Gestion de SMB avec l'interface de ligne de commandes

ONTAP 9

NetApp
April 24, 2024

Sommaire

Gestion de SMB avec l'interface de ligne de commandes

Présentation des références SMB

Les fonctionnalités d'accès aux fichiers ONTAP sont disponibles pour le protocole SMB. Vous pouvez activer un serveur CIFS, créer des partages et activer les services Microsoft.

> *SMB* (Server message Block) désigne les dialectes modernes du protocole CIFS (Common Internet File System). Vous verrez toujours *CIFS* dans l'interface de ligne de commande (CLI) ONTAP et dans les outils de gestion OnCommand.

Vous devez utiliser ces procédures dans les circonstances suivantes :

- Vous souhaitez connaître la plage de fonctionnalités du protocole SMB de ONTAP.
- Vous souhaitez effectuer des tâches de configuration et de maintenance moins courantes, et non pas une configuration SMB de base.
- Vous souhaitez utiliser l'interface de ligne de commande et non System Manager, ni un outil de création de scripts automatisé.

Prise en charge du serveur SMB

Présentation de la prise en charge du serveur SMB

Vous pouvez activer et configurer des serveurs SMB sur des SVM (Storage Virtual machines) pour que les clients SMB puissent accéder aux fichiers du cluster.

- Chaque SVM de données du cluster peut être lié à un domaine Active Directory exactement.
- Les SVM de données n'ont pas besoin d'être liés au même domaine.
- Plusieurs SVM peuvent être liés au même domaine.

Vous devez configurer les SVM et les LIF que vous utilisez pour transmettre des données avant de pouvoir créer un serveur SMB. Si votre réseau de données n'est pas stable, vous devrez peut-être aussi configurer les IPspaces, les domaines de diffusion et les sous-réseaux. Le *Network Management Guide* contient des détails.

Informations associées

"Gestion du réseau"

Modifier les serveurs SMB

"Administration du système"

Fonctionnalités et versions SMB prises en charge

Server message Block (SMB) est un protocole de partage de fichiers distant utilisé par les clients et les serveurs Microsoft Windows. Dans ONTAP 9, toutes les versions SMB

sont prises en charge, mais la prise en charge par défaut de SMB 1.0 dépend de votre version ONTAP. Vérifiez que le serveur ONTAP SMB prend en charge les clients et les fonctionnalités requis dans votre environnement.

Les dernières informations sur les clients SMB et les contrôleurs de domaine pris en charge par ONTAP sont disponibles dans l'outil *Interoperability Matrix Tool*.

SMB 2.0 et les versions ultérieures sont activées par défaut pour les serveurs SMB ONTAP 9 et peuvent être activées ou désactivées selon les besoins. Le tableau suivant présente le support SMB 1.0 et la configuration par défaut.

Fonctionnalité SMB 1.0 :	**Dans ces versions ONTAP 9 :**			
	9.0	9.1	9.2	9.3 et versions ultérieures
Est activé par défaut	Oui.	Oui.	Oui.	Non
Peut être activé ou désactivé	Non	Oui*9.1 P8 ou ultérieur requis.	Oui.	Oui.

Les paramètres par défaut des connexions SMB 1.0 et 2.0 aux contrôleurs de domaine dépendent également de la version de ONTAP. Pour plus d'informations, consultez le `vserver cifs security modify` page de manuel. Pour les environnements avec des serveurs CIFS existants exécutant SMB 1.0, vous devez migrer vers une version SMB ultérieure dès que possible pour préparer des améliorations en matière de sécurité et de conformité. Contactez votre représentant NetApp pour plus d'informations.

Le tableau suivant indique les fonctionnalités SMB prises en charge dans chaque version de SMB. Certaines fonctionnalités SMB sont activées par défaut et d'autres requièrent une configuration supplémentaire.

Cette fonctionnalité:	**Nécessite une activation:**	**Est pris en charge dans ONTAP 9 pour ces versions SMB:**				
		1.0	2.0	2.1	3.0	3.1.1
Fonctionnalité SMB 1.0 héritée		X	X	X	X	X
Poignées durables			X	X	X	X
Opérations cumulées			X	X	X	X

Cette fonctionnalité:	Nécessite une activation:	Est pris en charge dans ONTAP 9 pour ces versions SMB:				
Opérations asynchrones			X	X	X	X
Tailles de tampon de lecture et d'écriture améliorées			X	X	X	X
Évolutivité optimisée			X	X	X	X
Signature SMB	X	X	X	X	X	X
Autre format de fichier ADS (Data Stream)	X	X	X	X	X	X
MTU important (activé par défaut à partir de ONTAP 9.7)	X			X	X	X
Oplocks de location				X	X	X
Partages disponibles en permanence	X				X	X
Pointeurs permanents					X	X
Témoin					X	X
CHIFFREMENT SMB : AES-128-CCM	X				X	X

Cette fonctionnalité:	Nécessite une activation:	Est pris en charge dans ONTAP 9 pour ces versions SMB:				
Évolutivité horizontale (requise par les partages de CA)					X	X
Basculement transparent					X	X
Multicanal SMB (à partir de ONTAP 9.4)	X				X	X
Intégrité de la pré-authentification						X
Basculement client cluster v.2 (CCFv2)						X
Chiffrement SMB : AES-128-GCM (à partir de ONTAP 9.1)	X					X

Informations associées

Utilisation de la signature SMB pour améliorer la sécurité du réseau

Définition du niveau de sécurité d'authentification minimum du serveur SMB

Configuration du chiffrement SMB requis sur les serveurs SMB pour les transferts de données sur SMB

"Rapport technique de NetApp 4543 : meilleures pratiques relatives au protocole SMB"

"Interopérabilité NetApp"

Fonctionnalités Windows non prises en charge

Avant d'utiliser CIFS sur votre réseau, vous devez connaître certaines fonctionnalités Windows que ONTAP ne prend pas en charge.

ONTAP ne prend pas en charge les fonctionnalités Windows suivantes :

- Système de fichiers crypté (EFS)
- Consignation des événements NTFS (NT File System) dans le journal des modifications
- Service FRS (File Replication Service) Microsoft
- Service d'indexation Microsoft Windows
- Stockage distant via HSM (gestion hiérarchique du stockage)
- Gestion des quotas des clients Windows
- Sémantique du quota Windows
- Le fichier LMHOSTS
- Compression native NTFS

Configurer les services de noms NIS ou LDAP sur le SVM

L'accès SMB permet de mapper un utilisateur UNIX, même en cas d'accès aux données d'un volume NTFS de type sécurité. Si vous associez des utilisateurs Windows aux utilisateurs UNIX correspondants dont les informations sont stockées dans des magasins d'annuaire NIS ou LDAP, ou si vous utilisez LDAP pour le mappage de noms, vous devez configurer ces services de noms au cours de l'installation SMB.

Avant de commencer

Vous devez avoir personnalisé la configuration de votre base de données de services de noms afin qu'elle corresponde à votre infrastructure de service de noms.

Description de la tâche

Les SVM utilisent les bases de données de name services ns-switch pour déterminer l'ordre dans lequel rechercher les sources d'une base de données de name-service donnée. La source du commutateur ns peut être n'importe quelle combinaison de « fichiers », « nis » ou « ldap ». Pour la base de données des groupes, ONTAP tente d'obtenir les appartenances de groupe de toutes les sources configurées, puis utilise les informations d'appartenance de groupe consolidées pour les contrôles d'accès. Si l'une de ces sources n'est pas disponible au moment de l'obtention des informations du groupe UNIX, ONTAP ne peut pas obtenir les informations d'identification UNIX complètes et les vérifications d'accès ultérieures peuvent échouer. Par conséquent, vous devez toujours vérifier que toutes les sources du commutateur ns sont configurées pour la base de données du groupe dans les paramètres du commutateur ns.

Par défaut, le serveur SMB doit mapper tous les utilisateurs Windows à l'utilisateur UNIX par défaut stocké dans le serveur local `passwd` base de données. Si vous souhaitez utiliser la configuration par défaut, la configuration des services de nom d'utilisateur et de groupe NIS ou LDAP UNIX ou le mappage d'utilisateur LDAP est facultative pour l'accès SMB.

Étapes

1. Si les informations utilisateur, groupe et groupe de réseau UNIX sont gérées par les services de noms NIS, configurez les services de noms NIS :

   a. Déterminez la commande actuelle des services de noms à l'aide du `vserver services name-service ns-switch show` commande.

      Dans cet exemple, les trois bases de données (`group`, `passwd`, et `netgroup`) qui peut utiliser `nis` en tant que source de service de nom n'utilisent que `files` comme source.

```
vserver services name-service ns-switch show -vserver vs1
```

```
                                                Source
Vserver         Database       Enabled          Order
--------------- ------------   ---------        ---------
vs1             hosts          true             dns,
                                                files
vs1             group          true             files
vs1             passwd         true             files
vs1             netgroup       true             files
vs1             namemap        true             files
```

Vous devez ajouter le `nis` source vers le `group` et `passwd` les bases de données, et éventuellement au `netgroup` base de données.

b. Réglez l'ordre de la base de données du commutateur ns-service de noms en utilisant le `vserver services name-service ns-switch modify` commande.

   Pour obtenir des performances optimales, vous ne devez pas ajouter de service de noms à une base de données de services de noms, sauf si vous prévoyez de configurer ce service de noms sur la SVM.

   Si vous modifiez la configuration de plusieurs bases de données de service de noms, vous devez exécuter la commande séparément pour chaque base de données de service de noms que vous souhaitez modifier.

   Dans cet exemple, `nis` et `files` sont configurés comme sources pour le `group` et `passwd` les bases de données, dans cet ordre. Les bases de données restantes du service de noms ne sont pas modifiées.

   `vserver services name-service ns-switch modify -vserver vs1 -database group -sources nis,files` `vserver services name-service ns-switch modify -vserver vs1 -database passwd -sources nis,files`

c. Vérifiez que l'ordre des services de noms est correct en utilisant le `vserver services name-service ns-switch show` commande.

   `vserver services name-service ns-switch show -vserver vs1`

```
                                                    Source
Vserver         Database       Enabled          Order
--------------- ------------   ---------        ---------
vs1             hosts          true             dns,
                                                files
vs1             group          true             nis,
                                                files
vs1             passwd         true             nis,
                                                files
vs1             netgroup       true             files
vs1             namemap        true             files
```

d. Créer la configuration du service de nom NIS :
`vserver services name-service nis-domain create -vserver` *`vserver_name`* `-domain` *`NIS_domain_name`* `-servers` *`NIS_server_IPaddress`*`,… -active true+`

```
vserver services name-service nis-domain create -vserver vs1 -domain
example.com -servers 10.0.0.60 -active true
```

> À partir de ONTAP 9.2, le champ `-nis-servers` remplace le champ `-servers`. Ce nouveau champ peut prendre un nom d'hôte ou une adresse IP pour le serveur NIS.

e. Vérifiez que le service de nom NIS est correctement configuré et actif : `vserver services name-service nis-domain show vserver` *`vserver_name`*

```
vserver services name-service nis-domain show vserver vs1
```

```
Vserver       Domain              Active Server
------------- ------------------- ------ ---------------
vs1           example.com         true   10.0.0.60
```

2. Si les informations utilisateur, groupe et groupe de réseau UNIX ou le mappage de nom sont gérés par les services de noms LDAP, configurez les services de noms LDAP à l'aide des informations situées "Gestion NFS".

Fonctionnement de la configuration du commutateur de service name ONTAP

ONTAP stocke les informations de configuration du service de noms dans un tableau équivalent à `/etc/nsswitch.conf` Fichier sur les systèmes UNIX. Vous devez connaître les fonctions du tableau et savoir comment ONTAP l'utilise pour que vous puissiez le configurer de façon appropriée pour votre environnement.

La table commutateur de service de nom ONTAP détermine les sources de service de nom auxquelles ONTAP consulte afin de récupérer les informations relatives à un certain type d'informations de service de nom. ONTAP conserve une table de commutateur de service de noms distincte pour chaque SVM.

Types de base de données

La table stocke une liste de services de noms distincte pour chacun des types de bases de données suivants :

Type de base de données	Définit les sources de service de noms pour…	Les sources valides sont…
hôtes	Conversion des noms d'hôte en adresses IP	fichiers, dns
groupe	Recherche des informations sur les groupes d'utilisateurs	fichiers, nis, ldap
passwd	Recherche des informations utilisateur	fichiers, nis, ldap
groupe réseau	Recherche des informations de groupe réseau	fichiers, nis, ldap
carte de nom	Mappage des noms d'utilisateur	fichiers, ldap

Types de source

Les sources indiquent quelle source de service de nom utiliser pour récupérer les informations appropriées.

Spécifiez le type de source…	Pour rechercher des informations dans…	Géré par les familles de commande…

fichiers	Fichiers source locaux	`vserver services name-service unix-user` `vserver services name-service unix-group`
		
		`vserver services name-service netgroup`
		
		`vserver services name-service dns hosts`

nis	Serveurs NIS externes tels que spécifiés dans la configuration de domaine NIS du SVM	`vserver services name-service nis-domain`
ldap	Serveurs LDAP externes comme spécifié dans la configuration du client LDAP du SVM	`vserver services name-service ldap`

Spécifiez le type de source…	Pour rechercher des informations dans…	Géré par les familles de commande…
dns	Serveurs DNS externes comme spécifié dans la configuration DNS du SVM	`vserver services name-service dns`

Même si vous prévoyez d'utiliser NIS ou LDAP pour l'accès aux données et l'authentification d'administration des SVM, vous devez toujours inclure `files` Et configurer des utilisateurs locaux comme un repli en cas d'échec de l'authentification NIS ou LDAP.

Protocoles utilisés pour accéder à des sources externes

Pour accéder aux serveurs pour des sources externes, ONTAP utilise les protocoles suivants :

Source de service de nom externe	Protocole utilisé pour l'accès
NIS	UDP
DNS	UDP
LDAP	TCP

Exemple

L'exemple suivant affiche la configuration du commutateur de service de nom pour le SVM `svm_1`:

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
                                Source
Vserver         Database        Order
--------------- ------------    ---------
svm_1           hosts           files,
                                dns
svm_1           group           files
svm_1           passwd          files
svm_1           netgroup        nis,
                                files
```

Pour rechercher des informations sur les utilisateurs ou les groupes, ONTAP consulte uniquement les fichiers sources locales. Si la requête ne renvoie aucun résultat, la recherche échoue.

Pour rechercher des informations sur le groupe réseau, ONTAP consulte d'abord les serveurs NIS externes. Si la requête ne renvoie aucun résultat, le fichier netgroup local est coché ensuite.

Il n'y a pas d'entrées de nom de service pour le mappage de noms dans le tableau pour le SVM svm_1. Par conséquent, ONTAP consulte uniquement les fichiers source locaux par défaut.

Gérer les serveurs SMB

Modifier les serveurs SMB

Vous pouvez déplacer un serveur SMB d'un groupe de travail vers un domaine Active Directory, d'un groupe de travail vers un autre groupe de travail, ou d'un domaine Active Directory vers un groupe de travail à l'aide de l' `vserver cifs modify` commande.

Description de la tâche

Vous pouvez également modifier d'autres attributs du serveur SMB, tels que le nom du serveur SMB et l'état administratif. Voir la page man pour plus de détails.

Choix

- Déplacer le serveur SMB d'un groupe de travail vers un domaine Active Directory :

  a. Définissez l'état administratif du serveur SMB sur `down`.

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
  ```

  b. Déplacer le serveur SMB du groupe de travail vers un domaine Active Directory : `vsserver cifs modify -vserver` *`vserver_name`* `-domain` *`domain_name`*

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -domain example.com
  ```

  Pour créer un compte de machine Active Directory pour le serveur SMB, vous devez fournir le nom et le mot de passe d'un compte Windows disposant des privilèges suffisants pour ajouter des ordinateurs à l' `ou=`*`example`* `ou` conteneur dans le `*example*`domaine .com.

  À partir de ONTAP 9.7, votre administrateur AD peut vous fournir un URI vers un fichier keytab comme alternative à vous fournir un nom et un mot de passe à un compte Windows privilégié. Lorsque vous recevez l'URI, l'inclure dans le `-keytab-uri` paramètre avec le `vserver cifs` commandes.

- Déplacer le serveur SMB d'un groupe de travail vers un autre groupe de travail :

  a. Définissez l'état administratif du serveur SMB sur `down`.

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
  ```

  b. Modifiez le groupe de travail pour le serveur SMB : `vserver cifs modify -vserver` *`vserver_name`* `-workgroup` *`new_workgroup_name`*

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -workgroup workgroup2
  ```

- Déplacer le serveur SMB d'un domaine Active Directory vers un groupe de travail :

  a. Définissez l'état administratif du serveur SMB sur `down`.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

b. Déplacer le serveur SMB du domaine Active Directory vers un groupe de travail : `vserver cifs modify -vserver vserver_name -workgroup workgroup_name`

```
cluster1::> vserver cifs modify -vserver vs1 -workgroup workgroup1
```

> Pour passer en mode groupe de travail, toutes les fonctions basées sur un domaine doivent être désactivées et leur configuration doit être supprimée automatiquement par le système, y compris les partages disponibles en continu, les clichés instantanés et AES. Cependant, les listes de contrôle d'accès de partage configurées par domaine telles que « EXAMPLE.COM\userName" ne fonctionneront pas correctement, mais ne peuvent pas être supprimées par ONTAP. Supprimez ces ACL de partage dès que possible à l'aide d'outils externes une fois la commande terminée. Si AES est activé, vous pouvez être invité à fournir le nom et le mot de passe d'un compte Windows disposant de privilèges suffisants pour le désactiver dans le domaine "example.com".

- Modifiez d'autres attributs en utilisant le paramètre approprié de l' `vserver cifs modify` commande.

Utilisez les options pour personnaliser les serveurs SMB

Options de serveur SMB disponibles

Il est utile de connaître les options disponibles lorsque vous envisagez de personnaliser le serveur SMB. Bien que certaines options soient destinées à une utilisation générale sur le serveur SMB, plusieurs sont utilisées pour activer et configurer des fonctionnalités SMB spécifiques. Les options de serveur SMB sont contrôlées avec le `vserver cifs options modify` option.

La liste suivante indique les options du serveur SMB disponibles au niveau de privilège admin :

- **Configuration de la valeur du délai d'expiration de session SMB**

  La configuration de cette option vous permet de spécifier le nombre de secondes d'inactivité avant la déconnexion d'une session SMB. Une session inactive est une session dans laquelle un utilisateur ne dispose pas de fichiers ou de répertoires ouverts sur le client. La valeur par défaut est 900 secondes.

- **Configuration de l'utilisateur UNIX par défaut**

  La configuration de cette option vous permet de spécifier l'utilisateur UNIX par défaut utilisé par le serveur SMB. ONTAP crée automatiquement un utilisateur par défaut nommé « pcuser » (avec un UID de 65534), crée un groupe nommé « pcuser » (avec un GID de 65534) et ajoute l'utilisateur par défaut au groupe « pcuser ». Lorsque vous créez un serveur SMB, ONTAP configure automatiquement « pcuser » en tant qu'utilisateur UNIX par défaut.

- **Configuration de l'utilisateur UNIX invité**

  La configuration de cette option vous permet de spécifier le nom d'un utilisateur UNIX auquel les

utilisateurs qui se connectent à partir de domaines non fiables sont mappés, ce qui permet à un utilisateur d'un domaine non fiable de se connecter au serveur SMB. Par défaut, cette option n'est pas configurée (il n'y a pas de valeur par défaut) ; par conséquent, la valeur par défaut ne permet pas aux utilisateurs de domaines non approuvés de se connecter au serveur SMB.

- **Activation ou désactivation de l'exécution d'une subvention en lecture pour les bits de mode**

  L'activation ou la désactivation de cette option vous permet de spécifier si les clients SMB doivent autoriser l'exécution de fichiers exécutables avec les bits de mode UNIX auxquels ils ont accès en lecture, même lorsque le bit exécutable UNIX n'est pas défini. Cette option est désactivée par défaut.

- **Activation ou désactivation de la possibilité de supprimer des fichiers en lecture seule des clients NFS**

  L'activation ou la désactivation de cette option détermine s'il faut autoriser les clients NFS à supprimer des fichiers ou des dossiers avec l'ensemble d'attributs en lecture seule. La sémantique de suppression NTFS n'autorise pas la suppression d'un fichier ou d'un dossier lorsque l'attribut en lecture seule est défini. La sémantique de suppression UNIX ignore le bit en lecture seule, en utilisant les autorisations du répertoire parent à la place pour déterminer si un fichier ou un dossier peut être supprimé. Le paramètre par défaut est `disabled`, Ce qui entraîne la suppression de la sémantique en NTFS.

- **Configuration des adresses du serveur du service de noms Internet Windows**

  La configuration de cette option vous permet de spécifier une liste d'adresses de serveur WINS (Windows Internet Name Service) en tant que liste délimitée par des virgules. Vous devez indiquer des adresses IPv4. Les adresses IPv6 ne sont pas prises en charge. Il n'y a pas de valeur par défaut.

La liste suivante indique les options du serveur SMB disponibles au niveau de privilège avancé :

- **Octroi d'autorisations de groupe UNIX aux utilisateurs CIFS**

  La configuration de cette option détermine si l'utilisateur CIFS entrant qui n'est pas le propriétaire du fichier peut obtenir l'autorisation de groupe. Si l'utilisateur CIFS n'est pas le propriétaire du fichier de style de sécurité UNIX et que ce paramètre est défini sur `true`, puis l'autorisation de groupe est accordée pour le fichier. Si l'utilisateur CIFS n'est pas le propriétaire du fichier de style de sécurité UNIX et que ce paramètre est défini sur `false`, Les règles UNIX normales sont alors applicables pour accorder l'autorisation de fichier. Ce paramètre s'applique aux fichiers de style de sécurité UNIX dont l'autorisation est définie sur `mode bits` Et ne s'applique pas aux fichiers utilisant le mode de sécurité NTFS ou NFSv4. Le paramètre par défaut est `false`.

- **Activation ou désactivation de SMB 1.0**

  SMB 1.0 est désactivé par défaut sur un SVM pour lequel un serveur SMB est créé dans ONTAP 9.3.

  > À partir de ONTAP 9.3, SMB 1.0 est désactivé par défaut pour les nouveaux serveurs SMB créés dans ONTAP 9.3. Vous devez migrer vers une version SMB plus récente dès que possible pour préparer des améliorations en matière de sécurité et de conformité. Contactez votre représentant NetApp pour plus d'informations.

- **Activation ou désactivation de SMB 2.x**

  SMB 2.0 est la version minimale de SMB qui prend en charge le basculement de LIF. Si vous désactivez SMB 2.x, ONTAP désactive également automatiquement SMB 3.X.

SMB 2.0 est pris en charge uniquement sur les SVM. L'option est activée par défaut sur les SVM

- **Activation ou désactivation de SMB 3.0**

  SMB 3.0 est la version minimale de SMB qui prend en charge les partages disponibles en continu. Windows Server 2012 et Windows 8 sont les versions minimales de Windows qui prennent en charge SMB 3.0.

  SMB 3.0 n'est pris en charge que sur les SVM. L'option est activée par défaut sur les SVM

- **Activation ou désactivation de SMB 3.1**

  Windows 10 est la seule version de Windows qui prend en charge SMB 3.1.

  SMB 3.1 n'est pris en charge que sur les SVM. L'option est activée par défaut sur les SVM

- **Activation ou désactivation de l'allègement de charge des copies ODX**

  L'allègement de la charge des copies ODX est utilisé automatiquement par les clients Windows qui la prennent en charge. Cette option est activée par défaut.

- **Activation ou désactivation du mécanisme de copie directe pour le déchargement de copies ODX**

  Le mécanisme de copie directe augmente les performances de l'opération de déchargement de copie lorsque les clients Windows essaient d'ouvrir le fichier source d'une copie dans un mode qui empêche la modification du fichier pendant la copie. Par défaut, le mécanisme de copie directe est activé.

- **Activation ou désactivation des renvois de nœuds automatiques**

  Avec les référencements automatiques des nœuds, le serveur SMB fait automatiquement référence aux clients à une LIF de données locale au nœud qui héberge les données accédées via le partage demandé.

- **Activation ou désactivation des stratégies d'exportation pour SMB**

  Cette option est désactivée par défaut.

- **Activation ou désactivation de l'utilisation de points de jonction en tant que points de réanalyse**

  Si cette option est activée, le serveur SMB expose les points de jonction aux clients SMB comme points de réanalyse. Cette option n'est valide que pour les connexions SMB 2.x ou SMB 3.0. Cette option est activée par défaut.

  Cette option n'est prise en charge que sur les SVM. L'option est activée par défaut sur les SVM

- **Configuration du nombre maximal d'opérations simultanées par connexion TCP**

  La valeur par défaut est 255.

- **Activation ou désactivation de la fonctionnalité des groupes et des utilisateurs Windows locaux**

  Cette option est activée par défaut.

- **Activation ou désactivation de l'authentification des utilisateurs Windows locaux**

  Cette option est activée par défaut.

- **Activation ou désactivation de la fonctionnalité de copie en double VSS**

  ONTAP utilise la fonctionnalité Shadow Copy pour effectuer des sauvegardes distantes des données stockées à l'aide de la solution Hyper-V sur SMB.

  Cette option n'est prise en charge que sur les SVM et uniquement dans les configurations Hyper-V sur SMB. L'option est activée par défaut sur les SVM

- **Configuration de la profondeur du répertoire de copie en double**

  La configuration de cette option vous permet de définir la profondeur maximale des répertoires sur lesquels créer des clichés instantanés lors de l'utilisation de la fonctionnalité copie en double.

  Cette option n'est prise en charge que sur les SVM et uniquement dans les configurations Hyper-V sur SMB. L'option est activée par défaut sur les SVM

- **Activation ou désactivation des fonctionnalités de recherche multidomaine pour le mappage de noms**

  Si cette option est activée, lorsqu'un utilisateur UNIX est mappé à un utilisateur de domaine Windows à l'aide d'un caractère générique (*) dans la partie domaine du nom d'utilisateur Windows (par exemple *\joe), ONTAP recherche l'utilisateur spécifié dans tous les domaines avec des approbations bidirectionnelles vers le domaine d'origine. Le domaine personnel est le domaine qui contient le compte informatique du serveur SMB.

  Vous pouvez également configurer une liste de domaines de confiance préférés en alternative à la recherche de tous les domaines de confiance bidirectionnels. Si cette option est activée et qu'une liste préférée est configurée, la liste préférée est utilisée pour effectuer des recherches de mappage de noms de domaines multiples.

  La valeur par défaut est d'activer les recherches de mappage de noms multidomaine.

- **Configuration de la taille du secteur du système de fichiers**

  La configuration de cette option vous permet de configurer la taille du secteur du système de fichiers en octets que ONTAP communique aux clients SMB. Cette option comporte deux valeurs valides : `4096` et `512`. La valeur par défaut est `4096`. Vous devrez peut-être définir cette valeur sur `512` Si l'application Windows ne prend en charge qu'une taille de secteur de 512 octets.

- **Activation ou désactivation du contrôle d'accès dynamique**

  L'activation de cette option vous permet de sécuriser les objets sur le serveur SMB à l'aide du contrôle d'accès dynamique (DAC), y compris l'utilisation de l'audit pour définir des règles d'accès centrales et l'utilisation d'objets de stratégie de groupe pour mettre en œuvre des règles d'accès centrales. L'option est désactivée par défaut.

  Cette option n'est prise en charge que sur les SVM.

- **Définition des restrictions d'accès pour les sessions non authentifiées (restriction anonyme)**

  La définition de cette option détermine les restrictions d'accès pour les sessions non authentifiées. Les restrictions sont appliquées aux utilisateurs anonymes. Par défaut, il n'existe aucune restriction d'accès pour les utilisateurs anonymes.

- **Activation ou désactivation de la présentation des listes de contrôle d'accès NTFS sur des volumes**

avec sécurité effective UNIX (volumes de type sécurité UNIX ou volumes de type sécurité mixte avec sécurité effective UNIX)

L'activation ou la désactivation de cette option détermine comment la sécurité des fichiers sur les fichiers et les dossiers avec la sécurité UNIX est présentée aux clients SMB. Lorsqu'elle est activée, ONTAP présente aux clients SMB les fichiers et les dossiers des volumes dotés de la sécurité UNIX comme ayant la sécurité des fichiers NTFS avec les ACL NTFS. S'il est désactivé, ONTAP présente les volumes dont la sécurité UNIX est de type FAT, sans aucun fichier sécurisé. Par défaut, les volumes sont présentés comme ayant la sécurité de fichiers NTFS avec les ACL NTFS.

- **Activation ou désactivation de la fonctionnalité fausse ouverture SMB**

  L'activation de cette fonctionnalité améliore les performances de SMB 2.x et de SMB 3.0 en optimisant la manière dont ONTAP effectue des requêtes ouvertes et fermés lors des requêtes relatives aux attributs des fichiers et des répertoires. Par défaut, la fonctionnalité de faux ouverture SMB est activée. Cette option est utile uniquement pour les connexions effectuées avec SMB 2.x ou version ultérieure.

- **Activation ou désactivation des extensions UNIX**

  L'activation de cette option active les extensions UNIX sur un serveur SMB. Les extensions UNIX permettent d'afficher la sécurité du style POSIX/UNIX via le protocole SMB. Par défaut, cette option est désactivée.

  Si vous avez des clients SMB basés sur UNIX, tels que des clients Mac OSX, dans votre environnement, vous devez activer les extensions UNIX. L'activation des extensions UNIX permet au serveur SMB de transmettre des informations de sécurité POSIX/UNIX sur SMB au client UNIX, qui convertit ensuite les informations de sécurité en sécurité POSIX/UNIX.

- **Activation ou désactivation du support pour les recherches de noms courts**

  L'activation de cette option permet au serveur SMB d'effectuer des recherches sur des noms courts. Une requête de recherche avec cette option activée tente de faire correspondre 8.3 noms de fichier avec des noms de fichier longs. La valeur par défaut de ce paramètre est `false`.

- **Activation ou désactivation de la prise en charge de la publicité automatique des capacités DFS**

  L'activation ou la désactivation de cette option détermine si les serveurs SMB annoncent automatiquement les fonctionnalités DFS aux clients SMB 2.x et SMB 3.0 qui se connectent aux partages. ONTAP utilise des référencements DFS dans la mise en œuvre de liens symboliques pour l'accès SMB. Si cette option est activée, le serveur SMB annonce toujours les fonctionnalités DFS, que l'accès à la liaison symbolique soit activé ou non. S'il est désactivé, le serveur SMB annonce les fonctionnalités DFS uniquement lorsque les clients se connectent aux partages où l'accès à la liaison symbolique est activé.

- **Configuration du nombre maximum de crédits SMB**

  Depuis ONTAP 9.4, configurer le `-max-credits` Vous permet de limiter le nombre de crédits à accorder sur une connexion SMB lorsque les clients et le serveur exécutent SMB version 2 ou ultérieure. La valeur par défaut est 128.

- **Activation ou désactivation de la prise en charge de SMB Multichannel**

  Activation du `-is-multichannel-enabled` Option dans les versions ONTAP 9.4 et ultérieures permet au serveur SMB d'établir plusieurs connexions pour une seule session SMB lorsque les cartes réseau appropriées sont déployées sur le cluster et ses clients. Cela améliore le débit et la tolérance aux pannes. La valeur par défaut de ce paramètre est `false`.

Lorsque SMB Multichannel est activé, vous pouvez également spécifier les paramètres suivants :

- Nombre maximum de connexions autorisées par session multicanal. La valeur par défaut de ce paramètre est 32.
- Nombre maximum d'interfaces réseau annoncées par session multicanal. La valeur par défaut de ce paramètre est 256.

Configuration des options du serveur SMB

Vous pouvez configurer les options du serveur SMB à tout moment après avoir créé un serveur SMB sur une machine virtuelle de stockage (SVM).

Étape

1. Effectuez l'action souhaitée :

Si vous souhaitez configurer les options du serveur SMB…	Entrez la commande…
Au niveau de privilège admin	`vserver cifs options modify -vserver` *`vserver_name options`*
Au niveau de privilège avancé	a. `set -privilege advanced` b. `vserver cifs options modify -vserver` *`vserver_name options`* c. `set -privilege admin`

Pour plus d'informations sur la configuration des options du serveur SMB, reportez-vous à la page de manuel du `vserver cifs options modify` commande.

Configurez l'autorisation d'accorder le groupe UNIX aux utilisateurs SMB

Vous pouvez configurer cette option pour accorder des autorisations de groupe à des fichiers ou des répertoires, même si l'utilisateur SMB entrant n'est pas le propriétaire du fichier.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Configurez l'autorisation Grant UNIX Group comme il convient :

Si vous le souhaitez	Saisissez la commande
Activez l'accès aux fichiers ou répertoires pour obtenir les autorisations de groupe même si l'utilisateur n'est pas le propriétaire du fichier	`vserver cifs options modify –grant-unix-group-perms-to-others true`

Si vous le souhaitez	Saisissez la commande
Désactivez l'accès aux fichiers ou répertoires pour obtenir les autorisations de groupe même si l'utilisateur n'est pas le propriétaire du fichier	`vserver cifs options modify -grant-unix-group-perms-to-others false`

3. Vérifiez que l'option est réglée sur la valeur souhaitée : `vserver cifs options show -fields grant-unix-group-perms-to-others`
4. Retour au niveau de privilège admin : `set -privilege admin`

Configurez les restrictions d'accès pour les utilisateurs anonymes

Par défaut, un utilisateur anonyme et non authentifié (également appelé *null user*) peut accéder à certaines informations sur le réseau. Vous pouvez utiliser une option de serveur SMB pour configurer les restrictions d'accès pour l'utilisateur anonyme.

Description de la tâche

Le `-restrict-anonymous` L'option de serveur SMB correspond au `RestrictAnonymous` Entrée de registre dans Windows.

Les utilisateurs anonymes peuvent lister ou énumérer certains types d'informations système provenant des hôtes Windows sur le réseau, y compris les noms d'utilisateur et les détails, les stratégies de compte et les noms de partage. Vous pouvez contrôler l'accès de l'utilisateur anonyme en spécifiant l'un des trois paramètres de restriction d'accès suivants :

Valeur	Description
`no-restriction` (valeur par défaut)	Spécifie aucune restriction d'accès pour les utilisateurs anonymes.
`no-enumeration`	Spécifie que seule l'énumération est restreinte pour les utilisateurs anonymes.
`no-access`	Spécifie que l'accès est restreint pour les utilisateurs anonymes.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Configurez le paramètre restreindre l'anonymat : `vserver cifs options modify -vserver` *`vserver_name`* `-restrict-anonymous {no-restriction|no-enumeration|no-access}`
3. Vérifiez que l'option est réglée sur la valeur souhaitée : `vserver cifs options show -vserver` *`vserver_name`*
4. Retour au niveau de privilège admin : `set -privilege admin`

Informations associées

Options de serveur SMB disponibles

Gérer la manière dont la sécurité des fichiers est présentée aux clients SMB pour les données de type sécurité UNIX

Gérer la manière dont la sécurité des fichiers est présentée aux clients SMB pour une présentation des données de type sécurité UNIX

Vous pouvez choisir comment présenter la sécurité des fichiers aux clients SMB pour les données de style de sécurité UNIX en activant ou désactivant la présentation d'ACL NTFS aux clients SMB. Chaque paramètre présente des avantages, que vous devez comprendre pour choisir le paramètre le mieux adapté aux besoins de votre entreprise.

Par défaut, ONTAP présente des autorisations UNIX sur des volumes de type sécurité UNIX aux clients SMB comme des listes de contrôle d'accès NTFS. Dans certains cas, cette option est souhaitable, notamment :

- Vous souhaitez afficher et modifier les autorisations UNIX à l'aide de l'onglet **sécurité** de la zone Propriétés de Windows.

  Vous ne pouvez pas modifier les autorisations d'un client Windows si l'opération n'est pas autorisée par le système UNIX. Par exemple, vous ne pouvez pas modifier la propriété d'un fichier que vous ne possédez pas, car le système UNIX ne permet pas cette opération. Cette restriction empêche les clients SMB de contourner les autorisations UNIX définies sur les fichiers et dossiers.

- Les utilisateurs modifient et enregistrent des fichiers sur le volume de style de sécurité UNIX en utilisant certaines applications Windows, par exemple Microsoft Office, où ONTAP doit préserver les autorisations UNIX pendant les opérations de sauvegarde.
- Votre environnement compte certaines applications Windows qui doivent lire les listes de contrôle d'accès NTFS sur les fichiers qu'elles utilisent.

Dans certaines circonstances, vous pouvez désactiver la présentation des autorisations UNIX en tant que listes de contrôle d'accès NTFS. Si cette fonctionnalité est désactivée, ONTAP présente les volumes de style de sécurité UNIX en tant que volumes FAT aux clients SMB. Il existe des raisons spécifiques de vouloir présenter des volumes de style sécurité UNIX en tant que volumes FAT aux clients SMB :

- Vous ne modifiez que les autorisations UNIX en utilisant des montages sur des clients UNIX.

  L'onglet sécurité n'est pas disponible lorsqu'un volume de style de sécurité UNIX est mappé sur un client SMB. Le lecteur mappé semble être formaté avec le système de fichiers FAT, qui ne dispose pas d'autorisations de fichier.

- Vous utilisez des applications sur SMB qui définissent les listes de contrôle d'accès NTFS sur les fichiers et dossiers auxquels vous accédez, ce qui peut échouer si les données résident sur des volumes de style de sécurité UNIX.

  Si ONTAP signale le volume comme FAT, l'application n'essaie pas de modifier une ACL.

Informations associées

Configuration des styles de sécurité sur les volumes FlexVol

Configuration des styles de sécurité sur les qtrees

Activez ou désactivez la présentation des listes de contrôle d'accès NTFS pour les données de type de sécurité UNIX

Vous pouvez activer ou désactiver la présentation des listes de contrôle d'accès NTFS

aux clients SMB pour les données de style de sécurité UNIX (volumes de style sécurité UNIX et volumes de type sécurité mixte avec sécurité effective UNIX).

Description de la tâche

Si vous activez cette option, ONTAP présente les fichiers et les dossiers sur les volumes avec un style de sécurité UNIX efficace aux clients SMB comme ayant des listes de contrôle d'accès NTFS. Si vous désactivez cette option, les volumes sont présentés en tant que volumes FAT aux clients SMB. Par défaut, cette valeur doit présenter des listes de contrôle d'accès NTFS aux clients SMB.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Configurez le paramètre d'option ACL NTFS UNIX : `vserver cifs options modify -vserver` *`vserver_name`* `-is-unix-nt-acl-enabled {true|false}`
3. Vérifiez que l'option est réglée sur la valeur souhaitée : `vserver cifs options show -vserver` *`vserver_name`*
4. Retour au niveau de privilège admin : `set -privilege admin`

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.

Gérer les paramètres de sécurité du serveur SMB

Gestion de l'authentification client SMB par ONTAP

Avant que les utilisateurs puissent créer des connexions SMB pour accéder aux données contenues dans la SVM, ils doivent être authentifiés par le domaine auquel le serveur SMB appartient. Le serveur SMB prend en charge deux méthodes d'authentification, Kerberos et NTLM (NTLMv1 ou NTLMv2). Kerberos est la méthode par défaut utilisée pour authentifier les utilisateurs du domaine.

Authentification Kerberos

ONTAP supporte l'authentification Kerberos lors de la création de sessions SMB authentifiées.

Kerberos est le service principal d'authentification pour Active Directory. Le serveur Kerberos, ou le Kerberos Key distribution Center (KDC) service, stocke et récupère des informations sur les principes de sécurité dans Active Directory. A la différence du modèle NTLM, les clients Active Directory qui souhaitent établir une session avec un autre ordinateur, tel que le serveur SMB, contactez directement un KDC pour obtenir leurs credentials de session.

Authentification NTLM

L'authentification du client NTLM est effectuée à l'aide d'un protocole de réponse de défi basé sur une connaissance partagée d'un secret spécifique à un utilisateur basé sur un mot de passe.

Si un utilisateur crée une connexion SMB à l'aide d'un compte utilisateur Windows local, l'authentification est effectuée localement par le serveur SMB à l'aide de NTLMv2.

Instructions relatives aux paramètres de sécurité des serveurs SMB dans une configuration de reprise d'activité des SVM

Avant de créer un SVM configuré en tant que destination de reprise d'activité pour laquelle l'identité n'est pas conservée (le `-identity-preserve` l'option est définie sur `false` En configuration SnapMirror), il est important de savoir comment les paramètres

de sécurité des serveurs SMB sont gérés sur la SVM de destination.

- Les paramètres de sécurité du serveur SMB non par défaut ne sont pas répliqués sur la destination.

  Lorsque vous créez un serveur SMB sur le SVM de destination, tous les paramètres de sécurité du serveur SMB sont définis sur les valeurs par défaut. Lors de l'initialisation, de la destination de reprise après incident du SVM, de la mise à jour ou de la resynchronisation, les paramètres de sécurité du serveur SMB sur la source ne sont pas répliqués sur la destination.

- Vous devez configurer manuellement les paramètres de sécurité du serveur SMB non par défaut.

  Si vous avez configuré sur la SVM source des paramètres de sécurité du serveur SMB non par défaut, vous devez configurer manuellement ces mêmes paramètres sur le SVM de destination après que la destination devienne read-write (après une interruption de la relation SnapMirror).

Affiche des informations sur les paramètres de sécurité du serveur SMB

Vous pouvez afficher des informations sur les paramètres de sécurité du serveur SMB sur vos serveurs virtuels de stockage (SVM). Vous pouvez utiliser ces informations pour vérifier que les paramètres de sécurité sont corrects.

Description de la tâche

Un paramètre de sécurité affiché peut être la valeur par défaut pour cet objet ou une valeur non par défaut configurée à l'aide de l'interface de ligne de commande ONTAP ou à l'aide d'objets de stratégie de groupe Active Directory.

N'utilisez pas le `vserver cifs security show` Commande pour les serveurs SMB en mode groupe de travail, car certaines options ne sont pas valides.

Étape

1. Effectuez l'une des opérations suivantes :

Si vous voulez afficher des informations sur…	Entrez la commande…
Tous les paramètres de sécurité sur un SVM spécifié	`vserver cifs security show -vserver` *`vserver_name`*
Un paramètre de sécurité ou des paramètres spécifiques sur la SVM	`vserver cifs security show -vserver _vserver_name_ -fields [fieldname,...]` Vous pouvez entrer `-fields ?` pour déterminer les champs que vous pouvez utiliser.

Exemple

L'exemple suivant montre tous les paramètres de sécurité pour SVM vs1 :

```
cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                          Kerberos Clock Skew:        5 minutes
                          Kerberos Ticket Age:        10 hours
                         Kerberos Renewal Age:        7 days
                         Kerberos KDC Timeout:        3 seconds
                           Is Signing Required:       false
               Is Password Complexity Required:       true
          Use start_tls For AD LDAP connection:       false
                     Is AES Encryption Enabled:       false
                        LM Compatibility Level:       lm-ntlm-ntlmv2-krb
                    Is SMB Encryption Required:       false
                       Client Session Security:       none
               SMB1 Enabled for DC Connections:       false
               SMB2 Enabled for DC Connections:       system-default
LDAP Referral Enabled For AD LDAP connections:       false
             Use LDAPS for AD LDAP connection:       false
    Encryption is required for DC Connections:       false
 AES session key enabled for NetLogon channel:       false
  Try Channel Binding For AD LDAP Connections:       false
```

Notez que les paramètres affichés dépendent de la version ONTAP en cours d'exécution.

L'exemple suivant montre l'inclinaison de l'horloge Kerberos pour le SVM vs1 :

```
cluster1::> vserver cifs security show -vserver vs1 -fields kerberos-
clock-skew

            vserver kerberos-clock-skew
            ------- -------------------
            vs1     5
```

Informations associées

Affichage des informations sur les configurations GPO

Activez ou désactivez la complexité requise des mots de passe pour les utilisateurs SMB locaux

Au-dessus de vos SVM, la complexité requise par mot de passe renforce la sécurité des utilisateurs SMB locaux. La fonction de complexité de mot de passe requise est activée par défaut. Vous pouvez le désactiver et le réactiver à tout moment.

Avant de commencer

Les utilisateurs locaux, les groupes locaux et l'authentification des utilisateurs locaux doivent être activés sur le

serveur CIFS.

Description de la tâche

Vous ne devez pas utiliser le `vserver cifs security modify` Commande pour un serveur CIFS en mode groupe de travail car certaines options ne sont pas valides.

Étapes

1. Effectuez l'une des opérations suivantes :

Si vous voulez que les utilisateurs de PME locales aient besoin de complexité de mot de passe…	Entrez la commande…
Activé	`vserver cifs security modify -vserver` *`vserver_name`* `-is-password-complexity -required true`
Désactivé	`vserver cifs security modify -vserver` *`vserver_name`* `-is-password-complexity -required false`

2. Vérifiez le paramètre de sécurité pour connaître la complexité requise du mot de passe : `vserver cifs security show -vserver` *`vserver_name`*

Exemple

L'exemple suivant montre que la complexité requise des mots de passe est activée pour les utilisateurs SMB locaux pour le SVM vs1 :

```
cluster1::> vserver cifs security modify -vserver vs1 -is-password
-complexity-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-password-
complexity-required
vserver is-password-complexity-required
------- -------------------------------
vs1     true
```

Informations associées

Affichage d'informations sur les paramètres de sécurité du serveur CIFS

Utilisation d'utilisateurs et de groupes locaux pour l'authentification et l'autorisation

Conditions requises pour les mots de passe des utilisateurs locaux

Modification des mots de passe des comptes utilisateur locaux

Modifiez les paramètres de sécurité Kerberos du serveur CIFS

Vous pouvez modifier certains paramètres de sécurité Kerberos pour le serveur CIFS, notamment le temps d'inclinaison maximal autorisé de l'horloge Kerberos, la durée de vie du ticket Kerberos et le nombre maximum de jours de renouvellement de ticket.

Description de la tâche

Modification des paramètres Kerberos du serveur CIFS à l'aide de `vserver cifs security modify` La commande modifie les paramètres uniquement sur la machine virtuelle de stockage (SVM) que vous spécifiez avec le `-vserver` paramètre. Vous pouvez gérer de manière centralisée les paramètres de sécurité Kerberos pour tous les SVM du cluster appartenant au même domaine Active Directory à l'aide des objets de stratégie de groupe Active Directory.

Étapes

1. Effectuez une ou plusieurs des opérations suivantes :

Les fonctions que vous recherchez…	Entrer…
Spécifiez le temps maximal autorisé d'inclinaison de l'horloge Kerberos en minutes (9.13.1 et versions ultérieures) ou en secondes (9.12.1 ou versions antérieures).	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-clock-skew` *`integer_in_minutes`* La valeur par défaut est 5 minutes.
Spécifiez la durée de vie du ticket Kerberos en heures.	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-ticket-age integer_in_hours` Le paramètre par défaut est 10 heures.
Spécifiez le nombre maximum de jours de renouvellement de billet.	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-renew-age` *`integer_in_days`* Le paramètre par défaut est 7 jours.
Spécifiez le délai d'expiration des sockets sur les KDC après lequel tous les KDC sont marqués comme inaccessibles.	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-kdc-timeout` *`integer_in_seconds`* Le réglage par défaut est de 3 secondes.

2. Vérifiez les paramètres de sécurité Kerberos :

```
vserver cifs security show -vserver vserver_name
```

Exemple

L'exemple suivant apporte les modifications suivantes à la sécurité Kerberos : « Kerberos Clock Skew » est défini sur 3 minutes et « Kerberos Ticket Age » est défini sur 8 heures pour le SVM vs1 :

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock-skew
3 -kerberos-ticket-age 8

cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                    Kerberos Clock Skew:                   3 minutes
                    Kerberos Ticket Age:                   8 hours
                   Kerberos Renewal Age:                   7 days
                   Kerberos KDC Timeout:                   3 seconds
                    Is Signing Required:               false
        Is Password Complexity Required:                true
   Use start_tls For AD LDAP connection:               false
              Is AES Encryption Enabled:               false
                 LM Compatibility Level:  lm-ntlm-ntlmv2-krb
            Is SMB Encryption Required:               false
```

Informations associées

"Affichage d'informations sur les paramètres de sécurité du serveur CIFS"

"Stratégies de groupe prises en charge"

"Application d'objets de stratégie de groupe aux serveurs CIFS"

Définissez le niveau de sécurité d'authentification minimum du serveur SMB

Vous pouvez définir le niveau de sécurité minimum du serveur SMB, également appelé *LMCompatibilityLevel*, sur votre serveur SMB afin de répondre aux besoins de sécurité de votre entreprise pour l'accès client SMB. Le niveau de sécurité minimum est le niveau minimum des jetons de sécurité que le serveur SMB accepte des clients SMB.

Description de la tâche

- Les serveurs SMB en mode groupe de travail prennent uniquement en charge l'authentification NTLM. L'authentification Kerberos n'est pas prise en charge.
- LMCompatibilityLevel s'applique uniquement à l'authentification du client SMB, et non à l'authentification de l'administrateur.

Vous pouvez définir le niveau de sécurité d'authentification minimum sur l'un des quatre niveaux de sécurité pris en charge.

Valeur	Description
`lm-ntlm-ntlmv2-krb` (valeur par défaut)	La machine virtuelle de stockage (SVM) accepte les authentifications LM, NTLM, NTLMv2 et Kerberos.

Valeur	Description
`ntlm-ntlmv2-krb`	Le SVM accepte la sécurité d'authentification NTLM, NTLMv2, et Kerberos. Le SVM refuse l'authentification LM.
`ntlmv2-krb`	Le SVM accepte la sécurité d'authentification NTLMv2 et Kerberos. Le SVM refuse l'authentification LM et NTLM.
`krb`	Le SVM n'accepte que la sécurité d'authentification Kerberos. Le SVM refuse l'authentification LM, NTLM et NTLMv2.

Étapes

1. Définissez le niveau de sécurité d'authentification minimum : `vserver cifs security modify -vserver` *`vserver_name`* `-lm-compatibility-level {lm-ntlm-ntlmv2-krb|ntlm-ntlmv2-krb|ntlmv2-krb|krb}`
2. Vérifiez que le niveau de sécurité d'authentification est défini sur le niveau souhaité : `vserver cifs security show -vserver` *`vserver_name`*

Informations associées

Activation ou désactivation du chiffrement AES pour les communications basées sur Kerberos

Configurez une sécurité forte pour les communications Kerberos à l'aide du chiffrement AES

Pour une sécurité renforcée avec les communications basées sur Kerberos, vous pouvez activer le chiffrement AES-256 et AES-128 sur le serveur SMB. Par défaut, lorsque vous créez un serveur SMB sur le SVM, le chiffrement Advanced Encryption Standard (AES) est désactivé. Elle doit permettre aux services IT de bénéficier de la sécurité renforcée fournie par le cryptage AES.

La communication Kerberos pour SMB est utilisée lors de la création du serveur SMB sur le SVM, ainsi que lors de la phase d'installation de la session SMB. Le serveur SMB prend en charge les types de chiffrement suivants pour les communications Kerberos :

- AES 256
- AES 128
- DES
- RC4-HMAC

Si vous souhaitez utiliser le type de chiffrement le plus élevé pour les communications Kerberos, vous devez activer le chiffrement AES pour la communication Kerberos sur la SVM.

Lorsque le serveur SMB est créé, le contrôleur de domaine crée un compte de machine informatique dans Active Directory. À l'heure actuelle, le KDC prend connaissance des capacités de cryptage du compte machine particulier. Par la suite, un type de chiffrement particulier est sélectionné pour le chiffrement du ticket de service que le client présente au serveur lors de l'authentification.

À partir de ONTAP 9.12.1, vous pouvez spécifier les types de cryptage à publier sur le KDC Active Directory (AD). Vous pouvez utiliser le `-advertised-enc-types` pour activer les types de cryptage recommandés, vous pouvez l'utiliser pour désactiver les types de cryptage les plus faibles. Découvrez comment "Activez et désactivez les types de cryptage pour les communications Kerberos".

> Intel AES New instructions (Intel AES ni) est disponible dans SMB 3.0. Il améliore l'algorithme AES et accélère le chiffrement des données avec les familles de processeurs prises en charge.à partir de SMB 3.1.1, AES-128-GCM remplace AES-128-CCM en tant qu'algorithme de hachage utilisé par le chiffrement SMB.

Informations associées

Modification des paramètres de sécurité Kerberos du serveur CIFS

Activez ou désactivez le chiffrement AES pour les communications basées sur Kerberos

Pour bénéficier de la sécurité la plus forte des communications basées sur Kerberos, vous devez utiliser le chiffrement AES-256 et AES-128 sur le serveur SMB. À partir de ONTAP 9.13.1, le chiffrement AES est activé par défaut. Si vous ne souhaitez pas que le serveur SMB sélectionne les types de cryptage AES pour les communications basées sur Kerberos avec le KDC Active Directory (AD), vous pouvez désactiver le cryptage AES.

Le fait que le cryptage AES soit activé par défaut et que vous puissiez spécifier des types de cryptage dépend de votre version de ONTAP.

Version ONTAP	Le cryptage AES est activé …	Vous pouvez spécifier des types de cryptage ?
9.13.1 et versions ultérieures	Par défaut	Oui.
9.12.1	Manuellement	Oui.
9.11.1 et versions antérieures	Manuellement	Non

Depuis ONTAP 9.12.1, le chiffrement AES est activé et désactivé à l'aide du `-advertised-enc-types` Cette option permet de spécifier les types de cryptage annoncés dans AD KDC. Le paramètre par défaut est `rc4` et `des`, Mais lorsqu'un type AES est spécifié, le cryptage AES est activé. Vous pouvez également utiliser l'option pour désactiver explicitement les types de cryptage RC4 et DES les plus faibles. Dans ONTAP 9.11.1 et les versions antérieures, vous devez utiliser le `-is-aes-encryption-enabled` Option permettant d'activer et de désactiver le cryptage AES, et les types de cryptage ne peuvent pas être spécifiés.

Pour renforcer la sécurité, la machine virtuelle de stockage (SVM) modifie le mot de passe de son compte machine dans l'AD à chaque modification de l'option de sécurité AES. La modification du mot de passe peut nécessiter des informations d'identification AD administratives pour l'unité organisationnelle qui contient le compte de la machine.

Si un SVM est configuré en tant que destination de reprise sur incident où l'identité n'est pas conservée (le `-identity-preserve` l'option est définie sur `false` Dans la configuration SnapMirror), les paramètres de sécurité du serveur SMB non par défaut ne sont pas répliqués sur la destination. Si vous avez activé le chiffrement AES sur la SVM source, vous devez l'activer manuellement.

Exemple 1. Étapes

ONTAP 9.12.1 et versions ultérieures

1. Effectuez l'une des opérations suivantes :

Si vous souhaitez que les types de cryptage AES soient utilisés pour les communications Kerberos…	Entrez la commande…
Activé	`vserver cifs security modify -vserver vserver_name -advertised -enc-types aes-128,aes-256`
Désactivé	`vserver cifs security modify -vserver vserver_name -advertised -enc-types des,rc4`

   Remarque : le `-is-aes-encryption-enabled` Cette option est obsolète dans ONTAP 9.12.1 et peut être supprimée dans une version ultérieure.

2. Vérifiez que le chiffrement AES est activé ou désactivé selon les besoins : `vserver cifs security show -vserver vserver_name -fields advertised-enc-types`

Exemples

L'exemple suivant active les types de chiffrement AES pour le serveur SMB sur SVM vs1 :

```
cluster1::> vserver cifs security modify -vserver vs1 -advertised-enc
-types aes-128,aes-256

cluster1::> vserver cifs security show -vserver vs1 -fields advertised-
enc-types

vserver  advertised-enc-types
-------- --------------------
vs1      aes-128,aes-256
```

L'exemple suivant active les types de cryptage AES pour le serveur SMB sur le SVM vs2. L'administrateur est invité à saisir les informations d'identification AD d'administration pour l'UO contenant le serveur SMB.

```
cluster1::> vserver cifs security modify -vserver vs2 -advertised-enc
-types aes-128,aes-256

Info: In order to enable SMB AES encryption, the password for the SMB
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields advertised-
enc-types

vserver  advertised-enc-types
-------- --------------------
vs2      aes-128,aes-256
```

ONTAP 9.11.1 et versions antérieures

1. Effectuez l'une des opérations suivantes :

Si vous souhaitez que les types de cryptage AES soient utilisés pour les communications Kerberos…	Entrez la commande…
Activé	`vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled true`
Désactivé	`vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled false`

2. Vérifiez que le chiffrement AES est activé ou désactivé selon les besoins : `vserver cifs security show -vserver vserver_name -fields is-aes-encryption-enabled`

   Le `is-aes-encryption-enabled` s'affiche `true` Si le cryptage AES est activé et `false` s'il est désactivé.

Exemples

L'exemple suivant active les types de chiffrement AES pour le serveur SMB sur SVM vs1 :

```
cluster1::> vserver cifs security modify -vserver vs1 -is-aes
-encryption-enabled true

cluster1::> vserver cifs security show -vserver vs1 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-------- -------------------------
vs1      true
```

L'exemple suivant active les types de cryptage AES pour le serveur SMB sur le SVM vs2. L'administrateur est invité à saisir les informations d'identification AD d'administration pour l'UO contenant le serveur SMB.

```
cluster1::> vserver cifs security modify -vserver vs2 -is-aes
-encryption-enabled true

Info: In order to enable SMB AES encryption, the password for the CIFS
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-------- -------------------------
vs2      true
```

Utilisez la signature SMB pour améliorer la sécurité du réseau

Utilisez la signature SMB pour améliorer la présentation de la sécurité réseau

La signature SMB contribue à garantir que le trafic réseau entre le serveur SMB et le client n'est pas compromis. Elle empêche les attaques de relecture. Par défaut, ONTAP prend en charge la signature SMB sur demande du client. L'administrateur du stockage peut éventuellement configurer le serveur SMB afin de nécessiter une signature SMB.

Comment les stratégies de signature SMB affectent la communication avec un serveur CIFS

Outre les paramètres de sécurité de signature SMB du serveur CIFS, deux stratégies de signature SMB sur les clients Windows contrôlent la signature numérique des communications entre les clients et le serveur CIFS. Vous pouvez configurer le paramètre qui répond aux besoins de votre entreprise.

Les stratégies SMB du client sont contrôlées via les paramètres de stratégie de sécurité locale de Windows, qui sont configurés à l'aide des stratégies de groupe MMC (Microsoft Management Console) ou Active Directory. Pour plus d'informations sur les problèmes de sécurité et de signature SMB du client, consultez la documentation Microsoft Windows.

Voici les descriptions des deux stratégies de signature SMB sur les clients Microsoft :

- `Microsoft network client: Digitally sign communications (if server agrees)`

  Ce paramètre détermine si la fonctionnalité de signature SMB du client est activée. Elle est activée par défaut. Lorsque ce paramètre est désactivé sur le client, les communications client avec le serveur CIFS dépendent du paramètre de signature SMB sur le serveur CIFS.

- `Microsoft network client: Digitally sign communications (always)`

  Ce paramètre détermine si le client requiert la signature SMB pour communiquer avec un serveur. Elle est désactivée par défaut. Lorsque ce paramètre est désactivé sur le client, le comportement de signature SMB est basé sur le paramètre de stratégie pour `Microsoft network client: Digitally sign communications (if server agrees)` Et le paramètre sur le serveur CIFS.

> Si votre environnement inclut des clients Windows configurés pour exiger une signature SMB, vous devez activer la signature SMB sur le serveur CIFS. Dans le cas contraire, le serveur CIFS ne peut pas transmettre de données à ces systèmes.

Les résultats effectifs des paramètres de signature SMB du client et du serveur CIFS dépendent du fait que les sessions SMB utilisent SMB 1.0 ou SMB 2.x et versions ultérieures.

Le tableau suivant récapitule le comportement de signature SMB efficace si la session utilise SMB 1.0 :

Client	Signature ONTAP : non requise	Signature ONTAP requise
Signature désactivée et non requise	Non signé	Signé
Signature activée et non requise	Non signé	Signé
Signature désactivée et requise	Signé	Signé
Signature activée et requise	Signé	Signé

> Les anciens clients Windows SMB 1 et certains clients non Windows SMB 1 peuvent ne pas se connecter si la signature est désactivée sur le client mais requise sur le serveur CIFS.

Le tableau suivant récapitule le comportement de signature SMB efficace si la session utilise SMB 2.x ou SMB 3.0 :

> Pour les clients SMB 2.x et SMB 3.0, la signature SMB est toujours activée. Elle ne peut pas être désactivée.

Client	Signature ONTAP : non requise	Signature ONTAP requise
Signature non requise	Non signé	Signé
Signature requise	Signé	Signé

Le tableau suivant récapitule le comportement de signature SMB du serveur et du client Microsoft par défaut :

Protocole	Algorithme de hachage	Peut activer/désactiver	Peut exiger/non requis	Client par défaut	Serveur par défaut	DC par défaut
SMB 1.0	MD5	Oui.	Oui.	Activé (non requis)	Désactivé (non requis)	Obligatoire
SMB 2.x	HMAC SHA-256	Non	Oui.	Non requis	Non requis	Obligatoire
SMB 3.0	AES-CMAC.	Non	Oui.	Non requis	Non requis	Obligatoire

> Microsoft ne recommande plus d'utiliser `Digitally sign communications (if client agrees)` ou `Digitally sign communications (if server agrees)` Paramètres de stratégie de groupe. Microsoft ne recommande plus par ailleurs l'utilisation du `EnableSecuritySignature` paramètres du registre. Ces options n'affectent que le comportement du SMB 1 et peuvent être remplacées par le `Digitally sign communications (always)` Stratégie de groupe ou `RequireSecuritySignature` paramètre de registre. Vous pouvez également obtenir plus d'informations sur le blog Microsoft.principes de base de la signature SMB The (SMB1 et SMB2)

Impact de la signature SMB sur les performances

Lorsque les sessions SMB utilisent la signature SMB, toutes les communications SMB vers et depuis les clients Windows subissent un impact sur les performances, ce qui affecte à la fois les clients et le serveur (c'est-à-dire les nœuds sur le cluster exécutant le SVM contenant le serveur SMB).

L'impact sur les performances indique que l'utilisation accrue du CPU sur les clients et le serveur est augmentée, même si le volume du trafic réseau ne change pas.

La mesure de l'impact sur les performances dépend de la version de ONTAP 9 que vous utilisez. Depuis ONTAP 9.7, un nouvel algorithme de déchargement du cryptage peut permettre d'améliorer les performances du trafic SMB signé. L'allègement de la charge des signatures SMB est activé par défaut lorsque la signature SMB est activée.

L'amélioration des performances de signature SMB requiert une fonctionnalité de déchargement AES-ni. Consultez le Hardware Universe (HWU) pour vérifier que le déchargement AES-ni est pris en charge par votre plate-forme.

D'autres améliorations des performances sont également possibles si vous pouvez utiliser SMB version 3.11 qui prend en charge l'algorithme GCM beaucoup plus rapide.

Selon votre réseau, la version ONTAP 9, la version SMB et l'implémentation SVM, l'impact de la signature SMB sur les performances peut varier fortement. Vous pouvez la vérifier uniquement par le biais de tests dans l'environnement réseau.

La plupart des clients Windows négocient la signature SMB par défaut si elle est activée sur le serveur. Si vous avez besoin d'une protection SMB pour certains de vos clients Windows et si le SMB Signing génère des problèmes de performances, vous pouvez désactiver la signature SMB sur l'un de vos clients Windows ne nécessitant pas de protection contre les attaques de rejeu. Pour plus d'informations sur la désactivation de la signature SMB sur les clients Windows, consultez la documentation Microsoft Windows.

Recommandations pour la configuration de la signature SMB

Vous pouvez configurer le comportement de signature SMB entre les clients SMB et le serveur CIFS pour répondre à vos exigences de sécurité. Les paramètres que vous choisissez lors de la configuration de la signature SMB sur votre serveur CIFS dépendent de vos exigences de sécurité.

Vous pouvez configurer la signature SMB sur le client ou sur le serveur CIFS. Tenez compte des recommandations suivantes lors de la configuration de la signature SMB :

Si…	Recommandation…
Vous souhaitez augmenter la sécurité de la communication entre le client et le serveur	Assurez-vous que le SMB Signing est requis au niveau du client en activant le `Require Option (Sign always)` paramètre de sécurité sur le client.
Vous souhaitez que tous les trafics SMB vers une certaine machine virtuelle de stockage (SVM) signée	Configurez les paramètres de sécurité pour exiger la signature SMB sur le serveur CIFS.

Pour plus d'informations sur la configuration des paramètres de sécurité du client Windows, reportez-vous à la documentation Microsoft.

Consignes de signature SMB lorsque plusieurs LIF de données sont configurées

Si vous activez ou désactivez le SMB Signing requis sur le serveur SMB, vous devez connaître les instructions relatives aux configurations de plusieurs LIF de données pour un SVM.

Lorsque vous configurez un serveur SMB, plusieurs LIF de données peuvent être configurées. Si c'est le cas, le serveur DNS contient plusieurs `A` Entrées d'enregistrement pour le serveur CIFS, toutes utilisant le même nom d'hôte de serveur SMB, mais chacune avec une adresse IP unique. Par exemple, un serveur SMB dont deux LIF de données sont configurées peut avoir le DNS suivant `A` entrées d'enregistrement :

```
10.1.1.128 A VS1.IEPUB.LOCAL VS1
10.1.1.129 A VS1.IEPUB.LOCAL VS1
```

Le comportement normal est qu'après modification du paramètre de signature SMB requis, seules les nouvelles connexions des clients sont affectées par la modification du paramètre de signature SMB. Cependant, il y a une exception à ce comportement. Il existe un cas où un client dispose d'une connexion existante à un partage, et le client crée une nouvelle connexion au même partage après la modification du paramètre, tout en maintenant la connexion d'origine. Dans ce cas, la connexion SMB, nouvelle et existante, adopte les nouvelles exigences de signature SMB.

Prenons l'exemple suivant :

1. Client1 se connecte à un partage sans avoir à signer SMB à l'aide du chemin `O:\`.
2. L'administrateur du stockage modifie la configuration du serveur SMB afin de exiger la signature SMB.
3. Client1 se connecte au même partage avec la signature SMB requise à l'aide du chemin `S:\` (tout en maintenant la connexion à l'aide du chemin `O:\`).
4. Par conséquent, le SMB Signing est utilisé pour accéder aux données sur le système `O:\` et `S:\` disques.

Activer ou désactiver la signature SMB requise pour le trafic SMB entrant

Vous pouvez imposer aux clients l'exigence de signer les messages SMB en activant la signature SMB requise. S'il est activé, ONTAP n'accepte que les messages SMB s'ils ont une signature valide. Si vous souhaitez autoriser la signature SMB, mais pas l'exiger, vous pouvez désactiver la signature SMB requise.

Description de la tâche

Par défaut, le SMB Signing requis est désactivé. Vous pouvez activer ou désactiver la signature SMB requise à tout moment.

> La signature SMB n'est pas désactivée par défaut dans les cas suivants :
>
> 1. Le signature SMB requis est activé et le cluster est rétabli sur une version d'ONTAP qui ne prend pas en charge la signature SMB.
> 2. Le cluster est ensuite mis à niveau vers une version de ONTAP qui prend en charge la signature SMB.
>
> Dans ce cas, la configuration de signature SMB qui a été configurée à l'origine sur une version prise en charge de ONTAP est conservée par le biais d'une nouvelle version et d'une mise à niveau ultérieure.

Lorsque vous configurez une relation de reprise d'activité de machine virtuelle de stockage (SVM), la valeur que vous sélectionnez pour le système `-identity-preserve` de la `snapmirror create` La commande détermine les détails de configuration répliqués dans le SVM de destination.

Si vous définissez le `-identity-preserve` option à `true` (ID-preserve), le paramètre de sécurité de signature SMB est répliqué sur la destination.

Si vous définissez le `-identity-preserve` option à `false` (Non-ID-preserve), le paramètre de sécurité de

signature SMB n'est pas répliqué sur la destination. Dans ce cas, les paramètres de sécurité du serveur CIFS sur la destination sont définis sur les valeurs par défaut. Si vous avez activé la signature SMB requise sur le SVM source, vous devez activer manuellement le SMB Signing requis sur le SVM de destination.

Étapes

1. Effectuez l'une des opérations suivantes :

Si vous souhaitez que le SMB soit connecté…	Entrez la commande…
Activé	`vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required true`
Désactivé	`vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required false`

2. Vérifiez que la signature SMB requise est activée ou désactivée en déterminant si la valeur dans l' `Is Signing Required` le champ de la sortie de la commande suivante est défini sur la valeur souhaitée : `vserver cifs security show -vserver` *`vserver_name`* `-fields is-signing-required`

Exemple

L'exemple suivant active la signature SMB requise pour le SVM vs1 :

```
cluster1::> vserver cifs security modify -vserver vs1 -is-signing-required
true

cluster1::> vserver cifs security show -vserver vs1 -fields is-signing-
required
vserver  is-signing-required
-------- -------------------
vs1      true
```

Les modifications apportées aux paramètres de cryptage prennent effet pour les nouvelles connexions. Les connexions existantes ne sont pas affectées.

Déterminez si les sessions SMB sont signées

Vous pouvez afficher des informations sur les sessions SMB connectées sur le serveur CIFS. Vous pouvez utiliser ces informations pour déterminer si les sessions SMB sont signées. Cela peut être utile pour déterminer si les sessions client SMB se connectent aux paramètres de sécurité souhaités.

Étapes

1. Effectuez l'une des opérations suivantes :

Si vous voulez afficher des informations sur…	Entrez la commande…
Toutes les sessions signées sur une machine virtuelle de stockage (SVM) spécifiée	`vserver cifs session show -vserver` *`vserver_name`* `-is-session-signed true`
Détails d'une session signée avec un ID de session spécifique sur le SVM	`vserver cifs session show -vserver` *`vserver_name`* `-session-id integer -instance`

Exemples

La commande suivante affiche les informations relatives aux sessions signées sur le SVM vs1. La sortie de résumé par défaut n'affiche pas le champ de sortie « session signée is » :

```
cluster1::> vserver cifs session show -vserver vs1 -is-session-signed true
Node:    node1
Vserver: vs1
Connection Session                                    Open         Idle
ID          ID      Workstation      Windows User    Files         Time
----------  ------- ---------------- ------------- ------- ------------
3151272279  1       10.1.1.1         DOMAIN\joe          2          23s
```

La commande suivante affiche des informations détaillées sur la session, notamment si elle est signée, dans une session SMB avec l'ID de session 2 :

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                        Node: node1
                     Vserver: vs1
                  Session ID: 2
                Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
                  Workstation: 10.1.1.2
    Authentication Mechanism: Kerberos
                 Windows User: DOMAIN\joe
                    UNIX User: pcuser
                  Open Shares: 1
                   Open Files: 1
                   Open Other: 0
               Connected Time: 10m 43s
                    Idle Time: 1m 19s
            Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                 NetBIOS Name: CIFS_ALIAS1
       SMB Encryption Status: Unencrypted
```

Informations associées

Contrôle des statistiques de session signées SMB

Surveiller les statistiques de session signées SMB

Vous pouvez surveiller les statistiques des sessions SMB et déterminer les sessions établies qui sont signées et qui ne le sont pas.

Description de la tâche

Le `statistics` la commande au niveau de privilège avancé fournit le `signed_sessions` Compteur que vous pouvez utiliser pour surveiller le nombre de sessions SMB signées. Le `signed_sessions` le compteur est disponible avec les objets de statistiques suivants :

- `cifs` Permet de surveiller la signature SMB pour toutes les sessions SMB.
- `smb1` Permet de surveiller la signature SMB pour les sessions SMB 1.0.
- `smb2` Permet de surveiller la signature SMB pour les sessions SMB 2.x et SMB 3.0.

  Les statistiques SMB 3.0 sont incluses dans les résultats de `smb2` objet.

Si vous souhaitez comparer le nombre de sessions signées au nombre total de sessions, vous pouvez comparer les résultats de la session `signed_sessions` compteur avec la sortie pour le `established_sessions` compteur.

Vous devez démarrer une collecte d'échantillons de statistiques avant de pouvoir afficher les données

résultantes. Vous pouvez afficher les données de l'échantillon si vous n'arrêtez pas la collecte de données. L'arrêt de la collecte de données vous donne un échantillon fixe. L'option ne pas arrêter la collecte de données vous permet d'obtenir des données mises à jour que vous pouvez utiliser pour comparer à des requêtes précédentes. La comparaison vous aide à identifier les tendances.

Étapes

1. Définissez le niveau de privilège sur avancé :
   `set -privilege advanced`
2. Démarrer une collecte de données :
   `statistics start -object {cifs|smb1|smb2} -instance instance -sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   Si vous ne spécifiez pas le `-sample-id` Paramètre, la commande génère un exemple d'identificateur pour vous et définit cet échantillon comme échantillon par défaut pour la session de l'interface de ligne de commande. La valeur pour `-sample-id` est une chaîne de texte. Si vous exécutez cette commande pendant la même session CLI et ne spécifiez pas le `-sample-id` paramètre, la commande remplace l'échantillon par défaut précédent.

   Vous pouvez spécifier le nœud sur lequel vous souhaitez collecter les statistiques. Si vous ne spécifiez pas le nœud, l'exemple collecte les statistiques de tous les nœuds du cluster.
3. Utilisez le `statistics stop` commande pour arrêter la collecte des données de l'échantillon.
4. Afficher les statistiques de signature SMB :

Si vous souhaitez afficher les informations pour…	**Entrer…**
Sessions signées	`show -sample-id sample_ID -counter signed_sessions
node_name [-node *node_name*]`	Sessions signées et sessions établies
`show -sample-id *sample_ID* -counter signed_sessions	established_sessions

   Si vous souhaitez afficher les informations pour un seul nœud, spécifiez l'option `-node` paramètre.

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

Exemples

L'exemple suivant montre comment surveiller les statistiques de signature SMB 2.x et SMB 3.0 sur la machine virtuelle de stockage (SVM) vs1.

La commande suivante permet d'accéder au niveau de privilège avancé :

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

La commande suivante démarre la collecte de données pour un nouvel échantillon :

```
cluster1::*> statistics start -object smb2 -sample-id smbsigning_sample
-vserver vs1
Statistics collection is being started for Sample-id: smbsigning_sample
```

La commande suivante arrête la collecte des données de l'échantillon :

```
cluster1::*> statistics stop -sample-id smbsigning_sample
Statistics collection is being stopped for Sample-id: smbsigning_sample
```

La commande suivante affiche les sessions SMB signées et les sessions SMB établies par nœud à partir de l'exemple :

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|established_sessions|node_name

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:03:04
Cluster: cluster1

    Counter                                                  Value
    -------------------------------- -------------------------
    established_sessions                                         0
    node_name                                                node1
    signed_sessions                                              0
    established_sessions                                         1
    node_name                                                node2
    signed_sessions                                              1
    established_sessions                                         0
    node_name                                                node3
    signed_sessions                                              0
    established_sessions                                         0
    node_name                                                node4
    signed_sessions                                              0
```

La commande suivante affiche les sessions SMB signées pour le nœud 2 à partir de l'exemple :

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|node_name -node node2

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:22:43
Cluster: cluster1

    Counter                                                  Value
    -------------------------------- -------------------------
    node_name                                                node2
    signed_sessions                                              1
```

La commande suivante revient au niveau de privilège admin :

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

Informations associées

Détermination de la signature des sessions SMB

"Contrôle des performances et présentation de la gestion"

Configurez le chiffrement SMB requis sur les serveurs SMB pour les transferts de données via SMB

Présentation du chiffrement SMB

Le chiffrement SMB pour les transferts de données via SMB est une amélioration de sécurité que vous pouvez activer ou désactiver sur les serveurs SMB. Vous pouvez également configurer le paramètre de chiffrement SMB souhaité sur une base partage par partage à l'aide d'un paramètre de propriété de partage.

Par défaut, lorsque vous créez un serveur SMB sur la machine virtuelle de stockage (SVM), le chiffrement SMB est désactivé. Vous devez leur permettre de bénéficier de la sécurité améliorée fournie par le chiffrement SMB.

Pour créer une session SMB chiffrée, le client SMB doit prendre en charge le chiffrement SMB. Les clients Windows commençant par Windows Server 2012 et Windows 8 prennent en charge le cryptage SMB.

Le chiffrement SMB sur la SVM est contrôlé par deux paramètres :

- Option de sécurité du serveur SMB qui active la fonctionnalité sur le SVM
- Propriété de partage SMB qui configure le paramètre de chiffrement SMB partage par partage

Vous pouvez décider s'il faut un chiffrement pour accéder à toutes les données de la SVM ou bien demander un chiffrement SMB pour accéder aux données uniquement dans les partages sélectionnés. Les paramètres des SVM prévalent sur les paramètres de niveau partage.

La configuration de cryptage SMB efficace dépend de la combinaison des deux paramètres. Elle est décrite dans le tableau suivant :

Chiffrement SMB du serveur SMB activé	Le paramètre partage des données de chiffrement est activé	Comportement de cryptage côté serveur
Vrai	Faux	Le chiffrement au niveau du serveur est activé pour tous les partages du SVM. Avec cette configuration, le chiffrement s'effectue pour toute la session SMB.
Vrai	Vrai	Le chiffrement au niveau du serveur est activé pour tous les partages de la SVM indépendamment du chiffrement au niveau du partage. Avec cette configuration, le chiffrement s'effectue pour toute la session SMB.

Chiffrement SMB du serveur SMB activé	Le paramètre partage des données de chiffrement est activé	Comportement de cryptage côté serveur
Faux	Vrai	Le chiffrement au niveau du partage est activé pour les partages spécifiques. Avec cette configuration, le chiffrement se produit à partir de l'arborescence à connecter.
Faux	Faux	Aucun chiffrement n'est activé.

Les clients SMB qui ne prennent pas en charge le chiffrement ne peuvent pas se connecter à un serveur SMB ou à un partage qui nécessite un chiffrement.

Les modifications apportées aux paramètres de cryptage prennent effet pour les nouvelles connexions. Les connexions existantes ne sont pas affectées.

Impact du chiffrement SMB sur les performances

Lorsque les sessions SMB utilisent le chiffrement SMB, toutes les communications SMB vers et depuis les clients Windows rencontrent un impact sur les performances, qui affecte à la fois les clients et le serveur (c'est-à-dire les nœuds sur le cluster exécutant le SVM qui contient le serveur SMB).

L'impact sur les performances indique que l'utilisation accrue du CPU sur les clients et le serveur est augmentée, même si le volume du trafic réseau ne change pas.

La mesure de l'impact sur les performances dépend de la version de ONTAP 9 que vous utilisez. Depuis ONTAP 9.7, un nouvel algorithme de désactivation du chiffrement permet d'améliorer les performances du trafic SMB chiffré. Le délestage du chiffrement SMB est activé par défaut lorsque le chiffrement SMB est activé.

L'optimisation des performances de chiffrement SMB requiert une fonctionnalité de déchargement AES-ni. Consultez le Hardware Universe (HWU) pour vérifier que le déchargement AES-ni est pris en charge par votre plate-forme.

D'autres améliorations des performances sont également possibles si vous pouvez utiliser SMB version 3.11 qui prend en charge l'algorithme GCM beaucoup plus rapide.

Selon votre réseau, la version ONTAP 9, la version SMB et l'implémentation SVM, l'impact du cryptage SMB sur les performances peut varier fortement. Vous pouvez le vérifier uniquement par le biais de tests dans l'environnement réseau.

Le chiffrement SMB est désactivé par défaut sur le serveur SMB. Vous devez activer le chiffrement SMB uniquement sur les partages SMB ou les serveurs SMB qui nécessitent un chiffrement. Avec le cryptage SMB, ONTAP effectue un traitement supplémentaire du décryptage des demandes et du cryptage des réponses à chaque demande. Le chiffrement SMB ne doit donc être activé que lorsque cela est nécessaire.

Activez ou désactivez le chiffrement SMB requis pour le trafic SMB entrant

Si vous souhaitez exiger le cryptage SMB pour le trafic SMB entrant, vous pouvez l'activer sur le serveur CIFS ou au niveau du partage. Par défaut, le chiffrement SMB n'est pas requis.

Description de la tâche

Vous pouvez activer le chiffrement SMB sur le serveur CIFS, qui s'applique à tous les partages du serveur CIFS. Si vous ne souhaitez pas utiliser le cryptage SMB requis pour tous les partages du serveur CIFS ou si vous souhaitez activer le cryptage SMB requis pour le trafic SMB entrant, partage par partage, vous pouvez désactiver le cryptage SMB requis sur le serveur CIFS.

Lorsque vous configurez une relation de reprise d'activité de machine virtuelle de stockage (SVM), la valeur que vous sélectionnez pour le système `-identity-preserve` de la `snapmirror create` La commande détermine les détails de configuration répliqués dans le SVM de destination.

Si vous définissez le `-identity-preserve` option à `true` (ID-preserve), le paramètre de sécurité du cryptage SMB est répliqué sur la destination.

Si vous définissez le `-identity-preserve` option à `false` (Non ID-preserve), le paramètre de sécurité du cryptage SMB n'est pas répliqué sur la destination. Dans ce cas, les paramètres de sécurité du serveur CIFS sur la destination sont définis sur les valeurs par défaut. Si vous avez activé le chiffrement SMB sur le SVM source, vous devez activer manuellement le chiffrement SMB du serveur CIFS sur la destination.

Étapes

1. Effectuez l'une des opérations suivantes :

Si vous souhaitez que le chiffrement SMB soit requis pour le trafic SMB entrant sur le serveur CIFS…	Entrez la commande…
Activé	`vserver cifs security modify -vserver` *`vserver_name`* `-is-smb-encryption -required true`
Désactivé	`vserver cifs security modify -vserver` *`vserver_name`* `-is-smb-encryption -required false`

2. Vérifiez que le chiffrement SMB requis sur le serveur CIFS est activé ou désactivé, selon les besoins : `vserver cifs security show -vserver` *`vserver_name`* `-fields is-smb-encryption-required`

   Le `is-smb-encryption-required` s'affiche `true` Le cas échéant, le cryptage SMB est activé sur le serveur CIFS et `false` s'il est désactivé.

Exemple

L'exemple suivant permet le cryptage SMB requis pour le trafic SMB entrant pour le serveur CIFS sur le SVM vs1 :

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption
-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-
encryption-required
vserver  is-smb-encryption-required
-------- -------------------------
vs1      true
```

Déterminez si les clients sont connectés à l'aide de sessions SMB cryptées

Vous pouvez afficher des informations sur les sessions SMB connectées pour déterminer si les clients utilisent des connexions SMB chiffrées. Cela peut être utile pour déterminer si les sessions client SMB se connectent aux paramètres de sécurité souhaités.

Description de la tâche

Les sessions client SMB peuvent avoir l'un des trois niveaux de chiffrement suivants :

- `unencrypted`

  La session SMB n'est pas chiffrée. Ni le chiffrement au niveau des serveurs virtuels de stockage ou du partage n'est configuré.

- `partially-encrypted`

  Le chiffrement est lancé lorsque l'arborescence se connecte. Le chiffrement au niveau du partage est configuré. Le chiffrement au niveau des SVM n'est pas activé.

- `encrypted`

  La session SMB est entièrement chiffrée. Le chiffrement au niveau des SVM est activé. Le chiffrement au niveau du partage peut être activé ou non. Le paramètre de cryptage au niveau SVM remplace le paramètre de cryptage au niveau du partage.

Étapes

1. Effectuez l'une des opérations suivantes :

Si vous voulez afficher des informations sur…	Entrez la commande…
Sessions avec un paramètre de chiffrement spécifié pour les sessions sur un SVM spécifié	`vserver cifs session show -vserver *vserver_name* {unencrypted
partially-encrypted	encrypted} -instance`
Paramètre de chiffrement pour un ID de session spécifique sur un SVM spécifié	`vserver cifs session show -vserver *vserver_name* -session-id *integer* -instance`

Exemples

La commande suivante affiche des informations détaillées sur la session, y compris le paramètre de chiffrement, sur une session SMB avec l'ID de session 2 :

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                        Node: node1
                     Vserver: vs1
                  Session ID: 2
                Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
                  Workstation: 10.1.1.2
    Authentication Mechanism: Kerberos
                 Windows User: DOMAIN\joe
                    UNIX User: pcuser
                  Open Shares: 1
                   Open Files: 1
                   Open Other: 0
               Connected Time: 10m 43s
                    Idle Time: 1m 19s
            Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                 NetBIOS Name: CIFS_ALIAS1
       SMB Encryption Status: Unencrypted
```

Contrôle des statistiques de chiffrement SMB

Vous pouvez surveiller les statistiques de cryptage SMB et déterminer les sessions établies et les connexions de partage qui sont cryptées et qui ne le sont pas.

Description de la tâche

Le `statistics` Le niveau de privilège avancé fournit les compteurs suivants, que vous pouvez utiliser pour surveiller le nombre de sessions SMB chiffrées et de connexions pour le partage :

Nom du compteur	Descriptions
`encrypted_sessions`	Indique le nombre de sessions SMB 3.0 cryptées
`encrypted_share_connections`	Indique le nombre de partages cryptés sur lesquels une arborescence s'est connectée
`rejected_unencrypted_sessions`	Indique le nombre de configurations de session rejetées en raison d'un manque de capacité de chiffrement du client

Nom du compteur	Descriptions
`rejected_unencrypted_shares`	Indique le nombre de mappages de partage rejetés en raison d'un manque de capacité de chiffrement du client

Ces compteurs sont disponibles avec les objets de statistiques suivants :

- `cifs` Permet de surveiller le chiffrement SMB pour toutes les sessions SMB 3.0.

  Les statistiques SMB 3.0 sont incluses dans les résultats de `cifs` objet. Si vous souhaitez comparer le nombre de sessions chiffrées au nombre total de sessions, vous pouvez comparer les résultats de l' `encrypted_sessions` compteur avec la sortie pour le `established_sessions` compteur.

  Si vous souhaitez comparer le nombre de connexions de partage chiffrées au nombre total de connexions de partage, vous pouvez comparer la sortie du `encrypted_share_connections` compteur avec la sortie pour le `connected_shares` compteur.

- `rejected_unencrypted_sessions` Indique le nombre de tentatives d'établissement d'une session SMB nécessitant un chiffrement d'un client qui ne prend pas en charge le chiffrement SMB.
- `rejected_unencrypted_shares` Indique combien de fois une tentative de connexion à un partage SMB nécessite un chiffrement d'un client ne prenant pas en charge le chiffrement SMB.

Vous devez démarrer une collecte d'échantillons de statistiques avant de pouvoir afficher les données résultantes. Vous pouvez afficher les données de l'échantillon si vous n'arrêtez pas la collecte de données. L'arrêt de la collecte de données vous donne un échantillon fixe. L'option ne pas arrêter la collecte de données vous permet d'obtenir des données mises à jour que vous pouvez utiliser pour comparer à des requêtes précédentes. La comparaison vous aide à identifier les tendances.

Étapes

1. Définissez le niveau de privilège sur avancé :
   `set -privilege advanced`
2. Démarrer une collecte de données :
   `statistics start -object {cifs|smb1|smb2} -instance` *`instance`* `-sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   Si vous ne spécifiez pas le `-sample-id` Paramètre, la commande génère un exemple d'identificateur pour vous et définit cet échantillon comme échantillon par défaut pour la session de l'interface de ligne de commande. La valeur pour `-sample-id` est une chaîne de texte. Si vous exécutez cette commande pendant la même session CLI et ne spécifiez pas le `-sample-id` paramètre, la commande remplace l'échantillon par défaut précédent.

   Vous pouvez spécifier le nœud sur lequel vous souhaitez collecter les statistiques. Si vous ne spécifiez pas le nœud, l'exemple collecte les statistiques de tous les nœuds du cluster.

3. Utilisez le `statistics stop` commande pour arrêter la collecte des données de l'échantillon.
4. Afficher les statistiques de chiffrement SMB :

Si vous souhaitez afficher les informations pour…	Entrer…
Sessions chiffrées	`show -sample-id *sample_ID* -counter encrypted_sessions
node_name [-node *node_name*]`	Sessions chiffrées et sessions établies
`show -sample-id *sample_ID* -counter encrypted_sessions	established_sessions
node_name [-node *node_name*]`	Connexions de partage cryptées
`show -sample-id *sample_ID* -counter encrypted_share_connections	*node_name* [-node *node_name*]`
Connexions de partage cryptées et partages connectés	`show -sample-id *sample_ID* -counter encrypted_share_connections
connected_shares	*node_name* [-node *node_name*]`
Sessions non chiffrées rejetées rejetées	`show -sample-id *sample_ID* -counter rejected_unencrypted_sessions
node_name [-node *node_name*]`	Les connexions de partage non chiffrées ont été rejetées
`show -sample-id *sample_ID* -counter rejected_unencrypted_share	*node_name* [-node *node_name*]`

Si vous souhaitez afficher les informations uniquement pour un seul nœud, spécifiez l'option `-node` paramètre.

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

Exemples

L'exemple suivant montre comment surveiller les statistiques de cryptage SMB 3.0 sur la machine virtuelle de stockage (SVM) vs1.

La commande suivante permet d'accéder au niveau de privilège avancé :

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

La commande suivante démarre la collecte de données pour un nouvel échantillon :

```
cluster1::*> statistics start -object cifs -sample-id
smbencryption_sample -vserver vs1
Statistics collection is being started for Sample-id:
smbencryption_sample
```

La commande suivante arrête la collecte des données pour cet échantillon :

```
cluster1::*> statistics stop -sample-id smbencryption_sample
Statistics collection is being stopped for Sample-id:
smbencryption_sample
```

La commande suivante affiche les sessions SMB chiffrées et les sessions SMB établies par le nœud à partir de l'exemple :

```
cluster2::*> statistics show -object cifs -counter
established_sessions|encrypted_sessions|node_name -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:45
Scope: vsim2

    Counter                                Value
    ----------------------------  ----------------------
    established_sessions                      1
    encrypted_sessions                        1

2 entries were displayed
```

La commande suivante affiche le nombre de sessions SMB non chiffrées rejetées par le nœud à partir de l'exemple :

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_sessions -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:51
Scope: vsim2

    Counter                                     Value
    ----------------------------    ----------------------
    rejected_unencrypted_sessions                 1

1 entry was displayed.
```

La commande suivante indique le nombre de partages SMB connectés et de partages SMB chiffrés par le nœud à partir de l'exemple :

```
clus-2::*> statistics show -object cifs -counter
connected_shares|encrypted_share_connections|node_name -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:41:43
Scope: vsim2

    Counter                                     Value
    ----------------------------    ----------------------
    connected_shares                              2
    encrypted_share_connections                   1

2 entries were displayed.
```

La commande suivante affiche le nombre de connexions de partage SMB non chiffrées rejetées par le nœud à partir de l'exemple :

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_shares -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:42:06
Scope: vsim2

    Counter                                     Value
    --------------------------------    ----------------------
    rejected_unencrypted_shares                   1

1 entry was displayed.
```

Informations associées

Détermination des objets statistiques et des compteurs disponibles

"Contrôle des performances et présentation de la gestion"

Communication de session LDAP sécurisée

Concepts de signature et d'étanchéité LDAP

Depuis ONTAP 9, vous pouvez configurer la signature et le chiffrement pour activer la sécurité des sessions LDAP sur les requêtes vers un serveur Active Directory (AD). Vous

devez configurer les paramètres de sécurité du serveur CIFS sur la machine virtuelle de stockage (SVM) de sorte qu'ils correspondent à ceux du serveur LDAP.

La signature valide l'intégrité des données LDAP à l'aide d'une technologie à clé secrète. Le chiffrement crypte les données LDAP afin de ne pas transmettre de données sensibles en clair. Une option *LDAP Security Level* indique si le trafic LDAP doit être signé, signé et scellé, ou non. La valeur par défaut est `none`.

La signature et le chiffrement LDAP sur le trafic CIFS sont activés sur le SVM avec le `-session-security -for-ad-ldap` à la `vserver cifs security modify` commande.

Activez le chiffrement et la signature LDAP sur le serveur CIFS

Avant que votre serveur CIFS puisse utiliser la signature et le chiffrement pour sécuriser la communication avec un serveur LDAP Active Directory, vous devez modifier les paramètres de sécurité du serveur CIFS pour activer la signature et le chiffrement LDAP.

Avant de commencer

Vous devez consulter votre administrateur de serveur AD pour déterminer les valeurs de configuration de sécurité appropriées.

Étapes

1. Configurez le paramètre de sécurité du serveur CIFS qui autorise le trafic signé et scellé avec les serveurs LDAP Active Directory : `vserver cifs security modify -vserver vserver_name -session -security-for-ad-ldap {none|sign|seal}`

   Vous pouvez activer la signature (`sign`, intégrité des données), signature et scellage (`seal`, intégrité et chiffrement des données), ou ni l'un ni l'autre `none`, pas de signature ou d'étanchéité). La valeur par défaut est `none`.

2. Vérifiez que le paramètre de sécurité de signature et de chiffrement LDAP est défini correctement : `vserver cifs security show -vserver vserver_name`

> Si le SVM utilise le même serveur LDAP pour effectuer des requêtes name-mapping ou d'autres informations UNIX, comme les utilisateurs, les groupes et les netgroups, alors vous devez activer le paramètre correspondant avec le `-session-security` de la `vserver services name-service ldap client modify` commande.

Configurer LDAP sur TLS

Exporter une copie du certificat de l'autorité de certification racine auto-signé

Pour utiliser LDAP sur SSL/TLS pour sécuriser la communication Active Directory, vous devez d'abord exporter une copie du certificat d'autorité de certification racine auto-signé du service de certificats Active Directory en fichier de certificat et la convertir en fichier texte ASCII. Ce fichier texte est utilisé par ONTAP pour installer le certificat sur la machine virtuelle de stockage (SVM).

Avant de commencer

Le service de certificat Active Directory doit déjà être installé et configuré pour le domaine auquel le serveur CIFS appartient. Vous trouverez des informations sur l'installation et la configuration des services de certificats

Active Director en consultant la bibliothèque Microsoft TechNet.

"Bibliothèque Microsoft TechNet : technet.microsoft.com"

Étape

1. Obtenez un certificat d'autorité de certification racine du contrôleur de domaine qui se trouve dans le `.pem` format de texte.

   "Bibliothèque Microsoft TechNet : technet.microsoft.com"

Une fois que vous avez terminé

Installer le certificat sur le SVM.

Informations associées

"Bibliothèque Microsoft TechNet"

Installer le certificat d'autorité de certification racine auto-signé sur le SVM

Si l'authentification LDAP avec TLS est requise lorsqu'il s'agit de serveurs LDAP, vous devez d'abord installer le certificat AC racine auto-signé sur le SVM.

Description de la tâche

Lorsque LDAP sur TLS est activé, le client LDAP ONTAP sur la SVM ne prend pas en charge les certificats révoqués dans ONTAP 9.0 et 9.1.

Depuis ONTAP 9.2, toutes les applications de ONTAP qui utilisent les communications TLS peuvent vérifier le statut du certificat numérique à l'aide du protocole OCSP (Online Certificate Status Protocol). Si OCSP est activé pour LDAP sur TLS, les certificats révoqués sont rejetés et la connexion échoue.

Étapes

1. Installez le certificat d'autorité de certification racine auto-signé :

   a. Commencez l'installation du certificat : `security certificate install -vserver vserver_name -type server-ca`

      La sortie de la console affiche le message suivant : `Please enter Certificate: Press <Enter> when done`

   b. Ouvrez le certificat `.pem` fichier avec un éditeur de texte, copiez le certificat, y compris les lignes commençant par `-----BEGIN CERTIFICATE-----` et se terminant par `-----END CERTIFICATE-----`, puis collez le certificat après l'invite de commande.

   c. Vérifiez que le certificat s'affiche correctement.

   d. Terminez l'installation en appuyant sur entrée.

2. Vérifiez que le certificat est installé : `security certificate show -vserver vserver_name`

Activez LDAP sur TLS sur le serveur

Avant que votre serveur SMB puisse utiliser TLS pour sécuriser les communications avec un serveur LDAP Active Directory, vous devez modifier les paramètres de sécurité du serveur SMB pour activer LDAP sur TLS.

Depuis ONTAP 9.10.1, la liaison des canaux LDAP est prise en charge par défaut pour les connexions LDAP Active Directory (AD) et services de noms. ONTAP essaiera la liaison des canaux avec les connexions LDAP uniquement si Start-TLS ou LDAPS est activé avec la sécurité de session définie sur Sign ou SEAL. Pour désactiver ou réactiver la liaison des canaux LDAP avec les serveurs AD, utilisez le `-try-channel -binding-for-ad-ldap` paramètre avec le `vserver cifs security modify` commande.

Pour en savoir plus, voir :

- "Présentation LDAP"
- "2020 exigences de liaison des canaux LDAP et de signature LDAP pour Windows".

Étapes

1. Configurez le paramètre de sécurité du serveur SMB permettant une communication LDAP sécurisée avec les serveurs LDAP Active Directory : `vserver cifs security modify -vserver` *`vserver_name`* `-use-start-tls-for-ad-ldap true`
2. Vérifiez que le paramètre de sécurité LDAP sur TLS est défini sur `true`: `vserver cifs security show -vserver` *`vserver_name`*

> Si le SVM utilise le même serveur LDAP pour effectuer des requêtes name-mapping ou d'autres informations UNIX (par exemple, utilisateurs, groupes et netgroups), alors vous devez également modifier `-use-start-tls` à l'aide de `vserver services name-service ldap client modify` commande.

Configurez SMB Multichannel pour des performances et une redondance optimales

Depuis ONTAP 9.4, vous pouvez configurer SMB Multichannel pour fournir plusieurs connexions entre ONTAP et les clients dans une seule session SMB. Cela améliore le débit et la tolérance aux pannes.

Avant de commencer

La fonctionnalité SMB Multichannel ne peut être utilisée que lorsque les clients négocient avec SMB 3.0 ou une version ultérieure. SMB 3.0 et versions ultérieures sont activés par défaut sur le serveur ONTAP SMB.

Description de la tâche

Les clients SMB détectent et utilisent automatiquement plusieurs connexions réseau si une configuration adéquate est identifiée sur le cluster ONTAP.

Le nombre de connexions simultanées dans une session SMB dépend des cartes réseau que vous avez déployées :

- **NIC 1G sur le client et le cluster ONTAP**

  Le client établit une connexion par carte réseau et lie la session à toutes les connexions.

- **Cartes réseau 10G et de capacité supérieure sur le client et le cluster ONTAP**

  Le client établit jusqu'à quatre connexions par carte réseau et lie la session à toutes les connexions. Le client peut établir des connexions sur plusieurs cartes réseau 10G et supérieures.

Vous pouvez également modifier les paramètres suivants (privilège avancé) :

- **`-max-connections-per-session`**

  Nombre maximum de connexions autorisées par session multicanal. La valeur par défaut est 32 connexions.

  Si vous souhaitez activer plus de connexions que la configuration par défaut, vous devez effectuer des ajustements comparables à la configuration client, qui possède également une valeur par défaut de 32 connexions.

- **`-max-lifs-per-session`**

  Nombre maximum d'interfaces réseau annoncées par session multicanal. La valeur par défaut est 256 interfaces réseau.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Activez SMB Multichannel sur le serveur SMB : `vserver cifs options modify -vserver` *`vserver_name`* `-is-multichannel-enabled true`
3. Vérifiez que ONTAP signale les sessions SMB multicanaux : `vserver cifs session show` *`options`*
4. Retour au niveau de privilège admin : `set -privilege admin`

Exemple

L'exemple suivant affiche les informations relatives à toutes les sessions SMB, affichant plusieurs connexions pour une seule session :

```
cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
Connection Session                                          Open
Idle
IDs        ID      Workstation      Windows User         Files
Time
---------- ------- ---------------- ---------------- ---------
---------------
138683,
138684,
138685     1       10.1.1.1         DOMAIN\                   0
4s
                                    Administrator
```

L'exemple suivant affiche des informations détaillées sur une session SMB avec l'ID-session 1 :

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1
                           Node: node1
                     Session ID: 1
                 Connection IDs: 138683,138684,138685
               Connection Count: 3
   Incoming Data LIF IP Address: 192.1.1.1
         Workstation IP Address: 10.1.1.1
       Authentication Mechanism: NTLMv1
          User Authenticated as: domain-user
                   Windows User: DOMAIN\administrator
                      UNIX User: root
                    Open Shares: 2
                     Open Files: 5
                     Open Other: 0
                 Connected Time: 5s
                      Idle Time: 5s
               Protocol Version: SMB3
         Continuously Available: No
              Is Session Signed: false
                   NetBIOS Name: -
```

Configurez les mappages utilisateur Windows par défaut sur utilisateur UNIX sur le serveur SMB

Configurez l'utilisateur UNIX par défaut

Vous pouvez configurer l'utilisateur UNIX 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 l'utilisateur UNIX par défaut.

Description de la tâche

Par défaut, le nom de l'utilisateur UNIX par défaut est ""pcuser"", ce qui signifie que par défaut, le mappage d'utilisateur à l'utilisateur UNIX par défaut est activé. Vous pouvez spécifier un autre nom à utiliser comme utilisateur UNIX par défaut. Le nom que vous spécifiez doit exister dans les bases de données de service de noms configurées pour la machine virtuelle de stockage (SVM). Si cette option est définie sur une chaîne null, personne ne peut accéder au serveur CIFS en tant qu'utilisateur UNIX par défaut. En d'autres termes, chaque utilisateur doit avoir un compte dans la base de données de mots de passe avant d'accéder au serveur CIFS.

Pour qu'un utilisateur puisse se connecter au serveur CIFS à l'aide du compte utilisateur UNIX par défaut, l'utilisateur doit respecter les conditions préalables suivantes :

- L'utilisateur est authentifié.

- L'utilisateur se trouve dans la base de données utilisateur Windows locale du serveur CIFS, dans le domaine personnel du serveur CIFS ou dans un domaine approuvé (si les recherches de mappage de noms de domaines multiples sont activées sur le serveur CIFS).
- Le nom d'utilisateur n'est pas explicitement mappé à une chaîne nulle.

Étapes

1. Configurez l'utilisateur UNIX par défaut :

Si vous voulez …	Entrer …
Utiliser l'utilisateur UNIX par défaut « pcuser »	`vserver cifs options modify -default -unix-user pcuser`
Utiliser un autre compte utilisateur UNIX comme utilisateur par défaut	`vserver cifs options modify -default -unix-user` *`user_name`*
Désactivez l'utilisateur UNIX par défaut	`vserver cifs options modify -default -unix-user ""`

```
vserver cifs options modify -default-unix-user pcuser
```

2. Vérifiez que l'utilisateur UNIX par défaut est configuré correctement : `vserver cifs options show -vserver` *`vserver_name`*

   Dans l'exemple suivant, l'utilisateur UNIX par défaut et l'utilisateur UNIX invité sur le SVM vs1 sont configurés pour utiliser l'utilisateur UNIX « pcuser » :

```
vserver cifs options show -vserver vs1
```

```
Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : pcuser
  Guest Unix User        : pcuser
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -
```

Configurer l'utilisateur UNIX invité

Configurer l'option utilisateur UNIX invité signifie que les utilisateurs qui se connectent à partir de domaines non fiables sont mappés à l'utilisateur UNIX invité et peuvent se connecter au serveur CIFS. Si vous souhaitez que l'authentification des utilisateurs de domaines non fiables échoue, vous ne devez pas configurer l'utilisateur UNIX invité. La valeur par défaut est de ne pas autoriser les utilisateurs de domaines non fiables à se

connecter au serveur CIFS (le compte UNIX invité n’est pas configuré).

Description de la tâche

Lors de la configuration du compte UNIX invité, vous devez garder à l’esprit les éléments suivants :

- Si le serveur CIFS ne peut pas authentifier l’utilisateur par rapport à un contrôleur de domaine pour le domaine personnel, un domaine approuvé ou la base de données locale et que cette option est activée, le serveur CIFS considère l’utilisateur comme un utilisateur invité et mappe l’utilisateur avec l’utilisateur UNIX spécifié.
- Si cette option est définie sur une chaîne null, l’utilisateur UNIX invité est désactivé.
- Vous devez créer un utilisateur UNIX afin d’utiliser comme utilisateur UNIX invité dans l’une des bases de données de service de nom de la machine virtuelle de stockage (SVM).
- Un utilisateur connecté en tant qu’utilisateur invité est automatiquement membre du groupe BUILTIN\guest sur le serveur CIFS.
- L’option 'homedirs-public' s’applique uniquement aux utilisateurs authentifiés. Un utilisateur connecté en tant qu’utilisateur invité ne dispose pas d’un répertoire personnel et ne peut pas accéder aux répertoires d’accueil des autres utilisateurs.

Étapes

1. Effectuez l’une des opérations suivantes :

Les fonctions que vous recherchez…	Entrer…
Configurer l’utilisateur UNIX invité	`vserver cifs options modify -guest -unix-user` *`unix_name`*
Désactiver l’utilisateur UNIX invité	`vserver cifs options modify -guest -unix-user ""`

```
vserver cifs options modify -guest-unix-user pcuser
```

2. Vérifiez que l’utilisateur UNIX invité est configuré correctement : `vserver cifs options show -vserver` *`vserver_name`*

   Dans l’exemple suivant, l’utilisateur UNIX par défaut et l’utilisateur UNIX invité sur le SVM vs1 sont configurés pour utiliser l’utilisateur UNIX « pcuser » :

```
vserver cifs options show -vserver vs1
```

```
Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : pcuser
  Guest Unix User        : pcuser
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -
```

Mappez le groupe d'administrateurs à la racine

Si vous ne possédez que des clients CIFS dans votre environnement et que votre machine virtuelle de stockage (SVM) a été configurée comme un système de stockage multiprotocole, vous devez disposer d'au moins un compte Windows disposant de privilège racine pour accéder aux fichiers sur la SVM ; Sinon, vous ne pouvez pas gérer la SVM car vous ne disposez pas de droits d'utilisateur suffisants.

Description de la tâche

Si votre système de stockage a été configuré en NTFS-only, cependant, le `/etc` Le répertoire dispose d'une liste de contrôle d'accès de niveau fichier qui permet au groupe d'administrateurs d'accéder aux fichiers de configuration ONTAP.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Configurez l'option de serveur CIFS qui mappe le groupe d'administrateurs à root, le cas échéant :

Les fonctions que vous recherchez…	Alors…
Associez les membres du groupe d'administrateurs à la racine	`vserver cifs options modify -vserver` *`vserver_name`* `-is-admin-users-mapped-to -root-enabled true` Tous les comptes du groupe administrateurs sont considérés comme root, même si vous n'avez pas de `/etc/usermap.cfg` entrée mappant les comptes à la racine. Si vous créez un fichier à l'aide d'un compte appartenant au groupe d'administrateurs, le fichier est détenu par root lorsque vous affichez le fichier à partir d'un client UNIX.
Désactivez le mappage des membres du groupe d'administrateurs à la racine	`vserver cifs options modify -vserver` *`vserver_name`* `-is-admin-users-mapped-to -root-enabled false` Les comptes du groupe d'administrateurs ne sont plus mis en correspondance avec root. Vous ne pouvez mapper explicitement un seul utilisateur qu'à la racine.

3. Vérifiez que l'option est réglée sur la valeur souhaitée : `vserver cifs options show -vserver vserver_name`
4. Retour au niveau de privilège admin : `set -privilege admin`

Affiche des informations sur les types d'utilisateurs connectés via des sessions SMB

Vous pouvez afficher des informations sur le type d'utilisateurs connectés via des sessions SMB. Cela vous aide à vous assurer que seul le type d'utilisateur approprié est connecté via des sessions SMB sur la machine virtuelle de stockage (SVM).

Description de la tâche

Les types d'utilisateurs suivants peuvent se connecter via des sessions SMB :

- `local-user`

  Authentifié en tant qu'utilisateur CIFS local

- `domain-user`

  Authentifié en tant qu'utilisateur de domaine (soit à partir du domaine personnel du serveur CIFS ou d'un domaine de confiance)

- `guest-user`

  Authentifié en tant qu'utilisateur invité

- `anonymous-user`

  Authentifié en tant qu'utilisateur anonyme ou nul

Étapes

1. Déterminez le type d'utilisateur connecté au cours d'une session SMB : `vserver cifs session show -vserver vserver_name -windows-user windows_user_name -fields windows-user,address,lif-address,user-type`

Si vous souhaitez afficher les informations de type d'utilisateur pour les sessions établies…	Saisissez la commande suivante…
Pour toutes les sessions avec un type d'utilisateur spécifié	`vserver cifs session show -vserver *vserver_name* -user-type {local-user
domain-user	guest-user
anonymous-user}`	Pour un utilisateur spécifique

Exemples

La commande suivante affiche des informations sur le type d'utilisateur pour les sessions sur le SVM vs1 établies par l'utilisateur "` ipubs\user1'":

```
cluster1::> vserver cifs session show -vserver pub1 -windows-user
iepubs\user1 -fields windows-user,address,lif-address,user-type
node      vserver session-id connection-id lif-address  address
windows-user         user-type
--------- ------- ---------- ------------- ------------ -------------
-------------------- -----------
pub1node1 pub1    1          3439441860    10.0.0.1     10.1.1.1
IEPUBS\user1         domain-user
```

Options de commande pour limiter la consommation excessive de ressources client Windows

Les options du `vserver cifs options modify` La commande vous permet de contrôler la consommation des ressources pour les clients Windows. Cela peut être utile si un client se trouve en dehors des limites normales de consommation des ressources, par exemple si un nombre inhabituellement élevé de fichiers sont ouverts, si des sessions sont ouvertes ou si des demandes de modification sont envoyées.

Les options suivantes pour le `vserver cifs options modify` La commande a été ajoutée pour contrôler la consommation des ressources client Windows. Si la valeur maximale de l'une de ces options est dépassée, la demande est refusée et un message EMS est envoyé. Un message d'avertissement EMS est également envoyé lorsque 80 % de la limite configurée pour ces options sont atteintes.

- `-max-opens-same-file-per-tree`

  Nombre maximum d'ouvertures sur le même fichier par arborescence CIFS

- `-max-same-user-sessions-per-connection`

  Nombre maximal de sessions ouvertes par le même utilisateur par connexion

- `-max-same-tree-connect-per-session`

  Nombre maximal de connexions d'arborescence sur le même partage par session

- `-max-watches-set-per-tree`

  Nombre maximum de montres (également appelé *change notifie*) établi par arbre

Voir les pages de manuel pour les limites par défaut et pour afficher la configuration actuelle.

Depuis ONTAP 9.4, les serveurs exécutant SMB version 2 ou ultérieure peuvent limiter le nombre de requêtes en attente (*crédits SMB*) que le client peut envoyer au serveur sur une connexion SMB. La gestion des crédits SMB est initiée par le client et contrôlée par le serveur.

Le nombre maximal de requêtes en attente pouvant être accordées sur une connexion SMB est contrôlé par le `-max-credits` option. La valeur par défaut de cette option est 128.

Améliorez les performances de vos clients grâce aux oplocks classiques et de location

Améliorez les performances des clients grâce à une vue d'ensemble des oplocks classiques et des baux

Les oplocks traditionnels (verrous opportunistes) et les oplocks de location permettent à un client SMB dans certains scénarios de partage de fichiers d'effectuer une mise en cache côté client des informations de lecture anticipée, d'écriture différée et de verrouillage. Un client peut alors lire ou écrire dans un fichier sans rappeler régulièrement au serveur qu'il a besoin d'accéder au fichier en question. Ceci améliore les performances en réduisant le trafic réseau.

Les oplocks de location sont une forme améliorée de oplocks disponibles avec le protocole SMB 2.1 et les versions ultérieures. Les oplocks de location permettent à un client d'obtenir et de préserver l'état de mise en cache du client sur plusieurs ouvertures SMB en provenance de lui-même.

Les oplocks peuvent être contrôlés de deux façons :

- Par une propriété de partage, en utilisant `vserver cifs share create` lorsque le partage est créé, ou le `vserver share properties` commande après sa création.
- Par une propriété qtree, en utilisant le `volume qtree create` commande lors de la création du qtree, ou le `volume qtree oplock` commandes après leur création.

Écrire des considérations de perte de données dans le cache lors de l'utilisation de oplocks

Dans certaines circonstances, si un processus possède un oplock exclusif sur un fichier et qu'un deuxième processus tente d'ouvrir le fichier, le premier processus doit invalider les données mises en cache et vider les écritures et les verrous. Le client doit ensuite abandonner le oplock et accéder au fichier. En cas de panne du réseau pendant ce vidage, les données d'écriture mises en cache peuvent être perdues.

- Les possibilités de perte de données

  Toute application avec des données en cache d'écriture peut perdre ces données dans les circonstances suivantes :

  - La connexion s'effectue à l'aide de SMB 1.0.
  - Il a un oplock exclusif sur le fichier.
  - Il est dit de briser ce oplock ou de fermer le fichier.
  - Lors du vidage du cache d'écriture, le réseau ou le système cible génère une erreur.
- Erreur de gestion et de fin d'écriture

  Le cache lui-même n'a pas de traitement d'erreur—les applications le font. Lorsque l'application effectue une écriture dans le cache, l'écriture est toujours terminée. Si le cache, à son tour, effectue une écriture sur le système cible via un réseau, il doit supposer que l'écriture est terminée car si ce n'est pas le cas, les données sont perdues.

Activez ou désactivez les oplocks lors de la création de partages SMB

Les oplocks permettent aux clients de verrouiller des fichiers et de mettre du contenu en cache localement, ce qui peut augmenter les performances des opérations sur les fichiers. Les oplocks sont activés sur des partages SMB résidant sur des SVM (Storage Virtual machine). Dans certaines circonstances, vous pouvez désactiver les oplocks. Vous pouvez activer ou désactiver les oplocks sur une base de partage par partage.

Description de la tâche

Si les oplocks sont activés sur le volume contenant un partage mais que la propriété de partage oplock pour ce partage est désactivée, les oplocks sont désactivés pour ce partage. La désactivation des oplocks sur un partage a priorité sur le paramètre oplock de volume. La désactivation des oplocks sur le partage désactive à la fois les oplocks opportunistes et les oplocks de location.

Vous pouvez spécifier d'autres propriétés de partage en plus de spécifier la propriété de partage oplock à l'aide d'une liste délimitée par des virgules. Vous pouvez également spécifier d'autres paramètres de partage.

Étapes

1. Effectuez l'action appropriée :

Les fonctions que vous recherchez…	Alors…
Activez les oplocks sur un partage lors de la création du partage	Saisissez la commande suivante : `vserver cifs share create -vserver _vserver_name_ -share-name share_name -path path_to_share -share-properties [oplocks,...]` Si vous souhaitez que le partage n'ait que les propriétés de partage par défaut, c'est-à-dire `oplocks`, `browsable`, et `changenotify` activé, vous n'avez pas besoin de spécifier le `-share-properties` Paramètre lors de la création d'un partage SMB. Si vous souhaitez utiliser une combinaison de propriétés de partage autre que la valeur par défaut, vous devez spécifier l' `-share-properties` paramètre avec la liste des propriétés de partage à utiliser pour ce partage.

Les fonctions que vous recherchez…	Alors…
Désactiver les oplocks sur un partage lors de la création du partage	Saisissez la commande suivante : `vserver cifs share create -vserver _vserver_name_ -share-name _share_name_ -path _path_to_share_ -share-properties [other_share_property,...]` Lors de la désactivation des oplocks, vous devez spécifier une liste de propriétés de partage lors de la création du partage, mais vous ne devez pas spécifier le `oplocks` propriété.

Informations associées

Activation ou désactivation des oplocks sur des partages SMB existants

Surveillance de l'état du oplock

Commandes pour l'activation ou la désactivation des oplocks sur des volumes et des qtrees

Les oplocks permettent aux clients de verrouiller des fichiers et de mettre du contenu en cache localement, ce qui peut augmenter les performances des opérations sur les fichiers. Vous devez connaître les commandes permettant d'activer ou de désactiver les oplocks sur des volumes ou des qtrees. Vous devez également savoir quand vous pouvez activer ou désactiver les oplocks sur des volumes et des qtrees.

- Les oplocks sont activés par défaut sur les volumes.
- Vous ne pouvez pas désactiver les oplocks lorsque vous créez un volume.
- Vous pouvez à tout moment activer ou désactiver les oplocks sur des volumes existants pour des SVM.
- Vous pouvez activer les oplocks sur des qtrees pour les SVM.

  Le paramètre du mode oplock est une propriété de l'ID qtree 0, le qtree par défaut que tous les volumes ont. Si vous ne spécifiez pas de paramètre oplock lors de la création d'un qtree, le qtree hérite du paramètre oplock du volume parent, qui est activé par défaut. Cependant, si vous spécifiez un paramètre oplock sur le nouveau qtree, il est prioritaire sur le paramètre oplock sur le volume.

Les fonctions que vous recherchez…	Utilisez cette commande…
Activez les oplocks sur des volumes ou des qtrees	`volume qtree oplocks` avec le `-oplock-mode` paramètre défini sur `enable`
Désactiver les oplocks sur des volumes ou des qtrees	`volume qtree oplocks` avec le `-oplock-mode` paramètre défini sur `disable`

Informations associées

Activez ou désactivez les oplocks sur les partages SMB existants

Les oplocks sont activés par défaut sur des partages SMB sur des SVM (Storage Virtual machines). Dans certaines circonstances, vous pouvez désactiver les oplocks. Si vous avez précédemment désactivé les oplocks sur un partage, vous pouvez également réactiver les oplocks.

Description de la tâche

Si les oplocks sont activés sur le volume contenant un partage, mais que la propriété de partage oplock pour ce partage est désactivée, les oplocks sont désactivés pour ce partage. La désactivation des oplocks sur un partage a priorité sur l’activation des oplocks sur le volume. La désactivation des oplocks sur la part désactive les oplocks opportunistes et ceux de location. Vous pouvez à tout moment activer ou désactiver les oplocks sur des partages existants.

Étape

1. Effectuez l’action appropriée :

Les fonctions que vous recherchez…	Alors…
Activez les oplocks sur un partage en modifiant un partage existant	Saisissez la commande suivante : `vserver cifs share properties add -vserver` *`vserver_name`* `-share-name share_name -share-properties oplocks` Vous pouvez spécifier des propriétés de partage supplémentaires à ajouter à l’aide d’une liste délimitée par des virgules. Les nouvelles propriétés ajoutées sont ajoutées à la liste existante des propriétés de partage. Toutes les propriétés de partage que vous avez précédemment spécifiées restent en vigueur.

Les fonctions que vous recherchez…	Alors…
Désactivez les oplocks sur un partage en modifiant un partage existant	Saisissez la commande suivante : `vserver cifs share properties remove -vserver` *`vserver_name`* `-share-name` *`share_name`* `-share-properties oplocks` Vous pouvez spécifier des propriétés de partage supplémentaires à supprimer à l'aide d'une liste délimitée par des virgules. Les propriétés de partage que vous supprimez sont supprimées de la liste existante de propriétés de partage. Cependant, les propriétés de partage configurées précédemment que vous ne supprimez pas restent en vigueur.

Exemples

La commande suivante active les oplocks pour le partage nommé « Ingénierie » sur une machine virtuelle de stockage (SVM, précédemment connue sous le nom de Vserver) vs1 :

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
Engineering -share-properties oplocks

cluster1::> vserver cifs share properties show
Vserver          Share            Properties
---------------- ---------------- -----------------
vs1              Engineering      oplocks
                                  browsable
                                  changenotify
                                  showsnapshot
```

La commande suivante désactive les oplocks pour l'action nommée « Engineering » sur le SVM vs1 :

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
Engineering -share-properties oplocks

cluster1::> vserver cifs share properties show
Vserver          Share            Properties
---------------- ---------------- -----------------
vs1              Engineering      browsable
                                  changenotify
                                  showsnapshot
```

Informations associées

Activation ou désactivation des oplocks lors de la création de partages SMB

Surveillance de l'état du oplock

Ajout ou suppression de propriétés de partage sur un partage SMB existant

Surveiller l'état du oplock

Vous pouvez surveiller et afficher des informations sur l'état du oplock. Vous pouvez utiliser ces informations pour déterminer quels fichiers ont des oplocks, ce que sont le niveau de oplock et le niveau d'état de oplock et si le leasing oplock est utilisé. Vous pouvez également déterminer des informations sur les verrous que vous devrez peut-être briser manuellement.

Description de la tâche

Vous pouvez afficher des informations sur tous les oplocks sous forme de résumé ou sous forme de liste détaillée. Vous pouvez également utiliser des paramètres facultatifs pour afficher des informations sur un plus petit sous-ensemble de verrous existants. Par exemple, vous pouvez spécifier que le retour de sortie se verrouille uniquement avec l'adresse IP du client spécifiée ou avec le chemin d'accès spécifié.

Vous pouvez afficher les informations suivantes sur les oplocks classiques et de location :

- SVM, node, volume et LIF sur lequel le oplock est établi
- Verrouiller l'UUID
- Adresse IP du client avec le oplock
- Chemin auquel le oplock est établi
- Protocole de verrouillage (SMB) et type (oplock)
- État de verrouillage
- Niveau oplock
- État de connexion et heure d'expiration SMB
- ID de groupe ouvert si un oplock de bail est accordé

Voir la `vserver oplocks show` page man pour une description détaillée de chaque paramètre.

Étapes

1. Afficher l'état du oplock à l'aide de l' `vserver locks show` commande.

Exemples

La commande suivante affiche des informations par défaut sur tous les verrouillages. Le oplock du fichier affiché est accordé avec un `read-batch` niveau oplock :

```
cluster1::> vserver locks show

Vserver: vs0
Volume   Object Path        LIF         Protocol  Lock Type   Client
-------- ------------------ ----------- --------- ----------- ----------
vol1     /vol1/notes.txt    node1_data1
                                        cifs      share-level 192.168.1.5
         Sharelock Mode: read_write-deny_delete
                                                  op-lock     192.168.1.5
         Oplock Level: read-batch
```

L'exemple suivant affiche des informations plus détaillées sur le verrouillage d'un fichier avec le chemin d'accès `/data2/data2_2/intro.pptx`. Un oplock de bail est accordé sur le dossier avec un `batch` Niveau oplock vers un client avec une adresse IP de `10.3.1.3`:

> Lors de l'affichage d'informations détaillées, la commande fournit une sortie séparée pour les informations oplock et sharelock. Cet exemple montre uniquement la sortie de la section oplock.

```
cluster1::> vserver lock show -instance -path /data2/data2_2/intro.pptx

                   Vserver: vs1
                    Volume: data2_2
        Logical Interface: lif2
              Object Path: /data2/data2_2/intro.pptx
                Lock UUID: ff1cbf29-bfef-4d91-ae06-062bf69212c3
            Lock Protocol: cifs
                Lock Type: op-lock
   Node Holding Lock State: node3
               Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

Informations associées

Activation ou désactivation des oplocks lors de la création de partages SMB

Activation ou désactivation des oplocks sur des partages SMB existants

Commandes pour l'activation ou la désactivation des oplocks sur des volumes et des qtrees

Appliquez des objets de stratégie de groupe aux serveurs SMB

Présentation de l'application d'objets de stratégie de groupe aux serveurs SMB

Votre serveur SMB prend en charge les objets de stratégie de groupe (GPO, Group Policy Objects), un ensemble de règles appelées attributs de stratégie de groupe_ qui s'appliquent aux ordinateurs dans un environnement Active Directory. Vous pouvez utiliser des GPO pour gérer centralement les paramètres de toutes les machines virtuelles de stockage (SVM) sur le cluster appartenant au même domaine Active Directory.

Lorsque les stratégies de groupe sont activées sur votre serveur SMB, ONTAP envoie des requêtes LDAP au serveur Active Directory pour demander des informations de stratégie de groupe. Si des définitions de GPO sont applicables à votre serveur SMB, le serveur Active Directory renvoie les informations de GPO suivantes :

- Nom de l'objet GPO
- Version GPO actuelle
- Emplacement de la définition de GPO
- Listes d'UUID (identificateurs uniques universels) pour les jeux de stratégies GPO

Informations associées

Sécurisation de l'accès aux fichiers à l'aide du contrôle d'accès dynamique (DAC)

"Audit et suivi de sécurité SMB et NFS"

Stratégies de groupe prises en charge

Bien que tous les objets de stratégie de groupe (GPO) ne soient pas applicables à vos SVM (Storage Virtual machines) compatibles CIFS, les SVM peuvent reconnaître et traiter l'ensemble des GPO pertinents.

Les GPO suivants sont actuellement pris en charge sur SVM :

- Paramètres de configuration des règles d'audit avancées :

  Accès aux objets : staging de stratégie d'accès central

  Spécifie le type d'événements à auditer pour l'activation de la stratégie d'accès central (CAP), y compris les paramètres suivants :

  - Ne pas auditer
  - Vérifier uniquement les événements de réussite
  - Audit des événements d'échec uniquement
  - Vérifiez à la fois les événements de réussite et d'échec

  > Si l'une des trois options d'audit est définie (audit uniquement des événements de réussite, audit uniquement des événements d'échec, audit des événements de réussite et d'échec), ONTAP vérifie à la fois les événements de réussite et d'échec.

  Réglez à l'aide du `Audit Central Access Policy Staging` réglage dans le `Advanced Audit Policy Configuration/Audit Policies/Object Access` GPO.

  > Pour utiliser les paramètres de stratégie d'audit avancée, l'audit doit être configuré sur le SVM compatible CIFS auquel vous souhaitez appliquer ce paramètre. Si l'audit n'est pas configuré sur le SVM, les paramètres de GPO ne sont pas appliqués et seront supprimés.

- Paramètres du registre :

  - Intervalle d'actualisation des règles de groupe pour les SVM compatibles CIFS

    Réglez à l'aide du `Registry` GPO.

- Actualisation aléatoire de la stratégie de groupe

  Réglez à l'aide du `Registry` GPO.

- Publication de hachage pour BranchCache

  La publication Hash pour BranchCache correspond au mode de fonctionnement de BranchCache. Les trois modes de fonctionnement pris en charge sont les suivants :

  - Par action
  - Tous les partages
  - Désactivé Réglez à l'aide du `Registry` GPO.

- Prise en charge du hachage pour BranchCache

  Les trois paramètres de version de hachage suivants sont pris en charge :

  - BranchCache version 1
  - BranchCache version 2
  - BranchCache versions 1 et 2 Réglez à l'aide du `Registry` GPO.

> Pour utiliser les paramètres de BranchCache, BranchCache doit être configuré sur le SVM compatible CIFS auquel vous souhaitez appliquer ce paramètre. Si BranchCache n'est pas configuré sur le SVM, les paramètres de GPO ne sont pas appliqués et seront supprimés.

- Les paramètres de sécurité

  - Règle d'audit et journal des événements

    - Audit des événements de connexion

      Spécifie le type d'événements de connexion à auditer, notamment les paramètres suivants :

      - Ne pas auditer
      - Vérifier uniquement les événements de réussite
      - Audit sur les événements de panne
      - Vérifiez à la fois les événements de réussite et d'échec Réglez à l'aide du `Audit logon events` réglage dans le `Local Policies/Audit Policy` GPO.

        > Si l'une des trois options d'audit est définie (audit uniquement des événements de réussite, audit uniquement des événements d'échec, audit des événements de réussite et d'échec), ONTAP vérifie à la fois les événements de réussite et d'échec.

    - Auditer l'accès aux objets

      Spécifie le type d'accès aux objets à auditer, y compris les paramètres suivants :

      - Ne pas auditer
      - Vérifier uniquement les événements de réussite
      - Audit sur les événements de panne

- Vérifiez à la fois les événements de réussite et d'échec Réglez à l'aide du `Audit object access` réglage dans le `Local Policies/Audit Policy` GPO.

> Si l'une des trois options d'audit est définie (audit uniquement des événements de réussite, audit uniquement des événements d'échec, audit des événements de réussite et d'échec), ONTAP vérifie à la fois les événements de réussite et d'échec.

- Méthode de conservation des journaux

  Spécifie la méthode de conservation du journal d'audit, y compris les paramètres suivants :

  - Remplacez le journal des événements lorsque la taille du fichier journal dépasse la taille maximale du journal
  - Ne pas écraser le journal des événements (effacer le journal manuellement) Réglez à l'aide du `Retention method for security log` réglage dans le `Event Log` GPO.

- Taille maximale du journal

  Spécifie la taille maximale du journal d'audit.

  Réglez à l'aide du `Maximum security log size` réglage dans le `Event Log` GPO.

> Pour utiliser les paramètres de stratégie d'audit et de stratégie GPO du journal des événements, l'audit doit être configuré sur le SVM compatible CIFS auquel vous souhaitez appliquer ce paramètre. Si l'audit n'est pas configuré sur le SVM, les paramètres de GPO ne sont pas appliqués et seront supprimés.

◦ Sécurité du système de fichiers

Spécifie une liste de fichiers ou de répertoires sur lesquels la sécurité des fichiers est appliquée via un GPO.

Réglez à l'aide du `File System` GPO.

> Le chemin d'accès au volume auquel la stratégie de sécurité du système de fichiers est configurée doit exister au sein de la SVM.

◦ Règle Kerberos

- Inclinaison maximale de l'horloge

  Spécifie la tolérance maximale en minutes pour la synchronisation de l'horloge de l'ordinateur.

  Réglez à l'aide du `Maximum tolerance for computer clock synchronization` réglage dans le `Account Policies/Kerberos Policy` GPO.

- Âge maximum du billet

  Spécifie la durée de vie maximale en heures pour le ticket utilisateur.

  Réglez à l'aide du `Maximum lifetime for user ticket` réglage dans le `Account Policies/Kerberos Policy` GPO.

- Âge maximum de renouvellement du billet

  Spécifie la durée de vie maximale en jours pour le renouvellement du ticket utilisateur.

Réglez à l'aide du `Maximum lifetime for user ticket renewal` réglage dans le `Account Policies/Kerberos Policy` GPO.

- Attribution de droits utilisateur (droits de privilège)

  - Devenir propriétaire

    Indique la liste des utilisateurs et des groupes qui ont le droit de prendre possession de tout objet sécurisé.

    Réglez à l'aide du `Take ownership of files or other objects` réglage dans le `Local Policies/User Rights Assignment` GPO.

  - Privilège de sécurité

    Indique la liste des utilisateurs et des groupes qui peuvent spécifier des options d'audit pour l'accès aux objets de ressources individuelles, telles que des fichiers, des dossiers et des objets Active Directory.

    Réglez à l'aide du `Manage auditing and security log` réglage dans le `Local Policies/User Rights Assignment` GPO.

  - Changer le privilège de notification (vérification de la traverse de dérivation)

    Indique la liste des utilisateurs et des groupes qui peuvent traverser les arborescences de répertoires, même si les utilisateurs et les groupes ne disposent pas des autorisations sur le répertoire de traversée.

Le même privilège est requis pour que les utilisateurs reçoivent des notifications sur les modifications apportées aux fichiers et aux répertoires. Réglez à l'aide du `Bypass traverse checking` réglage dans le `Local Policies/User Rights Assignment` GPO.

- Valeurs de registre

  - Paramètre de signature requis

    Indique si la signature SMB requise est activée ou désactivée.

Réglez à l'aide du `Microsoft network server: Digitally sign communications (always)` réglage dans le `Security Options` GPO.

- Limiter l'anonymat

Indique les restrictions pour les utilisateurs anonymes et inclut les trois paramètres de stratégie de groupe suivants :

  - Pas d'énumération des comptes de Security Account Manager (SAM) :

    Ce paramètre de sécurité détermine les autorisations supplémentaires accordées pour les connexions anonymes à l'ordinateur. Cette option s'affiche sous la forme `no-enumeration` Dans ONTAP, si elle est activée.

Réglez à l'aide du `Network access: Do not allow anonymous enumeration of SAM accounts` réglage dans le `Local Policies/Security Options` GPO.

- Pas d'énumération des comptes et des partages SAM

  Ce paramètre de sécurité détermine si l'énumération anonyme des comptes et partages SAM est autorisée. Cette option s'affiche sous la forme `no-enumeration` Dans ONTAP, si elle est activée.

  Réglez à l'aide du `Network access: Do not allow anonymous enumeration of SAM accounts and shares` réglage dans le `Local Policies/Security Options` GPO.

- Limiter l'accès anonyme aux partages et aux canaux nommés

  Ce paramètre de sécurité limite l'accès anonyme aux partages et aux tuyaux. Cette option s'affiche sous la forme `no-access` Dans ONTAP, si elle est activée.

  Réglez à l'aide du `Network access: Restrict anonymous access to Named Pipes and Shares` réglage dans le `Local Policies/Security Options` GPO.

  Lors de l'affichage d'informations sur les stratégies de groupe définies et appliquées, le `Resultant restriction for anonymous user` Le champ sortie fournit des informations sur la restriction résultant des trois paramètres de GPO anonymes de restriction. Les restrictions possibles résultantes sont les suivantes :

° `no-access`

L'utilisateur anonyme refuse l'accès aux partages spécifiés et aux canaux nommés, et ne peut pas utiliser l'énumération des comptes et des partages SAM. Cette restriction résultante est visible si le `Network access: Restrict anonymous access to Named Pipes and Shares` L'objet GPO est activé.

° `no-enumeration`

L'utilisateur anonyme a accès aux partages spécifiés et aux canaux nommés, mais ne peut pas utiliser l'énumération des comptes et partages SAM. Cette restriction résultante est observée si les deux conditions suivantes sont remplies :

- Le `Network access: Restrict anonymous access to Named Pipes and Shares` GPO est désactivé.
- Soit le `Network access: Do not allow anonymous enumeration of SAM accounts` ou le `Network access: Do not allow anonymous enumeration of SAM accounts and shares` Les stratégies de groupe sont activées.

° `no-restriction`

L'utilisateur anonyme dispose d'un accès complet et peut utiliser l'énumération. Cette restriction résultante est observée si les deux conditions suivantes sont remplies :

- Le `Network access: Restrict anonymous access to Named Pipes and Shares` GPO est désactivé.
- Les deux `Network access: Do not allow anonymous enumeration of SAM accounts` et `Network access: Do not allow anonymous enumeration of SAM accounts and shares` Les GPO sont désactivés.

- Groupes restreints

  Vous pouvez configurer des groupes restreints pour gérer de manière centralisée l'appartenance à des groupes intégrés ou définis par l'utilisateur. Lorsque vous appliquez un groupe restreint via une stratégie de groupe, l'appartenance à un groupe local de serveur CIFS est automatiquement définie pour correspondre aux paramètres de liste d'appartenance définis dans la stratégie de groupe appliquée.

Réglez à l'aide du `Restricted Groups` GPO.

- Paramètres de stratégie d'accès centralisé

  Spécifie une liste de stratégies d'accès centralisé. Les politiques d'accès central et les règles de politique d'accès central associées déterminent les autorisations d'accès pour plusieurs fichiers sur la SVM.

Informations associées

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

Sécurisation de l'accès aux fichiers à l'aide du contrôle d'accès dynamique (DAC)

"Audit et suivi de sécurité SMB et NFS"

Modification des paramètres de sécurité Kerberos du serveur CIFS

Utilisation de BranchCache pour mettre en cache le contenu de partage SMB dans une succursale

Utilisation de la signature SMB pour améliorer la sécurité du réseau

Configuration de la vérification de la traverse de dérivation

Configuration des restrictions d'accès pour les utilisateurs anonymes

Conditions requises pour l'utilisation de stratégies de groupe avec votre serveur SMB

Pour utiliser des stratégies de groupe (GPO, Group Policy Objects) avec votre serveur SMB, votre système doit répondre à plusieurs exigences.

- SMB doit être sous licence sur le cluster. La licence SMB est incluse avec "ONTAP One". Si vous n'avez pas ONTAP One et que la licence n'est pas installée, contactez votre ingénieur commercial.
- Un serveur SMB doit être configuré et joint à un domaine Windows Active Directory.
- L'état admin du serveur SMB doit être on.
- Les GPO doivent être configurés et appliqués à l'unité organisationnelle (ou) Windows Active Directory contenant l'objet ordinateur serveur SMB.
- La prise en charge des GPO doit être activée sur le serveur SMB.

Activer ou désactiver la prise en charge de GPO sur un serveur CIFS

Vous pouvez activer ou désactiver la prise en charge des objets de stratégie de groupe (GPO, Group Policy Object) sur un serveur CIFS. Si vous activez la prise en charge GPO sur un serveur CIFS, les GPO applicables définis sur la stratégie de groupe—la stratégie appliquée à l'unité organisationnelle (ou) qui contient l'objet ordinateur de serveur CIFS—

sont appliqués au serveur CIFS.

Description de la tâche

Les GPO ne peuvent pas être activés sur les serveurs CIFS en mode Workgroup.

Étapes

1. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Entrez la commande…
Activer les stratégies de groupe	`vserver cifs group-policy modify -vserver vserver_name -status enabled`
Désactiver les stratégies de groupe	`vserver cifs group-policy modify -vserver vserver_name -status disabled`

2. Vérifiez que la prise en charge des stratégies de groupe est dans l'état souhaité : `vserver cifs group-policy show -vserver +vserver_name_`

   L'état de la stratégie de groupe pour les serveurs CIFS en mode groupe de travail s'affiche en tant que « désactivé ».

Exemple

L'exemple suivant illustre la prise en charge de GPO sur SVM (Storage Virtual machine) vs1 :

```
cluster1::> vserver cifs group-policy modify -vserver vs1 -status enabled

cluster1::> vserver cifs group-policy show -vserver vs1

            Vserver: vs1
Group Policy Status: enabled
```

Informations associées

Stratégies de groupe prises en charge

Configuration requise pour l'utilisation des objets de stratégie de groupe avec votre serveur CIFS

Mise à jour des stratégies de groupe sur le serveur CIFS

Mise à jour manuelle des paramètres GPO sur le serveur CIFS

Affichage des informations sur les configurations GPO

Mise à jour des objets GPO sur le serveur SMB

Mise à jour des stratégies de groupe sur la présentation du serveur CIFS

Par défaut, ONTAP récupère et applique les modifications des objets de stratégie de

groupe (GPO) toutes les 90 minutes. Les paramètres de sécurité sont actualisés toutes les 16 heures. Si vous voulez mettre à jour les GPO pour appliquer de nouveaux paramètres de stratégie GPO avant que ONTAP ne les mette à jour automatiquement, vous pouvez déclencher une mise à jour manuelle sur un serveur CIFS à l'aide d'une commande ONTAP.

- Par défaut, tous les GPO sont vérifiés et mis à jour au besoin toutes les 90 minutes.

  Cet intervalle est configurable et peut être défini à l'aide du `Refresh interval` et `Random offset` Paramètres GPO.

  ONTAP interroge Active Directory pour les modifications apportées aux stratégies de groupe. Si les numéros de version de GPO enregistrés dans Active Directory sont supérieurs à ceux du serveur CIFS, ONTAP récupère et applique les nouveaux GPO. Si les numéros de version sont identiques, les GPO sur le serveur CIFS ne sont pas mis à jour.

- Les stratégies de sécurité sont actualisées toutes les 16 heures.

  ONTAP récupère et applique les stratégies de groupe de paramètres de sécurité toutes les 16 heures, que ces stratégies de groupe aient été modifiées ou non.

  > La valeur par défaut de 16 heures ne peut pas être modifiée dans la version ONTAP actuelle. Il s'agit d'un paramètre par défaut du client Windows.

- Tous les GPO peuvent être mis à jour manuellement à l'aide d'une commande ONTAP.

  Cette commande simule Windows `gpupdate.exe``commande /force'.

Informations associées

Mise à jour manuelle des paramètres GPO sur le serveur CIFS

Mise à jour manuelle des paramètres GPO sur le serveur CIFS

Si vous souhaitez mettre à jour immédiatement les paramètres des objets GPO (Group Policy Object) sur votre serveur CIFS, vous pouvez mettre à jour les paramètres manuellement. Vous pouvez uniquement mettre à jour les paramètres modifiés ou forcer une mise à jour pour tous les paramètres, y compris les paramètres qui ont été appliqués auparavant mais qui n'ont pas été modifiés.

Étape

1. Effectuez l'action appropriée :

Si vous voulez mettre à jour…	Entrez la commande…
Paramètres de GPO modifiés	`vserver cifs group-policy update -vserver` *`vserver_name`*

Si vous voulez mettre à jour…	Entrez la commande…
Tous les paramètres GPO	`vserver cifs group-policy update -vserver vserver_name -force-reapply -all-settings true`

Informations associées

Mise à jour des stratégies de groupe sur le serveur CIFS

Affiche des informations sur les configurations GPO

Vous pouvez afficher des informations sur les configurations GPO (Group Policy Object) définies dans Active Directory et à propos des configurations GPO appliquées au serveur CIFS.

Description de la tâche

Vous pouvez afficher des informations sur toutes les configurations GPO définies dans Active Directory du domaine auquel appartient le serveur CIFS ou afficher des informations uniquement sur les configurations GPO appliquées à un serveur CIFS.

Étapes

1. Pour afficher des informations sur les configurations GPO, effectuez l'une des opérations suivantes :

Si vous souhaitez afficher des informations sur toutes les configurations de stratégie de groupe…	Entrez la commande…
Défini dans Active Directory	`vserver cifs group-policy show-defined -vserver vserver_name`
Appliquée à une machine virtuelle de stockage (SVM) compatible CIFS	`vserver cifs group-policy show-applied -vserver vserver_name`

Exemple

L'exemple suivant présente les configurations GPO définies dans Active Directory à laquelle la SVM compatible CIFS vs1 appartient :

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1

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 : version1
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
    Status: enabled
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication for Mode BranchCache: per-share
    Hash Version Support for BranchCache: version1
```

```
  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
```

L'exemple suivant présente les configurations GPO appliquées au SVM vs1 compatible CIFS :

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1

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
```

Informations associées

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

Affiche des informations détaillées sur les GPO de groupe restreints

Vous pouvez afficher des informations détaillées sur les groupes restreints qui sont définis comme objets de stratégie de groupe (GPO, Group Policy Objects) dans Active Directory et qui sont appliqués au serveur CIFS.

Description de la tâche

Par défaut, les informations suivantes sont affichées :

- Nom de la stratégie de groupe
- Version de la stratégie de groupe
- Lien

  Spécifie le niveau dans lequel la stratégie de groupe est configurée. Les valeurs de sortie possibles sont les suivantes :

- `Local` Lorsque la stratégie de groupe est configurée dans ONTAP
- `Site` lorsque la stratégie de groupe est configurée au niveau du site dans le contrôleur de domaine
- `Domain` lorsque la stratégie de groupe est configurée au niveau du domaine dans le contrôleur de domaine
- `OrganizationalUnit` Lorsque la stratégie de groupe est configurée au niveau de l'unité organisationnelle (ou) dans le contrôleur de domaine
- `RSOP` pour l'ensemble résultant de règles dérivées de toutes les stratégies de groupe définies à différents niveaux

- Nom de groupe restreint
- Utilisateurs et groupes qui appartiennent à et qui n'appartiennent pas au groupe restreint
- Liste des groupes auxquels le groupe restreint est ajouté

  Un groupe peut être membre de groupes autres que ceux répertoriés ici.

Étape

1. Afficher des informations sur tous les GPO de groupe restreints en effectuant l'une des actions suivantes :

Si vous souhaitez afficher des informations sur tous les GPO de groupe restreints…	Entrez la commande…
Défini dans Active Directory	`vserver cifs group-policy restricted-group show-defined -vserver vserver_name`
Appliqué à un serveur CIFS	`vserver cifs group-policy restricted-group show-applied -vserver vserver_name`

Exemple

L'exemple suivant affiche les informations relatives aux stratégies de groupe restreintes définies dans le domaine Active Directory auquel appartient la SVM compatible CIFS nommée vs1 :

```
cluster1::> vserver cifs group-policy restricted-group show-defined
-vserver vs1

Vserver: vs1
-------------

     Group Policy Name: gpo1
               Version: 16
                  Link: OrganizationalUnit
            Group Name: group1
               Members: user1
              MemberOf: EXAMPLE\group9

     Group Policy Name: Resultant Set of Policy
               Version: 0
                  Link: RSOP
            Group Name: group1
               Members: user1
              MemberOf: EXAMPLE\group9
```

L'exemple suivant affiche les informations relatives aux groupes restreints GPO appliqués au SVM vs1 activé pour CIFS :

```
cluster1::> vserver cifs group-policy restricted-group show-applied
-vserver vs1

Vserver: vs1
-------------

     Group Policy Name: gpo1
               Version: 16
                  Link: OrganizationalUnit
            Group Name: group1
               Members: user1
              MemberOf: EXAMPLE\group9

     Group Policy Name: Resultant Set of Policy
               Version: 0
                  Link: RSOP
            Group Name: group1
               Members: user1
              MemberOf: EXAMPLE\group9
```

Informations associées

Afficher des informations sur les stratégies d'accès central

Vous pouvez afficher des informations détaillées sur les stratégies d'accès central définies dans Active Directory. Vous pouvez également afficher des informations sur les stratégies d'accès central appliquées au serveur CIFS via des objets de stratégie de groupe (GPO).

Description de la tâche

Par défaut, les informations suivantes sont affichées :

- Nom du SVM
- Nom de la stratégie d'accès central
- SID
- Description
- Heure de création
- Heure de modification
- Règles des membres

> Les serveurs CIFS en mode groupe de travail ne sont pas affichés car ils ne prennent pas en charge les GPO.

Étape

1. Afficher des informations sur les stratégies d'accès central en effectuant l'une des actions suivantes :

Si vous souhaitez afficher des informations sur toutes les stratégies d'accès central…	Entrez la commande…
Défini dans Active Directory	`vserver cifs group-policy central-access-policy show-defined -vserver` *`vserver_name`*
Appliqué à un serveur CIFS	`vserver cifs group-policy central-access-policy show-applied -vserver` *`vserver_name`*

Exemple

L'exemple suivant affiche les informations pour toutes les stratégies d'accès central définies dans Active Directory :

```
cluster1::> vserver cifs group-policy central-access-policy show-defined

Vserver  Name                 SID
-------- --------------------
-----------------------------------------------
vs1      p1                   S-1-17-3386172923-1132988875-3044489393-
3993546205
       Description: policy #1
     Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                   S-1-17-1885229282-1100162114-134354072-
822349040
       Description: policy #2
     Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                    r2
```

L'exemple suivant affiche les informations de toutes les règles d'accès central appliquées aux SVM (Storage Virtual machine) sur le cluster :

```
cluster1::> vserver cifs group-policy central-access-policy show-applied

Vserver    Name                 SID
-------- --------------------
-----------------------------------------------
vs1      p1                   S-1-17-3386172923-1132988875-3044489393-
3993546205
       Description: policy #1
     Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                   S-1-17-1885229282-1100162114-134354072-
822349040
       Description: policy #2
     Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                    r2
```

Informations associées

Sécurisation de l'accès aux fichiers à l'aide du contrôle d'accès dynamique (DAC)

Affichage des informations sur les configurations GPO

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

Afficher des informations sur les règles de stratégie d'accès central

Vous pouvez afficher des informations détaillées sur les règles de stratégie d'accès central associées aux stratégies d'accès central définies dans Active Directory. Vous pouvez également afficher des informations sur les règles d'accès central appliquées au serveur CIFS via des stratégies d'accès centrales (objets de stratégie de groupe).

Description de la tâche

Vous pouvez afficher des informations détaillées sur les règles de stratégie d'accès central définies et appliquées. Par défaut, les informations suivantes sont affichées :

- Nom d'un vserver
- Nom de la règle d'accès central
- Description
- Heure de création
- Heure de modification
- Autorisations en cours
- Autorisations proposées
- Ressources cibles

Si vous souhaitez afficher des informations sur toutes les règles de stratégie d'accès central associées aux stratégies d'accès central…	Entrez la commande…
Défini dans Active Directory	`vserver cifs group-policy central-access-rule show-defined -vserver vserver_name`
Appliqué à un serveur CIFS	`vserver cifs group-policy central-access-rule show-applied -vserver vserver_name`

Exemple

L'exemple suivant affiche les informations de toutes les règles de stratégie d'accès central associées aux stratégies d'accès central définies dans Active Directory :

```
cluster1::> vserver cifs group-policy central-access-rule show-defined

Vserver    Name
---------- --------------------
vs1        r1
           Description: rule #1
         Creation Time: Tue Oct 22 09:33:48 2013
     Modification Time: Tue Oct 22 09:33:48 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1        r2
           Description: rule #2
         Creation Time: Tue Oct 22 10:27:57 2013
     Modification Time: Tue Oct 22 10:27:57 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

L'exemple suivant affiche les informations de toutes les règles d'accès central associées aux règles d'accès central appliquées aux SVM (Storage Virtual machine) sur le cluster :

```
cluster1::> vserver cifs group-policy central-access-rule show-applied

Vserver    Name
---------- --------------------
vs1        r1
           Description: rule #1
         Creation Time: Tue Oct 22 09:33:48 2013
     Modification Time: Tue Oct 22 09:33:48 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1        r2
           Description: rule #2
         Creation Time: Tue Oct 22 10:27:57 2013
     Modification Time: Tue Oct 22 10:27:57 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

Informations associées

Sécurisation de l'accès aux fichiers à l'aide du contrôle d'accès dynamique (DAC)

Affichage des informations sur les configurations GPO

Affichage d'informations sur les règles d'accès central

Commandes pour la gestion des mots de passe de compte d'ordinateur des serveurs SMB

Vous devez connaître les commandes permettant de modifier, de réinitialiser et de désactiver les mots de passe, ainsi que de configurer des planifications de mises à jour automatiques. Vous pouvez également configurer une planification sur le serveur SMB pour la mettre à jour automatiquement.

Les fonctions que vous recherchez…	Utilisez cette commande…
Modifiez ou réinitialisez le mot de passe du compte de domaine et vous connaissez le mot de passe	`vserver cifs domain password change`
Réinitialisez le mot de passe du compte de domaine et vous ne connaissez pas le mot de passe	`vserver cifs domain password reset`
Configurez les serveurs SMB pour les changements de mot de passe de compte d'ordinateur automatique	`vserver cifs domain password schedule modify -vserver vserver_name -is -schedule-enabled true`
Désactivez les modifications de mot de passe de compte informatique automatique sur les serveurs SMB	`vserver cifs domain password schedule modify -vserver vs1 -is-schedule -enabled false`

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

Gérer les connexions du contrôleur de domaine

Affiche des informations sur les serveurs découverts

Vous pouvez afficher les informations relatives aux serveurs LDAP découverts et aux contrôleurs de domaine sur votre serveur CIFS.

Étape

1. Pour afficher les informations relatives aux serveurs découverts, entrez la commande suivante : `vserver cifs domain discovered-servers show`

Exemple

L'exemple suivant montre les serveurs découverts pour le SVM vs1 :

```
cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

Domain Name     Type     Preference DC-Name     DC-Address    Status
--------------- -------- ---------- ----------- ------------- -------
example.com     MS-LDAP  adequate   DC-1        1.1.3.4       OK
example.com     MS-LDAP  adequate   DC-2        1.1.3.5       OK
example.com     MS-DC    adequate   DC-1        1.1.3.4       OK
example.com     MS-DC    adequate   DC-2        1.1.3.5       OK
```

Informations associées

Réinitialisation et détection à nouveau des serveurs

Arrêt ou démarrage du serveur CIFS

Réinitialiser et redécouvrir les serveurs

La réinitialisation et la redécouverte des serveurs sur votre serveur CIFS permet au serveur CIFS de supprimer les informations stockées sur les serveurs LDAP et les contrôleurs de domaine. Après l'abandon des informations sur le serveur, le serveur CIFS acquiert de nouveau les informations actuelles sur ces serveurs externes. Cela peut être utile lorsque les serveurs connectés ne répondent pas correctement.

Étapes

1. Saisissez la commande suivante : `vserver cifs domain discovered-servers reset-servers -vserver` *`vserver_name`*
2. Afficher les informations sur les nouveaux serveurs découverts : `vserver cifs domain discovered-servers show -vserver` *`vserver_name`*

Exemple

L'exemple suivant illustre la réinitialisation et la redécouverte des serveurs pour la machine virtuelle de stockage (SVM, anciennement Vserver) vs1 :

```
cluster1::> vserver cifs domain discovered-servers reset-servers -vserver
vs1

cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

Domain Name     Type     Preference DC-Name     DC-Address    Status
--------------- -------- ---------- ----------- ------------- -------
example.com     MS-LDAP  adequate   DC-1        1.1.3.4       OK
example.com     MS-LDAP  adequate   DC-2        1.1.3.5       OK
example.com     MS-DC    adequate   DC-1        1.1.3.4       OK
example.com     MS-DC    adequate   DC-2        1.1.3.5       OK
```

Informations associées

Affichage des informations sur les serveurs découverts

Arrêt ou démarrage du serveur CIFS

Gérer la découverte de contrôleurs de domaine

À partir de ONTAP 9.3, vous pouvez modifier le processus par défaut par lequel les contrôleurs de domaine (DCS) sont détectés. Cela vous permet de limiter la détection à votre site ou à un pool de data centers préférés, ce qui peut entraîner des améliorations des performances en fonction de l'environnement.

Description de la tâche

Par défaut, le processus de découverte dynamique détecte tous les DCS disponibles, y compris tous les DCS préférés, tous les DCS du site local et tous les DCS distants. Cette configuration peut entraîner des temps de latence pour l'authentification et l'accès aux partages dans certains environnements. Si vous avez déjà déterminé le pool de DCS que vous souhaitez utiliser ou si les DCS distants sont insuffisants ou inaccessibles, vous pouvez changer la méthode de découverte.

Dans ONTAP 9.3 et versions ultérieures, le `discovery-mode` paramètre du `cifs domain discovered-servers` la commande vous permet de sélectionner l'une des options de découverte suivantes :

- Tous les DCS du domaine sont découverts.
- Seuls les DCS du site local sont découverts.

  Le `default-site` Le paramètre du serveur SMB peut être défini pour utiliser ce mode avec des LIFs qui ne sont pas attribuées à un site dans sites-et-services.

- La détection de serveur n'est pas effectuée, la configuration du serveur SMB dépend uniquement des DCS préférés.

  Pour utiliser ce mode, vous devez d'abord définir le DCS préféré pour le serveur SMB.

Étape

1. Spécifiez l'option de découverte souhaitée : `vserver cifs domain discovered-servers discovery-mode modify -vserver vserver_name -mode {all|site|none}`

   Options du `mode` paramètre :

   - `all`

     Découvrez tous les DCS disponibles (par défaut).

   - `site`

     Limitez la détection de DC à votre site.

   - `none`

     Utilisez uniquement les DCS préférés sans effectuer de découverte.

Ajouter des contrôleurs de domaine préférés

ONTAP détecte automatiquement les contrôleurs de domaine via DNS. Vous pouvez éventuellement ajouter un ou plusieurs contrôleurs de domaine à la liste des contrôleurs de domaine privilégiés pour un domaine spécifique.

Description de la tâche

Si une liste de contrôleurs de domaine privilégiés existe déjà pour le domaine spécifié, la nouvelle liste est fusionnée avec la liste existante.

Étape

1. Pour ajouter à la liste des contrôleurs de domaine privilégiés, entrez la commande suivante : `vserver cifs domain preferred-dc add -vserver vserver_name -domain domain_name -preferred-dc IP_address, …+`

   `-vserver vserver_name` Spécifie le nom de la machine virtuelle de stockage (SVM).

   `-domain domain_name` Spécifie le nom Active Directory complet du domaine auquel appartiennent les contrôleurs de domaine spécifiés.

   `-preferred-dc IP_address,…` indique une ou plusieurs adresses IP des contrôleurs de domaine préférés, en tant que liste délimitée par des virgules, par ordre de préférence.

Exemple

La commande suivante ajoute des contrôleurs de domaine 172.17.102.25 et 172.17.102.24 à la liste des contrôleurs de domaine préférés que le serveur SMB du SVM vs1 utilise pour gérer l'accès externe au domaine cifs.lab.example.com.

```
cluster1::> vserver cifs domain preferred-dc add -vserver vs1 -domain
cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

Informations associées

Commandes pour la gestion des contrôleurs de domaine privilégiés

Commandes pour la gestion des contrôleurs de domaine privilégiés

Vous devez connaître les commandes permettant d'ajouter, d'afficher et de supprimer les contrôleurs de domaine préférés.

Les fonctions que vous recherchez…	Utilisez cette commande…
Ajouter un contrôleur de domaine préféré	`vserver cifs domain preferred-dc add`
Afficher les contrôleurs de domaine préférés	`vserver cifs domain preferred-dc show`
Supprimez un contrôleur de domaine préféré	`vserver cifs domain preferred-dc remove`

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

Informations associées

Ajout de contrôleurs de domaine préférés

Activez les connexions SMB2 vers les contrôleurs de domaine

Depuis ONTAP 9.1, vous pouvez activer SMB version 2.0 pour vous connecter à un contrôleur de domaine. Cela est nécessaire si vous avez désactivé SMB 1.0 sur les contrôleurs de domaine. Depuis ONTAP 9.2, SMB2 est activé par défaut.

Description de la tâche

Le `smb2-enabled-for-dc-connections` L'option de commande active le système par défaut pour la version de ONTAP que vous utilisez. La valeur par défaut du système pour ONTAP 9.1 est activée pour SMB 1.0 et désactivée pour SMB 2.0. La valeur par défaut du système pour ONTAP 9.2 est activée pour SMB 1.0 et activée pour SMB 2.0. Si le contrôleur de domaine ne peut pas négocier au départ SMB 2.0, il utilise SMB 1.0.

SMB 1.0 peut être désactivé de ONTAP vers un contrôleur de domaine. Dans ONTAP 9.1, si SMB 1.0 a été désactivé, SMB 2.0 doit être activé pour communiquer avec un contrôleur de domaine.

En savoir plus sur :

- "Vérification des versions SMB activées".
- "Fonctionnalités et versions SMB prises en charge".

> Si `-smb1-enabled-for-dc-connections` est défini sur `false` pendant `-smb1-enabled` est défini sur `true`, ONTAP refuse les connexions SMB 1.0 en tant que client, mais continue à accepter les connexions SMB 1.0 entrantes en tant que serveur.

Étapes

1. Avant de modifier les paramètres de sécurité SMB, vérifiez quelles versions SMB sont activées : `vserver cifs security show`

2. Faites défiler la liste pour voir les versions SMB.
3. Exécutez la commande appropriée, à l'aide de `smb2-enabled-for-dc-connections` option.

Si vous voulez que SMB2 soit…	Entrez la commande…
Activé	`vserver cifs security modify -vserver` *`vserver_name`* `-smb2-enabled-for-dc -connections true`
Désactivé	`vserver cifs security modify -vserver` *`vserver_name`* `-smb2-enabled-for-dc -connections false`

Activez les connexions cryptées aux contrôleurs de domaine

Depuis ONTAP 9.8, vous pouvez spécifier le cryptage des connexions aux contrôleurs de domaine.

Description de la tâche

ONTAP nécessite un cryptage pour les communications du contrôleur de domaine (DC) lorsque le système `-encryption-required-for-dc-connection` l'option est définie sur `true`; la valeur par défaut est `false`. Lorsque l'option est définie, seul le protocole SMB3 est utilisé pour les connexions ONTAP-DC, car le chiffrement n'est pris en charge que par SMB3.

Lorsque des communications DC cryptées sont requises, le `-smb2-enabled-for-dc-connections` L'option est ignorée, car ONTAP négocie uniquement les connexions SMB3. Si un DC ne prend pas en charge le SMB3 et le chiffrement, ONTAP ne se connecte pas avec lui.

Étape

1. Activer la communication chiffrée avec le DC : `vserver cifs security modify -vserver` *`svm_name`* `-encryption-required-for-dc-connection true`

Utilisez des sessions null pour accéder au stockage dans des environnements non Kerberos

Utilisez les sessions null pour accéder au stockage dans les environnements non Kerberos

L'accès aux sessions null fournit des autorisations pour les ressources réseau, telles que les données du système de stockage, ainsi que pour les services basés sur les clients s'exécutant sous le système local. Une session null se produit lorsqu'un processus client utilise le compte "système" pour accéder à une ressource réseau. La configuration de session null est spécifique à l'authentification non Kerberos.

Comment le système de stockage fournit un accès de session nul

Comme les partages de session NULL ne nécessitent pas d'authentification, les clients qui ont besoin d'un accès de session nul doivent avoir leurs adresses IP mappées sur le système de stockage.

Par défaut, les clients de session null non mappés peuvent accéder à certains services système ONTAP, tels que l'énumération de partage, mais l'accès aux données du système de stockage est limité.

> ONTAP prend en charge les valeurs des paramètres de registre Windows RestrictAnonymous avec l' `-restrict-anonymous` option. Cela vous permet de contrôler la mesure dans laquelle les utilisateurs nuls non mappés peuvent afficher ou accéder aux ressources système. Par exemple, vous pouvez désactiver l'énumération de partage et l'accès au partage IPC$ (le partage de tuyauterie nommé masqué). Le `vserver cifs options modify` et `vserver cifs options show` les pages man fournissent plus d'informations sur le `-restrict-anonymous` option.

Sauf configuration contraire, un client exécutant un processus local qui demande l'accès au système de stockage via une session nulle est membre uniquement de groupes non restrictifs, tels que « tout le monde ». Pour limiter l'accès à une session nulle aux ressources du système de stockage sélectionnées, vous pouvez créer un groupe auquel appartiennent tous les clients de session nulle. La création de ce groupe vous permet de limiter l'accès au système de stockage et de définir des autorisations de ressources du système de stockage qui s'appliquent spécifiquement aux clients de session nul.

ONTAP fournit une syntaxe de mappage dans le `vserver name-mapping` Ensemble de commandes permettant de spécifier l'adresse IP des clients autorisés à accéder aux ressources du système de stockage à l'aide d'une session utilisateur null. Une fois que vous avez créé un groupe pour les utilisateurs nuls, vous pouvez spécifier des restrictions d'accès pour les ressources du système de stockage et les autorisations de ressources qui s'appliquent uniquement aux sessions nulles. L'utilisateur null est identifié comme une connexion anonyme. Les utilisateurs null n'ont accès à aucun répertoire personnel.

Les autorisations d'utilisateur mappées sont accordées à tout utilisateur null accédant au système de stockage à partir d'une adresse IP mappée. Prenez les précautions appropriées pour empêcher tout accès non autorisé aux systèmes de stockage mappés avec des utilisateurs nuls. Pour une protection maximale, placez le système de stockage et tous les clients nécessitant un accès nul au système de stockage utilisateur sur un réseau distinct, afin d'éliminer la possibilité d'une adresse IP « couverture ».

Informations associées

Configuration des restrictions d'accès pour les utilisateurs anonymes

Accorder aux utilisateurs nuls l'accès aux partages de système de fichiers

Vous pouvez autoriser l'accès aux ressources de votre système de stockage par les clients de session null en attribuant un groupe à utiliser par les clients de session null et en enregistrant les adresses IP des clients de session null à ajouter à la liste des clients autorisés à accéder aux données à l'aide de sessions null du système de stockage.

Étapes

1. Utilisez le `vserver name-mapping create` Commande permettant de mapper l'utilisateur null à un utilisateur Windows valide, avec un qualificateur IP.

   La commande suivante mappe l'utilisateur null à user1 avec un nom d'hôte valide google.com :

   ```
   vserver name-mapping create -direction win-unix  -position 1 -pattern
   "ANONYMOUS LOGON" -replacement user1 - hostname google.com
   ```

La commande suivante mappe l'utilisateur null à utilisateur1 avec une adresse IP valide 10.238.2.54/32 :

```
vserver name-mapping create –direction win-unix  -position 2 –pattern
"ANONYMOUS LOGON" –replacement user1 –address 10.238.2.54/32
```

2. Utilisez le `vserver name-mapping show` commande pour confirmer le mappage de nom.

```
vserver name-mapping show

Vserver:   vs1
Direction: win-unix
Position Hostname         IP Address/Mask
-------- --------         ----------------
1       -                 10.72.40.83/32      Pattern: anonymous logon
                                         Replacement: user1
```

3. Utilisez le `vserver cifs options modify –win-name-for-null-user` Commande permettant d'attribuer l'appartenance à Windows à l'utilisateur nul.

   Cette option est applicable uniquement lorsqu'il existe un mappage de nom valide pour l'utilisateur nul.

```
vserver cifs options modify -win-name-for-null-user user1
```

4. Utilisez le `vserver cifs options show` Commande pour confirmer le mappage de l'utilisateur null à l'utilisateur ou au groupe Windows.

```
vserver cifs options show

Vserver :vs1

Map Null User to Windows User of Group: user1
```

Gérer les alias NetBIOS des serveurs SMB

Présentation de la gestion des alias NetBIOS des serveurs SMB

Les alias NetBIOS sont des noms alternatifs pour votre serveur SMB que les clients SMB peuvent utiliser lors de la connexion au serveur SMB. La configuration des alias NetBIOS d'un serveur SMB peut être utile lorsque vous regroupez des données provenant d'autres serveurs de fichiers vers le serveur SMB et que vous souhaitez que le serveur SMB réponde aux noms des serveurs de fichiers d'origine.

Vous pouvez spécifier une liste d'alias NetBIOS lorsque vous créez le serveur SMB ou à tout moment après

avoir créé le serveur SMB. Vous pouvez à tout moment ajouter ou supprimer des alias NetBIOS de la liste. Vous pouvez vous connecter au serveur SMB en utilisant l'un des noms de la liste d'alias NetBIOS.

Informations associées

Affichage des informations relatives à NetBIOS sur connexions TCP

Ajoutez une liste d'alias NetBIOS au serveur SMB

Si vous souhaitez que les clients SMB se connectent au serveur SMB à l'aide d'un alias, vous pouvez créer une liste d'alias NetBIOS ou ajouter des alias NetBIOS à une liste existante d'alias NetBIOS.

Description de la tâche

- Le nom d'alias NetBIOS peut contenir jusqu'à 15 caractères.
- Vous pouvez configurer jusqu'à 200 alias NetBIOS sur le serveur SMB.
- Les caractères suivants ne sont pas autorisés :

  @ # * ( ) = + [ ] | ; : " , < > \ / ?

Étapes

1. Ajoutez les alias NetBIOS:
   `vserver cifs add-netbios-aliases -vserver` *`vserver_name`* `-netbios-aliases` *`NetBIOS_alias`*`,…`

   ```
   vserver cifs add-netbios-aliases -vserver vs1 -netbios-aliases
   alias_1,alias_2,alias_3
   ```

   - Vous pouvez spécifier un ou plusieurs alias NetBIOS à l'aide d'une liste délimitée par des virgules.
   - Les alias NetBIOS spécifiés sont ajoutés à la liste existante.
   - Une nouvelle liste d'alias NetBIOS est créée si la liste est actuellement vide.
2. Vérifiez que les alias NetBIOS ont été correctement ajoutés : `vserver cifs show -vserver vserver_name -display-netbios-aliases`

   ```
   vserver cifs show -vserver vs1 -display-netbios-aliases
   ```

   ```
   Vserver: vs1

            Server Name: CIFS_SERVER
            NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
   ```

Informations associées

Suppression des alias NetBIOS de la liste des alias NetBIOS

Affichage de la liste des alias NetBIOS sur les serveurs CIFS

Supprimez les alias NetBIOS de la liste d'alias NetBIOS

Si vous n'avez pas besoin d'alias NetBIOS spécifiques pour un serveur CIFS, vous pouvez supprimer ces alias NetBIOS de la liste. Vous pouvez également supprimer tous les alias NetBIOS de la liste.

Description de la tâche

Vous pouvez supprimer plusieurs alias NetBIOS à l'aide d'une liste délimitée par des virgules. Vous pouvez supprimer tous les alias NetBIOS d'un serveur CIFS en spécifiant – comme valeur pour le `-netbios -aliases` paramètre.

Étapes

1. Effectuez l'une des opérations suivantes :

Si vous souhaitez supprimer…	Entrer…
Alias NetBIOS spécifiques dans la liste	`vserver cifs remove-netbios-aliases -vserver _vserver_name_ -netbios -aliases _NetBIOS_alias_,...`
Tous les alias NetBIOS de la liste	`vserver cifs remove-netbios-aliases -vserver` *`vserver_name`* `-netbios-aliases -`

```
vserver cifs remove-netbios-aliases -vserver vs1 -netbios-aliases alias_1
```

2. Vérifiez que les alias NetBIOS spécifiés ont été supprimés : `vserver cifs show -vserver` *`vserver_name`* `-display-netbios-aliases`

```
vserver cifs show -vserver vs1 -display-netbios-aliases
```

```
Vserver: vs1

         Server Name: CIFS_SERVER
         NetBIOS Aliases: ALIAS_2, ALIAS_3
```

Afficher la liste des alias NetBIOS sur les serveurs CIFS

Vous pouvez afficher la liste des alias NetBIOS. Cela peut être utile lorsque vous voulez déterminer la liste des noms sur lesquels les clients SMB peuvent établir des connexions au serveur CIFS.

Étape

1. Effectuez l'une des opérations suivantes :

Pour afficher des informations sur…	Entrer…
Alias NetBIOS d'un serveur CIFS	`vserver cifs show -display-netbios -aliases`
La liste des alias NetBIOS dans le cadre des informations détaillées du serveur CIFS	`vserver cifs show -instance`

L'exemple suivant affiche des informations sur les alias NetBIOS d'un serveur CIFS :

```
vserver cifs show -display-netbios-aliases
```

```
Vserver: vs1

         Server Name: CIFS_SERVER
         NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

L'exemple suivant affiche la liste des alias NetBIOS dans le cadre des informations détaillées du serveur CIFS :

```
vserver cifs show -instance
```

```
                                          Vserver: vs1
                        CIFS Server NetBIOS Name: CIFS_SERVER
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: ALIAS_1, ALIAS_2,
ALIAS_3
```

Consultez la page man pour les commandes pour plus d'informations.

Informations associées

Ajout d'une liste d'alias NetBIOS au serveur CIFS

Commandes pour la gestion des serveurs CIFS

Déterminez si les clients SMB sont connectés à l'aide d'alias NetBIOS

Vous pouvez déterminer si les clients SMB sont connectés à l'aide d'alias NetBIOS et, si oui, quel alias NetBIOS est utilisé pour établir la connexion. Cela peut être utile lors du dépannage des problèmes de connexion.

Description de la tâche

Vous devez utiliser le `-instance` Paramètre pour afficher l'alias NetBIOS (le cas échéant) associé à une connexion SMB. Si le nom du serveur CIFS ou une adresse IP est utilisé pour établir la connexion SMB, la sortie de l' `NetBIOS Name` c'est – (tiret).

Étape

1. Effectuez l'action souhaitée :

Si vous souhaitez afficher les informations NetBIOS pour…	Entrer…
Connexions SMB	`vserver cifs session show -instance`
Connexions utilisant un alias NetBIOS spécifié :	`vserver cifs session show -instance -netbios-name` *`netbios_name`*

L'exemple suivant affiche des informations sur l'alias NetBIOS utilisé pour établir la connexion SMB avec l'ID de session 1 :

```
vserver cifs session show -session-id 1 -instance
```

```
                        Node: node1
                     Vserver: vs1
                  Session ID: 1
                Connection ID: 127834
 Incoming Data LIF IP Address: 10.1.1.25
                  Workstation: 10.2.2.50
    Authentication Mechanism: NTLMv2
                 Windows User: EXAMPLE\user1
                    UNIX User: user1
                  Open Shares: 2
                   Open Files: 2
                   Open Other: 0
               Connected Time: 1d 1h 10m 5s
                    Idle Time: 22s
             Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                 NetBIOS Name: ALIAS1
       SMB Encryption Status: Unencrypted
```

Gérer diverses tâches de serveur SMB

Arrêtez ou démarrez le serveur CIFS

Vous pouvez arrêter le serveur CIFS sur un SVM, ce qui peut être utile lors d'opérations effectuées lorsque les utilisateurs n'accèdent pas aux données via les partages SMB. Vous pouvez redémarrer l'accès SMB en démarrant le serveur CIFS. En arrêtant le serveur CIFS, vous pouvez également modifier les protocoles autorisés sur la machine virtuelle de stockage (SVM).

Étapes

1. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Entrez la commande…
Arrêtez le serveur CIFS	`vserver cifs stop -vserver *vserver_name* [-foreground {true
false}]`	Démarrez le serveur CIFS
`vserver cifs start -vserver *vserver_name* [-foreground {true	false}]`

   `-foreground` indique si la commande doit s'exécuter au premier plan ou en arrière-plan. Si vous ne saisissez pas ce paramètre, il est défini sur `true`, et la commande est exécutée au premier plan.

2. Vérifiez que l'état administratif du serveur CIFS est correct à l'aide du `vserver cifs show` commande.

Exemple

Les commandes suivantes permettent de démarrer le serveur CIFS sur le SVM vs1 :

```
cluster1::> vserver cifs start -vserver vs1

cluster1::> vserver cifs show -vserver vs1

                                        Vserver: vs1
                        CIFS Server NetBIOS Name: VS1
                    NetBIOS Domain/Workgroup Name: DOMAIN
                      Fully Qualified Domain Name: DOMAIN.LOCAL
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
```

Informations associées

Affichage des informations sur les serveurs découverts

Réinitialisation et détection à nouveau des serveurs

Déplacement des serveurs CIFS vers différents UO

Le processus de création du serveur CIFS utilise les unités organisationnelles (ou) CN=ordinateurs par défaut lors de la configuration, sauf si vous spécifiez une autre unité administrative. Après l'installation, vous pouvez déplacer les serveurs CIFS vers différents UO.

Étapes

1. Sur le serveur Windows, ouvrez l'arborescence **utilisateurs et ordinateurs Active Directory**.
2. Recherchez l'objet Active Directory pour la machine virtuelle de stockage (SVM).
3. Cliquez avec le bouton droit de la souris sur l'objet et sélectionnez **déplacer**.
4. Sélectionnez l'unité d'organisation que vous souhaitez associer à la SVM

Résultats

L'objet SVM est placé dans l'UO sélectionnée.

Modifier le domaine DNS dynamique sur le SVM avant de déplacer le serveur SMB

Si vous souhaitez que le serveur DNS intégré à Active Directory enregistre de manière dynamique les enregistrements DNS du serveur SMB dans DNS lorsque vous déplacez le serveur SMB vers un autre domaine, vous devez modifier DNS dynamique (DDNS) sur la machine virtuelle de stockage (SVM) avant de déplacer le serveur SMB.

Avant de commencer

Les services de nom DNS doivent être modifiés sur le SVM afin d'utiliser le domaine DNS qui contient les enregistrements d'emplacement de service pour le nouveau domaine qui contiendra le compte ordinateur du serveur SMB. Si vous utilisez Secure DDNS, vous devez utiliser des serveurs de noms DNS intégrés à Active Directory.

Description de la tâche

Bien que DDNS (si configuré sur la SVM) ajoute automatiquement les enregistrements DNS des LIFs de données au nouveau domaine, les enregistrements DNS du domaine d'origine ne sont pas automatiquement supprimés du serveur DNS d'origine. Vous devez les supprimer manuellement.

Pour effectuer les modifications DDNS avant de déplacer le serveur SMB, reportez-vous à la rubrique suivante :

"Configuration des services DNS dynamiques"

Rejoignez un SVM vers un domaine Active Directory

Vous pouvez associer une machine virtuelle de stockage (SVM) à un domaine Active Directory sans supprimer le serveur SMB existant en modifiant le domaine à l'aide de `vserver cifs modify` commande. Vous pouvez rejoindre à nouveau le domaine actuel ou en rejoindre un nouveau.

Avant de commencer

- Le SVM doit déjà disposer d'une configuration DNS.
- La configuration DNS pour le SVM doit pouvoir représenter le domaine cible.

Les serveurs DNS doivent contenir les enregistrements SRV (Service Location Records) pour les serveurs LDAP de domaine et de contrôleur de domaine.

Description de la tâche

- Le statut administratif du serveur CIFS doit être défini sur "deown" pour pouvoir procéder à la modification du domaine Active Directory.
- Si la commande s'exécute avec succès, le statut administratif est automatiquement défini sur « actif ».
- Lorsque vous rejoignez un domaine, cette commande peut prendre plusieurs minutes.

Étapes

1. Relier le SVM au domaine du serveur CIFS : `vserver cifs modify -vserver` *`vserver_name`* `-domain` *`domain_name`* `-status-admin down`

   Pour plus d'informations, consultez la page de manuel du `vserver cifs modify` commande. Si vous devez reconfigurer le DNS pour le nouveau domaine, reportez-vous à la page de manuel de l' `vserver dns modify` commande.

   Pour créer un compte de machine Active Directory pour le serveur SMB, vous devez fournir le nom et le mot de passe d'un compte Windows disposant des privilèges suffisants pour ajouter des ordinateurs à l' `ou=` *`example`* `ou` conteneur dans le `*example*`domaine .com.

   À partir de ONTAP 9.7, votre administrateur AD peut vous fournir un URI vers un fichier keytab comme alternative à vous fournir un nom et un mot de passe à un compte Windows privilégié. Lorsque vous recevez l'URI, l'inclure dans le `-keytab-uri` paramètre avec le `vserver cifs` commandes.

2. Vérifiez que le serveur CIFS se trouve dans le domaine Active Directory souhaité : `vserver cifs show`

Exemple

Dans l'exemple suivant, le serveur SMB « CIFSSERVER1 » sur le SVM vs1 rejoint le domaine example.com à l'aide de keytab Authentication :

```
cluster1::> vserver cifs modify -vserver vs1 -domain example.com -status
-admin down -keytab-uri http://admin.example.com/ontap1.keytab

cluster1::> vserver cifs show

          Server       Status       Domain/Workgroup  Authentication
Vserver   Name         Admin        Name               Style
--------- -----------  ---------    ----------------  --------------
vs1       CIFSSERVER1  up           EXAMPLE           domain
```

Affiche des informations sur NetBIOS sur connexions TCP

Vous pouvez afficher des informations sur les connexions NetBIOS sur TCP (NBT). Cela peut être utile lors du dépannage des problèmes liés au NetBIOS.

Étape

1. Utilisez le `vserver cifs nbtstat` Commande pour afficher les informations relatives à NetBIOS sur

connexions TCP.

> Le service de noms NetBIOS (NNBNS) sur IPv6 n'est pas pris en charge.

Exemple

L'exemple suivant montre les informations relatives au service de nom NetBIOS affichées pour « cluster1 » :

```
cluster1::> vserver cifs nbtstat

          Vserver: vs1
          Node:    cluster1-01
          Interfaces:
                   10.10.10.32
                   10.10.10.33
        Servers:
                   17.17.1.2  (active  )
        NBT Scope:
                  [ ]
        NBT Mode:
                  [h]
        NBT Name    NetBIOS Suffix   State   Time Left   Type
        ----------- ---------------  ------- ---------   -----
        CLUSTER_1   00               wins    57
        CLUSTER_1   20               wins    57

        Vserver: vs1
        Node:    cluster1-02
        Interfaces:
                10.10.10.35
        Servers:
                17.17.1.2  (active  )
        CLUSTER_1          00               wins          58
        CLUSTER_1          20               wins          58
        4 entries were displayed.
```

Commandes pour la gestion des serveurs SMB

Vous devez connaître les commandes pour créer, afficher, modifier, arrêter, démarrer, Et suppression des serveurs SMB. Il existe également des commandes permettant de réinitialiser et de redécouvrir les serveurs, de modifier ou de réinitialiser les mots de passe des comptes machine, de planifier des modifications pour les mots de passe des comptes machine et d'ajouter ou de supprimer des alias NetBIOS.

Les fonctions que vous recherchez…	Utilisez cette commande…

Créez un serveur SMB	`vserver cifs create`
Affiche les informations relatives à un serveur SMB	`vserver cifs show`
Modifier un serveur SMB	`vserver cifs modify`
Déplacer un serveur SMB vers un autre domaine	`vserver cifs modify`
Arrêtez un serveur SMB	`vserver cifs stop`
Démarrez un serveur SMB	`vserver cifs start`
Supprimez un serveur SMB	`vserver cifs delete`
Réinitialisez et redécouvrez les serveurs pour le serveur SMB	`vserver cifs domain discovered-servers reset-servers`
Modifier le mot de passe du compte machine du serveur SMB	`vserver cifs domain password change`
Réinitialisez le mot de passe du compte machine du serveur SMB	`vserver cifs domain password change`
Planifier les modifications automatiques du mot de passe pour le compte machine du serveur SMB	`vserver cifs domain password schedule modify`
Ajoutez des alias NetBIOS pour le serveur SMB	`vserver cifs add-netbios-aliases`
Supprimez les alias NetBIOS du serveur SMB	`vserver cifs remove-netbios-aliases`

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

Informations associées

"Ce qui se passe pour les utilisateurs et les groupes locaux lors de la suppression des serveurs SMB"

Activez le service de noms NetBIOS

À partir de ONTAP 9, le service de noms NetBIOS (NBNS, parfois appelé Windows Internet Name Service ou WINS) est désactivé par défaut. Auparavant, les machines virtuelles de stockage compatibles CIFS (SVM) envoyaient des diffusions d'enregistrement de noms, même si WINS était activé sur un réseau. Pour limiter ces diffusions à des configurations où NBNS est nécessaire, vous devez activer explicitement NBNS pour les nouveaux serveurs CIFS.

Avant de commencer

- Si vous utilisez déjà NBNS et que vous effectuez une mise à niveau vers ONTAP 9, il n'est pas nécessaire d'effectuer cette tâche. NBNS continuera de fonctionner comme précédemment.
- NBNS est activé sur UDP (port 137).
- NBNS sur IPv6 n'est pas pris en charge.

Étapes

1. Définissez le niveau de privilège sur avancé.

```
set -privilege advanced
```

2. Activez NBNS sur un serveur CIFS.

```
vserver cifs options  modify -vserver <vserver name> -is-nbns-enabled
true
```

3. Revenir au niveau de privilège admin.

```
set -privilege admin
```

Utilisez IPv6 pour l'accès SMB et les services SMB

Conditions d'utilisation d'IPv6

Avant de pouvoir utiliser IPv6 sur votre serveur SMB, vous devez connaître les versions de ONTAP et SMB qui la prennent en charge et les exigences de licence.

Conditions requises pour les licences ONTAP

Aucune licence spéciale n'est requise pour IPv6 lorsque SMB est sous licence. La licence SMB est incluse avec "ONTAP One". Si vous n'avez pas ONTAP One et que la licence n'est pas installée, contactez votre ingénieur commercial.

Version requise du protocole SMB

- Pour les SVM, ONTAP prend en charge IPv6 sur toutes les versions du protocole SMB.

> Le service de noms NetBIOS (NNBNS) sur IPv6 n'est pas pris en charge.

Prise en charge d'IPv6 avec accès SMB et services CIFS

Si vous souhaitez utiliser IPv6 sur votre serveur CIFS, vous devez savoir comment ONTAP prend en charge IPv6 pour l'accès SMB et la communication réseau pour les services CIFS.

Prise en charge des serveurs et des clients Windows

ONTAP prend en charge les serveurs et clients Windows prenant en charge IPv6. La section suivante décrit la prise en charge du protocole IPv6 du serveur et du client Microsoft Windows :

- Windows 7, Windows 8, Windows Server 2008, Windows Server 2012 et versions ultérieures prennent en charge IPv6 à la fois pour le partage de fichiers SMB et les services Active Directory, notamment les services DNS, LDAP, CLDAP et Kerberos.

  Si les adresses IPv6 sont configurées, les versions Windows 7 et Windows Server 2008 et ultérieures utilisent IPv6 par défaut pour les services Active Directory. Les authentifications NTLM et Kerberos sur des connexions IPv6 sont prises en charge.

  Tous les clients Windows pris en charge par ONTAP peuvent se connecter à des partages SMB à l'aide d'adresses IPv6.

Pour obtenir les informations les plus récentes sur les clients Windows pris en charge par ONTAP, reportez-vous au "Matrice d'interopérabilité".

> Les domaines NT ne sont pas pris en charge pour IPv6.

Prise en charge supplémentaire de services CIFS

Outre la prise en charge IPv6 pour les partages de fichiers SMB et les services Active Directory, ONTAP prend en charge plusieurs protocoles :

- Services côté client, y compris les dossiers hors ligne, les profils itinérants, la redirection de dossiers et les versions précédentes
- Services côté serveur, y compris les répertoires locaux dynamiques (fonctionnalité Home Directory), les symlinks et les Widelinks, BranchCache, ODX, load des copies ODX, référencements automatiques des nœuds, Et versions précédentes
- Services de gestion de l'accès aux fichiers, y compris l'utilisation d'utilisateurs et de groupes Windows locaux pour le contrôle d'accès et la gestion des droits, la définition des autorisations de fichiers et des stratégies d'audit à l'aide de la CLI, le suivi de la sécurité, la gestion des verrous de fichiers et la surveillance de l'activité SMB
- Audit multiprotocole NAS
- FPolicy
- Partages disponibles en continu, protocole Witness et VSS distant (utilisés avec les configurations Hyper-V sur SMB)

Prise en charge du service d'authentification et du service de noms

La communication avec les services de noms suivants est prise en charge par IPv6 :

- Contrôleurs de domaine
- Serveurs DNS
- Serveurs LDAP
- Serveurs KDC
- Serveurs NIS

Comment les serveurs CIFS utilisent IPv6 pour se connecter aux serveurs externes

Pour créer une configuration qui répond à vos exigences, vous devez savoir comment les serveurs CIFS utilisent IPv6 lors de connexions à des serveurs externes.

- Sélection de l'adresse source

  Si une tentative de connexion à un serveur externe est effectuée, l'adresse source sélectionnée doit être du même type que l'adresse de destination. Par exemple, si vous vous connectez à une adresse IPv6, la machine virtuelle de stockage (SVM) hébergeant le serveur CIFS doit disposer d'une LIF de données ou d'une LIF de gestion dont l'adresse IPv6 est à utiliser comme adresse source. De la même manière, en cas de connexion à une adresse IPv4, le SVM doit disposer d'une LIF de données ou d'une LIF de gestion qui possède une adresse IPv4 à utiliser comme adresse source.

- Pour les serveurs découverts dynamiquement à l'aide de DNS, la découverte de serveur s'effectue comme suit :
  - Si IPv6 est désactivé sur le cluster, seules les adresses des serveurs IPv4 sont découvertes.
  - Si IPv6 est activé sur le cluster, les adresses des serveurs IPv4 et IPv6 sont découvertes. L'un ou l'autre type peut être utilisé en fonction de l'adéquation du serveur auquel appartient l'adresse et de la disponibilité des LIF de gestion ou des données IPv6 ou IPv4. La découverte de serveurs dynamiques est utilisée pour découvrir les contrôleurs de domaine et leurs services associés, tels que LSA, NETLOGON, Kerberos et LDAP.
- Connectivité du serveur DNS

  Si le SVM utilise IPv6 lors de la connexion à un serveur DNS dépend de la configuration des services de noms DNS. Si les services DNS sont configurés pour utiliser des adresses IPv6, les connexions sont effectuées à l'aide d'IPv6. Si vous le souhaitez, la configuration des services de noms DNS peut utiliser des adresses IPv4 afin que les connexions aux serveurs DNS continuent d'utiliser des adresses IPv4. Des combinaisons d'adresses IPv4 et IPv6 peuvent être spécifiées lors de la configuration des services de noms DNS.

- Connectivité du serveur LDAP

  Si le SVM utilise IPv6 lors de la connexion à un serveur LDAP dépend de la configuration du client LDAP. Si le client LDAP est configuré pour utiliser des adresses IPv6, les connexions sont effectuées à l'aide d'IPv6. Si vous le souhaitez, la configuration du client LDAP peut utiliser des adresses IPv4 pour que les connexions aux serveurs LDAP continuent d'utiliser des adresses IPv4. Des combinaisons d'adresses IPv4 et IPv6 peuvent être spécifiées lors de la configuration du client LDAP.

  > La configuration du client LDAP est utilisée lors de la configuration de LDAP pour les services d'utilisateur, de groupe et de nom de groupe de réseau UNIX.

- Connectivité serveur NIS

  La question de savoir si le SVM utilise IPv6 lors de la connexion à un serveur NIS dépend de la configuration des services de nom NIS. Si les services NIS sont configurés pour utiliser des adresses IPv6, les connexions sont effectuées à l'aide d'IPv6. Si vous le souhaitez, la configuration des services de noms NIS peut utiliser des adresses IPv4 pour que les connexions aux serveurs NIS continuent d'utiliser des adresses IPv4. Des combinaisons d'adresses IPv4 et IPv6 peuvent être spécifiées lors de la configuration de services de noms NIS.

Les services de noms NIS sont utilisés pour stocker et gérer des objets de nom d'utilisateur, de groupe, de groupe et d'hôte UNIX.

Informations associées

Activation d'IPv6 pour SMB (administrateurs du cluster uniquement)

Contrôle et affichage des informations relatives aux sessions SMB IPv6

Activer IPv6 pour SMB (administrateurs du cluster uniquement)

Les réseaux IPv6 ne sont pas activés lors de la configuration du cluster. Un administrateur de cluster doit activer IPv6 une fois l'installation du cluster terminée pour utiliser IPv6 pour SMB. Lorsque l'administrateur de cluster active IPv6, il est activé pour l'ensemble du cluster.

Étape

1. Activer IPv6 : `network options ipv6 modify -enabled true`

   Pour plus d'informations sur l'activation d'IPv6 sur le cluster et la configuration des LIF IPv6, reportez-vous au *Network Management Guide*.

   IPv6 est activé. Les LIF de données IPv6 pour un accès SMB peuvent être configurées.

Informations associées

Contrôle et affichage des informations relatives aux sessions SMB IPv6

"Gestion du réseau"

Désactivation de IPv6 pour SMB

Bien que IPv6 soit activé sur le cluster à l'aide d'une option réseau, vous ne pouvez pas désactiver IPv6 pour SMB en utilisant la même commande. En revanche, ONTAP désactive IPv6 lorsque l'administrateur de cluster désactive la dernière interface compatible IPv6 sur le cluster. Vous devez communiquer avec l'administrateur du cluster pour obtenir des informations sur la gestion de vos interfaces compatibles IPv6.

Pour plus d'informations sur la désactivation d'IPv6 sur le cluster, reportez-vous au *Network Management Guide*.

Informations associées

"Gestion du réseau"

Contrôle et affichage des informations relatives aux sessions SMB IPv6

Vous pouvez contrôler et afficher des informations relatives aux sessions SMB connectées via les réseaux IPv6. Ces informations sont utiles pour déterminer quels clients se connectent à l'aide d'IPv6 ainsi que d'autres informations utiles sur les sessions SMB IPv6.

Étape

1. Effectuez l'action souhaitée :

Si vous voulez déterminer si…	Entrez la commande…
Les sessions SMB vers une machine virtuelle de stockage (SVM) sont connectées via IPv6	`vserver cifs session show -vserver` *`vserver_name`* `-instance`
IPv6 est utilisé pour les sessions SMB via une adresse LIF spécifiée	`vserver cifs session show -vserver` *`vserver_name`* `-lif-address` *`LIF_IP_address`* `-instance` *`LIF_IP_address`* Est l'adresse IPv6 de la LIF de données.

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

Style de sécurité	Clients pouvant modifier des autorisations	Autorisations que les clients peuvent utiliser	Un style de sécurité efficace	Clients pouvant accéder aux fichiers
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.
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`*
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`
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`

Les fonctions que vous recherchez…	Utilisez cette commande…
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.

Propriétés du partage	Description
`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.
`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`*
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.
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

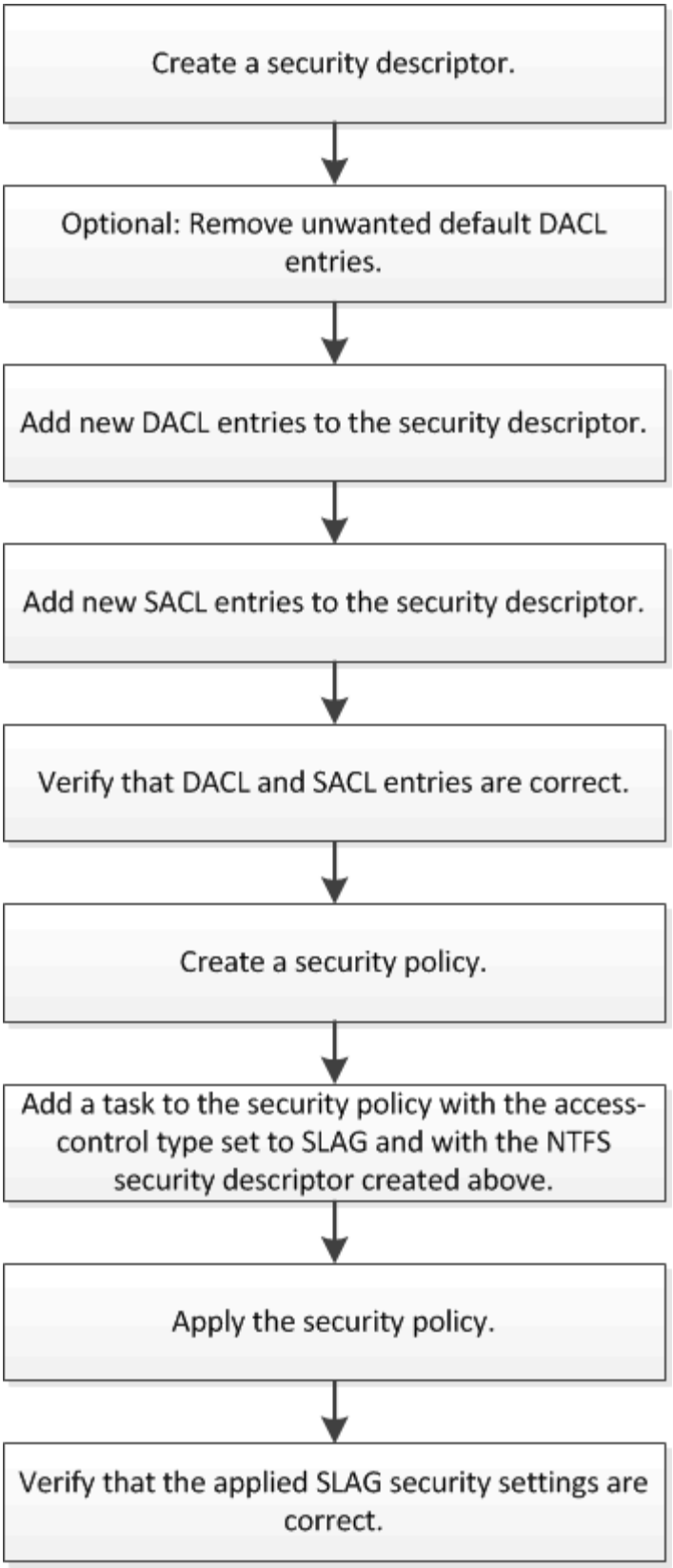
Storage-Level Access Guard fournit une sécurité supplémentaire au niveau du stockage, qui n'est pas visible du côté client. Par conséquent, il ne peut être révoqué par aucun des utilisateurs ou administrateurs de leur poste de travail. Dans certains cas, il est préférable de pouvoir contrôler l'accès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

Gérer l’accès aux fichiers via SMB

Utilisez des utilisateurs et des groupes locaux pour l’authentification et l’autorisation

Utilisation des utilisateurs et des groupes locaux par ONTAP

Concepts d’utilisateurs et de groupes locaux

Vous devez connaître les utilisateurs et les groupes locaux, ainsi que quelques informations de base à leur sujet, avant de déterminer si vous devez configurer et utiliser des utilisateurs et des groupes locaux dans votre environnement.

- **Utilisateur local**

  Un compte utilisateur avec un identifiant de sécurité unique (SID) qui n’a de visibilité que sur la machine virtuelle de stockage (SVM) sur laquelle elle est créée. Les comptes d’utilisateur locaux ont un ensemble d’attributs, y compris le nom d’utilisateur et le SID. Un compte utilisateur local s’authentifie localement sur le serveur CIFS à l’aide de l’authentification NTLM.

  Les comptes d’utilisateur ont plusieurs utilisations :

  - Permet d’accorder des privilèges *User Rights Management* à un utilisateur.
  - Permet de contrôler l’accès au niveau du partage et du fichier aux ressources de fichiers et de dossiers

détenues par la SVM.

- **Groupe local**

  Un groupe avec un SID unique n'a de visibilité que sur le SVM sur lequel il est créé. Les groupes contiennent un ensemble de membres. Les membres peuvent être des utilisateurs locaux, des utilisateurs de domaine, des groupes de domaines et des comptes de machine de domaine. Les groupes peuvent être créés, modifiés ou supprimés.

  Les groupes ont plusieurs utilisations :

  - Utilisé pour accorder des privilèges *User Rights Management* à ses membres.
  - Permet de contrôler l'accès au niveau du partage et du fichier aux ressources de fichiers et de dossiers détenues par la SVM.

- **Domaine local**

  Domaine qui dispose de son étendue locale, limitée par le SVM. Le nom du domaine local est le nom du serveur CIFS. Les utilisateurs et groupes locaux sont contenus dans le domaine local.

- **Identificateur de sécurité (SID)**

  Un SID est une valeur numérique de longueur variable qui identifie les entités de sécurité de type Windows. Par exemple, un SID type prend le format suivant : s-1-5-21-3139654847-1303905135-2517279418-123456.

- **Authentification NTLM**

  Méthode de sécurité Microsoft Windows utilisée pour authentifier les utilisateurs sur un serveur CIFS.

- **Cluster Replicated database (RDB)**

  Base de données répliquée avec une instance sur chaque nœud d'un cluster. Les objets utilisateur et groupe locaux sont stockés dans le RDB.

Raisons de la création d'utilisateurs et de groupes locaux

Il existe plusieurs raisons de créer des utilisateurs et des groupes locaux sur votre SVM (Storage Virtual machine). Par exemple, vous pouvez accéder à un serveur SMB à l'aide d'un compte d'utilisateur local si les contrôleurs de domaine (DCS) ne sont pas disponibles, vous pouvez utiliser des groupes locaux pour attribuer des privilèges ou si votre serveur SMB se trouve dans un groupe de travail.

Vous pouvez créer un ou plusieurs comptes utilisateur locaux pour les raisons suivantes :

- Votre serveur SMB se trouve dans un groupe de travail et les utilisateurs de domaine ne sont pas disponibles.

  Les utilisateurs locaux sont requis dans les configurations de groupe de travail.

- Vous souhaitez pouvoir vous authentifier et vous connecter au serveur SMB si les contrôleurs de domaine ne sont pas disponibles.

  Les utilisateurs locaux peuvent s'authentifier auprès du serveur SMB en utilisant l'authentification NTLM lorsque le contrôleur de domaine est en panne, ou en cas de problèmes réseau empêchant votre serveur

SMB de contacter le contrôleur de domaine.

- Vous souhaitez attribuer des privilèges *User Rights Management* à un utilisateur local.

  User Rights Management permet à un administrateur de serveurs SMB de contrôler les droits des utilisateurs et des groupes sur le SVM. Vous pouvez attribuer des privilèges à un utilisateur en lui attribuant des privilèges ou en faisant de l'utilisateur un membre d'un groupe local disposant de ces privilèges.

Vous pouvez créer un ou plusieurs groupes locaux pour les raisons suivantes :

- Votre serveur SMB se trouve dans un groupe de travail et les groupes de domaines ne sont pas disponibles.

  Les groupes locaux ne sont pas requis dans les configurations de groupes de travail, mais ils peuvent être utiles pour gérer les privilèges d'accès pour les utilisateurs de groupes de travail locaux.

- Vous souhaitez contrôler l'accès aux ressources de fichiers et de dossiers à l'aide des groupes locaux pour le contrôle du partage et de l'accès aux fichiers.
- Vous souhaitez créer des groupes locaux avec des privilèges *User Rights Management* personnalisés.

  Certains groupes d'utilisateurs intégrés ont des privilèges prédéfinis. Pour attribuer un ensemble personnalisé de privilèges, vous pouvez créer un groupe local et attribuer les privilèges nécessaires à ce groupe. Vous pouvez ensuite ajouter des utilisateurs locaux, des utilisateurs de domaine et des groupes de domaines au groupe local.

Informations associées

Fonctionnement de l'authentification des utilisateurs locaux

Liste des privilèges pris en charge

Fonctionnement de l'authentification des utilisateurs locaux

Avant qu'un utilisateur local puisse accéder aux données sur un serveur CIFS, il doit créer une session authentifiée.

SMB étant basé sur une session, l'identité de l'utilisateur peut être déterminée une seule fois, lors de la première configuration de la session. Le serveur CIFS utilise l'authentification NTLM lors de l'authentification des utilisateurs locaux. Les fournisseurs de NTLMv1 et NTLMv2 sont tous deux pris en charge.

ONTAP utilise l'authentification locale dans trois cas d'utilisation. Chaque cas d'utilisation dépend du fait que la partie du domaine du nom d'utilisateur (au format DOMAINE\utilisateur) correspond au nom de domaine local du serveur CIFS (le nom du serveur CIFS) :

- La partie domaine correspond

  Les utilisateurs qui fournissent des informations d'identification d'utilisateur local lors de la demande d'accès aux données sont authentifiés localement sur le serveur CIFS.

- La partie du domaine ne correspond pas

  ONTAP tente d'utiliser l'authentification NTLM avec un contrôleur de domaine dans le domaine auquel le serveur CIFS appartient. Si l'authentification réussit, la connexion est terminée. Si cela ne fonctionne pas, ce qui se passe ensuite dépend de la raison pour laquelle l'authentification n'a pas réussi.

Par exemple, si l'utilisateur existe dans Active Directory mais que le mot de passe est incorrect ou expiré, ONTAP ne tente pas d'utiliser le compte d'utilisateur local correspondant sur le serveur CIFS. Au lieu de cela, l'authentification échoue. Dans d'autres cas, ONTAP utilise le compte local correspondant sur le serveur CIFS, s'il existe, pour l'authentification, même si les noms de domaine NetBIOS ne correspondent pas. Par exemple, si un compte de domaine correspondant existe mais est désactivé, ONTAP utilise le compte local correspondant sur le serveur CIFS pour l'authentification.

- La partie domaine n'est pas spécifiée

  ONTAP tente d'abord l'authentification en tant qu'utilisateur local. Si l'authentification en tant qu'utilisateur local échoue, ONTAP authentifie l'utilisateur avec un contrôleur de domaine dans le domaine auquel le serveur CIFS appartient.

Une fois l'authentification des utilisateurs locaux ou de domaine terminée, ONTAP crée un jeton d'accès complet, qui tient compte de l'appartenance et des privilèges des groupes locaux.

Pour plus d'informations sur l'authentification NTLM pour les utilisateurs locaux, consultez la documentation Microsoft Windows.

Informations associées

Activation ou désactivation de l'authentification des utilisateurs locaux

Comment les jetons d'accès utilisateur sont construits

Lorsqu'un utilisateur mappe un partage, une session SMB authentifiée est établie et un jeton d'accès utilisateur est construit qui contient des informations sur l'utilisateur, l'appartenance au groupe de l'utilisateur et les privilèges cumulatifs, ainsi que l'utilisateur UNIX mappé.

À moins que la fonctionnalité ne soit désactivée, les informations d'utilisateur et de groupe locaux sont également ajoutées au jeton d'accès utilisateur. La manière dont les jetons d'accès sont créés dépend de la manière dont la connexion est destinée à un utilisateur local ou à un utilisateur de domaine Active Directory :

- Connexion de l'utilisateur local

  Bien que les utilisateurs locaux puissent être membres de groupes locaux différents, les groupes locaux ne peuvent pas être membres d'autres groupes locaux. Le jeton d'accès utilisateur local se compose d'une Union de tous les privilèges attribués aux groupes auxquels un utilisateur local particulier est membre.

- Connexion utilisateur du domaine

  Lorsqu'un utilisateur de domaine se connecte, ONTAP obtient un jeton d'accès utilisateur contenant le SID de l'utilisateur et les SID pour tous les groupes de domaine auxquels l'utilisateur est membre. ONTAP utilise l'Union du jeton d'accès d'utilisateur du domaine avec le jeton d'accès fourni par les membres locaux des groupes de domaine de l'utilisateur (le cas échéant), ainsi que tout privilège direct attribué à l'utilisateur du domaine ou à l'un de ses membres de groupe de domaine.

Pour les connexions utilisateur locales et de domaine, le GROUPE principal RID est également défini pour le jeton d'accès utilisateur. Le RID par défaut est `Domain Users` (RID 513). Vous ne pouvez pas modifier la valeur par défaut.

Le processus de mappage de noms Windows-to-UNIX et UNIX-to-Windows suit les mêmes règles pour les comptes locaux et de domaine.

Il n'y a pas de mappage automatique implicite d'un utilisateur UNIX vers un compte local. Si cela est nécessaire, une règle de mappage explicite doit être spécifiée à l'aide des commandes de mappage de noms existantes.

Consignes relatives à l'utilisation de SnapMirror sur des SVM contenant des groupes locaux

Notez les instructions lorsque vous configurez SnapMirror sur des volumes appartenant aux SVM contenant des groupes locaux.

Vous ne pouvez pas utiliser des groupes locaux dans des ACE appliqués à des fichiers, des répertoires ou des partages qui sont répliqués par SnapMirror vers une autre SVM. Si vous utilisez la fonctionnalité SnapMirror pour créer un miroir de reprise sur incident sur un volume situé sur un autre SVM et que le volume dispose d'une version ACE pour un groupe local, l'ACE n'est pas valide pour le miroir. Si les données sont répliquées sur un autre SVM, celles-ci se croisent efficacement et un autre domaine local. Les autorisations accordées aux utilisateurs et groupes locaux ne sont valides qu'au sein du périmètre de la SVM sur lequel ils ont été créés.

Ce qui arrive aux utilisateurs et aux groupes locaux lors de la suppression des serveurs CIFS

L'ensemble par défaut des utilisateurs et groupes locaux est créé lors de la création d'un serveur CIFS et ils sont associés au serveur virtuel de stockage (SVM) qui héberge le serveur CIFS. Les administrateurs SVM peuvent créer à tout moment des utilisateurs et groupes locaux. Lorsque vous supprimez le serveur CIFS, vous devez connaître ce qui arrive aux utilisateurs et aux groupes locaux.

Les utilisateurs et groupes locaux sont associés à des SVM ; ils ne sont donc pas supprimés lorsque des serveurs CIFS sont supprimés pour des raisons de sécurité. Bien que les utilisateurs et groupes locaux ne soient pas supprimés lors de la suppression du serveur CIFS, ils sont masqués. Vous ne pouvez ni afficher ni gérer des utilisateurs et groupes locaux tant que vous n'avez pas recréés un serveur CIFS sur la SVM.

L'état d'administration du serveur CIFS n'affecte pas la visibilité des utilisateurs ou des groupes locaux.

Utilisation de la console de gestion Microsoft avec des utilisateurs et des groupes locaux

Vous pouvez afficher des informations sur les utilisateurs et groupes locaux à partir de la console de gestion Microsoft. Avec cette version de ONTAP, vous ne pouvez pas effectuer d'autres tâches de gestion pour les utilisateurs et groupes locaux à partir de la console de gestion Microsoft.

Instructions pour le rétablissement

Si vous prévoyez de restaurer le cluster à une version de ONTAP qui ne prend pas en charge les utilisateurs et groupes locaux, ainsi que les utilisateurs et groupes locaux utilisés pour gérer l'accès aux fichiers ou les droits des utilisateurs, vous devez tenir compte de certaines considérations.

- Pour des raisons de sécurité, les informations concernant les utilisateurs, groupes et privilèges locaux configurés ne sont pas supprimées lorsque ONTAP est rétabli sur une version qui ne prend pas en charge les fonctionnalités des utilisateurs et des groupes locaux.

- Lors de la restauration d'une version majeure antérieure de ONTAP, ONTAP n'utilise pas d'utilisateurs et de groupes locaux pendant l'authentification et la création des informations d'identification.
- Les utilisateurs et groupes locaux ne sont pas supprimés des listes de contrôle d'accès aux fichiers et aux dossiers.
- Les demandes d'accès aux fichiers qui dépendent de l'accès sont refusées en raison des autorisations accordées aux utilisateurs ou groupes locaux.

  Pour autoriser l'accès, vous devez reconfigurer les autorisations d'accès aux fichiers afin d'autoriser l'accès en fonction des objets de domaine au lieu d'objets d'utilisateur et de groupe locaux.

Quels sont les privilèges locaux

Liste des privilèges pris en charge

ONTAP dispose d'un ensemble prédéfini de privilèges pris en charge. Certains groupes locaux prédéfinis ont certains de ces privilèges ajoutés par défaut. Vous pouvez également ajouter ou supprimer des privilèges des groupes prédéfinis ou créer de nouveaux utilisateurs ou groupes locaux et ajouter des privilèges aux groupes que vous avez créés ou aux utilisateurs et groupes de domaine existants.

Le tableau ci-dessous répertorie les privilèges pris en charge sur la machine virtuelle de stockage (SVM) et fournit la liste des groupes BUILTIN avec des privilèges attribués :

Nom de privilège	Paramètre de sécurité par défaut	Description
`SeTcbPrivilege`	Aucune	Faire partie du système d'exploitation
`SeBackupPrivilege`	`BUILTIN\Administrators`, `BUILTIN\Backup Operators`	Sauvegardez des fichiers et des répertoires, en remplaçant les listes de contrôle d'accès
`SeRestorePrivilege`	`BUILTIN\Administrators`, `BUILTIN\Backup Operators`	Restaurez les fichiers et les répertoires, en remplaçant les listes de contrôle d'accès, définissez tout ID utilisateur ou groupe valide comme propriétaire du fichier
`SeTakeOwnershipPrivilege`	`BUILTIN\Administrators`	Prendre possession de fichiers ou d'autres objets
`SeSecurityPrivilege`	`BUILTIN\Administrators`	Gérer les audits Cela inclut l'affichage, le vidage et l'effacement du journal de sécurité.

Nom de privilège	Paramètre de sécurité par défaut	Description
`SeChangeNotifyPrivilege`	`BUILTIN\Administrators`, `BUILTIN\Backup Operators`, `BUILTIN\Power Users`, `BUILTIN\Users`, `Everyone`	Vérification de la traverse de dérivation Les utilisateurs disposant de ce privilège ne sont pas tenus d'avoir des autorisations traverse (x) pour traverser des dossiers, des liens symboliques ou des jonctions.

Informations associées

- Attribuez des privilèges locaux
- Configuration de la vérification de la traverse de dérivation

Attribuer des privilèges

Vous pouvez attribuer des privilèges directement aux utilisateurs locaux ou aux utilisateurs du domaine. Vous pouvez également affecter des utilisateurs à des groupes locaux dont les privilèges attribués correspondent aux fonctions que vous souhaitez que ces utilisateurs disposent.

- Vous pouvez attribuer un ensemble de privilèges à un groupe que vous créez.

  Vous ajoutez ensuite un utilisateur au groupe disposant des privilèges que vous souhaitez que cet utilisateur dispose.

- Vous pouvez également attribuer des utilisateurs locaux et des utilisateurs de domaine à des groupes prédéfinis dont les privilèges par défaut correspondent aux privilèges que vous souhaitez accorder à ces utilisateurs.

Informations associées

- Ajout de privilèges aux utilisateurs ou groupes locaux ou de domaine
- Suppression des privilèges des utilisateurs ou groupes locaux ou de domaine
- Réinitialisation des privilèges pour les utilisateurs et groupes locaux ou de domaine
- Configuration de la vérification de la traverse de dérivation

Instructions d'utilisation des groupes BULILTIN et du compte administrateur local

Il y a certaines directives que vous devez garder à l'esprit lorsque vous utilisez les groupes BULTIN et le compte d'administrateur local. Par exemple, vous pouvez renommer le compte d'administrateur local, mais vous ne pouvez pas supprimer ce compte.

- Le compte Administrateur peut être renommé mais ne peut pas être supprimé.
- Le compte Administrateur ne peut pas être supprimé du groupe BULTIN\Administrators.
- Les groupes INTÉGRÉS peuvent être renommés mais ne peuvent pas être supprimés.

  Une fois le groupe BUILTIN renommé, un autre objet local peut être créé avec le nom connu ; cependant,

l'objet est affecté à un nouveau RID.

- Il n'y a pas de compte invité local.

Informations associées

Groupes et privilèges par défaut prédéfinis BUILTIN

Conditions requises pour les mots de passe des utilisateurs locaux

Par défaut, les mots de passe des utilisateurs locaux doivent répondre aux exigences de complexité. Les exigences de complexité des mots de passe sont similaires aux exigences définies dans la stratégie de sécurité Microsoft Windows *local*.

Le mot de passe doit répondre aux critères suivants :

- Doit comporter au moins six caractères
- Ne doit pas contenir le nom du compte d'utilisateur
- Doit contenir des caractères d'au moins trois des quatre catégories suivantes :
  - Caractères majuscules anglais (A à Z)
  - Caractères anglais minuscules (a à z)
  - Chiffres de base 10 (0 à 9)
  - Caractères spéciaux :

    ~ ! @ # $ % ^ et * _ - + = ` \ | ( ) [ ] : ; " < > , . ? /

Informations associées

Activation ou désactivation de la complexité requise des mots de passe pour les utilisateurs SMB locaux

Affichage d'informations sur les paramètres de sécurité du serveur CIFS

Modification des mots de passe des comptes utilisateur locaux

Groupes et privilèges par défaut prédéfinis BUILTIN

Vous pouvez affecter l'appartenance d'un utilisateur local ou d'un utilisateur de domaine à un ensemble prédéfini de groupes BUILTIN fourni par ONTAP. Les groupes prédéfinis ont des privilèges prédéfinis attribués.

Le tableau suivant décrit les groupes prédéfinis :

Groupe prédéfini BUILTIN	Privilèges par défaut
`BUILTIN\Administrators`RID 544 Lors de sa création initiale, le local `Administrator` Compte, avec UN RID de 500, est automatiquement fait membre de ce groupe. Lorsque l'ordinateur virtuel de stockage (SVM) est rejoint un domaine, le `domain\Domain Admins` le groupe est ajouté au groupe. Si le SVM laisse le domaine, le `domain\Domain Admins` le groupe est supprimé du groupe.	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeSecurityPrivilege` • `SeTakeOwnershipPrivilege` • `SeChangeNotifyPrivilege`
`BUILTIN\Power Users`RID 547 Lors de sa création initiale, ce groupe n'a aucun membre. Les membres de ce groupe ont les caractéristiques suivantes : • Peut créer et gérer des utilisateurs et des groupes locaux. • Impossible d'ajouter eux-mêmes ou tout autre objet au `BUILTIN\Administrators` groupe.	`SeChangeNotifyPrivilege`
`BUILTIN\Backup Operators`RID 551 Lors de sa création initiale, ce groupe n'a aucun membre. Les membres de ce groupe peuvent remplacer les autorisations de lecture et d'écriture sur des fichiers ou des dossiers s'ils sont ouverts avec l'intention de sauvegarde.	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeChangeNotifyPrivilege`
`BUILTIN\Users`RID 545 Lors de sa création initiale, ce groupe n'a pas de membres (outre les membres implicites) `Authenticated Users` groupe spécial). Lorsque le SVM est joint à un domaine, le `domain\Domain Users` le groupe est ajouté à ce groupe. Si le SVM laisse le domaine, le `domain\Domain Users` le groupe est supprimé de ce groupe.	`SeChangeNotifyPrivilege`
`Everyone`SID S-1-1-0 Ce groupe inclut tous les utilisateurs, y compris les invités (mais pas les utilisateurs anonymes). Il s'agit d'un groupe implicite avec une adhésion implicite.	`SeChangeNotifyPrivilege`

Informations associées

Instructions d'utilisation des groupes BULILTIN et du compte administrateur local

Liste des privilèges pris en charge

Configuration de la vérification de la traverse de dérivation

Activez ou désactivez la fonctionnalité utilisateurs et groupes locaux

Activer ou désactiver la présentation des fonctionnalités des utilisateurs et groupes locaux

Avant de pouvoir utiliser des utilisateurs et des groupes locaux pour contrôler l'accès aux données de style de sécurité NTFS, les fonctionnalités d'utilisateur et de groupe locaux doivent être activées. En outre, si vous souhaitez utiliser des utilisateurs locaux pour l'authentification SMB, la fonctionnalité d'authentification des utilisateurs locaux doit être activée.

Les fonctionnalités des utilisateurs et groupes locaux et l'authentification des utilisateurs locaux sont activées par défaut. Si elles ne sont pas activées, vous devez les activer avant de pouvoir configurer et utiliser des utilisateurs et des groupes locaux. Vous pouvez désactiver les fonctionnalités des utilisateurs et groupes locaux à tout moment.

En plus de désactiver explicitement la fonctionnalité des utilisateurs et groupes locaux, ONTAP désactive les fonctionnalités utilisateur et groupe locaux si un nœud du cluster est rétabli sur une version de ONTAP qui ne prend pas en charge cette fonctionnalité. Les fonctionnalités des utilisateurs et groupes locaux ne sont pas activées tant que tous les nœuds du cluster n'exécutent pas une version de ONTAP qui le prend en charge.

Informations associées

Modifier les comptes utilisateur locaux

Modifier les groupes locaux

Ajoutez des privilèges aux utilisateurs ou groupes locaux ou de domaine

Activez ou désactivez les utilisateurs et groupes locaux

Vous pouvez activer ou désactiver les utilisateurs et groupes locaux pour l'accès SMB sur des SVM (Storage Virtual machines). La fonctionnalité utilisateurs et groupes locaux est activée par défaut.

Description de la tâche

Vous pouvez utiliser des utilisateurs et des groupes locaux lors de la configuration des autorisations de partage SMB et de fichiers NTFS et, éventuellement, utiliser des utilisateurs locaux pour l'authentification lors de la création d'une connexion SMB. Pour utiliser les utilisateurs locaux pour l'authentification, vous devez également activer l'option d'authentification des utilisateurs et groupes locaux.

Étapes

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

Si vous voulez que les utilisateurs et les groupes locaux soient…	Entrez la commande…
Activé	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-users-and -groups-enabled true`
Désactivé	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-users-and -groups-enabled false`

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

Exemple

L'exemple suivant permet aux utilisateurs et groupes locaux de la fonctionnalité 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-local-users-and
-groups-enabled true

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

Informations associées

Activez ou désactivez l'authentification des utilisateurs locaux

Activez ou désactivez les comptes utilisateur locaux

Activez ou désactivez l'authentification des utilisateurs locaux

Vous pouvez activer ou désactiver l'authentification des utilisateurs locaux pour l'accès SMB sur des SVM (Storage Virtual machines). La valeur par défaut est d'autoriser l'authentification des utilisateurs locaux, ce qui est utile lorsque la SVM ne peut pas contacter un contrôleur de domaine ou si vous choisissez de ne pas utiliser de contrôles d'accès au niveau des domaines.

Avant de commencer

La fonctionnalité utilisateurs et groupes locaux doit être activée sur le serveur CIFS.

Description de la tâche

Vous pouvez activer ou désactiver l'authentification des utilisateurs locaux à tout moment. Si vous souhaitez utiliser des utilisateurs locaux pour l'authentification lors de la création d'une connexion SMB, vous devez également activer l'option utilisateurs et groupes locaux du serveur CIFS.

Étapes

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

Si vous voulez que l'authentification locale soit…	Entrez la commande…
Activé	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-auth-enabled true`
Désactivé	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-auth-enabled false`

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

Exemple

L'exemple suivant active l'authentification utilisateur local 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-local-auth
-enabled true

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

Informations associées

Fonctionnement de l'authentification des utilisateurs locaux

Activation ou désactivation des utilisateurs et groupes locaux

Gérez les comptes utilisateurs locaux

Modifier les comptes utilisateur locaux

Vous pouvez modifier un compte d'utilisateur local si vous souhaitez modifier le nom complet ou la description d'un utilisateur existant et si vous souhaitez activer ou désactiver le compte d'utilisateur. Vous pouvez également renommer un compte d'utilisateur local si le nom de l'utilisateur est compromis ou si un changement de nom est nécessaire à des fins administratives.

Les fonctions que vous recherchez…	Entrez la commande…
Modifier le nom complet de l'utilisateur local	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user-name` *`user_name`* `-full-name text` Si le nom complet contient un espace, il doit être placé entre guillemets.
Modifier la description de l'utilisateur local	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user-name` *`user_name`* `-description text` Si la description contient un espace, elle doit être placée entre guillemets.
Activez ou désactivez le compte utilisateur local	`vserver cifs users-and-groups local-user modify -vserver *vserver_name* -user-name *user_name* -is -account-disabled {true
false}`	Renommez le compte d'utilisateur local

Exemple

L'exemple suivant renomme l'utilisateur local « CIFS_SERVER\sue » en « CIFS_SERVER\sue_New » sur la machine virtuelle de stockage (SVM, précédemment appelé vServer) vs1 :

```
cluster1::> vserver cifs users-and-groups local-user rename -user-name
CIFS_SERVER\sue -new-user-name CIFS_SERVER\sue_new -vserver vs1
```

Activez ou désactivez les comptes utilisateur locaux

Vous activez un compte utilisateur local si vous souhaitez que l'utilisateur puisse accéder aux données contenues dans la machine virtuelle de stockage (SVM) via une connexion SMB. Vous pouvez également désactiver un compte utilisateur local si vous ne souhaitez pas que cet utilisateur accède aux données des SVM via SMB.

Description de la tâche

Vous activez un utilisateur local en modifiant le compte utilisateur.

Étape

1. Effectuez l'action appropriée :

Les fonctions que vous recherchez…	Entrez la commande…
Activez le compte utilisateur	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user-name` *`user_name`* `-is-account -disabled false`

Les fonctions que vous recherchez…	Entrez la commande…
Désactivez le compte utilisateur	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user-name` *`user_name`* `-is-account -disabled true`

Modifier les mots de passe des comptes utilisateur locaux

Vous pouvez modifier le mot de passe du compte d'un utilisateur local. Cela peut être utile si le mot de passe de l'utilisateur est compromis ou si l'utilisateur a oublié le mot de passe.

Étape

1. Modifiez le mot de passe en effectuant l'action appropriée : `vserver cifs users-and-groups local-user set-password -vserver` *`vserver_name`* `-user-name` *`user_name`*

Exemple

L'exemple suivant définit le mot de passe pour l'utilisateur local « CIFS_SERVER\sue » associé à une machine virtuelle de stockage (SVM, anciennement Vserver) vs1 :

```
cluster1::> vserver cifs users-and-groups local-user set-password -user
-name CIFS_SERVER\sue -vserver vs1

Enter the new password:
Confirm the new password:
```

Informations associées

Activation ou désactivation de la complexité requise des mots de passe pour les utilisateurs SMB locaux

Affichage d'informations sur les paramètres de sécurité du serveur CIFS

Affiche des informations sur les utilisateurs locaux

Vous pouvez afficher une liste de tous les utilisateurs locaux sous forme de résumé. Si vous souhaitez déterminer les paramètres de compte configurés pour un utilisateur spécifique, vous pouvez afficher des informations détaillées sur le compte de cet utilisateur ainsi que les informations sur le compte de plusieurs utilisateurs. Ces informations peuvent vous aider à déterminer si vous devez modifier les paramètres d'un utilisateur et à résoudre les problèmes d'authentification ou d'accès aux fichiers.

Description de la tâche

Les informations relatives au mot de passe d'un utilisateur ne s'affichent jamais.

Étape

1. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Entrez la commande…
Affichage des informations relatives à tous les utilisateurs sur la machine virtuelle de stockage (SVM)	`vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*
Affiche des informations détaillées sur le compte d'un utilisateur	`vserver cifs users-and-groups local-user show -instance -vserver` *`vserver_name`* `-user-name` *`user_name`*

D'autres paramètres facultatifs peuvent être choisis lors de l'exécution de la commande. Consultez la page man pour plus d'informations

Exemple

L'exemple suivant affiche les informations relatives à tous les utilisateurs locaux sur le SVM vs1 :

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                    Full Name     Description
-------- --------------------------- ------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith   Built-in administrator
account
vs1      CIFS_SERVER\sue             Sue   Jones
```

Affiche des informations sur les membres de groupe pour les utilisateurs locaux

Vous pouvez afficher des informations sur les groupes locaux auxquels un utilisateur local appartient. Vous pouvez utiliser ces informations pour déterminer l'accès que l'utilisateur doit avoir aux fichiers et dossiers. Ces informations peuvent être utiles pour déterminer les droits d'accès que l'utilisateur doit posséder aux fichiers et dossiers ou pour résoudre les problèmes d'accès aux fichiers.

Description de la tâche

Vous pouvez personnaliser la commande pour afficher uniquement les informations que vous souhaitez afficher.

Étape

1. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Entrez la commande…
Afficher les informations d'appartenance des utilisateurs locaux pour un utilisateur local spécifié	`vserver cifs users-and-groups local-user show-membership -user-name` *`user_name`*

Les fonctions que vous recherchez…	Entrez la commande…
Affiche les informations d'appartenance de l'utilisateur local pour le groupe local dont cet utilisateur local est membre	`vserver cifs users-and-groups local-user show-membership -membership` *`group_name`*
Afficher les informations d'appartenance des utilisateurs aux utilisateurs locaux associés à une machine virtuelle de stockage (SVM) spécifiée	`vserver cifs users-and-groups local-user show-membership -vserver` *`vserver_name`*
Affiche des informations détaillées pour tous les utilisateurs locaux sur un SVM spécifié	`vserver cifs users-and-groups local-user show-membership -instance -vserver` *`vserver_name`*

Exemple

L'exemple suivant affiche les informations d'appartenance de tous les utilisateurs locaux sur le SVM vs1 ; l'utilisateur « CIFS_SERVER\Administrator » est membre du groupe « BUILTIN\Administrators » et « CIFS_SERVER\sue » est membre du groupe « CIFS_SERVER\g1 » :

```
cluster1::> vserver cifs users-and-groups local-user show-membership
-vserver vs1
Vserver    User Name                     Membership
---------- ----------------------------- ------------------------
vs1        CIFS_SERVER\Administrator     BUILTIN\Administrators
           CIFS_SERVER\sue               CIFS_SERVER\g1
```

Supprimer les comptes utilisateur locaux

Vous pouvez supprimer des comptes utilisateurs locaux de votre machine virtuelle de stockage (SVM) s'ils ne sont plus nécessaires pour l'authentification SMB locale sur le serveur CIFS ou pour déterminer les droits d'accès aux données contenues dans votre SVM.

Description de la tâche

Tenez compte des points suivants lors de la suppression d'utilisateurs locaux :

- Le système de fichiers n'est pas modifié.

  Les descripteurs de sécurité Windows sur les fichiers et les répertoires qui font référence à cet utilisateur ne sont pas ajustés.

- Toutes les références aux utilisateurs locaux sont supprimées des bases de données d'appartenance et de privilèges.
- Les utilisateurs standard bien connus tels que Administrateur ne peuvent pas être supprimés.

Étapes

1. Déterminez le nom du compte d'utilisateur local que vous souhaitez supprimer : `vserver cifs users-`

and-groups local-user show -vserver *vserver_name*

2. Supprimez l'utilisateur local : `vserver cifs users-and-groups local-user delete -vserver *vserver_name* -user-name *username_name*`
3. Vérifiez que le compte utilisateur est supprimé : `vserver cifs users-and-groups local-user show -vserver *vserver_name*`

Exemple

L'exemple suivant supprime l'utilisateur local « CIFS_SERVER\sue » associé à la SVM vs1 :

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                   Full Name      Description
-------- --------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith    Built-in administrator
account
vs1      CIFS_SERVER\sue             Sue   Jones


cluster1::> vserver cifs users-and-groups local-user delete -vserver vs1
-user-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver      User Name                   Full Name      Description
-------- --------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith    Built-in administrator
account
```

Gérez des groupes locaux

Modifier les groupes locaux

Vous pouvez modifier les groupes locaux existants en modifiant la description d'un groupe local existant ou en renommant ce groupe.

Les fonctions que vous recherchez…	Utilisez la commande…
Modifier la description du groupe local	`vserver cifs users-and-groups local-group modify -vserver *vserver_name* -group-name *group_name* -description text` Si la description contient un espace, elle doit être placée entre guillemets.
Renommer le groupe local	`vserver cifs users-and-groups local-group rename -vserver *vserver_name* -group-name *group_name* -new-group-name *new_group_name*`

Exemples

L'exemple suivant renomme le groupe local « CIFS_SERVER\engineering » en « CIFS_SERVER\engineering_New » :

```
cluster1::> vserver cifs users-and-groups local-group rename -vserver vs1
-group-name CIFS_SERVER\engineering -new-group-name
CIFS_SERVER\engineering_new
```

L'exemple suivant modifie la description du groupe local « CIFS_SERVER\engineering » :

```
cluster1::> vserver cifs users-and-groups local-group modify -vserver vs1
-group-name CIFS_SERVER\engineering -description "New Description"
```

Affiche des informations sur les groupes locaux

Vous pouvez afficher la liste de tous les groupes locaux configurés sur le cluster ou sur une machine virtuelle de stockage (SVM) spécifiée. Ces informations peuvent être utiles pour résoudre les problèmes d'accès aux fichiers aux données contenues dans la SVM ou sur les problèmes liés aux droits d'utilisateur (privilège) sur la SVM.

Étape

1. Effectuez l'une des opérations suivantes :

Pour obtenir des informations sur…	Entrez la commande…
Tous les groupes locaux du cluster	`vserver cifs users-and-groups local-group show`
Tous les groupes locaux sur le SVM	`vserver cifs users-and-groups local-group show -vserver` *`vserver_name`*

D'autres paramètres facultatifs peuvent être choisis lors de l'exécution de cette commande. Consultez la page man pour plus d'informations

Exemple

L'exemple suivant affiche les informations sur tous les groupes locaux sur le SVM vs1 :

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver  Group Name                  Description
-------- --------------------------- ----------------------------
vs1      BUILTIN\Administrators      Built-in Administrators group
vs1      BUILTIN\Backup Operators    Backup Operators group
vs1      BUILTIN\Power Users         Restricted administrative privileges
vs1      BUILTIN\Users               All users
vs1      CIFS_SERVER\engineering
vs1      CIFS_SERVER\sales
```

Gérer l'appartenance à un groupe local

Vous pouvez gérer l'appartenance à un groupe local en ajoutant et en supprimant des utilisateurs locaux ou de domaine, ou en ajoutant et supprimant des groupes de domaines. Ceci est utile si vous souhaitez contrôler l'accès aux données en fonction des contrôles d'accès placés sur le groupe ou si vous souhaitez que les utilisateurs disposent de privilèges associés à ce groupe.

Description de la tâche

Directives pour l'ajout de membres à un groupe local :

- Vous ne pouvez pas ajouter d'utilisateurs au groupe spécial *Everyone*.
- Le groupe local doit exister avant de pouvoir y ajouter un utilisateur.
- L'utilisateur doit exister avant de pouvoir ajouter l'utilisateur à un groupe local.
- Vous ne pouvez pas ajouter un groupe local à un autre groupe local.
- Pour ajouter un utilisateur ou un groupe de domaine à un groupe local, Data ONTAP doit pouvoir résoudre le nom en SID.

Directives pour le retrait de membres d'un groupe local :

- Vous ne pouvez pas supprimer des membres du groupe spécial *Everyone*.
- Le groupe dont vous souhaitez supprimer un membre doit exister.
- ONTAP doit pouvoir résoudre les noms des membres que vous souhaitez supprimer du groupe vers un SID correspondant.

Étape

1. Ajouter ou supprimer un membre d'un groupe.

Les fonctions que vous recherchez…	Utilisez ensuite la commande…
Ajouter un membre à un groupe	`vserver cifs users-and-groups local-group add-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]` Vous pouvez spécifier une liste délimitée par des virgules d'utilisateurs locaux, d'utilisateurs de domaine ou de groupes de domaine à ajouter au groupe local spécifié.
Supprimer un membre d'un groupe	`vserver cifs users-and-groups local-group remove-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]` Vous pouvez spécifier une liste délimitée par des virgules d'utilisateurs locaux, d'utilisateurs de domaine ou de groupes de domaine à supprimer du groupe local spécifié.

L'exemple suivant ajoute un utilisateur local « `SMB_SERVER\sue` » et un groupe de domaine « AD_DOM\dom_eng »au groupe local « `SMB_SERVER\engineering' » sur la SVM vs1 :

```
cluster1::> vserver cifs users-and-groups local-group add-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,AD_DOMAIN\dom_eng
```

L'exemple suivant supprime les utilisateurs locaux « `SMB_SERVER\sue` » et « `SMB_SERVER\james` du groupe local « `SMB_SERVER\engineering' » sur la SVM vs1 :

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

Informations associées

Affichage des informations relatives aux membres des groupes locaux

Affiche des informations sur les membres des groupes locaux

Vous pouvez afficher la liste de tous les membres des groupes locaux configurés sur le cluster ou sur une machine virtuelle de stockage (SVM) spécifiée. Ces informations peuvent être utiles pour résoudre les problèmes d'accès aux fichiers ou de droits d'utilisateur (privilèges).

Étape

1. Effectuez l'une des opérations suivantes :

Pour afficher des informations sur…	Entrez la commande…
Membres de tous les groupes locaux du cluster	`vserver cifs users-and-groups local-group show-members`
Membres de tous les groupes locaux sur le SVM	`vserver cifs users-and-groups local-group show-members -vserver` *`vserver_name`*

Exemple

L'exemple suivant affiche les informations sur les membres de tous les groupes locaux sur le SVM vs1 :

```
cluster1::> vserver cifs users-and-groups local-group show-members
-vserver vs1
Vserver   Group Name                    Members
--------- ----------------------------- ------------------------
vs1       BUILTIN\Administrators        CIFS_SERVER\Administrator
                                        AD_DOMAIN\Domain Admins
                                        AD_DOMAIN\dom_grp1
          BUILTIN\Users                 AD_DOMAIN\Domain Users
                                        AD_DOMAIN\dom_usr1
          CIFS_SERVER\engineering       CIFS_SERVER\james
```

Supprimer un groupe local

Vous pouvez supprimer un groupe local de la machine virtuelle de stockage (SVM) s'il n'est plus nécessaire pour déterminer les droits d'accès aux données associées à ce SVM ou s'il n'est plus nécessaire d'attribuer des droits d'utilisateur de SVM (privilèges) aux membres du groupe.

Description de la tâche

Lors de la suppression de groupes locaux, tenez compte des points suivants :

- Le système de fichiers n'est pas modifié.

  Les descripteurs de sécurité Windows sur les fichiers et les répertoires faisant référence à ce groupe ne sont pas ajustés.

- Si le groupe n'existe pas, une erreur est renvoyée.
- Le groupe *Everyone* spécial ne peut pas être supprimé.
- Les groupes intégrés tels que *BUILTIN\Administrators BUILTIN\Users* ne peuvent pas être supprimés.

Étapes

1. Déterminer le nom du groupe local que vous souhaitez supprimer en affichant la liste des groupes locaux sur la SVM : `vserver cifs users-and-groups local-group show -vserver vserver_name`
2. Supprimez le groupe local : `vserver cifs users-and-groups local-group delete -vserver`

vserver_name -group-name *group_name*

3. Vérifiez que le groupe est supprimé : `vserver cifs users-and-groups local-user show -vserver vserver_name`

Exemple

L'exemple suivant supprime le groupe local « CIFS_SERVER\sales » associé à la SVM vs1 :

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- ----------------------------- ----------------------------
vs1       BUILTIN\Administrators        Built-in Administrators group
vs1       BUILTIN\Backup Operators      Backup Operators group
vs1       BUILTIN\Power Users           Restricted administrative
privileges
vs1       BUILTIN\Users                 All users
vs1       CIFS_SERVER\engineering
vs1       CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group delete -vserver vs1
-group-name CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- ----------------------------- ----------------------------
vs1       BUILTIN\Administrators        Built-in Administrators group
vs1       BUILTIN\Backup Operators      Backup Operators group
vs1       BUILTIN\Power Users           Restricted administrative
privileges
vs1       BUILTIN\Users                 All users
vs1       CIFS_SERVER\engineering
```

Mettre à jour les noms d'utilisateur et de groupe du domaine dans les bases de données locales

Vous pouvez ajouter des utilisateurs et des groupes de domaine aux groupes locaux d'un serveur CIFS. Ces objets de domaine sont enregistrés dans des bases de données locales sur le cluster. Si un objet domaine est renommé, les bases de données locales doivent être mises à jour manuellement.

Description de la tâche

On doit préciser le nom de la machine virtuelle de stockage (SVM) sur laquelle vous souhaitez mettre à jour les noms de domaine.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Effectuez l'action appropriée :

Si vous souhaitez mettre à jour les utilisateurs et les groupes du domaine et…	Utilisez cette commande…
Affiche les utilisateurs et groupes du domaine mis à jour avec succès et dont la mise à jour a échoué	`vserver cifs users-and-groups update-names -vserver vserver_name`
Afficher les utilisateurs et groupes du domaine mis à jour avec succès	`vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only false`
Afficher uniquement les utilisateurs et les groupes du domaine qui n'ont pas été mis à jour	`vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only true`
Supprimez toutes les informations d'état concernant les mises à jour	`vserver cifs users-and-groups update-names -vserver vserver_name -suppress -all-output true`

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

Exemple

L'exemple suivant met à jour les noms des utilisateurs et groupes de domaine associés à la machine virtuelle de stockage (SVM, anciennement Vserver) vs1. Pour la dernière mise à jour, une chaîne de noms dépendante doit être mise à jour :

```
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 users-and-groups update-names -vserver vs1

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-12345
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654322-23456
   Domain:            EXAMPLE2
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-123456
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user3
   Updated Name:      dom_user4
   Status:            Successfully updated; also updated SID "S-1-5-21-
123456789-234565432-987654321-123457"
                      to name "dom_user5"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123458"
                      to name "dom_user6"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123459"
                      to name "dom_user7"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123460"
                      to name "dom_user8"

The command completed successfully. 7 Active Directory objects have been
updated.

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

Gérer les privilèges locaux

Ajoutez des privilèges aux utilisateurs ou groupes locaux ou de domaine

Vous pouvez gérer les droits d'utilisateur pour les utilisateurs ou groupes locaux ou de domaine en ajoutant des privilèges. Les privilèges ajoutés remplacent les privilèges par défaut attribués à l'un de ces objets. Cela vous permet de renforcer la sécurité en vous permettant de personnaliser les privilèges d'un utilisateur ou d'un groupe.

Avant de commencer

L'utilisateur ou le groupe local ou de domaine auquel les privilèges seront ajoutés doit déjà exister.

Description de la tâche

L'ajout d'un privilège à un objet remplace les privilèges par défaut pour cet utilisateur ou ce groupe. L'ajout d'un privilège ne supprime pas les privilèges précédemment ajoutés.

Lorsque vous ajoutez des privilèges aux utilisateurs ou groupes locaux ou de domaine, vous devez garder à l'esprit les éléments suivants :

- Vous pouvez ajouter un ou plusieurs privilèges.
- Lors de l'ajout de privilèges à un utilisateur ou à un groupe de domaine, ONTAP peut valider l'utilisateur ou le groupe du domaine en contactant le contrôleur de domaine.

  La commande peut échouer si ONTAP n'est pas en mesure de contacter le contrôleur de domaine.

Étapes

1. Ajoutez un ou plusieurs privilèges à un utilisateur ou groupe local ou de domaine : `vserver cifs users-and-groups privilege add-privilege -vserver _vserver_name_ -user-or -group-name name -privileges _privilege_[,...]`
2. Vérifiez que les privilèges souhaités sont appliqués à l'objet : `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Exemple

L'exemple suivant ajoute les privilèges « `Enregistrer TcbPrivilege' » et « `Enregistrer OwnershipPrivilege » à l'utilisateur « CIFS_SERVER\sue » sur la machine virtuelle de stockage (SVM, précédemment connue sous le nom de Vserver) vs1 :

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege
```

Supprimez les privilèges des utilisateurs ou groupes locaux ou de domaine

Vous pouvez gérer les droits d'utilisateur pour les utilisateurs ou groupes locaux ou de

domaine en supprimant les privilèges. Cela vous permet de renforcer la sécurité en vous permettant de personnaliser le nombre maximal de privilèges dont disposent les utilisateurs et les groupes.

Avant de commencer

L'utilisateur ou le groupe local ou de domaine dont les privilèges seront supprimés doit déjà exister.

Description de la tâche

Vous devez garder à l'esprit les éléments suivants lorsque vous supprimez des privilèges des utilisateurs ou groupes locaux ou de domaine :

- Vous pouvez supprimer un ou plusieurs privilèges.
- Lors de la suppression de privilèges d'un utilisateur ou d'un groupe de domaines, ONTAP peut valider l'utilisateur ou le groupe de domaines en contactant le contrôleur de domaine.

  La commande peut échouer si ONTAP n'est pas en mesure de contacter le contrôleur de domaine.

Étapes

1. Supprimer un ou plusieurs privilèges d'un utilisateur ou groupe local ou de domaine : `vserver cifs users-and-groups privilege remove-privilege -vserver _vserver_name_ -user-or -group-name _name_ -privileges _privilege_[,...]`
2. Vérifiez que les privilèges souhaités ont été supprimés de l'objet : `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Exemple

L'exemple suivant supprime les privilèges « `Enregistrer TcbPrivilege' » et « `Saba OwnershipPrivilege » de l'utilisateur « CIFS_SERVER\sue » sur la machine virtuelle de stockage (SVM, précédemment connue sous le nom de Vserver) vs1 :

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- -------------------
vs1       CIFS_SERVER\sue       -
```

Réinitialisez les privilèges pour les utilisateurs et les groupes locaux ou de domaine

Vous pouvez réinitialiser les privilèges des utilisateurs et groupes locaux ou de domaine.

Cela peut s'avérer utile lorsque vous avez apporté des modifications aux privilèges d'un utilisateur ou d'un groupe local ou de domaine et que ces modifications ne sont plus nécessaires ou souhaitées.

Description de la tâche

La réinitialisation des privilèges d'un utilisateur ou groupe local ou de domaine supprime toutes les entrées de privilèges de cet objet.

Étapes

1. Réinitialisez les privilèges sur un utilisateur ou groupe local ou de domaine : `vserver cifs users-and-groups privilege reset-privilege -vserver vserver_name -user-or-group-name name`
2. Vérifiez que les privilèges sont réinitialisés sur l'objet : `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

Exemples

L'exemple suivant réinitialise les privilèges de l'utilisateur « CIFS_SERVER\sue » sur la machine virtuelle de stockage (SVM, anciennement appelée Vserver) vs1. Par défaut, les utilisateurs normaux ne disposent pas de privilèges associés à leurs comptes :

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name    Privileges
--------- --------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

L'exemple suivant réinitialise les privilèges du groupe « BUILTIN\Administrators », supprimant ainsi l'entrée de privilège :

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name       Privileges
--------- ------------------------ -------------------
vs1       BUILTIN\Administrators   SeRestorePrivilege
                                   SeSecurityPrivilege
                                   SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name BUILTIN\Administrators

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

Affiche des informations sur les remplacements de privilèges

Vous pouvez afficher des informations sur les privilèges personnalisés attribués à des comptes ou groupes d'utilisateurs locaux ou de domaine. Ces informations vous aident à déterminer si les droits d'utilisateur souhaités sont appliqués.

Étape

1. Effectuez l'une des opérations suivantes :

Pour afficher des informations sur…	Entrez cette commande…
Privilèges personnalisés pour tous les utilisateurs et groupes locaux et du domaine sur la machine virtuelle de stockage (SVM)	`vserver cifs users-and-groups privilege show -vserver` *`vserver_name`*
Privilèges personnalisés pour un domaine spécifique ou un utilisateur et groupe local sur le SVM	`vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

D'autres paramètres facultatifs peuvent être choisis lors de l'exécution de cette commande. Consultez la page man pour plus d'informations

Exemple

La commande suivante affiche tous les privilèges explicitement associés aux utilisateurs et groupes locaux ou de domaine pour le SVM vs1 :

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name     Privileges
--------- ---------------------   ---------------
vs1       BUILTIN\Administrators  SeTakeOwnershipPrivilege
                                  SeRestorePrivilege
vs1       CIFS_SERVER\sue         SeTcbPrivilege
                                  SeTakeOwnershipPrivilege
```

Configurer la vérification de la traverse de dérivation

Configurer la vue d'ensemble de vérification de la traverse de dérivation

La vérification du contournement de la traverse est un droit utilisateur (également appelé *Privilege*) qui détermine si un utilisateur peut traverser tous les répertoires du chemin d'accès à un fichier, même si l'utilisateur ne dispose pas des autorisations sur le répertoire de parcours. Vous devez comprendre ce qui se passe lors de l'autorisation ou de la désautorisation de la vérification transversale et comment configurer la vérification de dérivation pour les utilisateurs sur les machines virtuelles de stockage (SVM).

Que se passe-t-il lors de l'autorisation ou de la désautorisation du contrôle de la traverse de dérivation

- Si l'accès est autorisé, lorsqu'un utilisateur tente d'accéder à un fichier, ONTAP ne vérifie pas l'autorisation traverse pour les répertoires intermédiaires lorsqu'il détermine s'il faut accorder ou refuser l'accès au fichier.
- S'il n'est pas autorisé, ONTAP vérifie l'autorisation traverse (exécution) pour tous les répertoires du chemin d'accès au fichier.

  Si l'un des répertoires intermédiaires ne dispose pas de l'autorisation « X » (traverse), ONTAP refuse l'accès au fichier.

Configurer la vérification de la traverse de dérivation

Vous pouvez configurer la vérification de contournement via l'interface de ligne de commande ONTAP ou en configurant des règles de groupe Active Directory avec ce droit d'utilisateur.

Le `SeChangeNotifyPrivilege` privilège contrôle si les utilisateurs sont autorisés à contourner la vérification transversale.

- L'ajout aux utilisateurs ou groupes SMB locaux sur le SVM, ou aux utilisateurs ou groupes de domaine permet de contourner la vérification transversale.
- L'élimination de ce groupe ou des utilisateurs SMB locaux sur le SVM, ou des utilisateurs ou groupes de domaine permet de contourner la vérification des traversent.

Par défaut, les groupes BUILTIN suivants sur le SVM ont le droit de contourner le contrôle de la traverse :

- `BUILTIN\Administrators`
- `BUILTIN\Power Users`

- `BUILTIN\Backup Operators`
- `BUILTIN\Users`
- `Everyone`

Si vous ne souhaitez pas autoriser les membres de l'un de ces groupes à contourner la vérification de la traverse, vous devez supprimer ce privilège du groupe.

Lors de la configuration de la vérification de dérivation des utilisateurs et groupes SMB locaux sur le SVM, il faut garder ce qui suit à l'aide de l'interface de ligne de commande :

- Si vous souhaitez autoriser les membres d'un groupe local ou de domaine personnalisé à contourner la vérification transversale, vous devez ajouter le `SeChangeNotifyPrivilege` privilège de ce groupe.
- Si vous souhaitez autoriser un utilisateur local ou de domaine individuel à contourner la vérification de la traverse et que cet utilisateur n'est pas membre d'un groupe avec ce privilège, vous pouvez ajouter `SeChangeNotifyPrivilege` privilège de ce compte utilisateur.
- Vous pouvez désactiver la vérification de contournement pour les utilisateurs ou groupes locaux ou de domaine en supprimant le `SeChangeNotifyPrivilege` privilège à tout moment.

> Pour désactiver la vérification des trvers de contournement pour les utilisateurs ou groupes locaux ou de domaine spécifiés, vous devez également supprimer le `SeChangeNotifyPrivilege` privilège du `Everyone` groupe.

Informations associées

Permet aux utilisateurs ou aux groupes de contourner la vérification de la traverse du répertoire

Interdire aux utilisateurs ou aux groupes de contourner la vérification de la traverse de répertoire

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

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

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

Liste des privilèges pris en charge

Ajoutez des privilèges aux utilisateurs ou groupes locaux ou de domaine

Permet aux utilisateurs ou aux groupes de contourner la vérification de la traverse du répertoire

Si vous souhaitez qu'un utilisateur puisse parcourir tous les répertoires du chemin d'accès à un fichier, même si l'utilisateur ne dispose pas des autorisations sur un répertoire de parcours, vous pouvez ajouter le `SeChangeNotifyPrivilege` Privilège pour les utilisateurs ou groupes SMB locaux sur des SVM (Storage Virtual machine). Par défaut, les utilisateurs peuvent contourner la vérification par passage de répertoire.

Avant de commencer

- Un serveur SMB doit être existant sur le SVM.
- L'option serveur SMB des utilisateurs et groupes locaux doit être activée.

- Utilisateur ou groupe local ou de domaine auquel `SeChangeNotifyPrivilege` le privilège sera ajouté doit déjà exister.

Description de la tâche

Lors de l'ajout de privilèges à un utilisateur ou à un groupe de domaine, ONTAP peut valider l'utilisateur ou le groupe du domaine en contactant le contrôleur de domaine. La commande peut échouer si ONTAP ne parvient pas à contacter le contrôleur de domaine.

Étapes

1. Activer la vérification de la traverse de dérivation en ajoutant le `SeChangeNotifyPrivilege` privilège d'un utilisateur ou groupe local ou de domaine : `vserver cifs users-and-groups privilege add-privilege -vserver` *`vserver_name`* `-user-or-group-name` *`name`* `-privileges SeChangeNotifyPrivilege`

   La valeur pour le `-user-or-group-name` il s'agit d'un utilisateur ou d'un groupe local, ou d'un utilisateur ou d'un groupe de domaines.

2. Vérifiez que la vérification de la dérivation transversale est activée pour l'utilisateur ou le groupe spécifié : `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Exemple

La commande suivante permet aux utilisateurs qui appartiennent au groupe « EXEMPLE\eng » de contourner la vérification de la traverse de répertoire en ajoutant le `SeChangeNotifyPrivilege` privilège du groupe :

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\eng -privileges SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ---------------
vs1       EXAMPLE\eng           SeChangeNotifyPrivilege
```

Informations associées

Interdire aux utilisateurs ou aux groupes de contourner la vérification de la traverse de répertoire

Interdire aux utilisateurs ou aux groupes de contourner la vérification de la traverse de répertoire

Si vous ne souhaitez pas qu'un utilisateur traverse tous les répertoires du chemin d'accès à un fichier car l'utilisateur ne dispose pas des autorisations sur le répertoire de parcours, vous pouvez supprimer le `SeChangeNotifyPrivilege` Privilège des utilisateurs ou groupes SMB locaux sur des SVM (Storage Virtual machine).

Avant de commencer

L'utilisateur ou le groupe local ou de domaine dont les privilèges seront supprimés doit déjà exister.

Description de la tâche

Lors de la suppression de privilèges d'un utilisateur ou d'un groupe de domaines, ONTAP peut valider l'utilisateur ou le groupe de domaines en contactant le contrôleur de domaine. La commande peut échouer si

ONTAP ne parvient pas à contacter le contrôleur de domaine.

Étapes

1. Interdire la vérification de la traverse de dérivation : `vserver cifs users-and-groups privilege remove-privilege -vserver vserver_name -user-or-group-name name -privileges SeChangeNotifyPrivilege`

   La commande supprime le `SeChangeNotifyPrivilege` privilège de l'utilisateur ou groupe local ou de domaine que vous spécifiez avec la valeur pour le `-user-or-group-name name` paramètre.

2. Vérifiez que le contrôle de la traverse de dérivation de l'utilisateur ou du groupe spécifié est désactivé : `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

Exemple

La commande suivante empêche les utilisateurs appartenant au groupe « EXEMPLE\eng » de contourner la vérification de la traverse de répertoire :

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- -----------------------
vs1       EXAMPLE\eng           SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name EXAMPLE\eng -privileges
SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- -----------------------
vs1       EXAMPLE\eng           -
```

Informations associées

Possibilité pour les utilisateurs ou les groupes de contourner la vérification de la traverse du répertoire

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

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

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

Affichage des informations relatives à la sécurité des fichiers

Vous pouvez afficher les informations relatives à la sécurité des fichiers appliquées aux données contenues

dans des volumes et des qtrees (pour les volumes FlexVol) avec les styles de sécurité suivants :

- NTFS
- UNIX
- Mixte

Affichage des informations relatives aux stratégies d'audit

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

- SMB (toutes les versions)
- NFSv4.x

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

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

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

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

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

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

Informations associées

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

Affichage d'informations sur Storage-Level Access Guard

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

Vous pouvez afficher des informations sur la sécurité des fichiers et des répertoires sur les volumes de style de sécurité NTFS, notamment le style de sécurité et les styles de sécurité efficaces, les autorisations appliquées et les informations sur les attributs DOS. Les résultats vous permettent de valider votre configuration de sécurité ou de résoudre les problèmes d'accès aux fichiers.

Description de la tâche

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

- Étant donné que les volumes et les qtrees de style de sécurité NTFS utilisent uniquement les autorisations de fichier NTFS et les utilisateurs et groupes Windows lors de la détermination des droits d'accès aux

fichiers, les champs de sortie liés à UNIX contiennent des informations d'autorisation de fichier UNIX en affichage uniquement.

- Les valeurs de sortie ACL sont affichées pour les fichiers et les dossiers avec la sécurité NTFS.
- Étant donné que la sécurité Storage-Level Access Guard peut être configurée sur le volume racine ou qtree, le résultat d'un chemin de volume ou qtree dans lequel Storage-Level Access Guard est configuré peut afficher à la fois les listes de contrôle d'accès standard des fichiers et les listes de contrôle d'accès Storage-Level Access Guard.
- La sortie affiche également des informations sur les ACE de contrôle d'accès dynamique si le contrôle d'accès dynamique est configuré pour le chemin de fichier ou de répertoire donné.

Étape

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

Pour afficher les informations…	Saisissez la commande suivante…
Sous forme récapitulative	`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 affiche les informations de sécurité relatives au chemin d'accès `/vol4` Au SVM vs1 :

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

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

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

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

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

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

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

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

```
                              .... .... .... .... .... ...1 .... .... =
Write Attributes
                              .... .... .... .... .... .... 1... .... =
Read Attributes
                              .... .... .... .... .... .... .1.. .... =
Delete Child
                              .... .... .... .... .... .... ..1. .... =
Execute
                              .... .... .... .... .... .... ...1 .... =
Write EA
                              .... .... .... .... .... .... .... 1... =
Read EA
                              .... .... .... .... .... .... .... .1.. =
Append
                              .... .... .... .... .... .... .... ..1. =
Write
                              .... .... .... .... .... .... .... ...1 =
Read

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

```
                                .... .... .... .... .... .... ..0. .... =
Execute
                                .... .... .... .... .... .... ...0 .... =
Write EA
                                .... .... .... .... .... .... .... 0... =
Read EA
                                .... .... .... .... .... .... .... .0.. =
Append
                                .... .... .... .... .... .... .... ..0. =
Write
                                .... .... .... .... .... .... .... ...0 =
Read
```

L’exemple suivant affiche des informations de sécurité, y compris des informations de sécurité Storage-Level Access Guard, pour le volume avec le chemin d’accès `/datavol1` Au SVM vs1 :

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

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


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

Informations associées

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

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

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

Vous pouvez afficher des informations sur la sécurité des fichiers et des répertoires sur des volumes de style de sécurité mixtes, y compris le style de sécurité et les styles de sécurité efficaces, les autorisations appliquées et les informations sur les propriétaires et groupes UNIX. Les résultats vous permettent de valider votre configuration de sécurité ou de résoudre les problèmes d'accès aux fichiers.

Description de la tâche

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

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

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

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

Étape

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

Pour afficher les informations…	Saisissez la commande suivante…
Sous forme récapitulative	`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 affiche les informations de sécurité relatives au chemin d'accès `/projects` Dans le SVM vs1 sous forme de masque étendu. Ce chemin de sécurité mixte possède une sécurité efficace UNIX.

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

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

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

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

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

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

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

Informations associées

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

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

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

Vous pouvez afficher des informations sur la sécurité des fichiers et des répertoires sur les volumes de style de sécurité UNIX, notamment les styles de sécurité et les styles de sécurité efficaces, les autorisations appliquées et les informations sur les propriétaires et

groupes UNIX. Les résultats vous permettent de valider votre configuration de sécurité ou de résoudre les problèmes d'accès aux fichiers.

Description de la tâche

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

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

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

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

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

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

Étape

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

Pour afficher les informations…	Saisissez la commande suivante…
Sous forme récapitulative	`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 affiche les informations de sécurité relatives au chemin d'accès `/home` Au SVM vs1 :

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

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

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

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

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

Informations associées

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

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

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

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

Description de la tâche

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

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

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

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

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

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

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

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

Étape

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

Pour afficher les informations…	Saisissez la commande suivante…
Sous forme récapitulative	`vserver security file-directory show -vserver vserver_name -path path`
En tant que liste détaillée	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Exemples

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

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

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

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

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

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

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

Vous pouvez afficher des informations sur les stratégies d'audit NFSv4 sur les volumes

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

Description de la tâche

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

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

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

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

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

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

Étapes

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

Pour afficher les informations…	Saisissez la commande suivante…
Sous forme récapitulative	`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 affiche les informations de sécurité relatives au chemin d'accès `/lab` Au SVM vs1. Ce chemin de style de sécurité UNIX dispose d'un SACL NFSv4.

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

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

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

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

Le caractère générique (**) peut être utilisé comme dernier sous-composant d'un chemin d'accès de répertoire donné, sous lequel vous souhaitez afficher les informations de tous les fichiers et répertoires. Si vous souhaitez afficher les informations d'un fichier ou d'un répertoire donné nommé "*"**, vous devez alors indiquer le chemin complet à l'intérieur de guillemets doubles ("``""""""").

Exemple

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

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

                   Vserver: vs1
                 File Path: /1/1
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8514
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
                   Vserver: vs1
                 File Path: /1/1/abc
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8404
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

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

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

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

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

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

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

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

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

Storage-Level Access Guard peut être configuré et géré uniquement à partir de l'interface de ligne de commande ONTAP. Vous ne pouvez pas gérer les paramètres Storage-Level Access Guard à partir des clients SMB. De plus, si vous affichez les paramètres de sécurité d'un fichier ou d'un répertoire à partir d'un client NFS ou SMB, vous ne verrez pas la sécurité Storage-Level Access Guard. La sécurité Access Guard au niveau du stockage ne peut pas être révoquée d'un client, même par un administrateur système (Windows ou

UNIX). Par conséquent, Storage-Level Access Guard offre une couche supplémentaire de sécurité pour l'accès aux données, qui est défini et géré de façon indépendante par l'administrateur du stockage.

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

Volumes de sécurité NTFS

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

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

Volumes de sécurité mixtes

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

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

Volumes de style de sécurité UNIX

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

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

Informations associées

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

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

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

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

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

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

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

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

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

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

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

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

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

- **Autorisations**

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

- **Descripteurs de sécurité**

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

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

  Les listes de contrôle d’accès sont les listes contenues dans un descripteur de sécurité qui contiennent

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

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

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

  Les DACL contiennent la liste des SID pour les utilisateurs, les groupes et les objets d'ordinateur qui sont autorisés ou refusés à effectuer des actions sur des fichiers ou des dossiers. Les listes DALC contiennent au moins zéro entrée de contrôle d'accès (ACE).

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

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

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

  Ces sont des entrées individuelles dans DACL ou SACL :

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

- **Héritage des autorisations**

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

Informations associées

"Audit et suivi de sécurité SMB et NFS"

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

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

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

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

cluster de destination.

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

- Identité préservée

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

- Identité rejetée

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

Instructions pour les configurations éliminées par identité

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

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

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

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

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

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

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

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

Vserver: vs1
  NTFS Security Descriptor Name: sd1

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

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

Vserver: vs1_dst
  NTFS Security Descriptor Name: sd1

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

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

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

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

- Descripteur de sécurité

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

- Entrées DACL

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

- Entrées SACL

  Chaque entrée SACL doit être associée à un compte. Vous devez modifier les CLS qui utilisent des comptes utilisateur ou groupe locaux pour utiliser le nom de SVM de destination. Comme vous ne pouvez

pas modifier le nom du compte pour les entrées SACL existantes, vous devez supprimer les entrées SACL avec des utilisateurs ou des groupes locaux des descripteurs de sécurité, créer de nouvelles entrées SACL avec les noms de compte de destination corrigés et associer ces nouvelles entrées SACL aux descripteurs de sécurité appropriés.

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

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

Créez un descripteur de sécurité NTFS

La création d'un Security Descriptor (politique de sécurité des fichiers) NTFS constitue la première étape de configuration et d'application des listes de contrôle d'accès (ACL) NTFS aux fichiers et dossiers résidant sur les SVM (Storage Virtual machines). Vous pouvez associer le descripteur de sécurité au chemin du fichier ou du dossier dans une tâche de stratégie.

Description de la tâche

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

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

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

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

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

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

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

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

Description de la tâche

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

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

Vous pouvez éventuellement personnaliser les entrées DACL en spécifiant les droits que vous souhaitez autoriser ou refuser pour le compte spécifié dans `-account` paramètre. Il existe trois méthodes mutuellement exclusives de définition des droits :

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

> Si vous ne spécifiez pas de droits pour l'entrée DACL, la valeur par défaut est de définir les droits sur `Full Control`.

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

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

Étapes

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

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

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

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

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

Créer des stratégies de sécurité

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

Description de la tâche

Les tâches que vous ajoutez à une stratégie de sécurité contiennent des associations entre le descripteur de sécurité NTFS et les chemins de fichier ou de dossier. Vous devez donc associer la politique de sécurité à chaque SVM (qui contient des volumes de style de sécurité NTFS ou des volumes de type sécurité mixtes).

Étapes

1. Création d'une stratégie de sécurité : `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

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

2. Vérifiez la stratégie de sécurité : `vserver security file-directory policy show`

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

Ajoutez une tâche à la stratégie de sécurité

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

Description de la tâche

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

Il existe deux types de tâches :

- Tâches de fichier et de répertoire

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

- Tâches de Storage-Level Access Guard

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

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

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

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

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

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

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

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

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

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

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

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

Étapes

1. Ajoutez une tâche avec un descripteur de sécurité associé à la stratégie de sécurité : `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

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

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name
   policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2
   -index-num 1 -access-control file-directory
   ```

2. Vérifiez la configuration de la tâche de stratégie : `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

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

   ```
   Vserver: vs1
   Policy: policy1

   Index    File/Folder    Access           Security   NTFS       NTFS
   Security
            Path           Control          Type       Mode
   Descriptor Name
   -----    --------       -----------      --------   ------
   ----------------
   1        /home/dir1     file-directory   ntfs       propagate  sd2
   ```

Appliquez des règles de sécurité

L'application d'une politique de sécurité des fichiers aux SVM est la dernière étape de la création et de l'application de ces ACL NTFS aux fichiers ou aux dossiers.

Description de la tâche

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

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

Étape

1. Appliquer une politique de sécurité : `vserver security file-directory apply -vserver`

```
vserver_name -policy-name policy_name
```

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

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

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

Surveillez la tâche de stratégie de sécurité

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

Description de la tâche

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

Étape

1. Surveillez la tâche de stratégie de sécurité : `vserver security file-directory job show -vserver vserver_name`

   ```
   vserver security file-directory job show -vserver vs1
   ```

   ```
   Job ID Name                 Vserver    Node           State
   ------ -------------------- ---------- -------------- ----------
   53322  Fsecurity Apply      vs1        node1          Success
          Description: File Directory Security Apply Job
   ```

Vérifiez la sécurité appliquée des fichiers

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

Description de la tâche

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

Étape

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

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

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

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

                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                             0... .... .... .... .... .... .... .... =
```

```
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...0 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...1 .... .... .... .... .... =
Synchronize
                              .... .... .... 1... .... .... .... .... =
Write Owner
                              .... .... .... .1.. .... .... .... .... =
Write DAC
                              .... .... .... ..1. .... .... .... .... =
Read Control
                              .... .... .... ...1 .... .... .... .... =
Delete
                              .... .... .... .... .... ...1 .... .... =
Write Attributes
                              .... .... .... .... .... .... 1... .... =
Read Attributes
                              .... .... .... .... .... .... .1.. .... =
Delete Child
                              .... .... .... .... .... .... ..1. .... =
Execute
                              .... .... .... .... .... .... ...1 .... =
Write EA
                              .... .... .... .... .... .... .... 1... =
Read EA
                              .... .... .... .... .... .... .... .1.. =
Append
                              .... .... .... .... .... .... .... ..1. =
Write
                              .... .... .... .... .... .... .... ...1 =
Read

                            ALLOW-Everyone-0x10000000-OI|CI|IO
                              0... .... .... .... .... .... .... .... =
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...1 .... .... .... .... .... .... .... =
```

```
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...0 .... .... .... .... .... =
Synchronize
                              .... .... .... 0... .... .... .... .... =
Write Owner
                              .... .... .... .0.. .... .... .... .... =
Write DAC
                              .... .... .... ..0. .... .... .... .... =
Read Control
                              .... .... .... ...0 .... .... .... .... =
Delete
                              .... .... .... .... .... ...0 .... .... =
Write Attributes
                              .... .... .... .... .... .... 0... .... =
Read Attributes
                              .... .... .... .... .... .... .0.. .... =
Delete Child
                              .... .... .... .... .... .... ..0. .... =
Execute
                              .... .... .... .... .... .... ...0 .... =
Write EA
                              .... .... .... .... .... .... .... 0... =
Read EA
                              .... .... .... .... .... .... .... .0.. =
Append
                              .... .... .... .... .... .... .... ..0. =
Write
                              .... .... .... .... .... .... .... ...0 =
Read
```

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

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

Description de la tâche

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

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

Informations associées

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

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

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

"Audit et suivi de sécurité SMB et NFS"

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

Créez un descripteur de sécurité NTFS

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

Description de la tâche

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

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

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

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

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

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

Étapes

1. Si vous souhaitez utiliser les paramètres avancés, définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Créez un Security Descriptor: `vserver security file-directory ntfs create -vserver vserver_name -ntfs-sd SD_nameoptional_parameters`

   `vserver security file-directory ntfs create -ntfs-sd sd1 -vserver vs1 -owner DOMAIN\joe`

3. Vérifiez que la configuration du descripteur de sécurité est correcte : `vserver security file-directory ntfs show -vserver vserver_name -ntfs-sd SD_name`

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

   ```
                                   Vserver: vs1
                         Security Descriptor Name: sd1
                   Owner of the Security Descriptor: DOMAIN\joe
   ```

4. Si vous êtes au niveau de privilège avancé, revenez au niveau de privilège admin : `set -privilege admin`

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

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

Description de la tâche

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

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

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

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

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

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

Étapes

1. Ajoutez une entrée SACL à un descripteur de sécurité : `vserver security file-directory ntfs sacl add -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SIDoptional_parameters`

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

2. Vérifiez que l'entrée SACL est correcte : `vserver security file-directory ntfs sacl show -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SID`

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

   ```
                                 Vserver: vs1
                   Security Descriptor Name: sd1
   Access type for Specified Access Rights: failure
                       Account Name or SID: DOMAIN\joe
                             Access Rights: full-control
                     Advanced Access Rights: -
                                  Apply To: this-folder
                             Access Rights: full-control
   ```

Créer des stratégies de sécurité

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

Description de la tâche

Les tâches que vous ajoutez à une stratégie de sécurité contiennent des associations entre le descripteur de sécurité NTFS et les chemins de fichier ou de dossier. Par conséquent, vous devez associer la stratégie de

sécurité à chaque SVM (Storage Virtual machine) (contenant des volumes de style de sécurité NTFS ou des volumes de type sécurité mixtes).

Étapes

1. Création d'une stratégie de sécurité : `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

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

2. Vérifiez la stratégie de sécurité : `vserver security file-directory policy show`

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

Ajoutez une tâche à la stratégie de sécurité

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

Description de la tâche

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

Il existe deux types de tâches :

- Tâches de fichier et de répertoire

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

- Tâches de Storage-Level Access Guard

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

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

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

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

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

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

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

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

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

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

Étapes

1. Ajoutez une tâche avec un descripteur de sécurité associé à la stratégie de sécurité : `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

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

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2 -index-num 1 -access-control file-directory
   ```

2. Vérifiez la configuration de la tâche de stratégie : `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

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

```
Vserver: vs1
Policy: policy1

Index    File/Folder    Access           Security   NTFS       NTFS
Security
         Path           Control          Type       Mode
Descriptor Name
-----    --------       -----------      --------   ------
----------------
1        /home/dir1     file-directory   ntfs       propagate  sd2
```

Appliquez des règles de sécurité

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

Description de la tâche

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

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

Étape

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

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

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

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

Surveillez la tâche de stratégie de sécurité

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

Description de la tâche

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

Étape

1. Surveillez la tâche de stratégie de sécurité : `vserver security file-directory job show -vserver vserver_name`

   `vserver security file-directory job show -vserver vs1`

   ```
   Job ID Name                 Vserver    Node           State
   ------ -------------------- ---------- -------------- ----------
   53322  Fsecurity Apply      vs1        node1          Success
          Description: File Directory Security Apply Job
   ```

Vérifiez la règle d'audit appliquée

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

Description de la tâche

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

Étape

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

Exemple

La commande suivante affiche les informations de la politique d'audit appliquées au chemin "/corp" du SVM vs1. Le chemin a à la fois UN SUCCÈS et une entrée SACL SUCCÈS/ÉCHEC qui lui est appliquée :

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

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

Considérations relatives à la gestion des tâches de stratégie de sécurité

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

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

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

Dans les circonstances suivantes, si une tâche existe pour une stratégie de sécurité, vous pouvez modifier

avec succès cette stratégie de sécurité ou une tâche affectée à cette stratégie :

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

Commandes de gestion des descripteurs de sécurité NTFS

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

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

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

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

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

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

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

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

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

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

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

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

Commandes permettant de gérer les stratégies de sécurité

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

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

Les fonctions que vous recherchez…	Utilisez cette commande…
Supprimer des stratégies de sécurité	`vserver security file-directory policy delete`

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

Commandes permettant de gérer les tâches de stratégie de sécurité

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

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

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

Commandes permettant de gérer les tâches de stratégie de sécurité

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

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

Les fonctions que vous recherchez…	Utilisez cette commande…
Arrêtez les tâches de stratégie de sécurité	`vserver security file-directory job stop -vserver vserver_name -id integer`

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

Configurez le cache des métadonnées pour les partages SMB

Fonctionnement de la mise en cache des métadonnées SMB

La mise en cache des métadonnées permet la mise en cache des attributs de fichier sur les clients SMB 1.0 pour un accès plus rapide aux attributs des fichiers et des dossiers. Vous pouvez activer ou désactiver la mise en cache des attributs par partage. Vous pouvez également configurer le temps de mise en service des entrées mises en cache si la mise en cache des métadonnées est activée. La configuration de la mise en cache des métadonnées n'est pas nécessaire si les clients se connectent aux partages SMB 2.x ou SMB 3.0.

Lorsqu'il est activé, le cache de métadonnées SMB stocke les données d'attribut de chemin et de fichier pendant un temps limité. Ceci peut améliorer les performances SMB des clients SMB 1.0 avec des charges de travail communes.

Pour certaines tâches, SMB crée un trafic important, pouvant inclure plusieurs requêtes identiques pour les métadonnées des chemins d'accès et des fichiers. Vous pouvez réduire le nombre de requêtes redondantes et améliorer les performances des clients SMB 1.0 en utilisant la mise en cache de métadonnées SMB pour récupérer les informations du cache.

> Même si cela est peu probable, il est possible que le cache de métadonnées transmette des informations obsolètes aux clients SMB 1.0. Si votre environnement ne peut pas se permettre ce risque, vous ne devez pas activer cette fonctionnalité.

Activez le cache de métadonnées SMB

Vous pouvez améliorer les performances SMB des clients SMB 1.0 en activant le cache de métadonnées SMB. Par défaut, la mise en cache des métadonnées SMB est désactivée.

Étape

1. Effectuez l'action souhaitée :

Les fonctions que vous recherchez…	Entrez la commande…
Activez la mise en cache des métadonnées SMB lorsque vous créez un partage	`vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-share-properties attributecache`

Les fonctions que vous recherchez…	Entrez la commande…
Activez la mise en cache des métadonnées SMB sur un partage existant	`vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties attributecache`

Informations associées

Configuration de la durée de vie des entrées du cache de métadonnées SMB

Ajout ou suppression de propriétés de partage sur un partage SMB existant

Configurez la durée de vie des entrées du cache de métadonnées SMB

Vous pouvez configurer la durée de vie des entrées du cache de métadonnées SMB afin d'optimiser les performances du cache de métadonnées SMB dans votre environnement. La valeur par défaut est 10 secondes.

Avant de commencer

Vous devez avoir activé la fonctionnalité de cache de métadonnées SMB. Si le cache des métadonnées SMB n'est pas activé, le paramètre TTL du cache SMB n'est pas utilisé.

Étape

1. Effectuez l'action souhaitée :

Si vous souhaitez configurer la durée de vie des entrées du cache de métadonnées SMB lorsque vous…	Entrez la commande…
Créer un partage	`vserver cifs share -create -vserver vserver_name -share-name share_name -path path -attribute-cache-ttl [integerh][integerm][integers]`
Modifier un partage existant	`vserver cifs share -modify -vserver vserver_name -share-name share_name -attribute-cache-ttl [integerh][integerm][integers]`

Vous pouvez spécifier d'autres options et propriétés de configuration de partage lorsque vous créez ou modifiez des partages. Consultez les pages de manuels pour plus d'informations.

Gérer les verrous de fichier

A propos du verrouillage de fichier entre les protocoles

Le verrouillage de fichier est une méthode utilisée par les applications client pour empêcher un utilisateur d'accéder à un fichier précédemment ouvert par un autre

utilisateur. Le mode de verrouillage des fichiers par ONTAP dépend du protocole du client.

Si le client est un client NFS, les verrouillages sont consultatifs ; si le client est un client SMB, les verrous sont obligatoires.

En raison des différences entre les verrouillages de fichiers NFS et SMB, un client NFS peut ne pas accéder à un fichier précédemment ouvert par une application SMB.

Ce qui suit se produit lorsqu'un client NFS tente d'accéder à un fichier verrouillé par une application SMB :

- Dans les volumes mixtes ou NTFS, les opérations de manipulation de fichiers telles que `rm`, `rmdir`, et `mv` Peut entraîner l'échec de l'application NFS.
- Les opérations de lecture et d'écriture NFS sont refusées par les modes SMB Deny-read et deny-write open, respectivement.
- Les opérations d'écriture NFS échouent lorsque la plage d'écriture du fichier est verrouillée par un bytelock SMB exclusif.
- Dissocier
  - Pour les systèmes de fichiers NTFS, les opérations de suppression SMB et CIFS sont prises en charge.

    Le fichier sera supprimé après la dernière fermeture.
  - Les opérations de liaison NFS ne sont pas prises en charge.

    Elle n'est pas prise en charge car les sémantiques NTFS et SMB sont requises et l'opération dernière suppression-fermeture n'est pas prise en charge pour NFS.
  - Pour les systèmes de fichiers UNIX, l'opération de liaison est prise en charge.

    Il est pris en charge car la sémantique NFS et UNIX est requise.
- Renommer
  - Pour les systèmes de fichiers NTFS, si le fichier de destination est ouvert depuis SMB ou CIFS, le fichier de destination peut être renommé.
  - Le renommage NFS n'est pas pris en charge.

    Elle n'est pas prise en charge car NTFS et la sémantique SMB sont requises.

Dans les volumes de style de sécurité UNIX, les opérations de dissociation NFS et de renommage ignorent l'état du verrouillage SMB et permettent l'accès au fichier. Toutes les autres opérations NFS sur des volumes de type sécurité UNIX respectent l'état de verrouillage SMB.

Comment ONTAP traite les bits en lecture seule

Le bit de lecture seule est défini fichier par fichier pour indiquer si un fichier est inscriptible (désactivé) ou en lecture seule (activé).

Les clients SMB qui utilisent Windows peuvent définir un bit en lecture seule par fichier. Les clients NFS ne définissent pas de bit en lecture seule par fichier, car les clients NFS ne disposent d'aucune opération de protocole utilisant un bit en lecture seule par fichier.

ONTAP peut définir un bit en lecture seule sur un fichier lorsqu'un client SMB utilisant Windows crée ce fichier. ONTAP peut également définir un bit en lecture seule lorsqu'un fichier est partagé entre les clients NFS et les clients SMB. Certains logiciels, lorsqu'ils sont utilisés par des clients NFS et SMB, nécessitent l'activation du bit en lecture seule.

Pour que ONTAP garde les autorisations appropriées en lecture et écriture sur un fichier partagé entre les clients NFS et les clients SMB, il traite le bit en lecture seule conformément aux règles suivantes :

- NFS traite tous les fichiers dont le bit de lecture seule est activé comme s'il n'a pas de bits d'autorisation d'écriture activés.
- Si un client NFS désactive tous les bits d'autorisation d'écriture et qu'au moins un de ces bits avait été précédemment activé, ONTAP active le bit en lecture seule pour ce fichier.
- Si un client NFS active un bit d'autorisation d'écriture, ONTAP désactive le bit en lecture seule pour ce fichier.
- Si le bit de lecture seule d'un fichier est activé et qu'un client NFS tente de détecter les autorisations pour le fichier, les bits d'autorisation du fichier ne sont pas envoyés au client NFS. ONTAP envoie les bits d'autorisation au client NFS avec les bits d'autorisation d'écriture masqués.
- Si le bit de lecture seule d'un fichier est activé et qu'un client SMB désactive le bit de lecture seule, ONTAP active le bit d'autorisation d'écriture du propriétaire pour le fichier.
- Les fichiers dont le bit de lecture seule est activé sont accessibles en écriture uniquement par root.

> Les modifications des autorisations liées aux fichiers sont immédiatement appliquées aux clients SMB, mais elles peuvent ne pas être immédiatement appliquées aux clients NFS si le client NFS active la mise en cache des attributs.

La différence entre ONTAP et Windows en ce qui concerne la gestion des verrous sur les composants de chemin de partage

Contrairement à Windows, ONTAP ne verrouille pas chaque composant du chemin d'accès à un fichier ouvert lorsque le fichier est ouvert. Ce comportement affecte également les chemins de partage SMB.

Étant donné que ONTAP ne verrouille pas chaque composant du chemin d'accès, il est possible de renommer un composant de chemin au-dessus du fichier ou du partage ouvert, ce qui peut causer des problèmes pour certaines applications ou peut rendre le chemin de partage dans la configuration SMB invalide. Cela peut rendre le partage inaccessible.

Pour éviter les problèmes causés par la modification du nom des composants du chemin d'accès, vous pouvez appliquer des paramètres de sécurité qui empêchent les utilisateurs ou les applications de renommer les répertoires critiques.

Affiche des informations sur les verrous

Vous pouvez afficher des informations sur les verrous de fichier en cours, y compris les types de verrous qui sont conservés et l'état de verrouillage, les détails sur les verrous de plage d'octets, les modes de verrouillage de sharelock, les verrous de délégation et les verrous opportunistes, et si les verrous sont ouverts avec des poignées durables ou persistantes.

Description de la tâche

L'adresse IP du client ne peut pas être affichée pour les verrouillages établis via NFS V4 ou NFS v4.1.

Par défaut, la commande affiche des informations relatives à tous les verrouillages. Vous pouvez utiliser les paramètres de la commande pour afficher des informations sur les verrous d'une machine virtuelle de stockage (SVM) spécifique ou pour filtrer les résultats de la commande par d'autres critères.

Le `vserver locks show` la commande affiche des informations sur quatre types de verrous :

- Les verrous de plage d'octets, qui verrouillent uniquement une partie d'un fichier.
- Verrous de partage, qui verrouillent les fichiers ouverts.
- Verrouillages opportunistes, qui contrôlent la mise en cache côté client sur SMB.
- Des délégations qui contrôlent la mise en cache côté client sur NFSv4.x.

En spécifiant des paramètres facultatifs, vous pouvez déterminer des informations importantes sur chaque type de verrou. Consultez la page man pour la commande pour plus d'informations.

Étape

1. Affiche des informations sur les verrous à l'aide de `vserver locks show` commande.

Exemples

L'exemple suivant présente un récapitulatif des informations relatives à un verrouillage NFSv4 sur un fichier avec le chemin d'accès `/vol1/file1`. Le mode d'accès de sharelock est Write-deny_none et le verrou a été accordé avec la délégation d'écriture :

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path               LIF         Protocol  Lock Type   Client
------- ------------------------- ----------- --------- -----------
-------
vol1    /vol1/file1               lif1        nfsv4     share-level -
               Sharelock Mode: write-deny_none
                                                         delegation  -
               Delegation Type: write
```

L'exemple suivant affiche des informations détaillées sur le verrou SMB d'un fichier avec le chemin d'accès `/data2/data2_2/intro.pptx`. Un descripteur durable est accordé sur le fichier avec un mode d'accès à verrouillage de partage Write-Deny_none à un client dont l'adresse IP est 10.3.1.3. Un oplock de location est accordé avec un niveau de oplock de lot :

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

                   Vserver: vs1
                    Volume: data2_2
         Logical Interface: lif2
               Object Path: /data2/data2_2/intro.pptx
                 Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
```

```
             Lock Protocol: cifs
                 Lock Type: share-level
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: durable
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                   Vserver: vs1
                    Volume: data2_2
         Logical Interface: lif2
               Object Path: /data2/data2_2/test.pptx
                 Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
             Lock Protocol: cifs
                 Lock Type: op-lock
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

Verrous de rupture

Lorsque des verrous de fichier empêchent l'accès client aux fichiers, vous pouvez afficher des informations sur les verrous actuellement mis en attente, puis interrompre des verrous spécifiques. Les applications de débogage sont des exemples de scénarios dans lesquels vous devrez peut-être interrompre les verrous.

Description de la tâche

Le `vserver locks break` la commande n'est disponible que au niveau de privilège avancé et supérieur. La page man de la commande contient des informations détaillées.

Étapes

1. Pour trouver les informations dont vous avez besoin pour interrompre un verrouillage, utilisez le `vserver locks show` commande.

   La page man de la commande contient des informations détaillées.

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

Si vous voulez rompre un verrou en spécifiant…	Entrez la commande…
Le nom du SVM, le nom du volume, le nom de la LIF et le chemin de fichier	`vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif`
L'ID de verrouillage	`vserver locks break -lockid UUID`

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

Surveiller l'activité des PME

Affiche les informations relatives aux sessions SMB

Vous pouvez afficher des informations sur les sessions SMB établies, notamment la connexion SMB et l'ID de session ainsi que l'adresse IP du poste de travail à l'aide de la session. Vous pouvez afficher des informations sur la version du protocole SMB de la session et le niveau de protection disponible en continu, ce qui vous aide à déterminer si cette session prend en charge la continuité de l'activité.

Description de la tâche

Vous pouvez afficher les informations de toutes les sessions de votre SVM sous forme récapitulative. Cependant, dans de nombreux cas, la quantité de sortie renvoyée est importante. Vous pouvez personnaliser les informations affichées dans la sortie en spécifiant des paramètres facultatifs :

- Vous pouvez utiliser l'option `-fields` paramètre pour afficher la sortie des champs que vous choisissez.

  Vous pouvez entrer `-fields ?` pour déterminer les champs que vous pouvez utiliser.

- Vous pouvez utiliser le `-instance` Paramètre pour afficher des informations détaillées sur les sessions SMB établies.
- Vous pouvez utiliser le `-fields` ou le `-instance` paramètre seul ou associé à d'autres paramètres facultatifs.

Étape

1. Effectuez l'une des opérations suivantes :

Pour afficher les informations de session SMB…	Saisissez la commande suivante…
Pour toutes les sessions sur le SVM sous forme résumée	`vserver cifs session show -vserver vserver_name`
Sur un ID de connexion spécifié	`vserver cifs session show -vserver vserver_name -connection-id integer`
À partir d'une adresse IP de poste de travail spécifiée	`vserver cifs session show -vserver vserver_name -address workstation_IP_address`
Sur une adresse IP LIF spécifiée	`vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address`
Sur un nœud spécifié	`vserver cifs session show -vserver vserver_name -node {node_name
local}`	D'un utilisateur Windows spécifié
`vserver cifs session show -vserver vserver_name -windows-user domain_name\\user_name`	Avec un mécanisme d'authentification spécifié
`vserver cifs session show -vserver vserver_name -auth-mechanism {NTLMv1	NTLMv2
Kerberos	Anonymous}`
Avec une version de protocole spécifiée	`vserver cifs session show -vserver vserver_name -protocol-version {SMB1
SMB2	SMB2_1

Pour afficher les informations de session SMB…	Saisissez la commande suivante…
SMB3	SMB3_1}`  [NOTE] ==== La protection et SMB Multichannel sont disponibles en continu uniquement pour les sessions SMB 3.0 et ultérieures. Pour afficher leur statut sur toutes les sessions de qualification, vous devez spécifier ce paramètre avec la valeur définie sur `SMB3` ou ultérieure. ====
Avec un niveau spécifié de protection disponible en continu	`vserver cifs session show -vserver vserver_name -continuously-available {No
Yes	Partial}`  [NOTE] ==== Si l'état disponible en continu est de `Partial`, cela signifie que la session contient au moins un fichier ouvert en continu disponible, mais que la session contient certains fichiers qui ne sont pas ouverts avec une protection disponible en continu. Vous pouvez utiliser le `vserver cifs sessions file show` commande permettant de déterminer quels fichiers de la session établie ne sont pas ouverts avec une protection disponible en continu. ====
Avec un état de session de signature SMB spécifié	`vserver cifs session show -vserver vserver_name -is-session-signed {true

Exemples

La commande suivante affiche les informations relatives aux sessions sur le SVM vs1 établies à partir d'un poste de travail avec l'adresse IP 10.1.1.1 :

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session                                    Open         Idle
ID          ID      Workstation      Windows User    Files         Time
----------  ------- ---------------- ------------- ------- ------------
3151272279,
3151272280,
3151272281  1       10.1.1.1         DOMAIN\joe          2          23s
```

La commande suivante affiche des informations détaillées pour les sessions avec protection disponible en continu sur le SVM vs1. La connexion a été établie à l'aide du compte de domaine.

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
      Workstation IP address: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\SERVER1$
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
            Protocol Version: SMB3
      Continuously Available: Yes
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

La commande suivante affiche les informations relatives aux sessions sur une session utilisant SMB 3.0 et SMB Multichannel sur le SVM vs1. Dans l'exemple, l'utilisateur connecté à ce partage à un client SMB 3.0 en utilisant l'adresse IP du LIF ; par conséquent, le mécanisme d'authentification par défaut est NTLMv2. La connexion doit se faire à l'aide de l'authentification Kerberos pour se connecter à une protection disponible en continu.

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
              **Connection IDs: 3151272607,31512726078,3151272609
            Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
      Workstation IP address: 10.1.1.3
    Authentication Mechanism: NTLMv2
                Windows User: DOMAIN\administrator
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 0
                  Open Other: 0
              Connected Time: 6m 22s
                   Idle Time: 5m 42s
            Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

Informations associées

Affichage des informations relatives aux fichiers SMB ouverts

Affiche des informations sur les fichiers SMB ouverts

Vous pouvez afficher des informations sur les fichiers SMB ouverts, notamment la connexion SMB et l'ID de session, le volume hôte, le nom du partage et le chemin du partage. Vous pouvez afficher des informations sur le niveau de protection disponible en continu d'un fichier, ce qui permet de déterminer si un fichier ouvert est dans un état qui prend en charge la continuité de l'activité.

Description de la tâche

Vous pouvez afficher des informations sur les fichiers ouverts dans une session SMB établie. Les informations affichées sont utiles lorsque vous devez déterminer les informations de session SMB pour des fichiers particuliers dans une session SMB.

Par exemple, si vous disposez d'une session SMB où certains fichiers ouverts sont ouverts avec une protection disponible en continu et certains ne sont pas ouverts avec une protection disponible en continu (valeur pour le `-continuously-available` champ dans `vserver cifs session show` la sortie de la commande est `Partial`), vous pouvez déterminer quels fichiers ne sont pas disponibles en continu à l'aide de cette commande.

Vous pouvez afficher les informations de tous les fichiers ouverts sur des sessions SMB établies sur des SVM

(Storage Virtual machines) sous forme de récapitulatif à l'aide de `vserver cifs session file show` commande sans paramètres facultatifs.

Cependant, dans de nombreux cas, la quantité de production renvoyée est importante. Vous pouvez personnaliser les informations affichées dans la sortie en spécifiant des paramètres facultatifs. Cela peut être utile lorsque vous souhaitez afficher des informations pour un petit sous-ensemble de fichiers ouverts uniquement.

- Vous pouvez utiliser l'option `-fields` paramètre pour afficher la sortie sur les champs de votre choix.

  Vous pouvez utiliser ce paramètre seul ou en combinaison avec d'autres paramètres facultatifs.

- Vous pouvez utiliser le `-instance` Paramètre pour afficher des informations détaillées sur les fichiers SMB ouverts.

  Vous pouvez utiliser ce paramètre seul ou en combinaison avec d'autres paramètres facultatifs.

Étape

1. Effectuez l'une des opérations suivantes :

Si vous souhaitez afficher des fichiers SMB ouverts…	Saisissez la commande suivante…
Sur le SVM sous forme résumée	`vserver cifs session file show -vserver vserver_name`
Sur un nœud spécifié	`vserver cifs session file show -vserver vserver_name -node {node_name
local}`	Sur un ID de fichier spécifié
`vserver cifs session file show -vserver vserver_name -file-id integer`	Sur un ID de connexion SMB spécifié
`vserver cifs session file show -vserver vserver_name -connection-id integer`	Sur un ID de session SMB spécifié
`vserver cifs session file show -vserver vserver_name -session-id integer`	Sur l'agrégat d'hébergement spécifié
`vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name`	Sur le volume spécifié
`vserver cifs session file show -vserver vserver_name -hosting-volume volume_name`	Sur le partage SMB spécifié

Si vous souhaitez afficher des fichiers SMB ouverts…	Saisissez la commande suivante…
`vserver cifs session file show -vserver vserver_name -share share_name`	Sur le chemin SMB spécifié
`vserver cifs session file show -vserver vserver_name -path path`	Avec le niveau spécifié de protection disponible en continu
`vserver cifs session file show -vserver vserver_name -continuously-available {No	Yes}`  [NOTE] ==== Si l'état disponible en continu est de `No`, cela signifie que ces fichiers ouverts ne peuvent pas être rétablis sans interruption à partir du basculement et du rétablissement. Ils ne peuvent pas non plus récupérer d'une relocalisation générale entre les partenaires dans une relation de haute disponibilité. ====
Avec l'état reconnecté spécifié	`vserver cifs session file show -vserver vserver_name -reconnected {No

D'autres paramètres facultatifs peuvent être utilisés pour affiner les résultats de sortie. Consultez la page man pour plus d'informations

Exemples

L'exemple suivant affiche les informations sur les fichiers ouverts sur le SVM vs1 :

```
cluster1::> vserver cifs session file show -vserver vs1
Node:       node1
Vserver:    vs1
Connection: 3151274158
Session:    1
File    File      Open Hosting               Continuously
ID      Type      Mode Volume    Share       Available
------- --------- ---- --------- ----------- ------------
41      Regular   r    data      data        Yes
Path: \mytest.rtf
```

L'exemple suivant affiche des informations détaillées sur les fichiers SMB ouverts avec l'ID de fichier 82 sur le SVM vs1 :

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance

                  Node: node1
               Vserver: vs1
               File ID: 82
         Connection ID: 104617
            Session ID: 1
             File Type: Regular
             Open Mode: rw
Aggregate Hosting File: aggr1
   Volume Hosting File: data1
            CIFS Share: data1
  Path from CIFS Share: windows\win8\test\test.txt
            Share Mode: rw
           Range Locks: 1
Continuously Available: Yes
           Reconnected: No
```

Informations associées

Affichage des informations sur les sessions SMB

Déterminez les objets statistiques et les compteurs disponibles

Avant d'obtenir des informations sur les statistiques de hachage CIFS, SMB, d'audit et de BranchCache, ainsi que sur les performances, vous devez connaître les objets et compteurs disponibles, à partir desquels vous pouvez obtenir des données.

Étapes

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

Si vous voulez déterminer…	Entrer…
Les objets disponibles	`statistics catalog object show`
Objets spécifiques disponibles	`statistics catalog object show object object_name`
Quels compteurs sont disponibles	`statistics catalog counter show object object_name`

   Pour plus d'informations sur les objets et les compteurs disponibles, consultez les pages de manuels.

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

Exemples

La commande suivante affiche la description des objets statistiques sélectionnés relatifs à l'accès CIFS et SMB au cluster, comme s'il s'affiche au niveau de privilège avancé :

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog object show -object audit
    audit_ng                    CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                        The CIFS object reports activity of the
                                Common Internet File System protocol
                                ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs                 The Common Internet File System (CIFS)
                                protocol is an implementation of the
Server
                                ...

cluster1::*> statistics catalog object show -object smb1
    smb1                        These counters report activity from the
SMB
                                revision of the protocol. For information
                                ...

cluster1::*> statistics catalog object show -object smb2
    smb2                        These counters report activity from the
                                SMB2/SMB3 revision of the protocol. For
                                ...

cluster1::*> statistics catalog object show -object hashd
    hashd                       The hashd object provides counters to
measure
                                the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

La commande suivante affiche des informations sur certains compteurs de `cifs` objet tel qu'il apparaît au niveau de privilège avancé :

Cet exemple n'affiche pas tous les compteurs disponibles pour le `cifs` objet ; la sortie est tronquée.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    ---------------------------
----------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    ...                         ...

cluster2::> statistics start -object client -sample-id
Object: client
    Counter                                                     Value
    -------------------------------- --------------------------------
    cifs_ops                                                        0
    cifs_read_ops                                                   0
    cifs_read_recv_ops                                              0
    cifs_read_recv_size                                            0B
    cifs_read_size                                                 0B
    cifs_write_ops                                                  0
    cifs_write_recv_ops                                             0
    cifs_write_recv_size                                           0B
    cifs_write_size                                                0B
    instance_name                              vserver_1:10.72.205.179
    instance_uuid                                      2:10.72.205.179
    local_ops                                                       0
    mount_ops                                                       0


[...]
```

Informations associées

Affichage des statistiques

Affiche les statistiques

Vous pouvez afficher plusieurs statistiques, notamment des statistiques sur CIFS et SMB, l'audit et des hachages de BranchCache, pour surveiller les performances et diagnostiquer les problèmes.

Avant de commencer

Vous devez avoir collecté des échantillons de données à l'aide du `statistics start` et `statistics stop` commandes avant de pouvoir afficher les informations relatives aux objets.

Étapes

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

Pour afficher les statistiques de…	Entrer…
Toutes les versions de SMB	`statistics show -object cifs`
SMB 1.0	`statistics show -object smb1`
SMB 2.x et SMB 3.0	`statistics show -object smb2`
Sous-système CIFS du nœud	`statistics show -object nblade_cifs`
Audit multiprotocole	`statistics show -object audit_ng`
Service de hachage BranchCache	`statistics show -object hashd`
DNS dynamique	`statistics show -object ddns_update`

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

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

Informations associées

Détermination des objets statistiques et des compteurs disponibles

Contrôle des statistiques de session signées SMB

Affichage des statistiques de BranchCache

Utilisation des statistiques pour surveiller l'activité de renvoi automatique de nœud

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

"Configuration du contrôle des performances"

Déploiement des services basés sur les clients SMB

Utilisez les fichiers hors ligne pour permettre la mise en cache des fichiers pour une utilisation hors ligne

Utilisez les fichiers hors ligne pour permettre la mise en cache des fichiers pour une utilisation hors ligne

ONTAP prend en charge la fonctionnalité de fichiers hors ligne Microsoft, ou *mise en cache côté client*, qui permet de mettre les fichiers en cache sur l'hôte local pour une utilisation hors ligne. Les utilisateurs peuvent utiliser la fonctionnalité fichiers hors ligne pour continuer à travailler sur des fichiers même lorsqu'ils sont déconnectés du réseau.

Vous pouvez spécifier si les documents et programmes utilisateur Windows sont automatiquement mis en cache sur un partage ou si les fichiers doivent être sélectionnés manuellement pour la mise en cache. La mise en cache manuelle est activée par défaut pour les nouveaux partages. Les fichiers mis hors ligne sont synchronisés avec le disque local du client Windows. La synchronisation a lieu lorsque la connectivité réseau à un partage de système de stockage spécifique est restaurée.

Étant donné que les fichiers et dossiers hors ligne conservent les mêmes autorisations d'accès que la version des fichiers et dossiers enregistrés sur le serveur CIFS, l'utilisateur doit disposer des autorisations suffisantes sur les fichiers et dossiers enregistrés sur le serveur CIFS pour effectuer des actions sur les fichiers et dossiers hors ligne.

Lorsque l'utilisateur et une autre personne du réseau modifient le même fichier, l'utilisateur peut enregistrer la version locale du fichier sur le réseau, conserver l'autre version ou enregistrer les deux. Si l'utilisateur conserve les deux versions, un nouveau fichier avec les modifications de l'utilisateur local est enregistré localement et le fichier mis en cache est écrasé par des modifications de la version du fichier enregistré sur le serveur CIFS.

Vous pouvez configurer des fichiers hors ligne par partage à l'aide des paramètres de configuration du partage. Vous pouvez choisir l'une des quatre configurations de dossiers hors ligne lorsque vous créez ou modifiez des partages :

- Pas de mise en cache

  Désactive la mise en cache côté client pour le partage. Les fichiers et les dossiers ne sont pas automatiquement mis en cache localement sur les clients et les utilisateurs ne peuvent pas choisir de mettre en cache des fichiers ou des dossiers localement.

- Mise en cache manuelle

  Permet la sélection manuelle des fichiers à mettre en cache sur le partage. Il s'agit du paramètre par défaut. Par défaut, aucun fichier ni dossier n'est mis en cache sur le client local. Les utilisateurs peuvent choisir les fichiers et dossiers qu'ils souhaitent mettre en cache localement pour une utilisation hors ligne.

- Mise en cache automatique des documents

  Permet de mettre automatiquement en cache les documents utilisateur sur le partage. Seuls les fichiers et les dossiers accessibles sont mis en cache localement.

- Mise en cache automatique des programmes

  Permet de mettre automatiquement en cache les programmes et les documents utilisateur sur le partage. Seuls les fichiers, les dossiers et les programmes accessibles sont mis en cache localement. De plus, ce paramètre permet au client d'exécuter des exécutables mis en cache localement, même lorsqu'il est connecté au réseau.

Pour plus d'informations sur la configuration des fichiers hors ligne sur les serveurs et les clients Windows, consultez la bibliothèque Microsoft TechNet.

Informations associées

Utilisation de profils itinérants pour stocker les profils utilisateurs de façon centralisée sur un serveur CIFS associé à la SVM

Utilisation de la redirection de dossiers pour stocker des données sur un serveur CIFS

Utilisation de BranchCache pour mettre en cache le contenu de partage SMB dans une succursale

"Bibliothèque Microsoft TechNet : technet.microsoft.com/en-us/library/"

Conditions d'utilisation des fichiers hors ligne

Avant de pouvoir utiliser la fonctionnalité Microsoft Offline Files avec votre serveur CIFS, vous devez savoir quelles versions de ONTAP et SMB et quels clients Windows prennent en charge cette fonctionnalité.

Configuration requise pour la version ONTAP

Les versions d'ONTAP prennent en charge les fichiers hors ligne.

Version requise du protocole SMB

Pour le SVM (Storage Virtual machine), ONTAP prend en charge les fichiers hors ligne dans toutes les versions de SMB.

Configuration requise pour le client Windows

Le client Windows doit prendre en charge les fichiers hors ligne.

Pour obtenir les informations les plus récentes sur les clients Windows prenant en charge la fonctionnalité fichiers hors ligne, reportez-vous à la matrice d'interopérabilité.

"mysupport.netapp.com/matrix"

Instructions pour le déploiement de fichiers hors ligne

Il existe certaines directives importantes que vous devez comprendre lorsque vous déployez des fichiers hors ligne sur des partages de répertoire personnel qui possèdent le `showsnapshot` propriété de partage définie sur les répertoires d'accueil.

Si le `showsnapshot` La propriété Share est définie sur un partage de répertoire personnel sur lequel les fichiers hors ligne sont configurés. Les clients Windows mettent en cache toutes les copies Snapshot sous `~snapshot` dans le répertoire de base de l'utilisateur.

Les clients Windows mettent en cache toutes les copies Snapshot sous le home Directory si l'un des nombreux éléments suivants est vrai :

- L'utilisateur rend le répertoire personnel disponible hors ligne à partir du client.

  Le contenu du `~snapshot` le dossier du répertoire personnel est inclus et rendu disponible hors ligne.

- L'utilisateur configure la redirection de dossier pour rediriger un dossier tel que `My Documents` À la racine d'un répertoire local résidant sur le partage CIFS Server.

  Certains clients Windows peuvent rendre automatiquement le dossier redirigé hors ligne. Si le dossier est redirigé vers la racine du répertoire de base, le `~snapshot` le dossier est inclus dans le contenu hors ligne mis en cache.

> Déploiement de fichiers hors ligne où `~snapshot` le dossier est inclus dans les fichiers hors ligne doit être évité. Copies Snapshot dans le `~snapshot` Le dossier contient toutes les données du volume au point où ONTAP a créé la copie Snapshot. Par conséquent, la création d'une copie hors ligne du `~snapshot` la consommation d'un stockage local important dans le dossier du client consomme de la bande passante réseau lors de la synchronisation des fichiers hors ligne, et augmente le temps nécessaire à la synchronisation des fichiers hors ligne.

Configurer la prise en charge des fichiers hors ligne sur les partages SMB à l'aide de l'interface de ligne de commande

Vous pouvez configurer la prise en charge des fichiers hors ligne à l'aide de l'interface de ligne de commandes ONTAP en spécifiant l'un des quatre paramètres de fichier hors ligne lorsque vous créez des partages SMB ou en modifiant à tout moment des partages SMB existants. La prise en charge des fichiers manuels hors ligne est le paramètre par défaut.

Description de la tâche

Lors de la configuration de la prise en charge des fichiers hors ligne, vous pouvez choisir l'un des quatre paramètres de fichiers hors ligne suivants :

Réglage	Description
`none`	Interdire aux clients Windows de mettre en cache les fichiers sur ce partage.
`manual`	Permet aux utilisateurs des clients Windows de sélectionner manuellement les fichiers à mettre en cache.
`documents`	Permet aux clients Windows de mettre en cache les documents utilisateur qui sont utilisés par l'utilisateur pour l'accès hors ligne.

Réglage	Description
`programs`	Permet aux clients Windows de mettre en cache les programmes utilisés par l'utilisateur pour l'accès hors ligne. Les clients peuvent utiliser les fichiers de programme mis en cache en mode hors ligne, même si le partage est disponible.

Vous ne pouvez choisir qu'un seul paramètre de fichier hors ligne. Si vous modifiez un paramètre de fichiers hors ligne sur un partage SMB existant, le nouveau paramètre de fichiers hors ligne remplace le paramètre d'origine. Les autres paramètres de configuration et propriétés de partage SMB existants ne sont ni supprimés ni remplacés. Ils restent en vigueur jusqu'à ce qu'ils soient explicitement supprimés ou modifiés.

Étapes

1. Effectuez l'action appropriée :

Si vous souhaitez configurer des fichiers hors ligne sur…	Entrez la commande…
Un nouveau partage SMB	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -offline-files {none
manual	documents
programs}`	Un partage SMB existant
`vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files {none	manual
documents	programs}`

2. Vérifiez que la configuration du partage SMB est correcte : `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

Exemple

La commande suivante crée un partage SMB nommé "data1" avec des fichiers hors ligne définis sur `documents`:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -comment "Offline files" -offline-files documents

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
         CIFS Server NetBIOS Name: VS1
                             Path: /data1
                 Share Properties: oplocks
                                   browsable
                                   changenotify
               Symlink Properties: enable
          File Mode Creation Mask: -
     Directory Mode Creation Mask: -
                    Share Comment: Offline files
                        Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                      Volume Name: -
                    Offline Files: documents
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

La commande suivante modifie un partage SMB existant nommé "data1" en changeant le paramètre fichiers hors ligne sur `manual` et ajout de valeurs pour le masque de création de mode fichier et répertoire :

```
cluster1::> vserver cifs share modify -vserver vs1 -share-name data1
-offline-files manual -file-umask 644 -dir-umask 777

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
         CIFS Server NetBIOS Name: VS1
                             Path: /data1
                 Share Properties: oplocks
                                   browsable
                                   changenotify
               Symlink Properties: enable
          File Mode Creation Mask: 644
     Directory Mode Creation Mask: 777
                    Share Comment: Offline files
                        Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                      Volume Name: -
                    Offline Files: manual
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

Informations associées

Ajout ou suppression de propriétés de partage sur un partage SMB existant

Configurez la prise en charge des fichiers hors ligne sur les partages SMB à l'aide de la console MMC gestion de l'ordinateur

Si vous souhaitez autoriser les utilisateurs à mettre en cache des fichiers localement pour une utilisation hors ligne, vous pouvez configurer la prise en charge des fichiers hors ligne à l'aide de la console MMC gestion de l'ordinateur (Microsoft Management Console).

Étapes

1. Pour ouvrir la console MMC sur votre serveur Windows, dans l'Explorateur Windows, cliquez avec le bouton droit de la souris sur l'icône de l'ordinateur local, puis sélectionnez **gérer**.
2. Dans le panneau de gauche, sélectionnez **Computer Management**.
3. Sélectionnez **action** > **connexion à un autre ordinateur**.

   La boîte de dialogue Sélectionner un ordinateur s'affiche.

4. Tapez le nom du serveur CIFS ou cliquez sur **Browse** pour localiser le serveur CIFS.

   Si le nom du serveur CIFS est identique au nom d'hôte SVM (Storage Virtual machine), tapez le nom du

SVM. Si le nom du serveur CIFS est différent du nom d'hôte du SVM, tapez le nom du serveur CIFS.

5. Cliquez sur **OK**.
6. Dans l'arborescence de la console, cliquez sur **Outils système** > **dossiers partagés**.
7. Cliquez sur **partages**.
8. Dans le volet des résultats, cliquez avec le bouton droit de la souris sur le partage.
9. Cliquez sur **Propriétés**.

   Les propriétés du partage sélectionné s'affichent.

10. Dans l'onglet **général**, cliquez sur **Paramètres hors ligne**.

    La boîte de dialogue Paramètres hors ligne s'affiche.

11. Configurez les options de disponibilité hors ligne selon les besoins.
12. Cliquez sur **OK**.

Utilisez les profils itinérants pour stocker les profils utilisateurs de façon centralisée sur un serveur SMB associé à la SVM

Utilisez les profils itinérants pour stocker les profils utilisateurs de façon centralisée sur un serveur SMB associé à la présentation de la SVM

ONTAP prend en charge le stockage des profils itinérants Windows sur un serveur CIFS associé à la machine virtuelle de stockage (SVM). La configuration des profils itinérants d'utilisateurs offre des avantages à l'utilisateur, tels que la disponibilité automatique des ressources, quel que soit l'endroit où l'utilisateur se connecte. Les profils itinérants simplifient également l'administration et la gestion des profils utilisateur.

Les profils utilisateur itinérants présentent les avantages suivants :

- Disponibilité automatique des ressources

  Le profil unique d'un utilisateur est automatiquement disponible lorsque cet utilisateur se connecte à n'importe quel ordinateur du réseau exécutant Windows 8, Windows 7, Windows 2000 ou Windows XP. Les utilisateurs n'ont pas besoin de créer de profil sur chaque ordinateur qu'ils utilisent sur un réseau.

- Remplacement simplifié de l'ordinateur

  Étant donné que toutes les informations de profil de l'utilisateur sont conservées séparément sur le réseau, le profil de l'utilisateur peut être facilement téléchargé sur un nouvel ordinateur de remplacement. Lorsque l'utilisateur se connecte au nouvel ordinateur pour la première fois, la copie du profil de l'utilisateur est copiée sur le nouvel ordinateur.

Informations associées

Utilisation de fichiers hors ligne pour permettre la mise en cache de fichiers pour une utilisation hors ligne

Utilisation de la redirection de dossiers pour stocker des données sur un serveur CIFS

Conditions requises pour l'utilisation des profils itinérants

Avant de pouvoir utiliser les profils itinérants de Microsoft avec votre serveur CIFS, vous devez savoir quelles versions de ONTAP et SMB et quels clients Windows prennent en charge cette fonctionnalité.

Configuration requise pour la version ONTAP

ONTAP prend en charge les profils itinérants.

Version requise du protocole SMB

Pour le serveur virtuel de stockage (SVM), ONTAP prend en charge les profils itinérants sur toutes les versions de SMB.

Configuration requise pour le client Windows

Avant qu'un utilisateur puisse utiliser les profils itinérants, le client Windows doit prendre en charge cette fonctionnalité.

Pour obtenir les dernières informations sur les clients Windows qui prennent en charge les profils itinérants, consultez la matrice d'interopérabilité.

"Matrice d'interopérabilité NetApp"

Configurez les profils itinérants

Si vous souhaitez rendre automatiquement le profil d'un utilisateur disponible lorsque cet utilisateur se connecte à n'importe quel ordinateur du réseau, vous pouvez configurer des profils itinérants via le composant logiciel enfichable MMC utilisateurs et ordinateurs Active Directory. Si vous configurez des profils itinérants sur Windows Server, vous pouvez utiliser le Centre d'administration Active Directory.

Étapes

1. Sur le serveur Windows, ouvrez la MMC utilisateurs et ordinateurs Active Directory (ou le Centre d'administration Active Directory sur les serveurs Windows).
2. Recherchez l'utilisateur pour lequel vous souhaitez configurer un profil d'itinérance.
3. Cliquez avec le bouton droit de la souris sur l'utilisateur et cliquez sur **Propriétés**.
4. Dans l'onglet **profil**, entrez le chemin du profil vers le partage où vous souhaitez stocker le profil d'itinérance de l'utilisateur, suivi de `%username%`.

   Par exemple, un chemin de profil peut être le suivant : `\\vs1.example.com\profiles\%username%`. La première fois qu'un utilisateur se connecte, `%username%` est remplacé par le nom de l'utilisateur.

   > Dans le chemin `\\vs1.example.com\profiles\%username%`, `profiles` Est le nom de partage d'un partage sur SVM (Storage Virtual machine) vs1 qui dispose de droits de contrôle total pour tous.

5. Cliquez sur **OK**.

Utiliser la redirection de dossiers pour stocker des données sur un serveur SMB

Utiliser la redirection de dossiers pour stocker des données sur une présentation du serveur SMB

ONTAP prend en charge la redirection de dossiers Microsoft, qui permet aux utilisateurs ou aux administrateurs de rediriger le chemin d'un dossier local vers un emplacement sur le serveur CIFS. Il apparaît comme si les dossiers redirigés sont stockés sur le client Windows local, même si ces données sont stockées dans un partage SMB.

La redirection de dossiers s'adresse principalement aux entreprises qui ont déjà déployé des répertoires locaux et qui souhaitent maintenir la compatibilité avec leur environnement de home Directory existant.

- `Documents`, `Desktop`, et `Start Menu` sont des exemples de dossiers que vous pouvez rediriger.
- Les utilisateurs peuvent rediriger les dossiers à partir de leur client Windows.
- Les administrateurs peuvent configurer et gérer de façon centralisée la redirection de dossiers en configurant des GPO dans Active Directory.
- Si les administrateurs ont configuré des profils itinérants, la redirection de dossiers permet aux administrateurs de diviser les données utilisateur à partir des données de profil.
- Les administrateurs peuvent utiliser la redirection de dossiers et les fichiers hors ligne ensemble pour rediriger le stockage des données des dossiers locaux vers le serveur CIFS, tout en permettant aux utilisateurs de mettre le contenu en cache localement.

Informations associées

Utilisation de fichiers hors ligne pour permettre la mise en cache de fichiers pour une utilisation hors ligne

Utilisation de profils itinérants pour stocker les profils utilisateurs de façon centralisée sur un serveur CIFS associé à la SVM

Conditions requises pour l'utilisation de la redirection de dossiers

Avant de pouvoir utiliser la redirection de dossiers de Microsoft avec votre serveur CIFS, vous devez connaître les versions de ONTAP et SMB et les clients Windows qui prennent en charge cette fonctionnalité.

Configuration requise pour la version ONTAP

ONTAP prend en charge la redirection de dossiers Microsoft.

Version requise du protocole SMB

Pour le serveur virtuel de stockage (SVM), ONTAP prend en charge la redirection de dossiers de Microsoft sur toutes les versions de SMB.

Configuration requise pour le client Windows

Avant qu'un utilisateur puisse utiliser la redirection de dossier de Microsoft, le client Windows doit prendre en charge cette fonctionnalité.

Pour obtenir les dernières informations sur les clients Windows prenant en charge la redirection de dossiers, consultez la matrice d'interopérabilité.

"mysupport.netapp.com/matrix"

Configurer la redirection de dossier

Vous pouvez configurer la redirection de dossiers à l'aide de la fenêtre Propriétés de Windows. L'avantage de cette méthode est que l'utilisateur Windows peut configurer la redirection de dossiers sans l'aide de l'administrateur SVM.

Étapes

1. Dans l'Explorateur Windows, cliquez avec le bouton droit de la souris sur le dossier que vous souhaitez rediriger vers un partage réseau.
2. Cliquez sur **Propriétés**.

   Les propriétés du partage sélectionné s'affichent.

3. Dans l'onglet **raccourci**, cliquez sur **cible** et spécifiez le chemin d'accès à l'emplacement réseau où vous souhaitez rediriger le dossier sélectionné.

   Par exemple, si vous souhaitez rediriger un dossier vers le `data` dossier dans un répertoire personnel mappé sur `Q:\`, spécifiez `Q:\data` comme cible.

4. Cliquez sur **OK**.

   Pour plus d'informations sur la configuration des dossiers hors ligne, consultez la bibliothèque Microsoft TechNet.

Informations associées

"Bibliothèque Microsoft TechNet : technet.microsoft.com/en-us/library/"

Accéder au répertoire ~snapshot à partir de clients Windows à l'aide de SMB 2.x

La méthode que vous utilisez pour accéder à l' `~snapshot` Le répertoire des clients Windows utilisant SMB 2.x diffère de la méthode utilisée pour SMB 1.0. Vous devez comprendre comment accéder à l' `~snapshot` Répertoire lors de l'utilisation de connexions SMB 2.x pour accéder correctement aux données stockées dans des copies Snapshot.

L'administrateur du SVM contrôle si les utilisateurs des clients Windows peuvent afficher et accéder à l' `~snapshot` répertoire sur un partage en activant ou désactivant le `showsnapshot` partager la propriété en utilisant les commandes du vserver cifs share properties familles.

Lorsque le `showsnapshot` La propriété partager est désactivée, un utilisateur d'un client Windows utilisant SMB 2.x ne peut pas afficher `~snapshot` Et ne peut pas accéder aux copies Snapshot dans le `~snapshot` répertoire, même lors de la saisie manuelle du chemin d'accès au `~snapshot` Ou à des copies Snapshot spécifiques dans le répertoire.

Lorsque le `showsnapshot` La propriété partager est activée, un utilisateur sur un client Windows utilisant SMB 2.x ne peut toujours pas afficher `~snapshot` répertoire soit à la racine du partage, soit dans une jonction ou un répertoire sous la racine du partage. Toutefois, après la connexion à un partage, l'utilisateur peut accéder au système masqué `~snapshot` en ajoutant manuellement le répertoire `\~snapshot` à la fin du chemin de partage. Le masqué `~snapshot` le répertoire est accessible à partir de deux points d'entrée :

- À la racine du partage
- À chaque point de jonction de l'espace de partage

Le masqué `~snapshot` le répertoire n'est pas accessible à partir de sous-répertoires non-jonctions dans le partage.

Exemple

Avec la configuration indiquée dans l'exemple suivant, un utilisateur d'un client Windows avec une connexion SMB 2.x au partage « eng » peut accéder à l' `~snapshot` en ajoutant manuellement le répertoire `\~snapshot` au chemin de partage à la racine du partage et à chaque point de jonction du chemin. Le masqué `~snapshot` le répertoire est accessible à partir des trois chemins suivants :

- `\\vs1\eng\~snapshot`
- `\\vs1\eng\projects1\~snapshot`
- `\\vs1\eng\projects2\~snapshot`

```
cluster1::> volume show -vserver vs1 -fields volume,junction-path
vserver volume       junction-path
------- ------------ ----------------------------------------
vs1     vs1_root      /
vs1     vs1_vol1      /eng
vs1     vs1_vol2      /eng/projects1
vs1     vs1_vol3      /eng/projects2

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

Restaurez des fichiers et des dossiers à l'aide des versions précédentes

Restaurer des fichiers et des dossiers à l'aide de la présentation des versions précédentes

La possibilité d'utiliser les versions précédentes de Microsoft s'applique aux systèmes de fichiers prenant en charge les copies Snapshot sous une forme ou une autre et les permettant de les activer. La technologie Snapshot fait partie intégrante de ONTAP. Les utilisateurs peuvent restaurer des fichiers et des dossiers à partir de copies Snapshot à partir de leur client Windows à l'aide de la fonction versions précédentes de Microsoft.

Avec les versions précédentes, les utilisateurs peuvent parcourir les copies Snapshot ou restaurer des données à partir d'une copie Snapshot sans l'intervention d'un administrateur de stockage. Les versions précédentes ne peuvent pas être configurées. Elle est toujours activée. Si l'administrateur du stockage a mis des copies Snapshot disponibles sur un partage, l'utilisateur peut utiliser les versions précédentes pour

effectuer les tâches suivantes :

- Restaurer les fichiers supprimés par inadvertance.
- Récupération après écrasement accidentel d'un fichier.
- Comparer les versions du fichier pendant le fonctionnement.

Les données stockées dans les copies Snapshot sont en lecture seule. Les utilisateurs doivent enregistrer une copie d'un fichier à un autre emplacement pour apporter des modifications au fichier. Les copies Snapshot sont régulièrement supprimées. Les utilisateurs doivent donc créer des copies des fichiers contenus dans les versions précédentes s'ils souhaitent conserver indéfiniment une version précédente d'un fichier.

Conditions requises pour l'utilisation des versions précédentes de Microsoft

Avant de pouvoir utiliser les versions précédentes avec votre serveur CIFS, vous devez savoir quelles versions de ONTAP et SMB et quels clients Windows le prennent en charge. Vous devez également connaître les exigences relatives au paramètre de copie Snapshot.

Configuration requise pour la version ONTAP

Prend en charge les versions précédentes.

Version requise du protocole SMB

Pour les machines virtuelles de stockage (SVM), ONTAP prend en charge les versions précédentes sur toutes les versions de SMB.

Configuration requise pour le client Windows

Avant qu'un utilisateur puisse utiliser les versions précédentes pour accéder aux données de copies Snapshot, le client Windows doit prendre en charge cette fonction.

Pour obtenir les dernières informations sur les clients Windows prenant en charge les versions précédentes, consultez la matrice d'interopérabilité.

"Matrice d'interopérabilité NetApp"

Configuration requise pour les paramètres de copie Snapshot

Pour accéder aux données de copies Snapshot, une règle Snapshot activée doit être associée au volume contenant les données, les clients doivent pouvoir accéder aux données Snapshot et des copies Snapshot doivent exister.

Utilisez l'onglet versions précédentes pour afficher et gérer les données de copie Snapshot

Les utilisateurs des ordinateurs clients Windows peuvent utiliser l'onglet versions précédentes de la fenêtre Propriétés de Windows pour restaurer les données stockées dans des copies Snapshot sans avoir à faire appel à l'administrateur de la machine virtuelle de stockage (SVM).

Description de la tâche

Si l'administrateur a activé les copies Snapshot sur le volume contenant le partage, l'onglet versions

précédentes permet uniquement d'afficher et de gérer les données des copies Snapshot des données stockées sur la SVM et si l'administrateur configure le partage pour afficher les copies Snapshot.

Étapes

1. Dans l'Explorateur Windows, affichez le contenu du lecteur mappé des données stockées sur le serveur CIFS.
2. Cliquez avec le bouton droit de la souris sur le fichier ou le dossier dans le lecteur réseau mappé dont vous souhaitez afficher ou gérer les copies Snapshot.
3. Cliquez sur **Propriétés**.

   Les propriétés du fichier ou dossier sélectionné s'affichent.

4. Cliquez sur l'onglet **versions précédentes**.

   La liste des copies Snapshot disponibles du fichier ou dossier sélectionné s'affiche dans la case versions de dossier. Les copies Snapshot répertoriées sont identifiées par le préfixe du nom de la copie Snapshot et par l'horodatage de création.

5. Dans la zone **versions de dossier:**, cliquez avec le bouton droit de la souris sur la copie du fichier ou du dossier que vous souhaitez gérer.
6. Effectuez l'action appropriée :

Les fonctions que vous recherchez…	Procédez comme suit…
Affichez les données de cette copie Snapshot	Cliquez sur **Ouvrir**.
Créer une copie des données à partir de cette copie Snapshot	Cliquez sur **Copier**.

   Les données des copies Snapshot sont en lecture seule. Si vous souhaitez apporter des modifications aux fichiers et dossiers répertoriés dans l'onglet versions précédentes, vous devez enregistrer une copie des fichiers et dossiers que vous souhaitez modifier à un emplacement inscriptible et apporter des modifications aux copies.

7. Une fois que vous avez terminé de gérer les données de snapshot, fermez la boîte de dialogue **Propriétés** en cliquant sur **OK**.

   Pour plus d'informations sur l'utilisation de l'onglet versions précédentes pour afficher et gérer les données de snapshot, consultez la bibliothèque Microsoft TechNet.

Informations associées

"Bibliothèque Microsoft TechNet : technet.microsoft.com/en-us/library/"

Déterminez si des copies Snapshot sont disponibles pour les versions précédentes

Vous pouvez afficher les copies Snapshot depuis l'onglet versions précédentes uniquement si une règle Snapshot activée est appliquée au volume contenant le partage et si la configuration de volume permet d'accéder aux copies Snapshot. Il est utile de déterminer la disponibilité des copies Snapshot pour aider un utilisateur à accéder aux versions précédentes.

Étapes

1. Déterminez si le volume sur lequel résident les données du partage est activé pour les copies Snapshot automatiques et si les clients ont accès aux répertoires Snapshot : `volume show -vserver vserver-name -volume volume-name -fields vserver,volume,snapdir-access,snapshot-policy,snapshot-count`

   Le résultat de cette commande affiche la règle Snapshot associée au volume, l'activation ou non de l'accès au répertoire Snapshot client et le nombre de copies Snapshot disponibles.

2. Déterminez si la règle Snapshot associée est activée : `volume snapshot policy show -policy policy-name`
3. Lister les copies Snapshot disponibles : `volume snapshot show -volume volume_name`

   Pour plus d'informations sur la configuration et la gestion des règles Snapshot et des planifications Snapshot, reportez-vous à la section "La protection des données".

Exemple

L'exemple suivant présente des informations sur les politiques Snapshot associées au volume nommé « data1 » qui contient les données partagées et les copies Snapshot disponibles sur « data1 ».

```
cluster1::> volume show -vserver vs1 -volume data1 -fields
vserver,volume,snapshot-policy,snapdir-access,snapshot-count
vserver  volume snapdir-access snapshot-policy snapshot-count
-------- ------ -------------- --------------- --------------
vs1      data1  true           default         10

cluster1::> volume snapshot policy show -policy default
Vserver: cluster1
                   Number of Is
Policy Name        Schedules Enabled Comment
------------------ --------- ------- ---------------------------------
default                    3 true    Default policy with hourly, daily &
weekly schedules.
    Schedule         Count     Prefix                 SnapMirror Label
    ---------------- -----     ---------------------- -------------------
    hourly               6     hourly                 -
    daily                2     daily                  daily
    weekly               2     weekly                 weekly

cluster1::> volume snapshot show -volume data1
                                                            ---Blocks---
Vserver  Volume  Snapshot                  State        Size Total% Used%
-------- ------- ------------------------- -------- -------- ------ -----
vs1      data1
                 weekly.2012-12-16_0015    valid       408KB     0%    1%
                 daily.2012-12-22_0010     valid       420KB     0%    1%
                 daily.2012-12-23_0010     valid       192KB     0%    0%
                 weekly.2012-12-23_0015    valid       360KB     0%    1%
                 hourly.2012-12-23_1405    valid       196KB     0%    0%
                 hourly.2012-12-23_1505    valid       196KB     0%    0%
                 hourly.2012-12-23_1605    valid       212KB     0%    0%
                 hourly.2012-12-23_1705    valid       136KB     0%    0%
                 hourly.2012-12-23_1805    valid       200KB     0%    0%
                 hourly.2012-12-23_1905    valid       184KB     0%    0%
```

Informations associées

Création d'une configuration de snapshot pour activer l'accès aux versions précédentes

"Protection des données"

Créez une configuration de snapshot pour activer l'accès aux versions précédentes

Les versions précédentes sont toujours disponibles dans la mesure où l'accès du client aux copies Snapshot est activé et à condition que des copies Snapshot existent. Si votre configuration de copie Snapshot ne répond pas à ces exigences, vous pouvez créer une configuration de copie Snapshot qui le fait.

Étapes

1. Si le volume contenant le partage auquel vous souhaitez autoriser l'accès aux versions précédentes n'est pas associé à une stratégie Snapshot, associez une politique Snapshot au volume et activez-la à l'aide du `volume modify` commande.

   Pour plus d'informations sur l'utilisation du `volume modify` commandes, consultez les pages de manuels.

2. Accès aux copies Snapshot à l'aide du `volume modify` pour définir le `-snap-dir` option à `true`.

   Pour plus d'informations sur l'utilisation du `volume modify` commandes, consultez les pages de manuels.

3. Vérifiez que les règles Snapshot sont activées et que l'accès aux répertoires Snapshot est activé à l'aide du `volume show` et `volume snapshot policy show` commandes.

   Pour plus d'informations sur l'utilisation du `volume show` et `volume snapshot policy show` commandes, consultez les pages de manuels.

   Pour plus d'informations sur la configuration et la gestion des règles Snapshot et des planifications Snapshot, reportez-vous à la section "La protection des données".

Informations associées

"Protection des données"

Instructions pour la restauration de répertoires contenant des jonctions

Vous devez garder à l'esprit certaines consignes lorsque vous utilisez les versions précédentes pour restaurer des dossiers contenant des points de jonction.

Lorsque vous utilisez les versions précédentes pour restaurer des dossiers comportant des dossiers enfants qui sont des points de jonction, la restauration peut échouer avec un `Access Denied` erreur.

Vous pouvez déterminer si le dossier que vous essayez de restaurer contient une jonction à l'aide de l' `vol show` commande avec `-parent` option. Vous pouvez également utiliser le `vserver security trace` commandes permettant de créer des journaux détaillés sur les problèmes d'accès aux fichiers et aux dossiers.

Informations associées

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

Déployez les services basés sur serveur SMB

Gérer les répertoires locaux

Comment ONTAP rend possible les répertoires locaux dynamiques

Les home directories ONTAP vous permettent de configurer un partage SMB qui correspond à différents répertoires en fonction de l'utilisateur qui se connecte à celui-ci et d'un ensemble de variables. Au lieu de créer des partages distincts pour chaque utilisateur, vous pouvez configurer un partage avec quelques paramètres de home

Directory afin de définir la relation d'un utilisateur entre un point d'entrée (le partage) et le home Directory (un répertoire sur la SVM).

Un utilisateur connecté en tant qu'utilisateur invité ne dispose pas d'un répertoire personnel et ne peut pas accéder aux répertoires d'accueil d'autres utilisateurs. Il existe quatre variables qui déterminent la manière dont un utilisateur est mappé à un répertoire :

- **Nom de partage**

  Il s'agit du nom du partage que vous créez et auquel l'utilisateur se connecte. Vous devez définir la propriété du répertoire personnel pour ce partage.

  Le nom du partage peut utiliser les noms dynamiques suivants :

  - `%w` (Nom d'utilisateur Windows de l'utilisateur)
  - `%d` (Nom de domaine Windows de l'utilisateur)
  - `%u` (Nom d'utilisateur UNIX mappé de l'utilisateur) Pour que le nom du partage soit unique dans tous les répertoires d'accueil, le nom du partage doit contenir soit/`%w` ou le `%u` variable. Le nom du partage peut contenir les deux `%d` et le/`%w` variable (par exemple, `%d`/`%w`), ou le nom du partage peut contenir une partie statique et une partie variable (par exemple, home_/`%w`).

- **Chemin de partage**

  Il s'agit du chemin relatif, défini par le partage, et donc associé à l'un des noms de partage, qui est ajouté à chaque chemin de recherche pour générer le chemin d'accès complet du home Directory de l'utilisateur, à partir de la racine de la SVM. Il peut être statique (par exemple, `home`), dynamique (par exemple, `%w`), ou une combinaison des deux (par exemple, `eng/%w`).

- **Chemins de recherche**

  Il s'agit de l'ensemble des chemins absolus depuis la racine du SVM que vous spécifiez qui dirigent la recherche ONTAP pour les répertoires locaux. Vous pouvez spécifier un ou plusieurs chemins de recherche à l'aide du `vserver cifs home-directory search-path add` commande. Si vous spécifiez plusieurs chemins de recherche, ONTAP les essaie dans l'ordre spécifié jusqu'à ce qu'il trouve un chemin valide.

- **Répertoire**

  Il s'agit du répertoire de base de l'utilisateur que vous créez pour l'utilisateur. Le nom du répertoire est généralement le nom de l'utilisateur. Vous devez créer le répertoire personnel dans l'un des répertoires définis par les chemins de recherche.

Prenons l'exemple de la configuration suivante :

- Utilisateur : John Smith
- Domaine utilisateur : acme
- Nom d'utilisateur: Jsmith
- Nom du SVM : vs1
- Nom de partage du répertoire de base n°1 : Home_ `%w` - chemin de partage : `%w`
- Nom de partage du répertoire racine #2 : `%w` - chemin de partage : `%d/%w`

- Chemin de recherche n°1 : `/vol0home/home`
- Chemin de recherche n°2 : `/vol1home/home`
- Chemin de recherche n°3 : `/vol2home/home`
- Home Directory : `/vol1home/home/jsmith`

Scénario 1 : l'utilisateur se connecte à `\\vs1\home_jsmith`. Ceci correspond au premier nom de partage du répertoire racine et génère le chemin relatif `jsmith`. ONTAP recherche désormais un répertoire nommé `jsmith` en vérifiant chaque chemin de recherche dans l'ordre suivant :

- `/vol0home/home/jsmith` n'existe pas ; passer au chemin de recherche n°2.
- `/vol1home/home/jsmith` existe ; par conséquent, le chemin de recherche #3 n'est pas coché ; l'utilisateur est maintenant connecté à son répertoire de base.

Scénario 2 : l'utilisateur se connecte à `\\vs1\jsmith`. Ceci correspond au deuxième nom de partage du répertoire de base et génère le chemin relatif `acme/jsmith`. ONTAP recherche désormais un répertoire nommé `acme/jsmith` en vérifiant chaque chemin de recherche dans l'ordre suivant :

- `/vol0home/home/acme/jsmith` n'existe pas ; passer au chemin de recherche n°2.
- `/vol1home/home/acme/jsmith` n'existe pas ; passer au chemin de recherche #3.
- `/vol2home/home/acme/jsmith` n'existe pas ; le répertoire personnel n'existe pas ; la connexion échoue donc.

Partages de répertoires locaux

Ajouter un partage de répertoire de base

Si vous souhaitez utiliser la fonction de répertoire de base SMB, vous devez ajouter au moins un partage avec la propriété de répertoire de base incluse dans les propriétés de partage.

Description de la tâche

Vous pouvez créer un partage de répertoire personnel au moment de la création du partage en utilisant le `vserver cifs share create` vous pouvez également modifier un partage existant en un partage de répertoire personnel à tout moment à l'aide de l' `vserver cifs share modify` commande.

Pour créer un partage de répertoire personnel, vous devez inclure le `homedirectory` valeur dans le `-share -properties` lorsque vous créez ou modifiez un partage. Vous pouvez spécifier le nom du partage et le chemin du partage à l'aide de variables développées dynamiquement lorsque les utilisateurs se connectent à leurs répertoires locaux. Les variables disponibles que vous pouvez utiliser dans le chemin sont `%w`, `%d`, et `%u`, Correspondant respectivement au nom d'utilisateur Windows, au domaine et au nom d'utilisateur UNIX mappé.

Étapes

1. Ajouter un partage de répertoire de base :
   `vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-share-properties homedirectory[,…]`

   `-vserver vserver` Spécifie la machine virtuelle de stockage (SVM) compatible CIFS sur laquelle ajouter le chemin de recherche.

`-share-name share-name` spécifie le nom de partage du répertoire racine.

En plus de contenir l'une des variables requises, si le nom du partage contient l'une des chaînes littérales `%w`, `%u`, ou `%d`, Vous devez faire précéder la chaîne littérale d'un caractère % (pourcentage) pour empêcher ONTAP de traiter la chaîne littérale comme une variable (par exemple, `%%w`).

- Le nom du partage doit contenir soit le `%w` ou le `%u` variable.
- Le nom du partage peut également contenir le `%d` variable (par exemple, `%d/%w`) ou une partie statique dans le nom du partage (par exemple, home1_/`%w`).
- Si le partage est utilisé par les administrateurs pour se connecter aux répertoires d'accueil d'autres utilisateurs ou pour permettre aux utilisateurs de se connecter aux répertoires d'accueil d'autres utilisateurs, le modèle de nom de partage dynamique doit être précédé d'un tilde (~).

  Le `vserver cifs home-directory modify` est utilisé pour activer cet accès en configurant le `-is-home-dirs-access-for-admin-enabled` option à `true`) ou en définissant l'option avancée `-is-home-dirs-access-for-public-enabled` à `true`.

`-path path` spécifie le chemin relatif vers le répertoire de base.

`-share-properties homedirectory[,…]` spécifie les propriétés de partage pour ce partage. Vous devez spécifier le `homedirectory` valeur. Vous pouvez spécifier d'autres propriétés de partage à l'aide d'une liste délimitée par des virgules.

1. Vérifiez que vous avez correctement ajouté le partage du répertoire personnel à l'aide de l' `vserver cifs share show` commande.

Exemple

La commande suivante crée un partage de répertoire personnel nommé `%w`. Le `oplocks`, `browsable`, et `changenotify` les propriétés de partage sont définies en plus de la configuration du `homedirectory` propriété de partage.

> Cet exemple n'affiche pas les valeurs de sortie de tous les partages du SVM. La sortie est tronquée.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name %w -path %w
-share-properties oplocks,browsable,changenotify,homedirectory

vs1::> vserver cifs share show -vserver vs1
Vserver    Share    Path         Properties     Comment  ACL
---------- -------- ------------ -------------- -------- -----------
vs1        %w       %w           oplocks        -        Everyone / Full
Control
                                 browsable
                                 changenotify
                                 homedirectory
```

Informations associées

Ajout d'un chemin de recherche de répertoire personnel

Exigences et directives pour l'utilisation de référencements de nœuds automatiques

Gestion de l'accessibilité aux répertoires locaux des utilisateurs

Les partages de répertoires locaux requièrent des noms d'utilisateur uniques

Veillez à attribuer des noms d'utilisateur uniques lors de la création de partages de répertoires locaux à l'aide de l' `%w` (Nom d'utilisateur Windows) ou `%u` (Nom d'utilisateur UNIX) variables permettant de générer des partages de façon dynamique. Le nom du partage est mappé sur votre nom d'utilisateur.

Deux problèmes peuvent survenir lorsqu'un nom de partage statique et un nom d'utilisateur sont identiques :

- Lorsque l'utilisateur répertorie les partages sur un cluster utilisant le `net view` commande : deux partages portant le même nom d'utilisateur sont affichés.
- Lorsque l'utilisateur se connecte à ce nom de partage, l'utilisateur est toujours connecté au partage statique et ne peut pas accéder au partage de répertoire personnel portant le même nom.

Par exemple, il y a un partage nommé « administrateur » et vous avez un nom d'utilisateur Windows « administrateur ». Si vous créez un partage de répertoire personnel et vous connectez à ce partage, vous êtes connecté au partage statique « administrateur » et non à votre partage de répertoire personnel « administrateur ».

Vous pouvez résoudre le problème avec les noms de partage en double en suivant l'une des étapes suivantes :

- Renommer le partage statique de sorte qu'il n'entre plus en conflit avec le partage du répertoire personnel de l'utilisateur.
- Donner à l'utilisateur un nouveau nom d'utilisateur pour qu'il n'entre plus en conflit avec le nom du partage statique.
- Création d'un partage CIFS home Directory avec un nom statique tel que « home » au lieu d'utiliser le `%w` paramètre pour éviter les conflits avec les noms des partages.

Ce qui arrive aux noms de partage de répertoire personnel statique après la mise à niveau

Les noms de partage de répertoire racine doivent contenir soit le `%w` ou le `%u` variable dynamique. Vous devez savoir ce qui arrive aux noms de partage de répertoire personnel statiques après la mise à niveau vers une version de ONTAP avec la nouvelle exigence.

Si votre configuration de répertoire personnel contient des noms de partage statiques et que vous effectuez une mise à niveau vers ONTAP, les noms de partage de répertoire personnel statique ne sont pas modifiés et sont toujours valides. Cependant, vous ne pouvez pas créer de nouveaux partages de répertoire personnel qui ne contiennent ni `%w` ou `%u` variable.

Le fait de demander que l'une de ces variables soit incluse dans le nom de partage du répertoire de base de l'utilisateur garantit que chaque nom de partage est unique dans la configuration du répertoire de base. Si vous le souhaitez, vous pouvez modifier les noms de partage des répertoires d'accueil statiques en noms contenant l'un ou l'autre `%w` ou `%u` variable.

Ajouter un chemin de recherche de répertoire de base

Si vous souhaitez utiliser les home directories ONTAP SMB, vous devez ajouter au moins un chemin de recherche de répertoire personnel.

Description de la tâche

Vous pouvez ajouter un chemin de recherche de répertoire personnel à l'aide de la `vserver cifs home-directory search-path add` commande.

Le `vserver cifs home-directory search-path add` la commande vérifie le chemin d'accès spécifié dans `-path` option pendant l'exécution de la commande. Si le chemin spécifié n'existe pas, la commande génère un message vous invitant à continuer. Votre choix `y` ou `n`. Si vous le souhaitez `y` Pour continuer, ONTAP crée le chemin de recherche. Toutefois, vous devez créer la structure du répertoire avant de pouvoir utiliser le chemin de recherche dans la configuration du répertoire racine. Si vous choisissez de ne pas continuer, la commande échoue ; le chemin de recherche n'est pas créé. Vous pouvez ensuite créer la structure du répertoire de chemins d'accès et réexécuter le `vserver cifs home-directory search-path add` commande.

Étapes

1. Ajouter un chemin de recherche de répertoire de base : `vserver cifs home-directory search-path add -vserver vserver -path path`
2. Vérifiez que vous avez correctement ajouté le chemin de recherche à l'aide de l' `vserver cifs home-directory search-path show` commande.

Exemple

L'exemple suivant ajoute le chemin `/home1` Vers la configuration home Directory sur le SVM vs1.

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

vs1::> vserver cifs home-directory search-path show
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1
```

L'exemple suivant tente d'ajouter le chemin d'accès `/home2` Vers la configuration home Directory sur le SVM vs1. Le chemin d'accès n'existe pas. Le choix est de ne pas continuer.

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home2
Warning: The specified path "/home2" does not exist in the namespace
         belonging to Vserver "vs1".
Do you want to continue? {y|n}: n
```

Informations associées

Ajout d'un partage de répertoire personnel

Créez une configuration de répertoire personnel à l'aide des variables %w et %d

Vous pouvez créer une configuration de répertoire personnel à l'aide de l' `%w` et `%d` variables. Les utilisateurs peuvent ensuite se connecter à leur partage personnel à l'aide de partages créés de manière dynamique.

Étapes

1. Créer un qtree pour contenir les home directories de l'utilisateur : `volume qtree create -vserver vserver_name -qtree-path qtree_path`
2. Vérifier que le qtree utilise le style de sécurité approprié : `volume qtree show`
3. Si le qtree n'utilise pas le style de sécurité souhaité, modifiez le style de sécurité à l'aide de `volume qtree security` commande.
4. Ajouter un partage de répertoire de base : `vserver cifs share create -vserver vserver -share-name %w -path %d/%w -share-properties homedirectory\[,...\]`

   `-vserver vserver` Spécifie la machine virtuelle de stockage (SVM) compatible CIFS sur laquelle ajouter le chemin de recherche.

   `-share-name %w` spécifie le nom de partage du répertoire racine. ONTAP crée dynamiquement le nom du partage lorsque chaque utilisateur se connecte à son répertoire de base. Le nom du partage sera sous la forme *Windows_user_name*.

   `-path %d/%w` spécifie le chemin relatif vers le répertoire de base. Le chemin relatif est créé de façon dynamique au fur et à mesure que chaque utilisateur se connecte à son répertoire de départ et sera sous la forme *domain/Windows_user_name*.

   `-share-properties homedirectory[,…]+` spécifie les propriétés de partage pour ce partage. Vous devez spécifier le `homedirectory` valeur. Vous pouvez spécifier d'autres propriétés de partage à l'aide d'une liste délimitée par des virgules.

5. Vérifiez que le partage dispose de la configuration souhaitée à l'aide du `vserver cifs share show` commande.
6. Ajouter un chemin de recherche de répertoire de base : `vserver cifs home-directory search-path add -vserver vserver -path path`

   `-vserver` *`vserver-name`* Spécifie le SVM activé sur CIFS sur lequel ajouter le chemin de recherche.

   `-path` *`path`* spécifie le chemin absolu du répertoire vers le chemin de recherche.

7. Vérifiez que vous avez correctement ajouté le chemin de recherche à l'aide de l' `vserver cifs home-directory search-path show` commande.
8. Pour les utilisateurs disposant d'un home Directory, créez un répertoire correspondant dans le qtree ou le volume désigné pour contenir des home directories.

   Par exemple, si vous avez créé un qtree avec le chemin d'accès du groupe `/vol/vol1/users` et le nom d'utilisateur dont vous souhaitez créer le répertoire est mydomain\user1, vous devez créer un répertoire avec le chemin suivant : `/vol/vol1/users/mydomain/user1`.

   Si vous avez créé un volume nommé « home1 » monté à `/home1`, vous créeriez un répertoire avec le chemin suivant : `/home1/mydomain/user1`.

9. Vérifiez qu'un utilisateur peut se connecter avec succès au partage d'accueil en mappant un lecteur ou en vous connectant à l'aide du chemin UNC.

   Par exemple, si l'utilisateur mydomain\user1 souhaite se connecter au répertoire créé à l'étape 8 situé sur le SVM vs1, l'utilisateur 1 se connecte à l'aide du chemin UNC `\\vs1\user1`.

Exemple

Dans l'exemple suivant, les commandes permettent de créer une configuration de home Directory avec les paramètres suivants :

- Le nom du partage est %w.
- Le chemin relatif du répertoire d'accueil est %d/%w.
- Le chemin de recherche utilisé pour contenir les répertoires locaux, `/home1`, Est un volume configuré avec le style de sécurité NTFS.
- La configuration est créée sur le SVM vs1.

Vous pouvez utiliser ce type de configuration de répertoire personnel lorsque les utilisateurs accèdent à leurs répertoires personnels à partir d'hôtes Windows. Vous pouvez également utiliser ce type de configuration lorsque les utilisateurs accèdent à leurs répertoires personnels à partir d'hôtes Windows et UNIX et que l'administrateur du système de fichiers utilise des utilisateurs et des groupes Windows pour contrôler l'accès au système de fichiers.

```
cluster::> vserver cifs share create -vserver vs1 -share-name %w -path
%d/%w -share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vserver cifs share show -vserver vs1 -share-name %w

                      Vserver: vs1
                        Share: %w
     CIFS Server NetBIOS Name: VS1
                         Path: %d/%w
             Share Properties: oplocks
                               browsable
                               changenotify
                               homedirectory
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

cluster::> vserver cifs home-directory search-path show
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1
```

Informations associées

Configuration des répertoires d'accueil à l'aide de la variable %u

Configurations supplémentaires des home Directory

Affichage des informations sur le chemin du répertoire local d'un utilisateur SMB

Configurez les répertoires d'accueil à l'aide de la variable %u

Vous pouvez créer une configuration de répertoire personnel dans laquelle vous désignez le nom du partage à l'aide de l' `%w` variable mais vous utilisez `%u` variable pour désigner le chemin relatif vers le partage du répertoire racine. Les utilisateurs peuvent ensuite se connecter à leur partage d'origine à l'aide de partages dynamiques créés à l'aide de leur nom d'utilisateur Windows sans connaître le nom ou le chemin réel du répertoire d'accueil.

Étapes

1. Créer un qtree pour contenir les home directories de l'utilisateur : `volume qtree create -vserver vserver_name -qtree-path qtree_path`
2. Vérifier que le qtree utilise le style de sécurité approprié : `volume qtree show`
3. Si le qtree n'utilise pas le style de sécurité souhaité, modifiez le style de sécurité à l'aide de `volume qtree security` commande.
4. Ajouter un partage de répertoire de base : `vserver cifs share create -vserver vserver -share-name %w -path %u -share-properties homedirectory ,...]`

   `-vserver vserver` Spécifie la machine virtuelle de stockage (SVM) compatible CIFS sur laquelle ajouter le chemin de recherche.

   `-share-name %w` spécifie le nom de partage du répertoire racine. Le nom du partage est créé dynamiquement lorsque chaque utilisateur se connecte à son répertoire de départ et se présente sous la forme *Windows_user_name*.

   > Vous pouvez également utiliser le `%u` variable pour le `-share-name` option. Cela crée un chemin de partage relatif qui utilise le nom d'utilisateur UNIX mappé.

   `-path %u` spécifie le chemin relatif vers le répertoire de base. Le chemin relatif est créé dynamiquement au fur et à mesure que chaque utilisateur se connecte à son répertoire de départ et se présente sous la forme *mappé_UNIX_user_name*.

   > La valeur de cette option peut également contenir des éléments statiques. Par exemple : `eng/%u`.

   `-share-properties homedirectory\[,...\]` spécifie les propriétés de partage pour ce partage. Vous devez spécifier le `homedirectory` valeur. Vous pouvez spécifier d'autres propriétés de partage à l'aide d'une liste délimitée par des virgules.

5. Vérifiez que le partage dispose de la configuration souhaitée à l'aide du `vserver cifs share show` commande.
6. Ajouter un chemin de recherche de répertoire de base : `vserver cifs home-directory search-path add -vserver vserver -path path`

   `-vserver vserver` Spécifie le SVM activé sur CIFS sur lequel ajouter le chemin de recherche.

   `-path path` spécifie le chemin absolu du répertoire vers le chemin de recherche.

7. Vérifiez que vous avez correctement ajouté le chemin de recherche à l'aide de l' `vserver cifs home-directory search-path show` commande.
8. Si l'utilisateur UNIX n'existe pas, créez l'utilisateur UNIX à l'aide de `vserver services unix-user create` commande.

   > Le nom d'utilisateur UNIX auquel vous associez le nom d'utilisateur Windows doit exister avant le mappage de l'utilisateur.

9. Créer un mappage de nom pour l'utilisateur Windows auprès de l'utilisateur UNIX à l'aide de la commande

suivante : `vserver name-mapping create -vserver vserver_name -direction win-unix -priority integer -pattern windows_user_name -replacement unix_user_name`

> Si des mappages de noms existent déjà et mappent des utilisateurs Windows aux utilisateurs UNIX, vous n'avez pas besoin d'effectuer l'étape de mappage.

Le nom d'utilisateur Windows est mappé sur le nom d'utilisateur UNIX correspondant. Lorsque l'utilisateur Windows se connecte à son partage de répertoire personnel, il se connecte à un répertoire personnel créé dynamiquement avec un nom de partage qui correspond à son nom d'utilisateur Windows sans avoir à savoir que le nom de répertoire correspond au nom d'utilisateur UNIX.

10. Pour les utilisateurs disposant d'un home Directory, créez un répertoire correspondant dans le qtree ou le volume désigné pour contenir des home directories.

    Par exemple, si vous avez créé un qtree avec le chemin d'accès du groupe `/vol/vol1/users` Et le nom d'utilisateur UNIX mappé de l'utilisateur dont vous souhaitez créer le répertoire est « unixuser1 », vous devez créer un répertoire avec le chemin suivant : `/vol/vol1/users/unixuser1`.

    Si vous avez créé un volume nommé « home1 » monté à `/home1`, vous créeriez un répertoire avec le chemin suivant : `/home1/unixuser1`.

11. Vérifiez qu'un utilisateur peut se connecter avec succès au partage d'accueil en mappant un lecteur ou en vous connectant à l'aide du chemin UNC.

    Par exemple, si l'utilisateur mydomain\user1 est mappé sur l'utilisateur UNIX unixuser1 et souhaite se connecter au répertoire créé à l'étape 10 situé sur le SVM vs1, l'utilisateur 1 se connecte à l'aide du chemin UNC `\\vs1\user1`.

Exemple

Dans l'exemple suivant, les commandes permettent de créer une configuration de home Directory avec les paramètres suivants :

- Le nom du partage est %w.
- Le chemin relatif du répertoire d'accueil est %U.
- Le chemin de recherche utilisé pour contenir les répertoires locaux, `/home1`, Est un volume configuré avec le style de sécurité UNIX.
- La configuration est créée sur le SVM vs1.

Vous pouvez utiliser ce type de configuration de répertoire personnel lorsque les utilisateurs accèdent à leurs répertoires personnels à partir des hôtes Windows ou Windows et UNIX et que l'administrateur de système de fichiers utilise des utilisateurs et des groupes UNIX pour contrôler l'accès au système de fichiers.

```
cluster::> vserver cifs share create -vserver vs1 -share-name %w -path %u
-share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vserver cifs share show -vserver vs1 -share-name %u

                      Vserver: vs1
                        Share: %w
     CIFS Server NetBIOS Name: VS1
                         Path: %u
             Share Properties: oplocks
                               browsable
                               changenotify
                               homedirectory
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

cluster::> vserver cifs home-directory search-path show -vserver vs1
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1

cluster::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 5 -pattern user1 -replacement unixuser1

cluster::> vserver name-mapping show -pattern user1
Vserver        Direction Position
-------------- --------- --------
vs1            win-unix  5        Pattern: user1
                                Replacement: unixuser1
```

Informations associées

Création d'une configuration de répertoire personnel à l'aide des variables %w et %d

Configurations supplémentaires des home Directory

Affichage des informations sur le chemin du répertoire local d'un utilisateur SMB

Configurations supplémentaires des home Directory

Vous pouvez créer d'autres configurations de home Directory à l'aide du `%w`, `%d`, et `%u` variables, qui vous permettent de personnaliser la configuration du répertoire personnel pour répondre à vos besoins.

Vous pouvez créer un certain nombre de configurations de répertoire personnel en utilisant une combinaison de variables et de chaînes statiques dans les noms de partage et les chemins de recherche. Le tableau suivant fournit des exemples illustrant la création de différentes configurations de répertoires locaux :

Chemins d'accès créés lors de `/vol1/user` contient les répertoires locaux…	**Partager, commande…**
Pour créer un chemin de partage `\\vs1\~win_username` qui dirige l'utilisateur vers `/vol1/user/win_username`	`vserver cifs share create -share-name ~%w -path %w -share-properties oplocks,browsable,changenotify,homedirectory`
Pour créer un chemin de partage `\\vs1\win_username` qui dirige l'utilisateur vers `/vol1/user/domain/win_username`	`vserver cifs share create -share-name %w -path %d/%w -share-properties oplocks,browsable,changenotify,homedirectory`
Pour créer un chemin de partage `\\vs1\win_username` qui dirige l'utilisateur vers `/vol1/user/unix_username`	`vserver cifs share create -share-name %w -path %u -share-properties oplocks,browsable,changenotify,homedirectory`
Pour créer un chemin de partage `\\vs1\unix_username` qui dirige l'utilisateur vers `/vol1/user/unix_username`	`vserver cifs share create -share-name %u -path %u -share-properties oplocks,browsable,changenotify,homedirectory`

Commandes de gestion des chemins de recherche

Il existe des commandes ONTAP spécifiques permettant de gérer les chemins de recherche pour les configurations du home Directory SMB. Par exemple, il existe des commandes permettant d'ajouter, de supprimer et d'afficher les informations relatives aux chemins de recherche. Il existe également une commande permettant de modifier l'ordre du chemin de recherche.

Les fonctions que vous recherchez…	**Utilisez cette commande…**
Ajouter un chemin de recherche	`vserver cifs home-directory search-path add`
Afficher les chemins de recherche	`vserver cifs home-directory search-path show`

Les fonctions que vous recherchez…	Utilisez cette commande…
Modifier l'ordre du chemin de recherche	`vserver cifs home-directory search-path reorder`
Supprimer un chemin de recherche	`vserver cifs home-directory search-path remove`

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

Affiche des informations sur le chemin du répertoire personnel d'un utilisateur SMB

Vous pouvez afficher le chemin d'accès au home Directory d'un utilisateur SMB sur la machine virtuelle de stockage (SVM), que vous pouvez utiliser si plusieurs chemins de home Directory CIFS sont configurés et que vous souhaitez voir quel chemin contient le home Directory de l'utilisateur.

Étape

1. Afficher le chemin du répertoire racine à l'aide de la `vserver cifs home-directory show-user` commande.

   ```
   vserver cifs home-directory show-user -vserver vs1 -username user1
   ```

   ```
   Vserver      User                  Home Dir Path
   -----------  --------------------  -----------------------
   vs1          user1                 /home/user1
   ```

Informations associées

Gestion de l'accessibilité aux répertoires locaux des utilisateurs

Gérer l'accessibilité aux répertoires locaux des utilisateurs

Par défaut, le répertoire personnel d'un utilisateur est accessible uniquement par cet utilisateur. Pour les partages dont le nom dynamique du partage est précédé d'un tilde (~), vous pouvez activer ou désactiver l'accès aux répertoires d'accueil des utilisateurs par les administrateurs Windows ou par tout autre utilisateur (accès public).

Avant de commencer

Les partages de home Directory sur la machine virtuelle de stockage (SVM) doivent être configurés avec des noms de partage dynamiques précédés d'un tilde (~). Les cas suivants illustrent les conditions de dénomination des partages :

Nom de partage du répertoire racine	Exemple de commande pour se connecter au partage
~%d~%w	`net use * \\IPaddress\~domain~user/u:credentials`
~%w	`net use * \\IPaddress\~user/u:credentials`
~abc~%w	`net use * \\IPaddress\abc~user/u:credentials`

Étape

1. Effectuez l'action appropriée :

Si vous souhaitez activer ou désactiver l'accès aux répertoires d'accueil des utilisateurs à…	Entrez les informations suivantes…
Administrateurs Windows	`vserver cifs home-directory modify -vserver` *`vserver_name`* `-is-home-dirs -access-for-admin-enabled {true|false}` La valeur par défaut est `true`.
Tout utilisateur (accès public)	a. Définissez le niveau de privilège sur avancé : `set -privilege advanced` b. Activer ou désactiver l'accès : `vserver cifs home-directory modify -vserver` *`vserver_name`* `-is-home-dirs-access-for-public-enabled {true`

L'exemple suivant permet l'accès public aux répertoires locaux des utilisateurs :

```
set -privilege advanced
vserver cifs home-directory modify -vserver vs1 -is-home-dirs-access-for-public
-enabled true
set -privilege admin
```

Informations associées

Affichage des informations sur le chemin du répertoire local d'un utilisateur SMB

Configurez l'accès client SMB aux liens symboliques UNIX

Comment ONTAP vous permet de fournir un accès client SMB aux liens symboliques UNIX

Un lien symbolique est un fichier créé dans un environnement UNIX qui contient une référence à un autre fichier ou répertoire. Si un client accède à un lien symbolique, le client est redirigé vers le fichier ou répertoire cible auquel le lien symbolique fait référence. ONTAP prend en charge les liens symboliques relatifs et absolus, y compris les liens filaires (liens absolus avec des cibles en dehors du système de fichiers local).

ONTAP permet aux clients SMB de suivre des liens symboliques UNIX configurés sur la SVM. Cette fonction est facultative et vous pouvez la configurer par partage à l'aide de `-symlink-properties` de la `vserver cifs share create` avec l'un des paramètres suivants :

- Accès en lecture/écriture
- Activé avec accès en lecture seule
- Désactivé en masquant les liens symboliques des clients SMB
- Désactivé sans accès aux liens symboliques des clients SMB

Si vous activez des liens symboliques sur un partage, les liens symboliques relatifs fonctionnent sans configuration supplémentaire.

Si vous activez des liens symboliques sur un partage, les liens symboliques absolus ne fonctionnent pas immédiatement. Vous devez d'abord créer un mappage entre le chemin UNIX du lien symbolique et le chemin SMB de destination. Lors de la création de mappages de liens symboliques absolus, vous pouvez spécifier s'il s'agit d'un lien local ou d'un *widelink* ; les liens vers des systèmes de fichiers sur d'autres périphériques de stockage ou des liens vers des systèmes de fichiers hébergés dans des SVM distincts sur le même système ONTAP. Lorsque vous créez un lien, il doit inclure les informations que le client doit suivre, c'est-à-dire que vous créez un point de reanalyse pour que le client puisse découvrir le point de jonction du répertoire. Si vous créez un lien symbolique absolu vers un fichier ou un répertoire en dehors du partage local mais que vous définissez la localité sur local, ONTAP n'autorise pas l'accès à la cible.

> Si un client tente de supprimer un lien symbolique local (absolu ou relatif), seul le lien symbolique est supprimé, pas le fichier ou le répertoire cible. Toutefois, si un client tente de supprimer un lien vers le fil, il peut supprimer le fichier ou le répertoire cible auquel le lien vers le fil vers le fil. ONTAP n'a pas le contrôle sur cela, car le client peut explicitement ouvrir le fichier ou le répertoire cible en dehors du SVM et le supprimer.

- **Analyse des points et des services de système de fichiers ONTAP**

  Un *reparse point* est un objet système de fichiers NTFS qui peut éventuellement être stocké sur des volumes avec un fichier. Les points de reanalyse permettent aux clients SMB de recevoir des services de système de fichiers améliorés ou étendus lorsqu'ils travaillent avec des volumes de style NTFS. Les points de réanalyse se composent d'étiquettes standard identifiant le type de point de réanalyse et le contenu du point de réanalyse pouvant être récupéré par les clients SMB pour un traitement ultérieur par le client. Parmi les types d'objets disponibles pour la fonctionnalité étendue du système de fichiers, ONTAP met en œuvre la prise en charge des liens symboliques NTFS et des points de jonction de répertoire à l'aide de balises de point de reparse. Les clients SMB qui ne peuvent pas comprendre le contenu d'un point de reanalyse le ignorent et ne fournissent pas le service étendu de système de fichiers que le point de reanalyse peut activer.

- **Prise en charge des points de jonction de répertoire et de ONTAP pour les liens symboliques**

  Les points de jonction de répertoire sont des emplacements au sein d'une structure de répertoire de système de fichiers qui peuvent faire référence à des emplacements de remplacement où les fichiers sont stockés, soit sur un chemin différent (liens symboliques), soit sur un périphérique de stockage distinct (liens filaires). Les serveurs ONTAP SMB exposent les points de jonction de répertoire aux clients Windows sous forme de points de reanalyse, ce qui permet aux clients capables d'obtenir le contenu du point de reanalyse à partir de ONTAP lorsqu'un point de jonction de répertoire est en cours de traitement. Ils peuvent ainsi naviguer et se connecter à différents chemins ou périphériques de stockage comme s'ils faisaient partie du même système de fichiers.

- **Activation de la prise en charge wdelink à l'aide des options de point de réanalyse**

Le `-is-use-junctions-as-reparse-points-enabled` Cette option est activée par défaut dans ONTAP 9. Tous les clients SMB ne prennent pas en charge les widelinks. L'option d'activation des informations peut donc être configurée selon la version du protocole, ce qui permet aux administrateurs de prendre en charge à la fois les clients SMB pris en charge et les clients SMB non pris en charge. Dans ONTAP 9.2 et versions ultérieures, vous devez activer cette option `-widelink-as-reparse-point -versions` Pour chaque protocole client qui accède au partage à l'aide de widelinks, la valeur par défaut est SMB1. Dans les versions antérieures, seules les widelinks accessibles à l'aide de SMB1 par défaut ont été signalés et les systèmes utilisant SMB2 ou SMB3 n'ont pas pu accéder aux widelinks.

Pour plus d'informations, consultez la documentation Microsoft NTFS.

"Documentation Microsoft : analyse des points"

Limites lors de la configuration de liens symboliques UNIX pour l'accès SMB

Vous devez connaître certaines limites lors de la configuration de liens symboliques UNIX pour l'accès SMB.

Limite	Description
45	Longueur maximale du nom de serveur CIFS que vous pouvez spécifier lors de l'utilisation d'un FQDN pour le nom du serveur CIFS. Vous pouvez également spécifier le nom du serveur CIFS sous la forme d'un nom NetBIOS, limité à 15 caractères.
80	Longueur maximale du nom de partage.
256	Longueur maximale du chemin UNIX que vous pouvez spécifier lors de la création d'un lien symbolique ou lors de la modification du chemin UNIX d'un lien symbolique existant.le chemin UNIX doit commencer par un ""/" `(slash) and end with a` "/». Les barres obliques de début et de fin font partie de la limite de 256 caractères.
256	Longueur maximale du chemin CIFS que vous pouvez spécifier lors de la création d'un lien symbolique ou lors de la modification du chemin CIFS d'un lien symbolique existant.le chemin CIFS doit commencer par « »/" `(slash) and end with a` "/». Les barres obliques de début et de fin font partie de la limite de 256 caractères.

Informations associées

Création de mappages de liens symboliques pour les partages SMB

Contrôle des annonces DFS automatiques dans ONTAP avec une option de serveur CIFS

Une option de serveur CIFS contrôle la manière dont les fonctionnalités DFS sont annoncées aux clients SMB lors de la connexion aux partages. Étant donné que ONTAP utilise des référencements DFS lorsque les clients accèdent aux liens symboliques via SMB, vous devez savoir quel est l'impact lorsque cette option est désactivée ou activée.

Une option de serveur CIFS détermine si les serveurs CIFS annoncent automatiquement qu'ils sont compatibles DFS pour les clients SMB. Par défaut, cette option est activée et le serveur CIFS annonce toujours que DFS est capable pour les clients SMB (même lors de la connexion à des partages où l'accès aux liens symboliques est désactivé). Si vous voulez que le serveur CIFS annonce qu'il est compatible avec les clients uniquement lorsqu'ils se connectent à des partages où l'accès aux liens symboliques est activé, vous pouvez désactiver cette option.

Vous devez savoir ce qui se passe lorsque cette option est désactivée :

- Les configurations de partage des liens symboliques ne sont pas modifiées.
- Si le paramètre de partage est défini pour autoriser l'accès à la liaison symbolique (accès en lecture/écriture ou accès en lecture seule), le serveur CIFS transmet les fonctionnalités DFS aux clients se connectant à ce partage.

  Les connexions client et l'accès aux liens symboliques se poursuivent sans interruption.

- Si le paramètre de partage est défini sur ne pas autoriser l'accès aux liens symboliques (soit en désactivant l'accès, soit si la valeur du paramètre de partage est nulle), le serveur CIFS n'annonce pas les capacités DFS aux clients se connectant à ce partage.

  Comme les clients disposent d'informations en cache sur lesquelles le serveur CIFS prend en charge DFS et qu'il n'est plus publicitaire qu'il est, les clients connectés à des partages où l'accès à la liaison symbolique est désactivé risquent de ne pas pouvoir accéder à ces partages une fois que l'option de serveur CIFS est désactivée. Une fois l'option désactivée, vous devrez peut-être redémarrer les clients connectés à ces partages, ce qui vous permettra de supprimer les informations mises en cache.

Ces modifications ne s'appliquent pas aux connexions SMB 1.0.

Configurez la prise en charge des liens symboliques UNIX sur les partages SMB

Vous pouvez configurer la prise en charge des liens symboliques UNIX sur les partages SMB en spécifiant un paramètre de propriété de partage de liens symboliques lorsque vous créez des partages SMB ou en modifiant à tout moment des partages SMB existants. La prise en charge des liens symboliques UNIX est activée par défaut. Vous pouvez également désactiver la prise en charge des liens symboliques UNIX sur un partage.

Description de la tâche

Lors de la configuration de la prise en charge des liens symboliques UNIX pour les partages SMB, vous pouvez choisir l'un des paramètres suivants :

Réglage	Description
`enable` (OBSOLÈTE*)	Indique que les liens symboliques sont activés pour l'accès en lecture/écriture.
`read_only` (OBSOLÈTE*)	Indique que les symlinks sont activés pour l'accès en lecture seule. Ce paramètre ne s'applique pas aux boutons de mode. L'accès Widelink est toujours en lecture-écriture.
`hide` (OBSOLÈTE*)	Spécifie que les clients SMB ne peuvent pas voir les symlinks.
`no-strict-security`	Spécifie que les clients suivent des symlinks en dehors des limites de partage.
`symlinks`	Indique que les symlinks sont activés localement pour l'accès en lecture/écriture. Les annonces DFS ne sont pas générées même si l'option CIFS `is-advertise-dfs-enabled` est défini sur `true`. Il s'agit du paramètre par défaut.
`symlinks-and-widelinks`	Spécifie que les liens symlinks locaux et les widelinks pour l'accès en lecture-écriture. Les annonces DFS sont générées pour les symlinks locaux et les widelinks, même si l'option CIFS `is-advertise-dfs-enabled` est défini sur `false`.
`disable`	Spécifie que les liens symlinks et les liens de fil sont désactivés. Les annonces DFS ne sont pas générées même si l'option CIFS `is-advertise-dfs-enabled` est défini sur `true`.
`""` (nul, non défini)	Désactive les liens symboliques sur le partage.
– (non défini)	Désactive les liens symboliques sur le partage.

*Les paramètres *enable*, *hide* et *read-only* sont obsolètes et peuvent être supprimés dans une version future de ONTAP.

Étapes

1. Configurer ou désactiver la prise en charge des liens symboliques :

Si c'est…	Entrer…
Un nouveau partage SMB	`+vserver cifs share create -vserver vserver_name -share-name share_name -path path -symlink -properties {enable

Si c'est…	Entrer…
hide	read-only
""	-
symlinks	symlinks-and-widelinks
disable},…]+`	Un partage SMB existant
`+vserver cifs share modify -vserver vserver_name -share-name share_name -symlink-properties {enable	hide
read-only	""
-	symlinks
symlinks-and-widelinks	disable},…]+`

2. Vérifiez que la configuration du partage SMB est correcte : `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

Exemple

La commande suivante crée un partage SMB nommé "data1" avec la configuration de lien symbolique UNIX définie sur `enable`:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -symlink-properties enable

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
         CIFS Server NetBIOS Name: VS1
                             Path: /data1
                 Share Properties: oplocks
                                   browsable
                                   changenotify
               Symlink Properties: enable
          File Mode Creation Mask: -
     Directory Mode Creation Mask: -
                    Share Comment: -
                        Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                      Volume Name: -
                    Offline Files: manual
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

Informations associées

Création de mappages de liens symboliques pour les partages SMB

Créez des mappages de liens symboliques pour les partages SMB

Vous pouvez créer des mappages de liens symboliques UNIX pour les partages SMB. Vous pouvez soit créer un lien symbolique relatif, qui fait référence au fichier ou au dossier par rapport à son dossier parent, soit créer un lien symbolique absolu, qui fait référence au fichier ou au dossier à l'aide d'un chemin absolu.

Description de la tâche

Les Widelinks ne sont pas accessibles à partir de clients Mac OS X si vous utilisez SMB 2.x. Lorsqu'un utilisateur tente de se connecter à un partage à l'aide de liens de liaison d'un client Mac OS X, la tentative échoue. Toutefois, vous pouvez utiliser des liens de mode avec les clients Mac OS X si vous utilisez SMB 1.

Étapes

1. Pour créer des mappages de liens symboliques pour les partages SMB : `vserver cifs symlink create -vserver virtual_server_name -unix-path path -share-name share_name -cifs-path path [-cifs-server server_name] [-locality {local|free|widelink}] [-home-directory {true|false}]`

   `-vserver virtual_server_name` Spécifie le nom de la machine virtuelle de stockage (SVM).

`-unix-path path` Spécifie le chemin UNIX. Le chemin UNIX doit commencer par une barre oblique (`/`) et doit se terminer par une barre oblique (`/`).

`-share-name share_name` Spécifie le nom du partage SMB à mapper.

`-cifs-path path` Spécifie le chemin CIFS. Le chemin CIFS doit commencer par une barre oblique (`/`) et doit se terminer par une barre oblique (`/`).

`-cifs-server server_name` Spécifie le nom du serveur CIFS. Le nom du serveur CIFS peut être spécifié sous la forme d'un nom DNS (par exemple, mynetwork.cifs.server.com), d'une adresse IP ou d'un nom NetBIOS. Le nom NetBIOS peut être déterminé à l'aide du `vserver cifs show` commande. Si ce paramètre facultatif n'est pas spécifié, la valeur par défaut est le nom NetBIOS du serveur CIFS local.

`-locality local|free|widelink}` spécifie s'il faut créer un lien local, un lien libre ou un lien symbolique étendu. Un lien symbolique local correspond au partage SMB local. Un lien symbolique libre peut être mappé n'importe où sur le serveur SMB local. Un lien symbolique étendu correspond à n'importe quel partage SMB du réseau. Si vous ne spécifiez pas ce paramètre facultatif, la valeur par défaut est `local`.

`-home-directory true false}` indique si le partage cible est un répertoire de base. Même si ce paramètre est facultatif, vous devez définir ce paramètre sur `true` lorsque le partage cible est configuré en tant que répertoire de base. La valeur par défaut est `false`.

Exemple

La commande suivante crée un mappage de lien symbolique sur le SVM nommé vs1. Il a le chemin UNIX `/src/`, Le nom de partage SMB "SOUCE", le chemin CIFS `/mycompany/source/`, Et l'adresse IP 123.123.123.123 du serveur CIFS, et c'est un lien de type widelink.

```
cluster1::> vserver cifs symlink create -vserver vs1 -unix-path /src/
-share-name SOURCE -cifs-path "/mycompany/source/" -cifs-server
123.123.123.123 -locality widelink
```

Informations associées

Configuration de la prise en charge des liens symboliques UNIX sur les partages SMB

Commandes permettant de gérer les mappages de liens symboliques

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

Les fonctions que vous recherchez…	Utilisez cette commande…
Créer un mappage de lien symbolique	`vserver cifs symlink create`
Affiche des informations sur les mappages de liens symboliques	`vserver cifs symlink show`
Modifier un mappage de lien symbolique	`vserver cifs symlink modify`

Les fonctions que vous recherchez…	Utilisez cette commande…
Supprimer un mappage de lien symbolique	`vserver cifs symlink delete`

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

Utilisez BranchCache pour mettre en cache le contenu du partage SMB dans une succursale

Utilisez BranchCache pour mettre en cache le contenu du partage SMB dans une présentation destinée aux succursales

BranchCache a été développé par Microsoft afin de permettre la mise en cache du contenu sur les ordinateurs locaux pour les clients. L'implémentation par ONTAP de BranchCache permet de réduire l'utilisation du réseau étendu (WAN) et de réduire le temps de réponse d'accès lorsque les utilisateurs d'une succursale accèdent au contenu stocké sur des serveurs virtuels de stockage (SVM) avec SMB.

Si vous configurez BranchCache, les clients Windows BranchCache récupèrent le contenu du SVM, puis le mettent en cache sur un ordinateur au sein de la succursale. Si un autre client BranchCache du bureau de succursale demande le même contenu, le SVM procède d'abord à l'authentification et autorise l'utilisateur à demander. La SVM détermine ensuite si le contenu en cache est toujours à jour et, le cas échéant, elle envoie les métadonnées client relatives au contenu en cache. Le client utilise ensuite les métadonnées pour récupérer le contenu directement à partir du cache local.

Informations associées

Utilisation de fichiers hors ligne pour permettre la mise en cache de fichiers pour une utilisation hors ligne

Exigences et directives

Prise en charge de BranchCache

Notez bien les versions de BranchCache prises en charge par ONTAP.

ONTAP prend en charge BranchCache 1 et le BranchCache 2 optimisé :

- Lorsque vous configurez BranchCache sur le serveur SMB pour le serveur de stockage virtuel (SVM), vous pouvez activer BranchCache 1, BranchCache 2 ou toutes les versions.

  Par défaut, toutes les versions sont activées.

- Si vous n'activez que BranchCache 2, les ordinateurs clients Windows du bureau distant doivent prendre en charge BranchCache 2.

  Seuls les clients SMB 3.0 ou version ultérieure prennent en charge BranchCache 2.

Pour plus d'informations sur les versions de BranchCache, consultez la bibliothèque Microsoft TechNet.

Informations associées

"Bibliothèque Microsoft TechNet : technet.microsoft.com/en-us/library/"

Exigences de prise en charge des protocoles réseau

Pour implémenter ONTAP BranchCache, vous devez connaître les exigences en matière de protocoles réseau.

Vous pouvez implémenter la fonction ONTAP BranchCache sur des réseaux IPv4 et IPv6 à l'aide de SMB 2.1 ou version ultérieure.

Tous les serveurs CIFS et les succursales qui participent à l'implémentation de BranchCache doivent activer le protocole SMB 2.1 ou version ultérieure. Avec SMB 2.1, les extensions de protocole permettent à un client de participer à un environnement de BranchCache. Il s'agit de la version minimale du protocole SMB qui prend en charge BranchCache. SMB 2.1 prend en charge BranchCache version 1.

Si vous souhaitez utiliser BranchCache version 2, SMB 3.0 est la version minimale prise en charge. SMB 3.0 doit être activé sur tous les serveurs CIFS et les succursales qui participent à une implémentation de BranchCache 2.

Si vous disposez de bureaux distants où certains clients prennent uniquement en charge SMB 2.1 et que certains clients prennent en charge SMB 3.0, vous pouvez implémenter une configuration de BranchCache sur le serveur CIFS, qui prend en charge la mise en cache de BranchCache 1 et BranchCache 2.

> Même si la fonctionnalité de BranchCache de Microsoft prend en charge l'utilisation des protocoles HTTP/HTTPS et SMB comme protocoles d'accès aux fichiers, ONTAP BranchCache ne prend en charge que SMB.

Configuration requise pour la version des hôtes ONTAP et Windows

Avant de configurer BranchCache, les hôtes Windows du ONTAP et des succursales doivent répondre à certaines exigences de version.

Avant de configurer BranchCache, vous devez vérifier que la version de ONTAP est compatible avec le cluster et les clients des succursales participantes et prennent en charge SMB 2.1 ou version ultérieure, et prend en charge la fonctionnalité BranchCache. Si vous configurez le mode cache hébergé, vous devez également vous assurer que vous utilisez un hôte pris en charge pour le serveur de cache.

BranchCache 1 est pris en charge sur les versions ONTAP et hôtes Windows suivantes :

- Serveur de contenu : serveur virtuel de stockage (SVM) avec ONTAP
- Serveur de cache : Windows Server 2008 R2 ou Windows Server 2012 ou version ultérieure
- Poste ou client : Windows 7 Enterprise, Windows 7 Édition intégrale, Windows 8, Windows Server 2008 R2 ou Windows Server 2012 ou version ultérieure

BranchCache 2 est pris en charge sur les versions ONTAP et les hôtes Windows suivants :

- Serveur de contenu : SVM avec ONTAP
- Serveur de cache : Windows Server 2012 ou version ultérieure
- Poste ou client : Windows 8 ou Windows Server 2012 ou version ultérieure

Les raisons pour lesquelles ONTAP invalide des hachages de BranchCache

Pour planifier votre configuration de BranchCache, ONTAP permet de déterminer les raisons pour lesquelles des hachages sont validés. Elle vous aide à choisir le mode de

fonctionnement à configurer et à choisir les partages qui permettent d'activer BranchCache.

ONTAP doit gérer BranchCache pour vérifier que des hachages sont valides. Si un hachage n'est pas valide, ONTAP invalide le hachage et calcule un nouveau hachage la prochaine fois que le contenu est demandé, en supposant que BranchCache est toujours activé.

Des hachages de ONTAP valident les données pour les raisons suivantes :

- La clé de serveur est modifiée.

  Si la clé du serveur est modifiée, ONTAP invalide tous les hachages du magasin de hachage.

- Le hachage est transféré depuis le cache, car la taille maximale du magasin de hachage de BranchCache a été atteinte.

  Il s'agit d'un paramètre ajustable et peut être modifié pour répondre à vos exigences métier.

- Un fichier est modifié via un accès SMB ou NFS.
- Un fichier pour lequel des hachages sont calculés est restauré à l'aide de l' `snap restore` commande.
- Un volume qui contient des partages SMB qui sont activés pour BranchCache est restauré à l'aide du `snap restore` commande.

Directives pour choisir l'emplacement du magasin de hachage

Lors de la configuration de BranchCache, vous pouvez choisir l'emplacement de stockage des hachages et la taille du magasin de hachage. Comprendre les instructions à suivre lors du choix de l'emplacement et de la taille du magasin de hachage peut vous aider à planifier la configuration de BranchCache sur un SVM compatible CIFS.

- Vous devez localiser le magasin de hachage sur un volume où les mises à jour atime sont autorisées.

  Le temps d'accès sur un fichier de hachage est utilisé pour conserver les fichiers fréquemment utilisés dans le magasin de hachage. Si les mises à jour atime sont désactivées, l'heure de création est utilisée à cette fin. Il est préférable d'utiliser atime pour suivre les fichiers fréquemment utilisés.

- Vous ne pouvez pas stocker des hachages sur des systèmes de fichiers en lecture seule, tels que les destinations SnapMirror et les volumes SnapLock.
- Si la taille maximale du magasin de hachage est atteinte, des hachages plus anciens sont vidés pour faire de la place à de nouveaux hachages.

  Vous pouvez augmenter la taille maximale du magasin de hachage pour réduire la quantité de hachages vidés du cache.

- Si le volume sur lequel vous stockez des hachages est indisponible ou saturé, ou si une communication interne au cluster pose un problème, là où le service de BranchCache ne peut pas récupérer les informations de hachage, les services de BranchCache ne sont pas disponibles.

  Le volume peut être indisponible parce qu'il est hors ligne ou parce que l'administrateur du stockage a spécifié un nouvel emplacement pour le magasin de hachage.

  Cela ne cause pas de problèmes d'accès aux fichiers. Si l'accès au magasin de hachage est entravé, ONTAP renvoie une erreur définie par Microsoft au client, ce qui entraîne la demande du client concernant

le fichier à l'aide de la requête de lecture SMB normale.

Informations associées

Configurez BranchCache sur le serveur SMB

Modifier la configuration de BranchCache

Recommandations de BranchCache

Avant de configurer BranchCache, il est important de tenir compte de certaines recommandations lorsque vous décidez des partages SMB que vous souhaitez activer la mise en cache de BranchCache.

Veillez à respecter les recommandations suivantes lorsque vous décidez du mode d'exploitation à utiliser et des partages SMB pour activer BranchCache :

- Grâce à la mise en cache à distance des données, BranchCache est moins bénéfique.
- Les services de BranchCache sont avantageux pour les partages contenant du contenu de fichier, réutilisé par plusieurs clients distants ou par du contenu de fichier accessible de manière répétée par un seul utilisateur distant.
- Prenez l'activation de la mise en cache pour du contenu en lecture seule, tel que les données de copies Snapshot et de destinations SnapMirror.

Configurer BranchCache

Configurer la présentation de BranchCache

Vous pouvez configurer BranchCache sur votre serveur SMB à l'aide des commandes ONTAP. Pour implémenter BranchCache, vous devez également configurer vos clients et, éventuellement, vos serveurs de cache hébergés dans les succursales où vous souhaitez mettre en cache le contenu.

Si vous configurez BranchCache pour permettre la mise en cache partage par partage, vous devez activer BranchCache sur les partages SMB pour lesquels vous souhaitez fournir des services de mise en cache de BranchCache.

Configuration requise pour la configuration de BranchCache

Une fois que vous avez atteint certains prérequis, vous pouvez configurer BranchCache.

Les exigences suivantes doivent être respectées avant de configurer BranchCache sur le serveur CIFS pour le SVM :

- ONTAP doit être installé sur tous les nœuds du cluster.
- CIFS doit être sous licence et un serveur SMB doit être configuré. La licence SMB est incluse avec "ONTAP One". Si vous n'avez pas ONTAP One et que la licence n'est pas installée, contactez votre ingénieur commercial.
- La connectivité réseau IPv4 ou IPv6 doit être configurée.
- Pour BranchCache 1, SMB 2.1 ou version ultérieure doit être activé.
- Pour BranchCache 2, SMB 3.0 doit être activé et les clients Windows distants doivent prendre en charge

BranchCache 2.

Configurez BranchCache sur le serveur SMB

Vous pouvez configurer BranchCache pour fournir des services de BranchCache sur la base de chaque partage. Vous pouvez également configurer BranchCache pour activer automatiquement la mise en cache sur tous les partages SMB.

Description de la tâche

Vous pouvez configurer BranchCache sur des SVM.

- Vous pouvez créer une configuration de BranchCache pour tous les partages si vous souhaitez proposer des services de mise en cache pour tout le contenu contenu contenu contenu contenu dans tous les partages SMB sur le serveur CIFS.
- Vous pouvez créer une configuration de BranchCache par partage si vous souhaitez proposer des services de mise en cache pour le contenu contenu contenu hébergé dans des partages SMB sélectionnés sur le serveur CIFS.

Vous devez spécifier les paramètres suivants lors de la configuration de BranchCache :

Paramètres requis	Description
Nom du SVM	BranchCache est configuré pour chaque SVM. Vous devez spécifier sur quel SVM compatible CIFS vous souhaitez configurer le service de BranchCache.
Chemin vers magasin de hachage	Les hachages de BranchCache sont stockés dans des fichiers réguliers sur le volume du SVM. Vous devez spécifier le chemin d'accès à un répertoire existant dans lequel ONTAP doit stocker les données de hachage.le chemin de hachage BranchCache doit être accessible en lecture-écriture. Les chemins en lecture seule, tels que les répertoires Snapshot, ne sont pas autorisés. Vous pouvez stocker les données de hachage dans un volume contenant d'autres données ou créer un volume distinct pour stocker les données de hachage. Si le SVM est une source de reprise d'activité du SVM, le chemin de hachage ne peut pas se trouver sur le volume root. En effet, le volume racine n'est pas répliqué vers la destination de reprise après incident. Le chemin de hachage peut contenir des blancs et des caractères de nom de fichier valides.

Vous pouvez éventuellement spécifier les paramètres suivants :

Paramètres facultatifs	Description
Versions prises en charge	ONTAP prend en charge BranchCache 1 et 2. Vous pouvez activer la version 1, la version 2 ou les deux versions. La valeur par défaut est d'activer les deux versions.
Taille maximale du magasin de hachage	Vous pouvez spécifier la taille à utiliser pour le magasin de données de hachage. Si les données de hachage dépassent cette valeur, ONTAP supprime des hachages plus anciens pour faire de la place à des hachages plus récents. La taille par défaut du magasin de hachage est de 1 Go. BranchCache fonctionne plus efficacement si des hachages ne sont pas éliminés de manière trop agressive. Si vous déterminez que les hachages sont fréquemment ignorés car le magasin de hachage est plein, vous pouvez augmenter la taille du magasin de hachage en modifiant la configuration de BranchCache.
Clé du serveur	Vous pouvez spécifier une clé de serveur utilisée par le service BranchCache pour empêcher les clients d'imiter le serveur BranchCache. Si vous ne spécifiez pas de clé de serveur, une clé est générée de manière aléatoire lors de la création de la configuration de BranchCache. Vous pouvez définir la clé du serveur à une valeur spécifique. Ainsi, si plusieurs serveurs fournissent des données de BranchCache pour les mêmes fichiers, les clients peuvent utiliser des hachages à partir de n'importe quel serveur à l'aide de la même clé de serveur. Si la clé du serveur contient des espaces, vous devez inclure la clé du serveur entre guillemets.
Mode de fonctionnement	Par défaut, BranchCache est activé par partage. • Pour créer une configuration de BranchCache dans laquelle vous activez BranchCache par partage, vous pouvez soit spécifier ce paramètre facultatif, soit `per-share`. • Pour activer automatiquement BranchCache sur tous les partages, vous devez définir le mode de fonctionnement sur `all-shares`.

Étapes

1. SMB 2.1 et 3.0 si nécessaire :
   a. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
   b. Vérifier les paramètres du SVM SMB configurés pour déterminer si toutes les versions nécessaires de SMB sont activées : `vserver cifs options show -vserver` *`vserver_name`*

c. Si nécessaire, activez SMB 2.1 : `vserver cifs options modify -vserver vserver_name -smb2-enabled true`

   La commande active SMB 2.0 et SMB 2.1.

d. Si nécessaire, activez SMB 3.0 : `vserver cifs options modify -vserver vserver_name -smb3-enabled true`

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

2. Configurer BranchCache : `vserver cifs branchcache create -vserver vserver_name -hash -store-path path [-hash-store-max-size {integer[KB|MB|GB|TB|PB]}] [-versions {v1-enable|v2-enable|enable-all] [-server-key text] -operating-mode {per-share|all-shares}`

   Le chemin de stockage de hachage spécifié doit exister et doit résider sur un volume géré par la SVM. Le chemin doit également être situé sur un volume accessible en lecture-écriture. La commande échoue si le chemin d'accès est en lecture seule ou n'existe pas.

   Si vous souhaitez utiliser la même clé de serveur pour d'autres configurations de BranchCache du SVM, enregistrez la valeur que vous entrez pour la clé du serveur. La clé du serveur n'apparaît pas lorsque vous affichez des informations sur la configuration de BranchCache.

3. Vérifiez que la configuration de BranchCache est correcte : `vserver cifs branchcache show -vserver vserver_name`

Exemples

Les commandes suivantes vérifient que SMB 2.1 et 3.0 sont activées et configurent BranchCache pour activer automatiquement la mise en cache sur tous les partages SMB 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 show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
------- ------------ ------------
vs1     true         true


cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key" -operating-mode all-shares

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: all_shares
```

Les commandes suivantes vérifient que SMB 2.1 et 3.0 sont activées, configurent BranchCache pour permettre la mise en cache par partage sur le SVM vs1 et vérifient la configuration de BranchCache :

```
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 show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
------- ------------ ------------
vs1     true         true

cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key"

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Informations associées

Exigences et directives : prise en charge de la version de BranchCache

Où trouver des informations sur la configuration de BranchCache dans le bureau distant

Créez un partage SMB compatible BranchCache

Activez BranchCache sur un partage SMB existant

Modifier la configuration de BranchCache

Désactivez BranchCache sur les partages SMB

Supprimez la configuration de BranchCache sur les SVM

Où trouver des informations sur la configuration de BranchCache dans le bureau distant

Une fois BranchCache configuré sur le serveur SMB, vous devez installer et configurer BranchCache sur les ordinateurs clients et, éventuellement, sur les serveurs de mise en cache de votre bureau distant. Microsoft fournit des instructions pour configurer BranchCache dans le bureau distant.

Les instructions de configuration des clients des succursales et, éventuellement, des serveurs de mise en cache pour utiliser BranchCache sont disponibles sur le site Web Microsoft BranchCache.

"Microsoft BranchCache Docs : nouveautés"

Configurez des partages SMB compatibles avec BranchCache

Configurer les partages SMB compatibles avec BranchCache

Une fois que vous avez configuré BranchCache sur le serveur SMB et dans la succursale, vous pouvez activer BranchCache sur des partages SMB contenant du contenu que vous souhaitez autoriser les clients des succursales à mettre en cache.

La mise en cache de BranchCache peut être activée sur tous les partages SMB sur le serveur SMB ou sur la base du partage par partage.

- Si vous activez BranchCache sur le partage à partage, vous pouvez activer BranchCache pendant la création du partage ou en modifiant les partages existants.

  Si vous activez la mise en cache sur un partage SMB existant, ONTAP commence des hachages de calcul et envoie des métadonnées aux clients demandant du contenu dès que vous activez BranchCache sur ce partage.

- Les clients qui disposent d'une connexion SMB existante vers un partage n'bénéficient pas de la prise en charge de BranchCache si ce partage est ensuite activé.

  ONTAP annonce la prise en charge de BranchCache pour un partage au moment de la configuration de la session SMB. Les clients qui ont déjà établi des sessions lorsque BranchCache est activé doivent se déconnecter, puis se reconnecter pour utiliser le contenu mis en cache pour ce partage.

> Si BranchCache sur un partage SMB est ensuite désactivé, ONTAP arrête d'envoyer les métadonnées au client demandeur. Un client qui a besoin de données l'extrait directement du serveur de contenu (serveur SMB).

Créez un partage SMB compatible BranchCache

Vous pouvez activer BranchCache sur un partage SMB lors de la création du partage en configurant le `branchcache` propriété de partage.

Description de la tâche

- Si BranchCache est activé sur le partage SMB, le partage doit disposer de la configuration des fichiers hors ligne pour la mise en cache manuelle.

  Il s'agit du paramètre par défaut lorsque vous créez un partage.

- Vous pouvez également spécifier d'autres paramètres de partage facultatifs lorsque vous créez le partage avec BranchCache.
- Vous pouvez définir le `branchcache` Propriété sur un partage, même si BranchCache n'est pas configuré et activé sur le serveur virtuel de stockage (SVM).

  Toutefois, si vous souhaitez que le partage offre du contenu en cache, vous devez configurer et activer BranchCache sur le SVM.

- Puisqu'aucune propriété de partage par défaut n'est appliquée au partage lorsque vous utilisez le `-share -properties` paramètre, vous devez spécifier toutes les autres propriétés de partage que vous souhaitez appliquer au partage en plus de `branchcache` partager la propriété à l'aide d'une liste délimitée par des virgules.
- Pour plus d'informations, consultez la page de manuel du `vserver cifs share create` commande.

Étape

1. Création d'un partage SMB compatible avec BranchCache :
   `vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-share-properties branchcache[,…]`
2. Vérifiez que la propriété de partage BranchCache est définie sur le partage SMB à l'aide du `vserver cifs share show` commande.

Exemple

La commande suivante crée un partage SMB avec fonction de BranchCache nommé « data » avec le chemin d'accès de `/data` Sur la SVM vs1. Par défaut, le paramètre fichiers hors ligne est défini sur `manual`:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data -path
/data -share-properties branchcache,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name data
                      Vserver: vs1
                        Share: data
     CIFS Server NetBIOS Name: VS1
                         Path: /data
             Share Properties: branchcache
                               oplocks
                               browsable
                               changenotify
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: data
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Informations associées

Désactivation de BranchCache sur un partage SMB unique

Activez BranchCache sur un partage SMB existant

Vous pouvez activer BranchCache sur un partage SMB existant en ajoutant le `branchcache` partager la propriété dans la liste existante des propriétés de partage.

Description de la tâche

- Si BranchCache est activé sur le partage SMB, le partage doit disposer de la configuration des fichiers hors ligne pour la mise en cache manuelle.

  Si le paramètre fichiers hors ligne du partage existant n'est pas défini sur mise en cache manuelle, vous devez le configurer en modifiant le partage.

- Vous pouvez définir le `branchcache` Propriété sur un partage, même si BranchCache n'est pas configuré et activé sur le serveur virtuel de stockage (SVM).

  Toutefois, si vous souhaitez que le partage offre du contenu en cache, vous devez configurer et activer BranchCache sur le SVM.

- Lorsque vous ajoutez le `branchcache` la propriété de partage sur le partage, les paramètres de partage existants et les propriétés de partage sont conservés.

  La propriété de partage BranchCache est ajoutée à la liste existante des propriétés de partage. Pour plus d'informations sur l'utilisation du `vserver cifs share properties add` commandes, consultez les pages de manuels.

Étapes

1. Si nécessaire, configurez le paramètre de partage de fichiers hors ligne pour la mise en cache manuelle :
   a. Déterminez ce que le paramètre de partage de fichiers hors ligne est défini à l'aide de l' `vserver cifs share show` commande.
   b. Si le paramètre de partage de fichiers hors ligne n'est pas défini sur manuel, remplacez-le par la valeur requise : `vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files manual`
2. Activer BranchCache sur un partage SMB existant : `vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties branchcache`
3. Vérifiez que la propriété de partage BranchCache est définie sur le partage SMB : `vserver cifs share show -vserver vserver_name -share-name share_name`

Exemple

La commande suivante permet d'activer BranchCache sur un partage SMB existant nommé « data2 » avec le chemin d'accès de `/data2` Sur la SVM vs1 :

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
             Share Properties: oplocks
                               browsable
                               changenotify
                               showsnapshot
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share properties add  -vserver vs1 -share-name
data2 -share-properties branchcache

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
             Share Properties: oplocks
                               browsable
                               showsnapshot
                               changenotify
                               branchcache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Informations associées

Ajout ou suppression de propriétés de partage sur un partage SMB existant

Désactivation de BranchCache sur un partage SMB unique

Gestion et surveillance de la configuration de BranchCache

Modifier les configurations de BranchCache

Vous pouvez modifier la configuration du service de BranchCache sur les SVM, notamment la modification du chemin du répertoire du magasin de hachage, la taille maximale du répertoire, le mode de fonctionnement et les versions de BranchCache prises en charge. Vous pouvez également augmenter la taille du volume contenant le magasin de hachage.

Étapes

1. Effectuez l'action appropriée :

Les fonctions que vous recherchez…	Entrez les informations suivantes…
Modifier la taille du répertoire du magasin de hachage	`vserver cifs branchcache modify -vserver vserver_name -hash-store-max-size {integer[KB
MB	GB
TB	PB]}`
Augmentez la taille du volume contenant le magasin de hachage	`volume size -vserver vserver_name -volume volume_name -new-size new_size[k
m	g
t]` Si le volume contenant le magasin de hachage se remplit, vous pourrez peut-être augmenter la taille du volume. Vous pouvez spécifier la nouvelle taille du volume comme un nombre suivi d'une désignation d'unité. En savoir plus sur "Gestion des volumes FlexVol"	Modifiez le chemin du répertoire du magasin de hachage

Les fonctions que vous recherchez…	Entrez les informations suivantes…
`vserver cifs branchcache modify -vserver vserver_name -hash-store-path path -flush-hashes {true	false}` Si le SVM est une source de reprise d'activité du SVM, le chemin de hachage ne peut pas se trouver sur le volume root. En effet, le volume racine n'est pas répliqué vers la destination de reprise après incident. Le chemin de hachage BranchCache peut contenir des blancs et des caractères de nom de fichier valides. Si vous modifiez le chemin de hachage, `-flush -hashes` Est un paramètre requis qui spécifie si vous souhaitez que ONTAP affleure les hachages à partir de l'emplacement de magasin de hachage d'origine. Vous pouvez définir les valeurs suivantes pour le `-flush-hashes` paramètre : **Si vous spécifiez `true`, ONTAP supprime les hachages dans l'emplacement d'origine et crée de nouveaux hachages à l'emplacement du nouveau, car les nouvelles demandes sont effectuées par des clients compatibles BranchCache.** Si vous spécifiez `false`, les hachages ne sont pas vidés. + Dans ce cas, vous pouvez choisir de réutiliser les hachages existants ultérieurement en retrouvant le chemin du magasin de hachage à l'emplacement d'origine.
Changer le mode de fonctionnement	`vserver cifs branchcache modify -vserver vserver_name -operating-mode {per-share
all-shares	disable}` Lors de la modification du mode de fonctionnement, vous devez connaître les éléments suivants : **ONTAP annonce la prise en charge de BranchCache pour un partage lors de la configuration de la session SMB.** Les clients qui ont déjà établi des sessions lorsque BranchCache est activé doivent se déconnecter, puis se reconnecter pour utiliser le contenu mis en cache pour ce partage.
Modifier la prise en charge de BranchCache	`vserver cifs branchcache modify -vserver vserver_name -versions {v1-enable
v2-enable	enable-all}`

2. Vérifiez les modifications de configuration à l'aide de la `vserver cifs branchcache show` commande.

Affiche des informations sur les configurations de BranchCache

Vous pouvez afficher des informations sur les configurations de BranchCache sur les SVM (Storage Virtual machines), qui peuvent être utilisées lors de la vérification d'une configuration ou lors de la détermination des paramètres actuels avant de modifier une configuration.

Étape

1. Effectuez l'une des opérations suivantes :

Si vous voulez afficher…	Entrez cette commande…
Récapitulatif des informations sur les configurations de BranchCache sur tous les SVM	`vserver cifs branchcache show`
Informations détaillées sur la configuration d'un SVM spécifique	`vserver cifs branchcache show -vserver` *`vserver_name`*

Exemple

L'exemple suivant affiche des informations sur la configuration de BranchCache sur le SVM vs1 :

```
cluster1::> vserver cifs branchcache show -vserver vs1

                                 Vserver: vs1
            Supported BranchCache Versions: enable_all
                       Path to Hash Store: /hash_data
            Maximum Size of the Hash Store: 20GB
  Encryption Key Used to Secure the Hashes: -
         CIFS BranchCache Operating Modes: per_share
```

Changer la clé du serveur BranchCache

Il est possible de modifier la clé du serveur de BranchCache en modifiant la configuration de BranchCache sur le serveur virtuel de stockage (SVM) et en indiquant une clé de serveur différente.

Description de la tâche

Vous pouvez définir la clé du serveur à une valeur spécifique. Ainsi, si plusieurs serveurs fournissent des données de BranchCache pour les mêmes fichiers, les clients peuvent utiliser des hachages à partir de n'importe quel serveur à l'aide de la même clé de serveur.

Lorsque vous modifiez la clé du serveur, vous devez également vider le cache de hachage. Après avoir effectué des hachages, ONTAP crée des hachages de nouvelles demandes des clients compatibles avec BranchCache.

Étapes

1. Modifiez la clé du serveur à l'aide de la commande suivante : `vserver cifs branchcache modify`

```
-vserver vserver_name -server-key text -flush-hashes true
```

Lors de la configuration d'une nouvelle clé de serveur, vous devez également spécifier `-flush-hashes` et définissez la valeur sur `true`.

2. Vérifiez que la configuration de BranchCache est correcte à l'aide du `vserver cifs branchcache show` commande.

Exemple

L'exemple suivant définit une nouvelle clé de serveur qui contient des espaces et purge le cache de hachage sur la SVM vs1 :

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -server-key "new
vserver secret" -flush-hashes true

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Informations associées

Les raisons pour lesquelles ONTAP invalide des hachages de BranchCache

Des hachages de pré-calcul de BranchCache sur des chemins spécifiés

Vous pouvez configurer le service de BranchCache pour précalculer les hachages pour un seul fichier, un répertoire ou tous les fichiers d'une structure de répertoires. Cette fonctionnalité est utile pour calculer des hachages de données dans un partage de BranchCache pendant les heures creuses.

Description de la tâche

Si vous souhaitez collecter un échantillon de données avant d'afficher les statistiques de hachage, vous devez utiliser le `statistics start` et en option `statistics stop` commandes.

- Vous devez spécifier la machine virtuelle de stockage (SVM) et le chemin d'accès sur lequel vous souhaitez précalculer les hachages.
- Vous devez également indiquer si vous voulez que des hachages soient calculés de manière récursive.
- Si vous souhaitez calculer des hachages de façon récursive, le service BranchCache traverse l'intégralité de l'arborescence du répertoire sous le chemin spécifié et calcule des hachages pour chaque objet éligible.

Étapes

1. Des hachages de pré-calcul si vous le souhaitez :

Si vous voulez précalculer des hachages sur…	Entrez la commande…
Un seul fichier ou répertoire	`vserver cifs branchcache hash-create -vserver vserver_name -path path -recurse false`
Récursivement sur tous les fichiers d'une structure de répertoires	`vserver cifs branchcache hash-create -vserver vserver_name -path absolute_path -recurse true`

2. Vérifiez que des hachages sont calculés à l'aide de l' `statistics` commande :
   a. Affiche les statistiques du `hashd` Objet sur l'instance SVM souhaitée : `statistics show -object hashd -instance vserver_name`
   b. Vérifiez que le nombre de hachages créés augmente en répétant la commande.

Exemples

L'exemple suivant crée des hachages sur le chemin d'accès `/data` Et sur tous les fichiers et sous-répertoires contenus dans la SVM vs1 :

```
cluster1::> vserver cifs branchcache hash-create -vserver vs1 -path /data
-recurse true

cluster1::> statistics show -object hashd -instance vs1
Object: hashd
Instance: vs1
Start-time: 9/6/2012 19:09:54
End-time: 9/6/2012 19:11:15
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_created                                       85
    branchcache_hash_files_replaced                                 0
    branchcache_hash_rejected                                       0
    branchcache_hash_store_bytes                                    0
    branchcache_hash_store_size                                     0
    instance_name                                                 vs1
    node_name                                                   node1
    node_uuid
                                11111111-1111-1111-1111-111111111111
    process_name                                                    -

cluster1::> statistics show -object hashd -instance vs1
Object: hashd
Instance: vs1
Start-time: 9/6/2012 19:09:54
End-time: 9/6/2012 19:11:15
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_created                                       92
    branchcache_hash_files_replaced                                 0
    branchcache_hash_rejected                                       0
    branchcache_hash_store_bytes                                    0
    branchcache_hash_store_size                                     0
    instance_name                                                 vs1
    node_name                                                   node1
    node_uuid
                                11111111-1111-1111-1111-111111111111
    process_name                                                    -
```

Informations associées

"Configuration du contrôle des performances"

Des hachages à plat du magasin de hachage SVM BranchCache

Vous pouvez vider toutes les hachages en cache du magasin de hachage BranchCache sur la machine virtuelle de stockage (SVM). Cette fonction est utile si vous avez modifié la configuration de BranchCache du bureau de succursale. Par exemple, si vous avez récemment reconfiguré le mode de mise en cache de la mise en cache distribuée au mode de mise en cache hébergée, vous devrez vider le magasin de hachage.

Description de la tâche

Après avoir effectué des hachages, ONTAP crée des hachages de nouvelles demandes des clients compatibles avec BranchCache.

Étape

1. Rincez les hachages à partir du magasin de hachage BranchCache : `vserver cifs branchcache hash-flush -vserver` *`vserver_name`*

   ```
   vserver cifs branchcache hash-flush -vserver vs1
   ```

Afficher les statistiques de BranchCache

Vous pouvez afficher des statistiques de BranchCache, notamment, afin d'identifier le niveau de mise en cache efficace, déterminer si votre configuration fournit du contenu mis en cache aux clients et déterminer si les fichiers de hachage ont été supprimés pour prendre de l'espace pour les données de hachage les plus récentes.

Description de la tâche

Le `hashd` L'objet statistique contient des compteurs qui fournissent des informations statistiques sur les hachages de BranchCache. Le `cifs` L'objet statistique contient des compteurs qui fournissent des informations statistiques sur l'activité liée à BranchCache. Vous pouvez collecter et afficher les informations relatives à ces objets au niveau de privilège avancé.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`

   ```
   cluster1::> set -privilege advanced

   Warning: These advanced commands are potentially dangerous; use them
   only when directed to do so by support personnel.
   Do you want to continue? {y|n}: y
   ```

2. Afficher les compteurs liés à BranchCache à l'aide du `statistics catalog counter show` commande.

   Pour plus d'informations sur les compteurs de statistiques, reportez-vous à la page man de cette commande.

   ```
   cluster1::*> statistics catalog counter show -object hashd
   ```

```
Object: hashd
    Counter                     Description
    ---------------------------
----------------------------------------------
    branchcache_hash_created    Number of times a request to generate
                                BranchCache hash for a file succeeded.
    branchcache_hash_files_replaced
                                Number of times a BranchCache hash file
was
                                deleted to make room for more recent
hash
                                data. This happens if the hash store
size is
                                exceeded.
    branchcache_hash_rejected   Number of times a request to generate
                                BranchCache hash data failed.
    branchcache_hash_store_bytes
                                Total number of bytes used to store hash
data.
    branchcache_hash_store_size Total space used to store BranchCache
hash
                                data for the Vserver.
    instance_name               Instance Name
    instance_uuid               Instance UUID
    node_name                   System node name
    node_uuid                   System node id
9 entries were displayed.

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    ---------------------------
----------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    avg_junction_depth          Average number of junctions crossed by
SMB
                                and SMB2 path-based commands
    branchcache_hash_fetch_fail Total number of times a request to fetch
hash
```

```
                                 data failed. These are failures when
                                 attempting to read existing hash data.
It
                                 does not include attempts to fetch hash
data
                                 that has not yet been generated.
    branchcache_hash_fetch_ok   Total number of times a request to fetch
hash
                                 data succeeded.
    branchcache_hash_sent_bytes Total number of bytes sent to clients
                                 requesting hashes.
    branchcache_missing_hash_bytes
                                 Total number of bytes of data that had
to be
                                 read by the client because the hash for
that
                                 content was not available on the server.
   ....Output truncated....
```

3. Collectez les statistiques liées à BranchCache à l'aide du `statistics start` et `statistics stop` commandes.

```
cluster1::*> statistics start -object cifs -vserver vs1 -sample-id 11
Statistics collection is being started for Sample-id: 11

cluster1::*> statistics stop -sample-id 11
Statistics collection is being stopped for Sample-id: 11
```

4. Afficher les statistiques de BranchCache collectées à l'aide de `statistics show` commande.

```
cluster1::*> statistics show -object cifs -counter
branchcache_hash_sent_bytes -sample-id 11

Object: cifs
Instance: vs1
Start-time: 12/26/2012 19:50:24
End-time: 12/26/2012 19:51:01
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0

cluster1::*> statistics show -object cifs -counter
branchcache_missing_hash_bytes -sample-id 11

Object: cifs
Instance: vs1
Start-time: 12/26/2012 19:50:24
End-time: 12/26/2012 19:51:01
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
```

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

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

Informations associées

Affichage des statistiques

"Configuration du contrôle des performances"

Prise en charge des objets de stratégie de groupe BranchCache

ONTAP BranchCache prend en charge les objets de stratégie de groupe (GPO) de BranchCache, ce qui permet une gestion centralisée de certains paramètres de

configuration de BranchCache. Deux GPO sont utilisés pour BranchCache, la publication Hash pour BranchCache et la prise en charge de la version Hash pour BranchCache.

- **Publication Hash pour BranchCache**

  La publication Hash pour BranchCache de BranchCache correspond à `-operating-mode` paramètre. Lors des mises à jour de GPO, cette valeur est appliquée aux objets SVM (Storage Virtual machine) contenus dans l'unité organisationnelle à laquelle s'applique la stratégie de groupe.

- **Prise en charge de la version de hachage pour BranchCache**

  La prise en charge de la version de hachage pour BranchCache correspond au `-versions` paramètre. Lors des mises à jour de GPO, cette valeur est appliquée aux objets SVM contenus dans l'unité organisationnelle à laquelle la politique de groupe s'applique.

Informations associées

Application d'objets de stratégie de groupe aux serveurs CIFS

Affiche des informations sur les objets de stratégie de groupe BranchCache

Vous pouvez afficher des informations sur la configuration GPO (Group Policy Object) du serveur CIFS pour déterminer si des GPO de BranchCache sont définis pour le domaine auquel le serveur CIFS appartient et, le cas échéant, quels sont les paramètres autorisés. Vous pouvez également déterminer si les paramètres GPO de BranchCache sont appliqués au serveur CIFS.

Description de la tâche

Bien qu'un paramètre GPO soit défini au sein du domaine auquel le serveur CIFS appartient, il n'est pas nécessairement appliqué à l'unité organisationnelle contenant la machine virtuelle de stockage (SVM) compatible CIFS. Le paramètre GPO appliqué est le sous-ensemble de tous les GPO définis qui sont appliqués à la SVM compatible CIFS. Les paramètres BranchCache appliqués via les GPO remplacent les paramètres appliqués via l'interface CLI.

Étapes

1. Affichez le paramètre GPO de BranchCache défini pour le domaine Active Directory à l'aide du `vserver cifs group-policy show-defined` commande.

   Cet exemple n'affiche pas tous les champs de sortie disponibles pour la commande. La sortie est tronquée.

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1

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: version1
  [...]

    GPO Name: Resultant Set of Policy
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication for Mode BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]
```

2. Affichez le paramètre GPO de BranchCache appliqué au serveur CIFS à l'aide de `vserver cifs group-policy show-applied` commande. ``

> Cet exemple n'affiche pas tous les champs de sortie disponibles pour la commande. La sortie est tronquée.

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1

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: version1
  [...]

    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: version1
 [...]
```

Informations associées

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

Désactiver BranchCache sur les partages SMB

Désactivez BranchCache sur les partages SMB

Si vous ne souhaitez pas fournir de services de mise en cache de BranchCache sur certains partages SMB, mais que vous pouvez ensuite fournir des services de mise en cache, vous pouvez désactiver BranchCache sur le partage à partager. Si BranchCache est configuré pour assurer la mise en cache sur tous les partages, mais que vous souhaitez désactiver temporairement tous les services de mise en cache, vous pouvez modifier la configuration de BranchCache afin d'arrêter la mise en cache automatique sur tous les partages.

Si BranchCache sur un partage SMB est ensuite désactivé après son activation, ONTAP arrête d'envoyer les métadonnées au client qui demande. Client qui a besoin de données la récupère directement depuis le serveur

de contenu (serveur CIFS sur la machine virtuelle de stockage (SVM)).

Informations associées

Configuration de partages SMB compatibles avec BranchCache

Désactivez BranchCache sur un partage SMB unique

Si vous ne souhaitez pas offrir de services de mise en cache sur certains partages qui proposaient déjà du contenu en cache, vous pouvez désactiver BranchCache sur un partage SMB existant.

Étape

1. Saisissez la commande suivante : `vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties branchcache`

   La propriété de partage BranchCache est supprimée. Les autres propriétés de partage appliquées restent en vigueur.

Exemple

La commande suivante désactive BranchCache sur un partage SMB existant nommé « data2 » :

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
             Share Properties: oplocks
                               browsable
                               changenotify
                               attributecache
                               branchcache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
data2 -share-properties branchcache

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
             Share Properties: oplocks
                               browsable
                               changenotify
                               attributecache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Arrêt de la mise en cache automatique sur tous les partages SMB

Si votre configuration de BranchCache permet automatiquement la mise en cache de tous les partages SMB sur chaque serveur virtuel de stockage (SVM), vous pouvez modifier la configuration de BranchCache afin d'arrêter automatiquement la mise en cache du contenu pour tous les partages SMB.

Description de la tâche

Pour arrêter la mise en cache automatique sur tous les partages SMB, il est possible de basculer le mode d'exploitation de BranchCache vers la mise en cache par partage.

Étapes

1. Configurer BranchCache pour arrêter la mise en cache automatique sur tous les partages SMB : `vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share`
2. Vérifiez que la configuration de BranchCache est correcte : `vserver cifs branchcache show -vserver vserver_name`

Exemple

La commande suivante modifie la configuration de BranchCache sur le serveur de stockage virtuel (SVM, précédemment appelé vServer) vs1 pour arrêter la mise en cache automatique sur tous les partages SMB :

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
per-share

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Désactivation ou activation de BranchCache sur le SVM

Que se passe-t-il lorsque vous désactivez ou réactivez BranchCache sur le serveur CIFS

Si vous avez déjà configuré BranchCache, mais que vous ne souhaitez pas que les clients des succursales utilisent le contenu en cache, vous pouvez désactiver la mise en cache sur le serveur CIFS. Vous devez savoir ce qui se passe lorsque vous désactivez BranchCache.

Lorsque vous désactivez BranchCache, ONTAP ne calcule plus de hachages et n'envoie plus les métadonnées au client qui demande. Toutefois, l'accès aux fichiers n'est pas interrompu. Par la suite, lorsque des clients compatibles avec BranchCache demandent des informations de métadonnées pour le contenu auquel ils doivent accéder, ONTAP répond par une erreur définie par Microsoft, ce qui entraîne l'envoi d'une seconde demande par le client, demandant le contenu réel. En réponse à la demande de contenu, le serveur CIFS envoie le contenu réel stocké sur la machine virtuelle de stockage (SVM).

Une fois que BranchCache est désactivé sur le serveur CIFS, les partages SMB n'annoncent pas les fonctionnalités de BranchCache. Pour accéder aux données lors de nouvelles connexions SMB, les clients font des requêtes SMB en lecture standard.

Vous pouvez réactiver BranchCache sur le serveur CIFS à tout moment.

- Comme le magasin de hachage n'est pas supprimé lorsque vous désactivez BranchCache, ONTAP peut utiliser les hachages stockés pour répondre aux demandes de hachage après la réactivation de BranchCache, à condition que le hachage demandé soit toujours valide.
- Tout client qui a établi des connexions SMB vers des partages compatibles avec BranchCache au cours de la désactivation de BranchCache n'est pas pris en charge si BranchCache est ensuite réactivé.

  En effet, ONTAP annonce la prise en charge de BranchCache pour un partage au moment de la configuration de la session SMB. Les clients qui ont établi des sessions vers des partages compatibles BranchCache alors que ce dernier était désactivé doivent se déconnecter et se reconnecter pour utiliser le contenu en cache pour ce partage.

> Si vous ne souhaitez pas enregistrer le magasin de hachage après avoir désactivé BranchCache sur un serveur CIFS, vous pouvez le supprimer manuellement. Si vous réactivez BranchCache, vous devez vous assurer que le répertoire du magasin de hachage existe. Une fois que BranchCache est activé à nouveau, les partages compatibles avec BranchCache publicité des fonctionnalités de BranchCache. ONTAP crée de nouvelles hachages lorsque de nouvelles demandes sont faites par des clients compatibles avec BranchCache.

Désactiver ou activer BranchCache

Vous pouvez désactiver BranchCache sur le serveur virtuel de stockage (SVM) en changeant le mode d'exploitation BranchCache en `disabled`. Vous pouvez activer BranchCache à tout moment en modifiant le mode d'exploitation afin d'offrir soit des services de BranchCache par partage, soit automatiquement pour tous les partages.

Étapes

1. Exécutez la commande appropriée :

Les fonctions que vous recherchez…	Puis entrez les informations suivantes…
Désactivez BranchCache	`vserver cifs branchcache modify -vserver vserver_name -operating-mode disable`
Activez BranchCache par partage	`vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share`
Activez BranchCache pour tous les partages	`vserver cifs branchcache modify -vserver vserver_name -operating-mode all-shares`

2. Vérifiez que le mode de fonctionnement de BranchCache est configuré avec le paramètre souhaité : `vserver cifs branchcache show -vserver vserver_name`

Exemple

L'exemple suivant désactive BranchCache sur le SVM vs1 :

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
disable

cluster1::> vserver cifs branchcache show -vserver vs1

                                 Vserver: vs1
          Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: disable
```

Supprimez la configuration de BranchCache sur les SVM

Que se passe-t-il lorsque vous supprimez la configuration de BranchCache

Si vous avez déjà configuré BranchCache, mais que vous ne souhaitez pas que le serveur de stockage virtuel (SVM) puisse continuer à fournir du contenu en cache, vous pouvez supprimer la configuration de BranchCache sur le serveur CIFS. Vous devez connaître ce qui se passe lorsque vous supprimez la configuration.

Lorsque vous supprimez la configuration, ONTAP supprime du cluster les informations de configuration du SVM et arrête le service de BranchCache. Vous pouvez choisir si ONTAP doit supprimer le magasin de hachage sur la SVM.

La suppression de la configuration de BranchCache n'interrompt pas l'accès des clients compatibles avec BranchCache. Par la suite, lorsque les clients compatibles avec BranchCache demandent des informations de métadonnées sur les connexions SMB existantes pour du contenu déjà mis en cache, ONTAP répond par une erreur définie par Microsoft, ce qui entraîne l'envoi par le client d'une seconde demande, demandant le contenu réel. En réponse à la demande de contenu, le serveur CIFS envoie le contenu réel stocké sur le SVM

Une fois la configuration de BranchCache supprimée, les partages SMB n'annoncent pas les fonctionnalités de BranchCache. Pour accéder au contenu qui n'avait pas encore été mis en cache par de nouvelles connexions SMB, les clients effectuent des requêtes SMB en lecture standard.

Supprimez la configuration de BranchCache

La commande que vous utilisez pour supprimer le service de BranchCache sur le serveur de stockage virtuel (SVM) diffère selon que vous souhaitez supprimer ou conserver des hachages existants.

Étape

1. Exécutez la commande appropriée :

Les fonctions que vous recherchez…	Puis entrez les informations suivantes…
Supprimez la configuration de BranchCache et supprimez des hachages existants	`vserver cifs branchcache delete -vserver vserver_name -flush-hashes true`
Supprimez la configuration de BranchCache, mais conservez des hachages existants	`vserver cifs branchcache delete -vserver vserver_name -flush-hashes false`

Exemple

L'exemple suivant supprime la configuration de BranchCache sur le SVM vs1 et supprime toutes les hachages existants :

```
cluster1::> vserver cifs branchcache delete -vserver vs1 -flush-hashes
true
```

Utilisation de BranchCache lors du rétablissement

Il est important de comprendre ce qui se passe lorsque vous restaurez ONTAP vers une version qui ne prend pas en charge BranchCache.

- Lorsque vous restaurez vers une version d'ONTAP qui ne prend pas en charge BranchCache, les partages SMB n'publient pas de fonctionnalités de BranchCache pour les clients compatibles avec BranchCache. Ainsi, les clients ne demandent pas d'informations de hachage.

  À la place, ils demandent le véritable contenu à l'aide de demandes de lecture SMB normales. En réponse à la demande de contenu, le serveur SMB envoie le contenu réel qui est stocké sur la machine virtuelle de stockage (SVM).

- Lorsqu'un nœud qui héberge un magasin de hachage est rétabli dans une version qui ne prend pas en charge BranchCache, l'administrateur du stockage doit restaurer manuellement la configuration de BranchCache à l'aide d'une commande imprimée pendant la restauration.

  Cette commande supprime la configuration de BranchCache et des hachages.

  Une fois la restauration terminée, l'administrateur du stockage peut supprimer manuellement le répertoire qui contient le magasin de hachage si nécessaire.

Informations associées

Suppression de la configuration de BranchCache sur les SVM

Améliorez les performances de la copie à distance Microsoft

Améliorer les performances de copie à distance Microsoft

Microsoft Offloaded Data Transfer (ODX), également appelé *copy Offload*, permet le transfert direct de données au sein d'un périphérique de stockage compatible ou entre

ces périphériques, sans transférer les données via l'ordinateur hôte.

ONTAP prend en charge ODX à la fois pour les protocoles SMB et SAN. La source peut être un serveur CIFS ou une LUN et la destination peut être un serveur CIFS ou une LUN.

Dans les transferts de fichiers non ODX, les données sont lues à partir de la source et transférées sur le réseau vers l'ordinateur client. L'ordinateur client transfère les données via le réseau vers la destination. En résumé, l'ordinateur client lit les données à partir de la source et les écrit vers la destination. Grâce aux transferts de fichiers ODX, les données sont copiées directement de la source vers la destination.

Les copies déchargées d'ODX étant effectuées directement entre le stockage source et le stockage de destination, les performances sont considérablement améliorées. Les avantages obtenus en termes de performances comprennent l'accélération du délai de copie entre la source et la destination, la réduction de l'utilisation des ressources (CPU, mémoire) sur le client et la réduction de l'utilisation de la bande passante E/S du réseau.

Dans les environnements SMB, cette fonctionnalité n'est disponible que lorsque le client et le serveur de stockage prennent en charge SMB 3.0 et la fonctionnalité ODX. Dans les environnements SAN, cette fonctionnalité n'est disponible que lorsque le client et le serveur de stockage prennent en charge la fonctionnalité ODX. Les ordinateurs clients qui prennent en charge ODX et où ODX est activé automatiquement et de manière transparente utilisent le transfert de fichiers déchargées lors du déplacement ou de la copie des fichiers. ODX est utilisé par glisser-déposer des fichiers via l'Explorateur Windows ou utiliser des commandes de copie de fichier en ligne de commande, ou bien si une application client génère des demandes de copie de fichiers.

Informations associées

Amélioration des temps de réponse client en fournissant des référencements de nœuds automatiques SMB avec Auto Location

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

Fonctionnement d'ODX

L'allègement de la charge de copies (ODX) utilise un mécanisme basé sur des jetons pour la lecture et l'écriture des données dans et entre des serveurs CIFS compatibles avec ODX. Au lieu d'acheminer les données via l'hôte, le serveur CIFS envoie un petit jeton qui représente les données au client. Le client ODX présente ce token au serveur de destination, qui peut ensuite transférer les données représentées par ce token de la source vers la destination.

Lorsqu'un client ODX apprend que le serveur CIFS prend en charge ODX, il ouvre le fichier source et demande un jeton au serveur CIFS. Après l'ouverture du fichier de destination, le client utilise le jeton pour demander au serveur de copier les données directement de la source vers la destination.

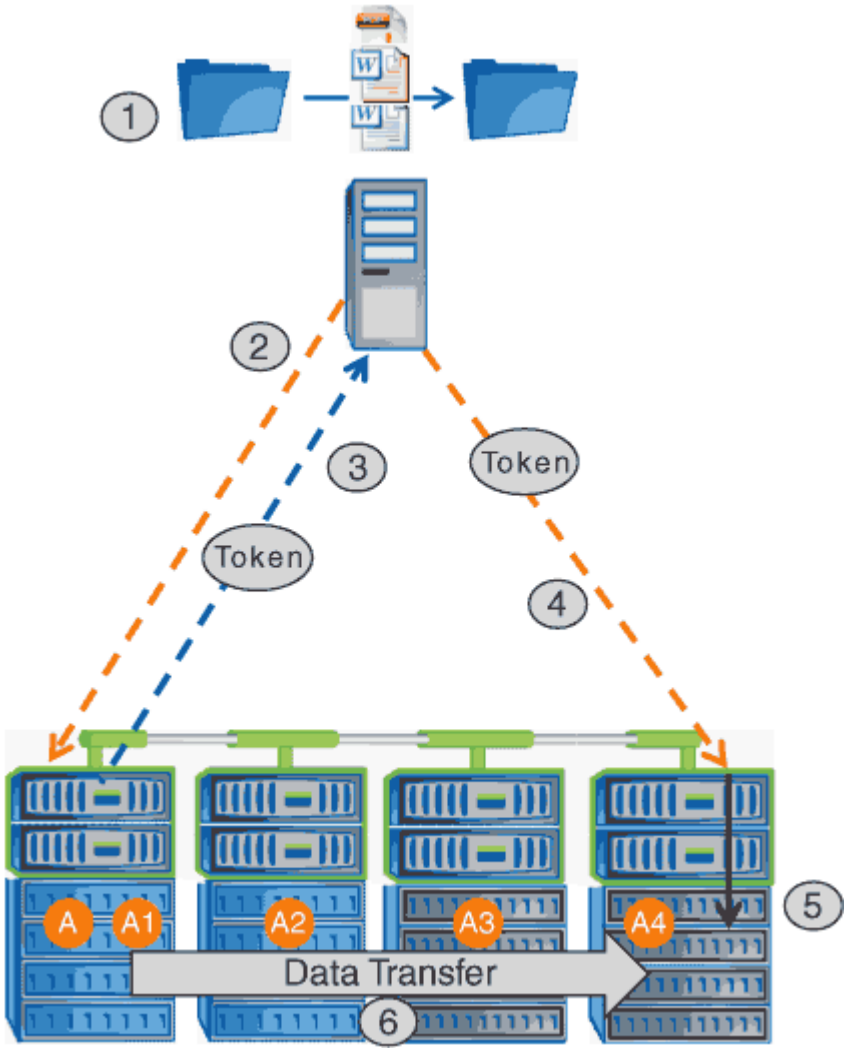
> La source et la destination peuvent se trouver sur le même SVM (Storage Virtual machine) ou sur différents SVM, selon le cadre de l'opération de copie.

Ce token sert de représentation des données à un point dans le temps. Par exemple, lorsque vous copiez des données entre des emplacements de stockage, un token représentant un segment de données est renvoyé au client requérant, que le client copie vers la destination, ce qui élimine la nécessité de copier les données sous-jacentes via le client.

ONTAP prend en charge les jetons représentant 8 Mo de données. Des copies ODX de plus de 8 Mo sont

effectuées à l'aide de plusieurs jetons, chaque jeton représentant 8 Mo de données.

La figure suivante décrit les étapes du processus de copie d'ODX :



1. Un utilisateur copie ou déplace un fichier à l'aide de l'Explorateur Windows, d'une interface de ligne de commande ou dans le cadre d'une migration d'un serveur virtuel, ou une application crée des copies ou des déplacements de fichiers.
2. Le client compatible ODX convertit automatiquement cette demande de transfert en requête d'ODX.

   La demande ODX envoyée au serveur CIFS contient une demande de jeton.

3. Si ODX est activé sur le serveur CIFS et que la connexion est via SMB 3.0, le serveur CIFS génère un jeton, qui est une représentation logique des données sur la source.
4. Le client reçoit un jeton représentant les données et l'envoie avec la demande d'écriture au serveur CIFS de destination.

   Il s'agit des seules données copiées sur le réseau de la source vers le client, puis du client vers la destination.

5. Ce jeton est fourni au sous-système de stockage.
6. La SVM effectue en interne la copie ou déplacement.

Si le fichier copié ou déplacé dépasse 8 Mo, plusieurs jetons sont nécessaires pour effectuer la copie. Les étapes 2 à 6 ont été effectuées selon les besoins pour compléter la copie.

> En cas de défaillance de la copie ODX déchargée, l'opération de copie ou de déplacement retourne aux lectures et écritures traditionnelles de la copie ou du déplacement. De même, si le serveur CIFS de destination ne prend pas en charge ODX ou ODX est désactivé, l'opération de copie ou de déplacement retourne aux opérations classiques de lecture et d'écriture pour la copie ou de déplacement.

Conditions requises pour l'utilisation d'ODX

Avant de pouvoir utiliser ODX pour la réduction des déchargements de copies avec votre machine virtuelle de stockage (SVM), vous devez prendre en compte certaines exigences.

Configuration requise pour la version ONTAP

Les versions d'ONTAP prennent en charge ODX pour la réduction des copies.

Conditions requises pour la version SMB

- ONTAP prend en charge ODX avec SMB 3.0 et versions ultérieures.
- SMB 3.0 doit être activé sur le serveur CIFS pour que ODX puisse être activé :
  - L'activation d'ODX active également SMB 3.0, si elle n'est pas déjà activée.
  - La désactivation de SMB 3.0 désactive également ODX.

Configuration requise pour le serveur et le client Windows

Avant de pouvoir utiliser ODX pour la réduction des tâches de copie, le client Windows doit prendre en charge cette fonctionnalité.

Le "Matrice d'interopérabilité NetApp"Contient les informations les plus récentes sur les clients Windows pris en charge.

Besoins en termes de volume

- Les volumes source doivent être d'au moins 1.25 Go.
- Si vous utilisez des volumes compressés, le type de compression doit être adaptatif et seule la taille de groupe de compression de 8 Ko est prise en charge.

  Le type de compression secondaire n'est pas pris en charge.

Instructions d'utilisation d'ODX

Avant de pouvoir utiliser ODX pour l'allègement de la charge des copies, vous devez prendre connaissance des instructions. Par exemple, vous devez connaître les types de volumes que vous pouvez utiliser ODX, et connaître les considérations d'ODX au sein du cluster et entre clusters.

Règles relatives aux volumes

- ODX ne peut pas être utilisé pour l'allègement de la charge des copies avec les configurations de volume suivantes :
  - La taille du volume source est inférieure à 1.25 Go

    La taille du volume doit être supérieure ou égale à 1.25 Go pour utiliser ODX.
  - Volumes en lecture seule

    ODX n'est pas utilisé pour les fichiers et les dossiers résidant dans des miroirs de partage de charge ou dans des volumes de destination SnapMirror ou SnapVault.
  - Si le volume source n'est pas dédupliqué
- Les copies ODX sont prises en charge uniquement pour les copies intra-cluster.

  Vous ne pouvez pas utiliser ODX pour copier des fichiers ou des dossiers vers un volume d'un autre cluster.

Autres lignes directrices

- Dans les environnements SMB, pour utiliser ODX pour l'allègement de la charge des copies, les fichiers doivent être d'une taille supérieure ou égale à 256 Ko.

  Les fichiers plus petits sont transférés à l'aide d'une opération de copie traditionnelle.
- La fonctionnalité de déchargement des copies d'ODX utilise la déduplication dans le cadre du processus de copie.

  Si vous ne souhaitez pas que la déduplication s'exécute sur les volumes SVM lors de la copie ou du déplacement de données, vous devez désactiver la décharge des copies ODX sur ce SVM.
- L'application qui effectue le transfert de données doit être écrite pour prendre en charge ODX.

  Les opérations applicatives prenant en charge ODX sont les suivantes :
  - Les opérations de gestion Hyper-V, telles que la création et la conversion de disques durs virtuels (VHD), la gestion des copies Snapshot et la copie de fichiers entre les machines virtuelles
  - Opérations de l'Explorateur Windows
  - Commandes de copie Windows PowerShell
  - Commandes de copie de l'invite de commande Windows

    Robocopy à l'invite de commandes Windows prend en charge ODX.

    > Les applications doivent être exécutées sur des serveurs Windows ou des clients prenant en charge ODX.

  + Pour plus d'informations sur les applications ODX prises en charge sur les serveurs et clients Windows, consultez la bibliothèque Microsoft TechNet.

Informations associées

"Bibliothèque Microsoft TechNet : technet.microsoft.com/en-us/library/"

Cas d'utilisation d'ODX

Vous devez tenir compte des cas d'utilisation d'ODX sur des SVM afin de pouvoir déterminer dans quelles circonstances ODX vous fournit des avantages en matière de performances.

Par défaut, les serveurs et clients Windows qui prennent en charge ODX utilisent la fonction d'allègement de la charge des copies pour copier des données sur des serveurs distants. Si le serveur ou le client Windows ne prend pas en charge ODX, ou si l'allègement de la charge des copies ODX échoue à tout moment, l'opération de copie ou de déplacement retourne aux lectures et écritures classiques pour la copie ou le déplacement.

Les cas d'utilisation suivants prennent en charge l'utilisation de copies et de déplacements d'ODX :

- Intra-volume

  Les fichiers ou LUN source et de destination se trouvent dans le même volume.

- Inter-volume, même nœud, même SVM

  Les fichiers ou LUN source et de destination se trouvent sur des volumes différents situés sur le même nœud. Les données sont détenues par le même SVM.

- Inter-volumes, nœuds différents, même SVM

  Les fichiers ou LUN source et de destination se trouvent sur des volumes différents situés sur des nœuds différents. Les données sont détenues par le même SVM.

- Inter-SVM, même nœud

  Les fichiers source et de destination ou les LUN se trouvent sur des volumes différents situés sur le même nœud. Les données sont détenues par différents SVM.

- Inter-SVM, nœuds différents

  Les fichiers ou LUN source et de destination se trouvent sur des volumes différents situés sur des nœuds différents. Les données sont détenues par différents SVM.

- Inter-cluster

  Les LUN source et de destination se trouvent sur des volumes différents, sur différents nœuds, sur l'ensemble des clusters. Ceci n'est pris en charge que pour SAN et ne fonctionne pas pour CIFS.

Il existe d'autres cas d'utilisation spéciaux :

- Dans l'implémentation de ONTAP ODX, vous pouvez utiliser ODX pour copier des fichiers entre des partages SMB et des disques virtuels connectés FC ou iSCSI.

  Vous pouvez utiliser Windows Explorer, l'interface de ligne de commande Windows ou PowerShell, Hyper-V ou d'autres applications prenant en charge ODX pour copier ou déplacer des fichiers de manière transparente à l'aide de l'allègement de la charge des copies ODX entre les partages SMB et les LUN connectés, à condition que les partages SMB et les LUN soient sur le même cluster.

- Hyper-V fournit des cas d'utilisation supplémentaires pour la décharge de copies ODX :

  - Vous pouvez utiliser le pass-through ODX qui décharge les copies et Hyper-V pour copier des données

dans ou sur des fichiers de disque dur virtuel (VHD), ou pour copier des données entre les partages SMB mappés et les LUN iSCSI connectés au sein du même cluster.

Ainsi, des copies des systèmes d'exploitation invités peuvent être transmis au stockage sous-jacent.

- Lors de la création de VHD de taille fixe, ODX permet d'initialiser le disque avec des zéros, à l'aide d'un jeton bien connu mis à zéro.
- L'allègement de la charge des copies d'ODX est utilisé pour la migration du stockage de machines virtuelles si le stockage source et cible est situé sur le même cluster.

> Pour tirer parti des cas d'utilisation liés au délestage des copies ODX par Hyper-V, le système d'exploitation invité doit prendre en charge ODX. Les disques du système d'exploitation invité doivent être des disques SCSI pris en charge par le stockage (SMB ou SAN) prenant en charge ODX. Les disques IDE du système d'exploitation invité ne prennent pas en charge le pass-through ODX.

Activer ou désactiver ODX

Vous pouvez activer ou désactiver ODX sur des SVM. Par défaut, est d'activer la prise en charge de l'allègement de la charge des copies (ODX) si SMB 3.0 est également activé.

Avant de commencer

SMB 3.0 doit être activé.

Description de la tâche

Si vous désactivez SMB 3.0, ONTAP désactive également SMB ODX. Si vous réactivez SMB 3.0, vous devez réactiver manuellement SMB ODX.

Étapes

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

Si vous voulez que l'allègement de la charge des copies ODX soit…	Entrez la commande…
Activé	`vserver cifs options modify -vserver vserver_name -copy-offload-enabled true`
Désactivé	`vserver cifs options modify -vserver vserver_name -copy-offload-enabled false`

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

Exemple

L'exemple suivant active la décharge de la copie ODX 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 -copy-offload
-enabled true

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

Informations associées

Options de serveur SMB disponibles

Améliorer le temps de réponse des clients en fournissant des référencements de nœuds automatiques SMB avec Auto Location

Améliorer le temps de réponse des clients en fournissant des référencements de nœuds automatiques SMB avec vue d'ensemble de l'emplacement automatique

Auto Location utilise les référencements automatiques des nœuds SMB pour augmenter les performances des clients SMB sur les machines virtuelles de stockage (SVM). Les référencements automatiques du nœud reconnectent automatiquement le client demandeur à une LIF sur le SVM du nœud qui héberge le volume dans lequel résident les données, ce qui peut améliorer les temps de réponse du client.

Lorsqu'un client SMB se connecte à un partage SMB hébergé sur le SVM, il peut se connecter à l'aide d'une LIF qui se trouve sur un nœud qui ne possède pas les données demandées. Le nœud auquel le client est connecté accède aux données détenues par un autre nœud via le réseau de cluster. Le client peut bénéficier de temps de réponse plus rapides si la connexion SMB utilise une LIF située sur le nœud contenant les données demandées :

- ONTAP fournit cette fonctionnalité à l'aide des référencements Microsoft DFS pour informer les clients SMB qu'un fichier ou dossier demandé dans l'espace de noms est hébergé quelque part.

  Un nœud fait une recommandation lorsqu'il détermine qu'il existe une LIF de SVM sur le nœud qui contient les données.

- Les référencements de nœuds automatiques sont pris en charge pour les adresses IP LIF IPv4 et IPv6.
- Les renvois sont effectués en fonction de l'emplacement de la racine du partage auquel le client est connecté.
- Le renvoi se produit pendant la négociation avec les PME.

  Le renvoi est effectué avant l'établissement de la connexion. Après que ONTAP désigne le client SMB au nœud cible, la connexion est établie et le client accède aux données via le chemin LIF référencé à partir de ce point. Les clients accèdent ainsi plus rapidement aux données et évitent toute communication supplémentaire avec le cluster.

> Si un partage couvre plusieurs points de jonction et que certaines des jonctions sont vers les volumes contenus sur les autres nœuds, les données du partage sont réparties sur plusieurs nœuds. Étant donné que ONTAP fournit des référencements locaux à la racine du partage, ONTAP doit utiliser le réseau cluster pour récupérer les données contenues dans ces volumes non locaux. Avec ce type d'architecture de namespace, les référencements automatiques des nœuds ne peuvent pas être significatifs pour les performances.

Si le nœud qui héberge les données ne dispose pas de LIF disponible, ONTAP établit la connexion en utilisant la LIF choisie par le client. Une fois qu'un fichier est ouvert par un client SMB, il continue à accéder au fichier via la même connexion référencée.

Si, pour une raison quelconque, le serveur CIFS ne peut pas faire de recommandation, le service SMB ne subit aucune perturbation. La connexion SMB est établie comme si les référencements de nœuds automatiques n'étaient pas activés.

Informations associées

Amélioration des performances de la copie à distance Microsoft

Exigences et directives pour l'utilisation de référencements de nœuds automatiques

Avant de pouvoir utiliser les référencements de nœud automatiques SMB, également appelés *autolocalisation*, vous devez connaître certaines exigences, y compris les versions de ONTAP qui prennent en charge la fonctionnalité. Vous devez également connaître les versions du protocole SMB prises en charge et d'autres directives spéciales.

Version ONTAP et conditions requises pour les licences

- Tous les nœuds du cluster doivent exécuter une version de ONTAP qui prend en charge les référencements de nœuds automatiques.
- Les Widelinks doivent être activés sur un partage SMB pour utiliser l'autolocalisation.
- CIFS doit être sous licence et un serveur SMB doit exister sur les SVM. La licence SMB est incluse avec "ONTAP One". Si vous n'avez pas ONTAP One et que la licence n'est pas installée, contactez votre ingénieur commercial.

Version requise du protocole SMB

- Pour les SVM, ONTAP prend en charge les référencements de nœuds automatiques sur toutes les versions de SMB.

Exigences des clients PME

Tous les clients Microsoft pris en charge par ONTAP prennent en charge les référencements automatiques des nœuds SMB.

La matrice d'interopérabilité contient les dernières informations sur les clients Windows pris en charge par ONTAP.

"Matrice d'interopérabilité NetApp"

Configuration requise pour Data LIF

Si vous souhaitez utiliser une LIF de données comme référence potentielle pour les clients SMB, vous devez créer des LIF de données avec NFS et CIFS activés.

Les référencements de nœuds automatiques peuvent ne fonctionner que si le nœud cible contient des LIFs de données qui sont activées uniquement pour le protocole NFS ou uniquement pour le protocole SMB.

Si cette exigence n'est pas respectée, l'accès aux données n'est pas affecté. Le client SMB mappe le partage à l'aide de la LIF d'origine que le client a utilisée pour se connecter à la SVM.

Exigences d'authentification NTLM lors de la connexion SMB référencée

L'authentification NTLM doit être autorisée sur le domaine contenant le serveur CIFS et sur les domaines contenant des clients qui souhaitent utiliser des référencements de nœud automatiques.

Lors d'une recommandation, le serveur SMB renvoie une adresse IP au client Windows. Étant donné que l'authentification NTLM est utilisée lors de la connexion à l'aide d'une adresse IP, l'authentification Kerberos n'est pas réalisée pour les connexions mentionnées.

Cela se produit car le client Windows ne peut pas créer le nom principal de service utilisé par Kerberos (qui est de la forme `service/NetBIOS name` et `service/FQDN`), ce qui signifie que le client ne peut pas demander un ticket Kerberos au service.

Instructions pour l'utilisation de renvois de nœuds automatiques avec la fonction home Directory

Lorsque les partages sont configurés avec la propriété de partage de répertoire personnel activée, il peut y avoir un ou plusieurs chemins de recherche de répertoire racine configurés pour une configuration de répertoire personnel. Les chemins de recherche peuvent pointer vers les volumes contenus dans chaque nœud contenant des volumes du SVM. Les clients reçoivent une recommandation et, si une LIF de données locale active est disponible, connectez-vous via une LIF référencée qui est locale au home Directory de l'utilisateur.

Il existe des directives lorsque les clients SMB 1.0 accèdent aux home directories dynamiques avec l'activation automatique des référencements de nœuds. En effet, les clients SMB 1.0 nécessitent le renvoi automatique de nœud avant d'avoir été authentifiés, c'est-à-dire avant que le serveur SMB ait le nom de l'utilisateur. Cependant, l'accès au répertoire local SMB fonctionne correctement pour les clients SMB 1.0 si les instructions suivantes sont vraies :

- Les répertoires locaux SMB sont configurés pour utiliser des noms simples, tels que "%W" (nom d'utilisateur Windows) ou "%u" (nom d'utilisateur UNIX mappé), et non des noms de style de nom de domaine, tels que "`%d\%W `" (nom-domaine\nom-utilisateur).
- Lors de la création de partages de répertoires locaux CIFS, les noms de partages de répertoire racine CIFS sont configurés avec des variables ("`%W'" ou "`%u'"), et non avec des noms statiques, tels que ""HOME"".

Pour les clients SMB 2.x et SMB 3.0, il n'y a pas de directives spéciales lors de l'accès aux répertoires locaux en utilisant des référencements de nœuds automatiques.

Instructions relatives à la désactivation des référencements de nœuds automatiques sur les serveurs CIFS avec les connexions existantes désignées

Si vous désactivez les référencements de nœuds automatiques après l'activation de l'option, les clients actuellement connectés à une LIF référencée conservent la connexion référencée. Étant donné que ONTAP utilise les référencements DFS comme mécanisme pour les référencements automatiques des nœuds SMB,

les clients peuvent même se reconnecter au LIF référencé après que vous avez désactivé l'option jusqu'à ce que le renvoi DFS mis en cache du client pour les connexions mentionnées soit trop court. Cela est vrai même dans le cas d'une restauration vers une version de ONTAP qui ne prend pas en charge les référencements de nœuds automatiques. Les clients continuent d'utiliser les référencements jusqu'à ce que la référence DFS soit hors du cache du client.

La géolocalisation automatique utilise les référencements automatiques des nœuds SMB pour augmenter les performances des clients SMB en orientant les clients vers la LIF sur le nœud qui possède le volume de données d'un SVM. Lorsqu'un client SMB se connecte à un partage SMB hébergé sur un SVM, il peut se connecter à l'aide d'une LIF sur un nœud qui ne détient pas les données demandées et utilise un réseau d'interconnexion de cluster pour récupérer les données. Le client peut bénéficier de temps de réponse plus rapides si la connexion SMB utilise une LIF située sur le nœud contenant les données demandées.

ONTAP fournit cette fonctionnalité à l'aide des référencements DFS (système de fichiers distribués Microsoft) pour informer les clients SMB qu'un fichier ou dossier demandé dans l'espace de noms est hébergé quelque part. Un nœud fait une recommandation lorsqu'il détermine qu'il existe une LIF de SVM sur le nœud qui contient les données. Les renvois sont effectués en fonction de l'emplacement de la racine du partage auquel le client est connecté.

Le renvoi se produit pendant la négociation avec les PME. Le renvoi est effectué avant l'établissement de la connexion. Après que ONTAP désigne le client SMB au nœud cible, la connexion est établie et le client accède aux données via le chemin LIF référencé à partir de ce point. Les clients accèdent ainsi plus rapidement aux données et évitent toute communication supplémentaire avec le cluster.

Instructions pour l'utilisation de renvois de nœuds automatiques avec des clients Mac OS

Les clients Mac OS X ne prennent pas en charge les renvois de nœuds automatiques SMB, même si le système d'exploitation Mac prend en charge le système de fichiers distribué (DFS, Distributed File System) de Microsoft. Les clients Windows effectuent une demande de recommandation DFS avant de se connecter à un partage SMB. ONTAP fournit une référence à une LIF de données située sur le même nœud qui héberge les données requises, ce qui entraîne une amélioration des temps de réponse du client. Bien que le système d'exploitation Mac prend en charge DFS, les clients Mac OS ne se comportent pas exactement comme les clients Windows dans cette zone.

Informations associées

Comment ONTAP rend possible les répertoires locaux dynamiques

"Gestion du réseau"

"Matrice d'interopérabilité NetApp"

Prise en charge des référencements automatiques des nœuds SMB

Avant d'activer les référencements automatiques des nœuds SMB, sachez que certaines fonctionnalités ONTAP ne prennent pas en charge les référencements.

- Les types de volumes suivants ne prennent pas en charge les référencements automatiques des nœuds SMB :
  - Membres en lecture seule d'un miroir de partage de charge
  - Volume de destination d'un miroir de protection des données
- Les référencements des nœuds ne bougent pas parallèlement à un déplacement LIF.

  Lorsqu'un client utilise une connexion référencée sur une connexion SMB 2.x ou SMB 3.0 et qu'une LIF de

données se déplace sans interruption, le client continue d'utiliser la même connexion référencée, même si la LIF n'est plus locale des données.

- Les référencements de nœuds ne se déplacent pas parallèlement à un déplacement des volumes.

  Lorsqu'un client utilise une connexion référencée sur une connexion SMB et qu'un déplacement de volume se produit, le client continue à utiliser la même connexion référencée, même si le volume n'est plus situé sur le même nœud que la LIF de données.

Activez ou désactivez les référencements automatiques des nœuds SMB

Vous pouvez activer les référencements automatiques des nœuds SMB pour augmenter les performances d'accès des clients SMB. Vous pouvez désactiver les référencements automatiques des nœuds si vous ne souhaitez pas que ONTAP fait des référencements aux clients SMB.

Avant de commencer

Un serveur CIFS doit être configuré et exécuté sur la machine virtuelle de stockage (SVM).

Description de la tâche

La fonctionnalité de référencements automatiques des nœuds SMB est désactivée par défaut. Vous pouvez activer ou désactiver cette fonctionnalité sur chaque SVM si nécessaire.

Cette option est disponible au niveau de privilège avancé.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Activez ou désactivez les référencements automatiques des nœuds SMB si nécessaire :

Si vous voulez que les référencements automatiques des nœuds SMB soient…	Saisissez la commande suivante…
Activé	`vserver cifs options modify -vserver vserver_name -is-referral-enabled true`
Désactivé	`vserver cifs options modify -vserver vserver_name -is-referral-enabled false`

   Le paramètre d'option prend effet pour les nouvelles sessions SMB. Les clients ayant une connexion existante ne peuvent utiliser la référence de nœud que lorsque leur délai d'expiration de cache existant expire.

3. Basculer vers le niveau de privilège admin : `set -privilege admin`

Informations associées

Options de serveur SMB disponibles

Utilisez les statistiques pour surveiller l'activité de renvoi automatique des nœuds

Pour déterminer le nombre de connexions SMB mentionnées, vous pouvez surveiller l'activité de renvoi automatique des nœuds à l'aide du `statistics` commande. En surveillant les référencements, vous pouvez déterminer dans quelle mesure les référencements automatiques localise des connexions sur des nœuds hébergeant les partages et si vous devez redistribuer vos LIFs de données pour fournir un meilleur accès local aux partages sur le serveur CIFS.

Description de la tâche

Le `cifs` Objet fournit plusieurs compteurs au niveau de privilèges avancés qui sont utiles lors du suivi des référencements automatiques des nœuds SMB :

- `node_referral_issued`

  Nombre de clients ayant été aiguillage vers le nœud racine du partage après que le client ait connecté via une LIF hébergée par un nœud différent du nœud racine du partage.

- `node_referral_local`

  Nombre de clients connectés via une LIF hébergée par le même nœud qui héberge la racine du partage. L'accès local offre généralement des performances optimales.

- `node_referral_not_possible`

  Nombre de clients qui n'ont pas été aiguillage vers le nœud hébergeant la racine du partage après connexion à une LIF hébergée par un nœud différent du nœud racine du partage. En effet, une LIF de données actives pour le nœud racine du partage n'a pas été trouvée.

- `node_referral_remote`

  Nombre de clients connectés via une LIF hébergée par un nœud différent du nœud qui héberge la racine du partage. L'accès à distance peut affecter les performances.

Vous pouvez surveiller les statistiques de référence automatique des nœuds sur votre SVM en collectant et en affichant les données d'une période donnée (échantillon). Vous pouvez afficher les données de l'échantillon si vous n'arrêtez pas la collecte de données. L'arrêt de la collecte de données vous donne un échantillon fixe. L'option ne pas arrêter la collecte de données vous permet d'obtenir des données mises à jour que vous pouvez utiliser pour comparer à des requêtes précédentes. La comparaison peut vous aider à identifier les tendances en matière de performances.

> Pour évaluer et utiliser les informations que vous recueillez à partir du `statistics` command, vous devez comprendre la distribution des clients dans vos environnements.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Afficher les statistiques de référence de nœud automatique à l'aide du `statistics` commande.

   Cet exemple affiche les statistiques d'aiguillage automatique des nœuds en recueillant et en visualisant les données d'une période d'échantillonnage :

a. Lancez la collection : `statistics start -object cifs -instance vs1 -sample-id sample1`

```
Statistics collection is being started for Sample-id: sample1
```

b. Attendez que le délai de collecte souhaité s'écoule.

c. Arrêter la collection : `statistics stop -sample-id sample1`

```
Statistics collection is being stopped for Sample-id: sample1
```

d. Afficher les statistiques de référence automatique des nœuds : `statistics show -sample-id sample1 -counter` **`node`**

```
Object: cifs
Instance: vs1
Start-time: 2/4/2013 19:27:02
End-time: 2/4/2013 19:30:11
Cluster: cluster1

    Counter                                                  Value
    ---------------------------- ---------------------------
    node_name                                               node1
    node_referral_issued                                        0
    node_referral_local                                         1
    node_referral_not_possible                                  2
    node_referral_remote                                        2
    ...

    node_name                                               node2
    node_referral_issued                                        2
    node_referral_local                                         1
    node_referral_not_possible                                  0
    node_referral_remote                                        2
    ...
```

Le résultat affiche des compteurs pour tous les nœuds participant au SVM vs1. Pour plus de clarté, seuls les champs de sortie liés aux statistiques de renvoi automatique de nœud sont fournis dans l'exemple.

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

Informations associées

Affichage des statistiques

"Configuration du contrôle des performances"

Surveiller les informations de renvoi automatique de nœud SMB côté client à l'aide d'un client Windows

Pour déterminer les références faites du point de vue du client, vous pouvez utiliser Windows `dfsutil.exe` informatique.

Le kit Remote Server Administration Tools (RSAT) disponible avec les clients Windows 7 et versions ultérieures contient le `dfsutil.exe` informatique. Cet utilitaire vous permet d'afficher des informations sur le contenu du cache de référence ainsi que des informations sur chaque référence que le client utilise actuellement. Vous pouvez également utiliser l'utilitaire pour effacer le cache de référence du client. Pour plus d'informations, consultez la bibliothèque Microsoft TechNet.

Informations associées

"Bibliothèque Microsoft TechNet : technet.microsoft.com/en-us/library/"

Sécurité des dossiers sur les partages dotés d'une énumération basée sur l'accès

Assurez la sécurité des dossiers sur les partages dotés d'une vue d'ensemble de l'énumération basée sur l'accès

Lorsque l'énumération basée sur l'accès (ABE) est activée sur un partage SMB, les utilisateurs qui n'ont pas l'autorisation d'accéder à un dossier ou un fichier contenu dans le partage (que ce soit par le biais de restrictions d'autorisation individuelles ou de groupe) ne voient pas cette ressource partagée affichée dans leur environnement, bien que le partage lui-même reste visible.

Les propriétés de partage conventionnelles vous permettent de spécifier quels utilisateurs (individuellement ou en groupes) ont l'autorisation d'afficher ou de modifier les fichiers ou dossiers contenus dans le partage. Cependant, elles ne vous permettent pas de contrôler si les dossiers ou les fichiers contenus dans le partage sont visibles pour les utilisateurs qui ne disposent pas de l'autorisation d'y accéder. Cela peut poser des problèmes si les noms de ces dossiers ou fichiers dans le partage décrivent des informations sensibles, telles que les noms des clients ou des produits en cours de développement.

L'énumération basée sur l'accès (ABE) étend les propriétés de partage pour inclure l'énumération des fichiers et dossiers dans le partage. ABE vous permet donc de filtrer l'affichage des fichiers et dossiers dans le partage en fonction des droits d'accès des utilisateurs. C'est-à-dire que le partage lui-même est visible pour tous les utilisateurs, mais les fichiers et les dossiers du partage peuvent être affichés ou masqués par les utilisateurs désignés. En plus de protéger les informations sensibles sur votre lieu de travail, ABE vous permet de simplifier l'affichage de grandes structures de répertoires pour le bénéfice des utilisateurs qui n'ont pas besoin d'accéder à toute votre gamme de contenus. Par exemple, le partage lui-même est visible pour tous les utilisateurs, mais les fichiers et dossiers du partage peuvent être affichés ou masqués.

Découvrez "Impact sur les performances lors de l'utilisation d'une énumération basée sur SMB/CIFS".

Activez ou désactivez l'énumération basée sur l'accès pour les partages SMB

Vous pouvez activer ou désactiver l'énumération basée sur l'accès (ABE) sur les partages SMB afin d'autoriser ou d'empêcher les utilisateurs de voir les ressources partagées qu'ils ne disposent pas des autorisations d'accès.

Description de la tâche

Par défaut, ABE est désactivé.

Étapes

1. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Entrez la commande…
Activer ABE sur un nouveau partage	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties access-based-enumeration` Vous pouvez spécifier des paramètres de partage facultatifs supplémentaires et d'autres propriétés de partage lorsque vous créez un partage SMB. Pour plus d'informations, consultez la page de manuel du `vserver cifs share create` commande.
Activer ABE sur un partage existant	`vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties access-based-enumeration` Les propriétés de partage existantes sont conservées. La propriété partage ABE est ajoutée à la liste existante des propriétés de partage.
Désactivez ABE sur un partage existant	`vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties access-based-enumeration` Les autres propriétés de partage sont conservées. Seule la propriété partage ABE est supprimée de la liste des propriétés de partage.

2. Vérifiez que la configuration du partage est correcte à l'aide du `vserver cifs share show` commande.

Exemples

L'exemple suivant crée un partage ABE SMB nommé "sales" avec un chemin de `/sales` Sur la SVM vs1. Le partage est créé avec `access-based-enumeration` en tant que propriété de partage :

```
cluster1::> vserver cifs share create -vserver vs1 -share-name sales -path
/sales  -share-properties access-based-
enumeration,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name sales

                      Vserver: vs1
                        Share: sales
     CIFS Server NetBIOS Name: VS1
                         Path: /sales
             Share Properties: access-based-enumeration
                               oplocks
                               browsable
                               changenotify
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

L'exemple suivant ajoute le `access-based-enumeration` Partagez la propriété dans un partage SMB nommé "data2":

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
data2 -share-properties access-based-enumeration

cluster1::> vserver cifs share show -vserver vs1 -share-name data2 -fields
share-name,share-properties
server  share-name share-properties
------- ---------- ----------------------------------------------------
vs1     data2      oplocks,browsable,changenotify,access-based-enumeration
```

Informations associées

Ajout ou suppression de propriétés de partage sur un partage SMB existant

Activez ou désactivez l'énumération basée sur l'accès à partir d'un client Windows

Vous pouvez activer ou désactiver l'énumération basée sur l'accès (ABE) sur des partages SMB à partir d'un client Windows, ce qui vous permet de configurer ce paramètre de partage sans avoir à vous connecter au serveur CIFS.

Le `abecmd` Utilitaire non disponible dans les nouvelles versions de Windows Server et des clients Windows. Elle a été publiée dans le cadre de Windows Server 2008. Le support de Windows Server 2008 a pris fin le 14 janvier 2020.

Étapes

1. À partir d'un client Windows prenant en charge ABE, entrez la commande suivante : `abecmd [/enable | /disable] [/server CIFS_server_name] {/all | share_name}`

   Pour plus d'informations sur le `abecmd` Consultez la documentation de votre client Windows.

Dépendances de nommage des fichiers et des répertoires NFS et SMB

Présentation des dépendances de nommage des fichiers et des répertoires NFS et SMB

Les conventions d'appellation des fichiers et des répertoires dépendent à la fois des systèmes d'exploitation des clients réseau et des protocoles de partage de fichiers, en plus des paramètres de langue sur le cluster ONTAP et les clients.

Le système d'exploitation et les protocoles de partage de fichiers déterminent ce qui suit :

- Caractères un nom de fichier peut utiliser
- Sensibilité à la casse d'un nom de fichier

ONTAP prend en charge les caractères multi-octets dans les noms de fichier, de répertoire et de qtree, en fonction de la version de ONTAP utilisée.

Caractères un nom de fichier ou de répertoire peut utiliser

Si vous accédez à un fichier ou à un répertoire à partir de clients ayant différents systèmes d'exploitation, vous devez utiliser des caractères valides dans les deux systèmes d'exploitation.

Par exemple, si vous utilisez UNIX pour créer un fichier ou un répertoire, n'utilisez pas de deux-points (:) dans le nom car le deux-points n'est pas autorisé dans les noms de fichiers ou de répertoires MS-DOS. Comme les restrictions sur les caractères valides varient d'un système d'exploitation à l'autre, consultez la documentation de votre système d'exploitation client pour plus d'informations sur les caractères interdits.

Sensibilité à la casse des noms de fichiers et de répertoires dans un environnement multiprotocole

Les noms de fichiers et de répertoires sont sensibles à la casse pour les clients NFS et non sensibles à la casse, mais ils préservent la casse pour les clients SMB. Vous devez comprendre les implications dans un environnement multiprotocole et les actions nécessaires lorsque vous spécifiez le chemin lors de la création des partages SMB et lors de l'accès aux données au sein des partages.

Si un client SMB crée un répertoire nommé `testdir`, Les clients SMB et NFS affichent le nom de fichier comme `testdir`. Toutefois, si un utilisateur SMB tente par la suite de créer un nom de répertoire `TESTDIR`, Le nom n'est pas autorisé car, pour le client SMB, ce nom existe actuellement. Si un utilisateur NFS crée par la suite un répertoire nommé `TESTDIR`, Les clients NFS et SMB affichent le nom du répertoire différemment, comme suit :

- Sur les clients NFS, vous voyez les deux noms de répertoire tels qu'ils ont été créés, par exemple `testdir` et `TESTDIR`, car les noms de répertoire sont sensibles à la casse.
- Les clients SMB utilisent les 8.3 noms pour faire la distinction entre les deux répertoires. Un répertoire porte le nom du fichier de base. Un nom de fichier 8.3 est attribué aux répertoires supplémentaires.
  - Sur les clients SMB, vous voyez `testdir` et `TESTDI~1`.
  - ONTAP crée le `TESTDI~1` nom du répertoire pour différencier les deux répertoires.

    Dans ce cas, vous devez utiliser le nom 8.3 lorsque vous spécifiez un chemin de partage lors de la création ou de la modification d'un partage sur un SVM (Storage Virtual machine).

De la même manière pour les fichiers, si un client SMB crée `test.txt`, Les clients SMB et NFS affichent le nom de fichier comme `text.txt`. Toutefois, si un utilisateur SMB tente par la suite de le créer `Test.txt`, Le nom n'est pas autorisé car, pour le client SMB, ce nom existe actuellement. Si un utilisateur NFS crée par la suite un fichier nommé `Test.txt`, Les clients NFS et SMB affichent le nom de fichier différemment, comme suit :

- Sur les clients NFS, les deux noms de fichiers sont ceux qu'ils ont créés, `test.txt` et `Test.txt`, car les noms de fichiers sont sensibles à la casse.
- Les clients SMB utilisent les 8.3 noms pour distinguer les deux fichiers. Un fichier porte le nom du fichier de base. Un nom de fichier 8.3 est attribué aux fichiers supplémentaires.
  - Sur les clients SMB, vous voyez `test.txt` et `TEST~1.TXT`.
  - ONTAP crée le `TEST~1.TXT` nom de fichier pour différencier les deux fichiers.

> Si vous avez activé ou modifié le mappage de caractères à l'aide des commandes Vserver CIFS Character-mapping, une recherche Windows sensible à la casse devient normalement sensible à la casse.

Comment ONTAP crée des noms de fichiers et de répertoires

ONTAP crée et conserve deux noms pour les fichiers ou les répertoires de tout répertoire ayant accès à partir d'un client SMB : le nom long et le nom d'origine au format 8.3.

Pour les noms de fichier ou de répertoire dépassant le nom de huit caractères ou la limite d'extension de trois caractères (pour les fichiers), ONTAP génère un nom de format 8.3 comme suit :

- Il tronque le nom de fichier ou de répertoire d'origine à six caractères, si le nom dépasse six caractères.
- Il ajoute un tilde (~) et un nombre, un à cinq, aux noms de fichier ou de répertoire qui ne sont plus uniques après être tronqués.

  S'il manque des nombres parce qu'il y a plus de cinq noms similaires, il crée un nom unique qui n'a aucune relation avec le nom original.

- Dans le cas des fichiers, il tronque l'extension du nom de fichier à trois caractères.

Par exemple, si un client NFS crée un fichier nommé `specifications.html`, Le nom de fichier au format 8.3 créé par ONTAP est `specif~1.htm`. Si ce nom existe déjà, ONTAP utilise un numéro différent à la fin du nom du fichier. Par exemple, si un client NFS crée un autre fichier nommé `specifications_new.html`, le format 8.3 de `specifications_new.html` est `specif~2.htm`.

Comment ONTAP gère les noms de fichier, de répertoire et de qtree à plusieurs octets

À partir de ONTAP 9.5, la prise en charge des noms codés UTF-8 de 4 octets permet la création et l'affichage des noms de fichier, de répertoire et d'arborescence qui incluent des caractères supplémentaires Unicode à l'extérieur du plan multilingue de base (BMP). Dans les versions précédentes, ces caractères supplémentaires ne s'affichent pas correctement dans les environnements multiprotocoles.

Pour activer la prise en charge des noms codés UTF-8 à 4 octets, un nouveau code de langue *utf8mb4* est disponible pour l' `vserver` et `volume` familles de commandement.

Vous devez créer un volume de l'une des manières suivantes :

- Réglage du volume `-language` explicitement option : `volume create -language utf8mb4 {…}`
- Hériter du volume `-language` Option d'un SVM qui a été créé avec ou modifié pour l'option : `vserver [create|modify] -language utf8mb4 {…}``volume create {…}`
- Dans ONTAP 9.6 et les versions antérieures, vous ne pouvez pas modifier les volumes existants pour le support utf8mb4 ; vous devez créer un nouveau volume prêt pour utf8mb4, puis migrer les données à l'aide d'outils de copie basés sur le client.

  Vous pouvez mettre à jour les SVM pour la prise en charge de utf8mb4, mais les volumes existants conservent leurs codes de langue d'origine.

  Si vous utilisez ONTAP 9.7P1 ou une version ultérieure, vous pouvez modifier les volumes existants pour utf8mb4 avec une demande de support. Pour plus d'informations, voir "Est-il possible de modifier la langue du volume après sa création dans ONTAP ?".

- À partir de ONTAP 9.8, vous pouvez utiliser le `[-language <Language code>]` Paramètre permettant de changer le langage de volume de *.UTF-8 à utf8mb4. Pour modifier la langue d'un volume, contactez "Support NetApp".

> Les noms de LUN portant des caractères UTF-8 de 4 octets ne sont pas pris en charge actuellement.

- Les données de caractères Unicode sont généralement représentées dans les applications de systèmes de fichiers Windows utilisant le format de transformation Unicode 16 bits (UTF-16) et dans les systèmes de fichiers NFS utilisant le format de transformation Unicode 8 bits (UTF-8).

  Dans les versions antérieures à ONTAP 9.5, les noms, y compris les caractères supplémentaires UTF-16 créés par les clients Windows, étaient correctement affichés sur d'autres clients Windows mais n'étaient pas traduits correctement en UTF-8 pour les clients NFS. De même, les noms comportant des caractères supplémentaires UTF-8 par les clients NFS créés n'ont pas été correctement traduits en UTF-16 pour les clients Windows.

- Lorsque vous créez des noms de fichier sur des systèmes exécutant ONTAP 9.4 ou une version antérieure

contenant des caractères supplémentaires valides ou non valides, ONTAP rejette le nom de fichier et renvoie une erreur de nom de fichier non valide.

Pour éviter ce problème, utilisez uniquement des caractères BMP dans les noms de fichiers et évitez d'utiliser des caractères supplémentaires, ou mettez à niveau vers ONTAP 9.5 ou version ultérieure.

À partir de ONTAP 9, les caractères Unicode sont autorisés dans les noms de qtree.

- Vous pouvez utiliser le `volume qtree` Famille de commandes ou System Manager pour définir ou modifier les noms des qtree.
- Les noms des qtrees peuvent inclure des caractères multi-octets au format Unicode, comme les caractères japonais et chinois.
- Dans les versions antérieures à ONTAP 9.5, seuls les caractères BMP (c'est-à-dire ceux qui pouvaient être représentés en 3 octets) étaient pris en charge.

> Dans les versions antérieures à ONTAP 9.5, le Junction-path du volume parent du qtree peut contenir des noms de qtree et de répertoire avec des caractères Unicode. Le `volume show` La commande affiche ces noms correctement lorsque le volume parent a un paramètre de langue UTF-8. Cependant, si la langue du volume parent n'est pas l'un des paramètres de langue UTF-8, certaines parties du chemin de jonction sont affichées à l'aide d'un nom de remplacement NFS numérique.

- Dans les versions 9.5 et ultérieures, les noms des qtree prennent en charge des caractères de 4 octets, à condition que le qtree se trouve dans un volume activé pour utf8m4.

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

Les clients NFS peuvent créer des noms de fichiers contenant des caractères non valides pour les clients SMB et certaines applications Windows. Vous pouvez configurer le mappage de caractères pour la conversion de noms de fichiers sur des volumes pour permettre aux clients SMB d'accéder aux fichiers avec des noms NFS qui ne seraient autrement pas valides.

Description de la tâche

Lorsque les fichiers créés par des clients NFS sont accessibles par des clients SMB, ONTAP recherche le nom du fichier. Si le nom n'est pas un nom de fichier SMB valide (par exemple, s'il comporte un caractère «`:`") inclus, ONTAP renvoie le nom de fichier 8.3 qui est conservé pour chaque fichier. Cependant, cela cause des problèmes pour les applications qui codent des informations importantes dans des noms de fichiers longs.

Par conséquent, si vous partagez un fichier entre des clients sur des systèmes d'exploitation différents, vous devez utiliser des caractères dans les noms de fichiers valides dans les deux systèmes d'exploitation.

Cependant, si vous avez des clients NFS qui créent des noms de fichier contenant des caractères qui ne sont pas des noms de fichier valides pour les clients SMB, vous pouvez définir une carte qui convertit les caractères NFS non valides en caractères Unicode acceptés par SMB et certaines applications Windows. Par exemple, cette fonctionnalité prend en charge les applications CATIA MCAD et Mathematica, ainsi que d'autres applications qui ont cette exigence.

Vous pouvez configurer le mappage de caractères sur une base volume par volume.

Lors de la configuration du mappage de caractères sur un volume, vous devez garder à l'esprit les éléments suivants :

- Le mappage de caractères n'est pas appliqué à travers les points de jonction.

  Vous devez configurer explicitement le mappage de caractères pour chaque volume de jonction.

- Vous devez vous assurer que les caractères Unicode utilisés pour représenter des caractères non valides ou illégaux sont des caractères qui n'apparaissent normalement pas dans les noms de fichiers ; sinon, des mappages indésirables se produisent.

  Par exemple, si vous essayez de mapper un deux-points (:) à un tiret (-) mais que le tiret (-) a été utilisé correctement dans le nom de fichier, un client Windows essayant d'accéder à un fichier nommé ""a-b" aurait sa demande mappée au nom NFS de ""a:b" (pas le résultat souhaité).

- Après l'application du mappage de caractères, si le mappage contient toujours un caractère Windows non valide, ONTAP revient aux noms de fichier Windows 8.3.
- Dans les notifications FPolicy, les journaux d'audit NAS et les messages de suivi de sécurité, les noms de fichiers mappés sont affichés.
- Lors de la création d'une relation SnapMirror de type DP, le mappage de caractères du volume source n'est pas répliqué sur le volume DP de destination.
- Sensibilité à la casse : comme les noms Windows mappés se transforment en noms NFS, la recherche des noms suit la sémantique NFS. Ainsi, les recherches NFS sont sensibles à la casse. Cela signifie que les applications qui accèdent aux partages mappés ne doivent pas se fier au comportement non sensible à la casse de Windows. Cependant, le nom 8.3 est disponible, et cela n'est pas sensible à la casse.
- Mappages partiels ou non valides : après le mappage d'un nom pour revenir aux clients faisant une énumération de répertoire (« dir »), le nom Unicode obtenu est vérifié pour la validité de Windows. Si ce nom contient toujours des caractères non valides ou s'il n'est pas valide pour Windows (par exemple, il se termine par "." ou vierge), le nom 8.3 est renvoyé à la place du nom non valide.

Étape

1. Configurer le mappage de caractères :

```
vserver cifs character-mapping create -vserver vserver_name -volume volume_name
-mapping mapping_text, …
```

Le mappage se compose d'une liste de paires de caractères source-cible séparées par «»:». Les caractères sont des caractères Unicode saisis à l'aide de chiffres hexadécimaux. Par exemple : 3C:E03C.

La première valeur de chaque `mapping_text` La paire séparée par deux-points est la valeur hexadécimale du caractère NFS que vous souhaitez traduire, et la seconde est la valeur Unicode utilisée par SMB. Les paires de mappage doivent être uniques (un mappage un-à-un doit exister).

- Mappage de source

Le tableau suivant montre le jeu de caractères Unicode autorisé pour le mappage de source :

+

Caractère Unicode	Caractère imprimé	Description
0x01-0x19	Sans objet	Caractères de contrôle sans impression
0x5C		Barre oblique inversée
0x3A	:	Deux-points
0x2A	*	Astérisque
0x3F	?	Point d'interrogation
0x22	«	Devis
0x3C	<	Inférieur à
0x3E	>	Supérieur à
0x7C		
Ligne verticale	0xb1	±

- Mappage de cible

  Vous pouvez spécifier des caractères cibles dans la « zone d'utilisation privée » d'Unicode dans la plage suivante : U+E0000…U+F8FF.

Exemple

La commande suivante crée un mappage de caractères pour un volume nommé « `dates' » sur la machine virtuelle de stockage (SVM) vs1 :

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show

Vserver         Volume Name  Character Mapping
--------------  -----------  ----------------------------------------
vs1             data         3c:e17c, 3e:f17d, 2a:f745
```

Informations associées

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

Commandes permettant de gérer les mappages de caractères pour la conversion de noms de fichiers SMB

Vous pouvez gérer le mappage de caractères en créant, en modifiant, en affichant des informations sur et en supprimant des mappages de caractères de fichiers utilisés pour la conversion de noms de fichiers SMB sur des volumes FlexVol.

Les fonctions que vous recherchez…	Utilisez cette commande…
Créer de nouveaux mappages de caractères de fichier	`vserver cifs character-mapping create`
Affiche des informations sur les mappages de caractères de fichier	`vserver cifs character-mapping show`
Modifier les mappages de caractères de fichier existants	`vserver cifs character-mapping modify`
Supprimer les mappages de caractères de fichier	`vserver cifs character-mapping delete`

Pour plus d'informations, consultez la page man pour chaque commande

Informations associées

Configuration du mappage de caractères pour la conversion de noms de fichiers SMB sur des volumes