



Gérer les serveurs SMB

ONTAP 9

NetApp
September 12, 2024

Sommaire

Gérer les serveurs SMB	1
Modifier les serveurs SMB	1
Utilisez les options pour personnaliser les serveurs SMB	2
Gérer les paramètres de sécurité du serveur SMB	11
Configurez SMB Multichannel pour des performances et une redondance optimales	44
Configurez les mappages utilisateur Windows par défaut sur utilisateur UNIX sur le serveur SMB	47
Affiche des informations sur les types d'utilisateurs connectés via des sessions SMB	50
Options de commande pour limiter la consommation excessive de ressources client Windows	51
Améliorez les performances de vos clients grâce aux oplocks classiques et de location	52
Appliquez des objets de stratégie de groupe aux serveurs SMB	59
Commandes pour la gestion des mots de passe de compte d'ordinateur des serveurs SMB	79
Gérer les connexions du contrôleur de domaine	79
Utilisez des sessions null pour accéder au stockage dans des environnements non Kerberos	84
Gérer les alias NetBIOS des serveurs SMB	86
Gérer diverses tâches de serveur SMB	91
Utilisez IPv6 pour l'accès SMB et les services SMB	96

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 : `vserver 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 fermées lors des requêtes relatives aux attributs des fichiers et des répertoires. Par défaut, la fonctionnalité de fausse 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	<code>vserver cifs options modify -vserver vserver_name options</code>
Au niveau de privilège avancé	<div>a. <code>set -privilege advanced</code> b. <code>vserver cifs options modify -vserver vserver_name options</code> c. <code>set -privilege admin</code></div>

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	<code>vserver cifs options modify -grant-unix-group-perms-to-others true</code>

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	<code>vserver cifs options modify -grant-unix-group-perms-to-others false</code>

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
<code>no-restriction</code> (valeur par défaut)	Spécifie aucune restriction d'accès pour les utilisateurs anonymes.
<code>no-enumeration</code>	Spécifie que seule l'énumération est restreinte pour les utilisateurs anonymes.
<code>no-access</code>	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	<code>vserver cifs security show -vserver <i>vserver_name</i></code>
Un paramètre de sécurité ou des paramètres spécifiques sur la SVM	<code>vserver cifs security show -vserver <i>_vserver_name_</i> -fields [fieldname,...]</code> Vous pouvez entrer <code>-fields ?</code> pour déterminer les champs que vous pouvez utiliser.

Exemple

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

```
cluster1::> vsserver cifs security show -vsserver 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::> vsserver cifs security show -vsserver vs1 -fields 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	<pre>vserver cifs security modify -vserver vserver_name -is-password-complexity -required true</pre>
Désactivé	<pre>vserver cifs security modify -vserver vserver_name -is-password-complexity -required false</pre>

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).	<pre>vserver cifs security modify -vserver vserver_name -kerberos-clock-skew integer_in_minutes</pre> <p>La valeur par défaut est 5 minutes.</p>
Spécifiez la durée de vie du ticket Kerberos en heures.	<pre>vserver cifs security modify -vserver vserver_name -kerberos-ticket-age integer_in_hours</pre> <p>Le paramètre par défaut est 10 heures.</p>
Spécifiez le nombre maximum de jours de renouvellement de billet.	<pre>vserver cifs security modify -vserver vserver_name -kerberos-renew-age integer_in_days</pre> <p>Le paramètre par défaut est 7 jours.</p>
Spécifiez le délai d'expiration des sockets sur les KDC après lequel tous les KDC sont marqués comme inaccessibles.	<pre>vserver cifs security modify -vserver vserver_name -kerberos-kdc-timeout integer_in_seconds</pre> <p>Le réglage par défaut est de 3 secondes.</p>

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

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

Vservice: 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	<pre>vserver cifs security modify -vserver vserver_name -advertised -enc-types aes-128,aes-256</pre>
Désactivé	<pre>vserver cifs security modify -vserver vserver_name -advertised -enc-types des,rc4</pre>

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::> vsriver cifs security modify -vsriver 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::> vsriver cifs security show -vsriver vs2 -fields advertised-
enc-types
```

```
vsriver  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	<pre>vsriver cifs security modify -vsriver vsriver_name -is-aes -encryption-enabled true</pre>
Désactivé	<pre>vsriver cifs security modify -vsriver vsriver_name -is-aes -encryption-enabled false</pre>

2. Vérifiez que le chiffrement AES est activé ou désactivé selon les besoins :

```
vsriver cifs
security show -vsriver vsriver_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::> vsserver cifs security modify -vsserver vs1 -is-aes
-encryption-enabled true

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

vsserver  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::> vsserver cifs security modify -vsserver 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::> vsserver cifs security show -vsserver vs2 -fields is-aes-
encryption-enabled

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

Informations associées

"L'utilisateur du domaine ne parvient pas à se connecter au cluster avec Domain-tunnel"

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 <code>Require Option (Sign always)</code> 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	<code>vserver cifs security modify -vserver vserver_name -is-signing-required true</code>
Désactivé	<code>vserver cifs security modify -vserver vserver_name -is-signing-required false</code>

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	<code>vserver cifs session show -vserver <i>vserver_name</i> -is-session-signed true</code>
Détails d'une session signée avec un ID de session spécifique sur le SVM	<code>vserver cifs session show -vserver <i>vserver_name</i> -session-id integer -instance</code>

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
ID          ID      Workstation      Windows User      Open      Idle
-----
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	<code>`show -sample-id sample_ID -counter signed_sessions</code>
<code>node_name [-node node_name]</code>	Sessions signées et sessions établies
<code>`show -sample-id sample_ID -counter signed_sessions</code>	<code>established_sessions</code>

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.

Chiffrement SMB du serveur SMB activé	Le paramètre partage des données de chiffrement est activé	Comportement de cryptage côté serveur
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.
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	<code>vserver cifs security modify -vserver vserver_name -is-smb-encryption -required true</code>
Désactivé	<code>vserver cifs security modify -vserver vserver_name -is-smb-encryption -required false</code>

- 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 <i>vserver_name</i> {unencrypted
partially-encrypted	encrypted} -instance`

Si vous voulez afficher des informations sur...	Entrez la commande...
Paramètre de chiffrement pour un ID de session spécifique sur un SVM spécifié	<code>vserver cifs session show -vserver <i>vserver_name</i> -session-id <i>integer</i> -instance</code>

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
<code>encrypted_sessions</code>	Indique le nombre de sessions SMB 3.0 cryptées

Nom du compteur	Descriptions
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
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	<code>`show -sample-id <i>sample_ID</i> -counter encrypted_sessions`</code>
<code><i>node_name</i> [-node <i>node_name</i>]</code>	Sessions chiffrées et sessions établies
<code>`show -sample-id <i>sample_ID</i> -counter encrypted_sessions`</code>	<code>established_sessions</code>
<code><i>node_name</i> [-node <i>node_name</i>]</code>	Connexions de partage cryptées
<code>`show -sample-id <i>sample_ID</i> -counter encrypted_share_connections`</code>	<code><i>node_name</i> [-node <i>node_name</i>]</code>
Connexions de partage cryptées et partages connectés	<code>`show -sample-id <i>sample_ID</i> -counter encrypted_share_connections`</code>
<code>connected_shares</code>	<code><i>node_name</i> [-node <i>node_name</i>]</code>
Sessions non chiffrées rejetées rejetées	<code>`show -sample-id <i>sample_ID</i> -counter rejected_unencrypted_sessions`</code>
<code><i>node_name</i> [-node <i>node_name</i>]</code>	Les connexions de partage non chiffrées ont été rejetées
<code>`show -sample-id <i>sample_ID</i> -counter rejected_unencrypted_share`</code>	<code><i>node_name</i> [-node <i>node_name</i>]</code>

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"](http://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"](http://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 vservice_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 vservice_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
```

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\
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 »	<code>vserver cifs options modify -default -unix-user pcuser</code>
Utiliser un autre compte utilisateur UNIX comme utilisateur par défaut	<code>vserver cifs options modify -default -unix-user user_name</code>
Désactivez l'utilisateur UNIX par défaut	<code>vserver cifs options modify -default -unix-user ""</code>

```
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	<pre>vserver cifs options modify -guest -unix-user <i>unix_name</i></pre>

Les fonctions que vous recherchez...	Entrer...
Désactiver l'utilisateur UNIX invité	<code>vserver cifs options modify -guest -unix-user ""</code>

```
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	<code>vserver cifs options modify -vserver vserver_name -is-admin-users-mapped-to -root-enabled true</code> Tous les comptes du groupe administrateurs sont considérés comme root, même si vous n'avez pas de <code>/etc/usermap.cfg</code> 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	<code>vserver cifs options modify -vserver vserver_name -is-admin-users-mapped-to -root-enabled false</code> 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.

- Vérifiez que l'option est réglée sur la valeur souhaitée : `vserver cifs options show -vserver vserver_name`
- 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	<code>`vserver cifs session show -vserver vserver_name -user-type {local-user</code>
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 publ -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
-----
publnode1 publ      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	<p>Saisissez la commande suivante : <code>vserver cifs share create -vserver _vserver_name_ -share-name share_name -path path_to_share -share-properties [oplocks,...]</code></p> <div>  <p>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 <code>-share-properties</code> 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' <code>-share-properties</code> paramètre avec la liste des propriétés de partage à utiliser pour ce partage.</p> </div>
Désactiver les oplocks sur un partage lors de la création du partage	<p>Saisissez la commande suivante : <code>vserver cifs share create -vserver _vserver_name_ -share-name _share_name_ -path _path_to_share_ -share-properties [other_share_property,...]</code></p> <div>  <p>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.</p> </div>

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	<code>volume qtree oplocks avec le -oplock-mode paramètre défini sur enable</code>
Désactiver les oplocks sur des volumes ou des qtrees	<code>volume qtree oplocks avec le -oplock-mode paramètre défini sur disable</code>

Informations associées

[Surveillance de l'état du oplock](#)

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	<p>Saisissez la commande suivante : <code>vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties oplocks</code></p> <div>  <p>Vous pouvez spécifier des propriétés de partage supplémentaires à ajouter à l'aide d'une liste délimitée par des virgules.</p> </div> <p>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.</p>
Désactivez les oplocks sur un partage en modifiant un partage existant	<p>Saisissez la commande suivante : <code>vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties oplocks</code></p> <div>  <p>Vous pouvez spécifier des propriétés de partage supplémentaires à supprimer à l'aide d'une liste délimitée par des virgules.</p> </div> <p>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.</p>

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	<code>vserver cifs group-policy modify -vserver vserver_name -status enabled</code>
Désactiver les stratégies de groupe	<code>vserver cifs group-policy modify -vserver vserver_name -status disabled</code>

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	<code>vserver cifs group-policy update -vserver vserver_name</code>

Si vous voulez mettre à jour...	Entrez la commande...
Tous les paramètres GPO	<code>vserver cifs group-policy update -vserver vserver_name -force-reapply -all-settings true</code>

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	<code>vserver cifs group-policy show-defined -vserver vserver_name</code>
Appliquée à une machine virtuelle de stockage (SVM) compatible CIFS	<code>vserver cifs group-policy show-applied -vserver vserver_name</code>

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/dirl
  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	<code>vserver cifs group-policy restricted-group show-defined -vserver vserver_name</code>
Appliqué à un serveur CIFS	<code>vserver cifs group-policy restricted-group show-applied -vserver vserver_name</code>

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

```
Vserver: vs1
```

```
-----
```

```
Group Policy Name: gp01
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::> vsserver cifs group-policy restricted-group show-applied
-vserver vs1
```

```
Vserver: vs1
```

```
-----
```

```
Group Policy Name: gp01
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	<code>vserver cifs group-policy central-access-policy show-defined -vserver <i>vserver_name</i></code>
Appliqué à un serveur CIFS	<code>vserver cifs group-policy central-access-policy show-applied -vserver <i>vserver_name</i></code>

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

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	<code>vserver cifs group-policy central-access-rule show-defined -vserver vserver_name</code>
Appliqué à un serveur CIFS	<code>vserver cifs group-policy central-access-rule show-applied -vserver vserver_name</code>

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::> vservers 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::> vservers 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	<code>vserver cifs domain password change</code>
Réinitialisez le mot de passe du compte de domaine et vous ne connaissez pas le mot de passe	<code>vserver cifs domain password reset</code>
Configurez les serveurs SMB pour les changements de mot de passe de compte d'ordinateur automatique	<code>vserver cifs domain password schedule modify -vserver vserver_name -is -schedule-enabled true</code>
Désactivez les modifications de mot de passe de compte informatique automatique sur les serveurs SMB	<code>vserver cifs domain password schedule modify -vserver vs1 -is-schedule -enabled false</code>

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.

Avant de commencer

Vous devez avoir le niveau de privilège avancé.

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	<code>vserver cifs domain preferred-dc add</code>
Afficher les contrôleurs de domaine préférés	<code>vserver cifs domain preferred-dc show</code>
Supprimez un contrôleur de domaine préféré	<code>vserver cifs domain preferred-dc remove</code>

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	<code>vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc-connections true</code>
Désactivé	<code>vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc-connections false</code>

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 nul 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'option `-restrict-anonymous`. 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 nul. 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 nul est identifié comme une connexion anonyme. Les utilisateurs nul n'ont accès à aucun répertoire personnel.

Les autorisations d'utilisateur mappées sont accordées à tout utilisateur nul 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 nul en attribuant un groupe à utiliser par les clients de session nul et en enregistrant les adresses IP des clients de session nul à ajouter à la liste des clients autorisés à accéder aux données à l'aide de sessions nul du système de stockage.

Étapes

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

La commande suivante mappe l'utilisateur nul 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

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	<pre>vserver cifs remove-netbios-aliases -vserver _vserver_name_ -netbios -aliases _NetBIOS_alias_,...</pre>
Tous les alias NetBIOS de la liste	<pre>vserver cifs remove-netbios-aliases -vserver vserver_name -netbios-aliases -</pre>

```
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	<code>vserver cifs show -display-netbios -aliases</code>
La liste des alias NetBIOS dans le cadre des informations détaillées du serveur CIFS	<code>vserver cifs show -instance</code>

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	<code>vserver cifs session show -instance</code>
Connexions utilisant un alias NetBIOS spécifié :	<code>vserver cifs session show -instance -netbios-name <i>netbios_name</i></code>

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	<code>`vserver cifs stop -vserver <i>vserver_name</i> [-foreground {true</code>
<code>false}]]`</code>	Démarrez le serveur CIFS
<code>`vserver cifs start -vserver <i>vserver_name</i> [-foreground {true</code>	<code>false}]]`</code>

`-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	<code>vserver cifs create</code>
Affiche les informations relatives à un serveur SMB	<code>vserver cifs show</code>
Modifier un serveur SMB	<code>vserver cifs modify</code>
Déplacer un serveur SMB vers un autre domaine	<code>vserver cifs modify</code>
Arrêtez un serveur SMB	<code>vserver cifs stop</code>
Démarrez un serveur SMB	<code>vserver cifs start</code>
Supprimez un serveur SMB	<code>vserver cifs delete</code>
Réinitialisez et redécouvrez les serveurs pour le serveur SMB	<code>vserver cifs domain discovered-servers reset-servers</code>
Modifier le mot de passe du compte machine du serveur SMB	<code>vserver cifs domain password change</code>
Réinitialisez le mot de passe du compte machine du serveur SMB	<code>vserver cifs domain password change</code>
Planifier les modifications automatiques du mot de passe pour le compte machine du serveur SMB	<code>vserver cifs domain password schedule modify</code>
Ajoutez des alias NetBIOS pour le serveur SMB	<code>vserver cifs add-netbios-aliases</code>
Supprimez les alias NetBIOS du serveur SMB	<code>vserver cifs remove-netbios-aliases</code>

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	<pre>vserver cifs session show -vserver vserver_name -instance</pre>
IPv6 est utilisé pour les sessions SMB via une adresse LIF spécifiée	<pre>vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address -instance</pre> <p><i>LIF_IP_address</i> Est l'adresse IPv6 de la LIF de données.</p>

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.