendre et agir sur certaines considérations importantes concernant la restauration des fichiers et dossiers avec les ACE Dynamic Access Control :

- Si le cluster est rétabli, les ACE de contrôle d'accès dynamique existants ne sont pas supprimés ; cependant, ils seront ignorés lors des vérifications d'accès aux fichiers.
- Comme les ACE de contrôle d'accès dynamique sont ignorés après réversion, l'accès aux fichiers change sur les fichiers avec les ACE de contrôle d'accès dynamique.

  Cela pourrait permettre aux utilisateurs d'accéder aux fichiers qu'ils ne pouvaient pas accéder ou ne pouvaient pas accéder aux fichiers qu'ils pouvaient auparavant.

- Vous devez appliquer des ACE de contrôle d'accès non dynamique aux fichiers concernés pour restaurer leur niveau de sécurité précédent.

  Cette opération peut être effectuée avant le rétablissement ou immédiatement après la fin de la nouvelle version.

> Les ACE de contrôle d'accès dynamique étant ignorés après la réversion, il n'est pas nécessaire de les supprimer lors de l'application d'ACE de contrôle d'accès non dynamique aux fichiers affectés. Toutefois, si vous le souhaitez, vous pouvez les supprimer manuellement.

Où trouver des informations supplémentaires sur la configuration et l'utilisation du contrôle d'accès dynamique et des stratégies d'accès central

Des ressources supplémentaires sont disponibles pour vous aider à configurer et utiliser le contrôle d'accès dynamique et les stratégies d'accès central.

Vous trouverez des informations sur la configuration des stratégies de contrôle d'accès dynamique et d'accès central dans Active Directory dans la bibliothèque Microsoft TechNet.

"Microsoft TechNet : présentation des scénarios de contrôle d'accès dynamique"

"Microsoft TechNet : scénario de stratégie d'accès centralisé"

Les références suivantes peuvent vous aider à configurer le serveur SMB afin qu'il utilise et prend en charge les stratégies de contrôle d'accès dynamique et d'accès central :

- **Utilisation de stratégies de groupe sur le serveur SMB**

  Application d'objets de stratégie de groupe aux serveurs SMB

- **Configuration de l'audit NAS sur le serveur SMB**

"Audit et suivi de sécurité SMB et NFS"

Sécurisez l'accès SMB à l'aide de règles d'exportation

Mode d'utilisation des export-policy avec les accès SMB

Si les export policy pour accès SMB sont activées sur le serveur SMB, les export policies sont utilisées lors du contrôle de l'accès aux volumes du SVM par les clients SMB. Pour accéder aux données, vous pouvez créer une export policy qui autorise l'accès SMB, puis associer la policy aux volumes contenant des partages SMB.

Une export policy applique une ou plusieurs règles qui lui permettent de spécifier les clients autorisés à accéder aux données et les protocoles d'authentification pris en charge pour l'accès en lecture seule et en lecture/écriture. Vous pouvez configurer des stratégies d'exportation afin d'autoriser l'accès via SMB à tous les clients, à un sous-réseau de clients ou à un client spécifique et autoriser l'authentification à l'aide de l'authentification Kerberos, de l'authentification NTLM ou des deux authentifications Kerberos et NTLM lors de la détermination de l'accès en lecture seule et en lecture/écriture aux données.

Après le traitement de toutes les règles d'exportation appliquées à l'export policy, ONTAP peut déterminer si le client dispose d'un accès et quel niveau d'accès. Les règles d'exportation s'appliquent aux ordinateurs clients et non aux utilisateurs et groupes Windows. Les règles d'exportation ne remplacent pas l'authentification et l'autorisation basées sur les utilisateurs et les groupes Windows. Les règles d'exportation offrent une autre couche de sécurité d'accès en plus des autorisations de partage et d'accès aux fichiers.

Vous associez exactement une export policy à chaque volume pour configurer l'accès client au volume. Chaque SVM peut contenir plusieurs export policy. Vous pouvez ainsi effectuer les opérations suivantes pour les SVM avec plusieurs volumes :

- Assigner différentes export policy à chaque volume du SVM pour le contrôle d'accès client individuel à chaque volume du SVM.
- Assigner la même export policy à plusieurs volumes du SVM pour un contrôle d'accès client identique sans avoir à créer de nouvelles export policy pour chaque volume.

Chaque SVM possède au moins une export policy appelée « default », qui ne contient aucune règle. Vous ne pouvez pas supprimer cette export-policy, mais vous pouvez la renommer ou la modifier. Par défaut, chaque volume du SVM est associé aux export policy par défaut. Si les export policy pour accès SMB sont désactivées sur le SVM, la « default » export policy n'a aucun impact sur l'accès SMB.

Vous pouvez configurer les règles fournissant l'accès aux hôtes NFS et SMB et associer cette règle à une export policy, qui peut ensuite être associée au volume qui contient des données auxquelles les hôtes NFS et SMB ont besoin d'accéder. Alternativement, s'il existe des volumes dans lesquels seuls les clients SMB ont besoin d'accéder, vous pouvez configurer une export policy avec des règles qui autorisent uniquement l'accès à l'aide du protocole SMB et qui utilisent uniquement Kerberos ou NTLM (ou les deux) pour l'authentification en lecture seule et l'accès en écriture. L'export policy est ensuite associée aux volumes pour lesquels seul l'accès SMB est souhaité.

Si les export policy pour SMB sont activées et qu'un client effectue une demande d'accès qui n'est pas autorisée par les export policy applicables, la requête échoue et un message d'autorisation refusée. Si un client ne correspond à aucune règle de l'export policy du volume, l'accès est refusé. Si une export policy est vide, alors tous les accès sont implicitement refusés. Ceci est vrai même si les autorisations de partage et de fichier autorisent autrement l'accès. Cela signifie que vous devez configurer votre export policy de manière à limiter les possibilités suivantes sur les volumes contenant des partages SMB :

- Autoriser l'accès à tous les clients ou au sous-ensemble de clients approprié
- Autoriser l'accès via SMB
- Autoriser un accès en lecture seule et en écriture approprié via l'authentification Kerberos ou NTLM (ou les deux)

Découvrez "configuration et gestion des export-policies".

Fonctionnement des règles d'exportation

Les règles d'exportation sont les éléments fonctionnels d'une export-policy. Les règles d'exportation correspondent aux demandes d'accès client à un volume par rapport à des paramètres spécifiques que vous configurez pour déterminer comment traiter les demandes d'accès client.

Une export-policy doit contenir au moins une règle d'exportation pour permettre l'accès aux clients. Si une export-policy contient plusieurs règles, celles-ci sont traitées dans l'ordre dans lequel elles apparaissent dans l'export-policy. L'ordre des règles est dicté par le numéro d'index des règles. Si une règle correspond à un client, les autorisations de cette règle sont utilisées et aucune autre règle n'est traitée. Si aucune règle ne correspond, l'accès au client est refusé.

Vous pouvez configurer des règles d'exportation pour déterminer les autorisations d'accès client à l'aide des critères suivants :

- Protocole d'accès aux fichiers utilisé par le client envoyant la requête, par exemple, NFSv4 ou SMB.
- Identifiant client, par exemple, nom d'hôte ou adresse IP.

  La taille maximale du `-clientmatch` le champ est composé de 4096 caractères.

- Type de sécurité utilisé par le client pour l'authentification, par exemple Kerberos v5, NTLM ou AUTH_SYS.

Si une règle spécifie plusieurs critères, le client doit tous les correspondre pour que la règle s'applique.

Exemple

La export policy contient une règle d'exportation avec les paramètres suivants :

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

La requête d'accès client est envoyée à l'aide du protocole NFSv3 et le client a l'adresse IP 10.1.17.37.

Bien que le protocole d'accès client corresponde, l'adresse IP du client se trouve dans un sous-réseau différent de celui spécifié dans la règle d'exportation. Par conséquent, la correspondance des clients échoue et cette règle ne s'applique pas à ce client.

Exemple

La export policy contient une règle d'exportation avec les paramètres suivants :

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

La requête d'accès client est envoyée via le protocole NFSv4 et le client a l'adresse IP 10.1.16.54.

Le protocole d'accès client correspond et l'adresse IP du client se trouve dans le sous-réseau spécifié. Par conséquent, la correspondance du client a réussi et cette règle s'applique à ce client. Le client obtient un accès en lecture-écriture quel que soit son type de sécurité.

Exemple

La export policy contient une règle d'exportation avec les paramètres suivants :

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`

Le client #1 a l'adresse IP 10.1.16.207, envoie une demande d'accès à l'aide du protocole NFSv3 et est authentifié avec Kerberos v5.

Le client #2 a l'adresse IP 10.1.16.211, envoie une demande d'accès à l'aide du protocole NFSv3 et est authentifié avec AUTH_SYS.

Le protocole d'accès client et l'adresse IP correspondent pour les deux clients. Le paramètre en lecture seule permet l'accès en lecture seule à tous les clients, quel que soit le type de sécurité auquel ils sont authentifiés. Par conséquent, les deux clients bénéficient d'un accès en lecture seule. Cependant, seul le client #1 obtient l'accès en lecture-écriture car il a utilisé le type de sécurité approuvé Kerberos v5 pour s'authentifier. Le client n° 2 ne dispose pas d'un accès en lecture/écriture.

Exemples de règles d'export-policy qui limitent ou autorisent l'accès à SMB

Les exemples montrent comment créer des règles d'export policy qui limitent ou autorisent l'accès via SMB sur un SVM dont les export policy pour l'accès SMB sont activées.

Les export policy pour accès SMB sont désactivées par défaut. Vous devez configurer des règles d'export policy qui limitent ou autorisent l'accès sur SMB uniquement si vous avez activé les export policy pour l'accès SMB.

Règle d'exportation pour l'accès SMB uniquement

La commande suivante crée une règle d'exportation sur le SVM nommé « vs1 » qui dispose de la configuration suivante :

- Nom de la politique: Cifs1
- Numéro d'index : 1
- Correspondance client : correspond uniquement aux clients sur le réseau 192.168.1.0/24

- Protocole : autorise uniquement l'accès SMB
- Accès en lecture seule : aux clients utilisant l'authentification NTLM ou Kerberos
- Accès en lecture/écriture : aux clients utilisant l'authentification Kerberos

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifs1 -ruleindex 1 -protocol cifs -clientmatch 192.168.1.0/255.255.255.0
-rorule krb5,ntlm -rwrule krb5
```

Règle d'exportation pour les accès SMB et NFS

La commande suivante crée une règle d'exportation sur le SVM nommé « vs1 », qui dispose de la configuration suivante :

- Nom de la politique: Cifs1
- Numéro d'index : 2
- Correspondance client : correspond à tous les clients
- Protocole : accès SMB et NFS
- Accès en lecture seule : pour tous les clients
- Accès en lecture/écriture : aux clients utilisant l'authentification Kerberos (NFS et SMB) ou NTLM (SMB)
- Mappage de l'ID utilisateur UNIX 0 (zéro) : mappé à l'ID utilisateur 65534 (qui correspond généralement au nom utilisateur personne)
- L'accès SUID et sgID permet

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifsnfs1 -ruleindex 2 -protocol cifs,nfs -clientmatch 0.0.0.0/0 -rorule any
-rwrule krb5,ntlm -anon 65534 -allow-suid true
```

Règle d'exportation pour accès SMB uniquement à l'aide de NTLM

La commande suivante crée une règle d'exportation sur le SVM nommé « vs1 » qui dispose de la configuration suivante :

- Nom de la stratégie : ntlm1
- Numéro d'index : 1
- Correspondance client : correspond à tous les clients
- Protocole : autorise uniquement l'accès SMB
- Accès en lecture seule : uniquement aux clients utilisant NTLM
- Accès en lecture/écriture : uniquement aux clients utilisant NTLM

Si vous configurez l'option lecture seule ou l'option lecture/écriture pour l'accès NTLM uniquement, vous devez utiliser des entrées basées sur l'adresse IP dans l'option de correspondance client. Autrement, vous recevez `access denied` erreurs. En effet, ONTAP utilise les noms de service Kerberos (SPN) lors de l'utilisation d'un nom d'hôte pour vérifier les droits d'accès du client. L'authentification NTLM ne prend pas en charge les noms SPN.

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
ntlm1 -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule ntlm
-rwrule ntlm
```

Activez ou désactivez les export policy pour l'accès SMB

Vous pouvez activer ou désactiver les export policy pour l'accès SMB sur les SVM (Storage Virtual machines). L'utilisation des règles d'exportation pour contrôler l'accès SMB aux ressources est facultative.

Avant de commencer

Les conditions suivantes sont requises pour l'activation des export policy pour SMB :

- Le client doit avoir un enregistrement « PTR » dans DNS avant de créer les règles d'exportation pour ce client.
- Un ensemble supplémentaire d'enregistrements « A » et « PTR » pour les noms d'hôte est nécessaire si la SVM fournit l'accès aux clients NFS et que le nom d'hôte que vous souhaitez utiliser pour l'accès NFS est différent du nom du serveur CIFS.

Description de la tâche

Lors de la configuration d'un nouveau serveur CIFS sur votre SVM, l'utilisation des export policies pour l'accès SMB est désactivée par défaut. Vous pouvez activer des export policy pour l'accès SMB si vous souhaitez contrôler l'accès en fonction du protocole d'authentification, des adresses IP clientes ou des noms d'hôte. Vous pouvez activer ou désactiver des export policy pour l'accès SMB à tout moment.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Activer ou désactiver les export-policies :
   - Activer les export-policies : `vserver cifs options modify -vserver` *`vserver_name`* `-is -exportpolicy-enabled true`
   - Désactiver les export-policies : `vserver cifs options modify -vserver` *`vserver_name`* `-is -exportpolicy-enabled false`
3. Retour au niveau de privilège admin : `set -privilege admin`

Exemple

L'exemple suivant permet d'utiliser les export policy pour contrôler l'accès des clients SMB aux ressources sur le SVM vs1 :

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-exportpolicy
-enabled true

cluster1::*> set -privilege admin
```

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

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

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

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

Comportement de la protection d'accès au niveau du stockage

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

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

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

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

  - Sécurité des fichiers

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

  - Sécurité de l'annuaire

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

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

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

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

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

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

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

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

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

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

Ordre des contrôles d'accès

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

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

Cas d'utilisation de Storage-Level Access Guard

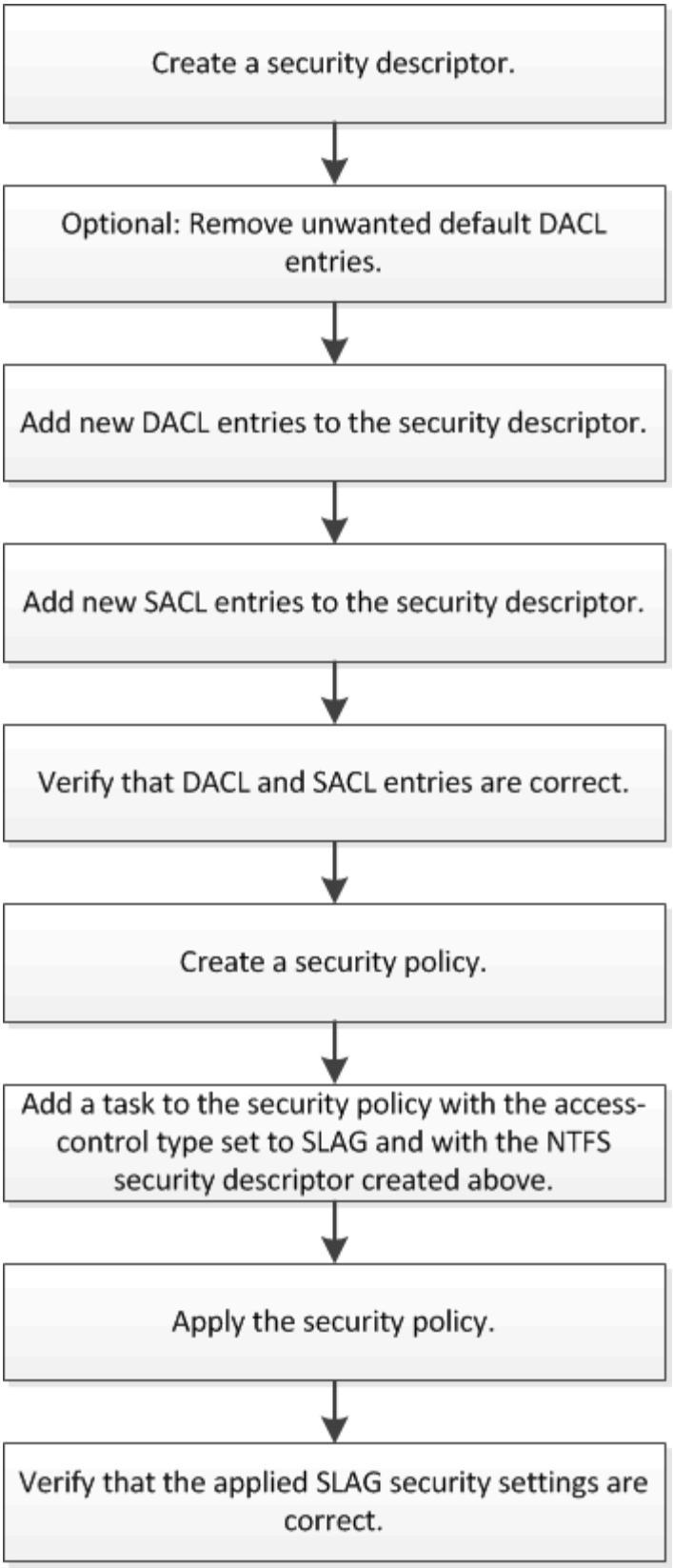
Storage-Level Access Guard fournit une sécurité supplémentaire au niveau du stockage, qui n'est pas visible du côté client. Par conséquent, il ne peut être révoqué par aucun des utilisateurs ou administrateurs de leur poste de travail. Dans certains cas, il est préférable de pouvoir contrôler l'accès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

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

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

Workflow de configuration de Storage-Level Access Guard

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



Informations associées

Configuration de Storage-Level Access Guard

Configurer Storage-Level Access Guard

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

Étapes

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

   `vserver security file-directory ntfs create -vserver vs1 -ntfs-sd sd1` `vserver security file-directory ntfs show -vserver vs1`

   ```
   Vserver: vs1

      NTFS Security    Owner Name
      Descriptor Name
      ------------     --------------
      sd1              -
   ```

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

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       BUILTIN\Administrators
                        allow    full-control   this-folder, sub-folders,
   files
       BUILTIN\Users    allow    full-control   this-folder, sub-folders,
   files
       CREATOR OWNER    allow    full-control   this-folder, sub-folders,
   files
       NT AUTHORITY\SYSTEM
                        allow    full-control   this-folder, sub-folders,
   files
   ```

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

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

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

   Dans cet exemple, trois ACE DACL par défaut sont supprimés du descripteur de sécurité : BUILTIN\Administrators, BULTIN\Users et CRÉATEUR OWNER.

   ```
   vserver security file-directory ntfs dacl remove -vserver vs1 -ntfs-sd sd1
   -access-type allow -account builtin\users vserver security file-directory
   ntfs dacl remove -vserver vs1 -ntfs-sd sd1 -access-type allow -account
   builtin\administrators vserver security file-directory ntfs dacl remove
   -vserver vs1 -ntfs-sd sd1 -access-type allow -account "creator owner"
   ```

b. Vérifiez que les ACE DACL que vous ne souhaitez pas utiliser pour la sécurité Storage-Level Access Guard sont supprimés du descripteur de sécurité à l'aide de `vserver security file-directory ntfs dacl show` commande.

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

   ```
   vserver security file-directory ntfs dacl show -vserver vs1
   ```

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    NT AUTHORITY\SYSTEM
                     allow    full-control   this-folder, sub-folders,
files
```

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

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

   ```
   vserver security file-directory ntfs dacl add -vserver vs1 -ntfs-sd sd1
   -access-type allow -account example\engineering -rights full-control -apply-to
   this-folder,sub-folders,files vserver security file-directory ntfs dacl add
   -vserver vs1 -ntfs-sd sd1 -access-type allow -account "example\Domain Users"
   -rights read -apply-to this-folder,sub-folders,files
   ```

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

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

   ```
   vserver security file-directory ntfs sacl add -vserver vs1 -ntfs-sd sd1
   -access-type failure -account "example\Domain Users" -rights read -apply-to
   ```

```
this-folder,sub-folders,files vserver security file-directory ntfs sacl add
-vserver vs1 -ntfs-sd sd1 -access-type success -account example\engineering
-rights full-control -apply-to this-folder,sub-folders,files
```

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

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

   ```
   vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
   ```

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       EXAMPLE\Domain Users
                        allow    read           this-folder, sub-folders,
   files
       EXAMPLE\engineering
                        allow    full-control   this-folder, sub-folders,
   files
       NT AUTHORITY\SYSTEM
                        allow    full-control   this-folder, sub-folders,
   files
   ```

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

   ```
   vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
   ```

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       EXAMPLE\Domain Users
                        failure  read           this-folder, sub-folders,
   files
       EXAMPLE\engineering
                        success  full-control   this-folder, sub-folders,
   files
   ```

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

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

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

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

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

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

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

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

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

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name
   policy1 -path /datavol1 -access-control slag -security-type ntfs -ntfs-mode
   propagate -ntfs-sd sd1
   ```

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

   ```
   vserver security file-directory policy task show -vserver vs1 -policy-name
   policy1
   ```

```
 Vserver: vs1
  Policy: policy1

   Index  File/Folder  Access           Security  NTFS       NTFS
Security
          Path         Control          Type      Mode       Descriptor
Name
   -----  -----------  ---------------  --------  ----------
---------------
   1      /datavol1    slag             ntfs      propagate  sd1
```

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

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

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

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

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

    ```
    vserver security file-directory show -vserver vs1 -path /datavol1
    ```

```
                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


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

Informations associées

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

Workflow de configuration de Storage-Level Access Guard

Affichage d'informations sur Storage-Level Access Guard

Retrait de Storage-Level Access Guard

Matrice de SCORIES efficace

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

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

Afficher des informations sur Storage-Level Access Guard

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

sécurité de Storage-Level Access Guard, que vous pouvez utiliser pour valider votre configuration ou pour résoudre les problèmes d'accès aux fichiers.

Description de la tâche

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

Étape

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

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

Exemples

L'exemple suivant présente les informations de sécurité Storage-Level Access Guard pour le volume de style de sécurité NTFS avec le chemin d'accès `/datavol1` Au SVM vs1 :

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

                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


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

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

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5
                Vserver: vs1
              File Path: /datavol5
      File Inode Number: 3374
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
                   ACLs: Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Retirez la protection d’accès au niveau du stockage

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

Étapes

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

   ```
   vserver security file-directory show -vserver vs1 -path /datavol2
   ```

```
                Vserver: vs1
              File Path: /datavol2
      File Inode Number: 99
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xbf14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI

                         Storage-Level Access Guard security
                         DACL (Applies to Directories):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         DACL (Applies to Files):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

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

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

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

   ```
   vserver security file-directory show -vserver vs1 -path /datavol2
   ```

```
                Vserver: vs1
              File Path: /datavol2
      File Inode Number: 99
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xbf14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI
```