Gérez NFS avec l'interface de ligne de commande

ONTAP 9

NetApp
November 14, 2025

Sommaire

Gérez NFS avec l'interface de ligne de commande

En savoir plus sur l'accès aux fichiers ONTAP pour le protocole NFS

ONTAP inclut des fonctionnalités d'accès aux fichiers disponibles pour le protocole NFS. Vous pouvez activer un serveur NFS et exporter des volumes ou des qtrees.

Vous effectuez cette procédure dans les cas suivants :

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

Compréhension de l'accès aux fichiers NAS

Espaces de noms et points de jonction

En savoir plus sur les espaces de noms et les points de jonction NAS ONTAP

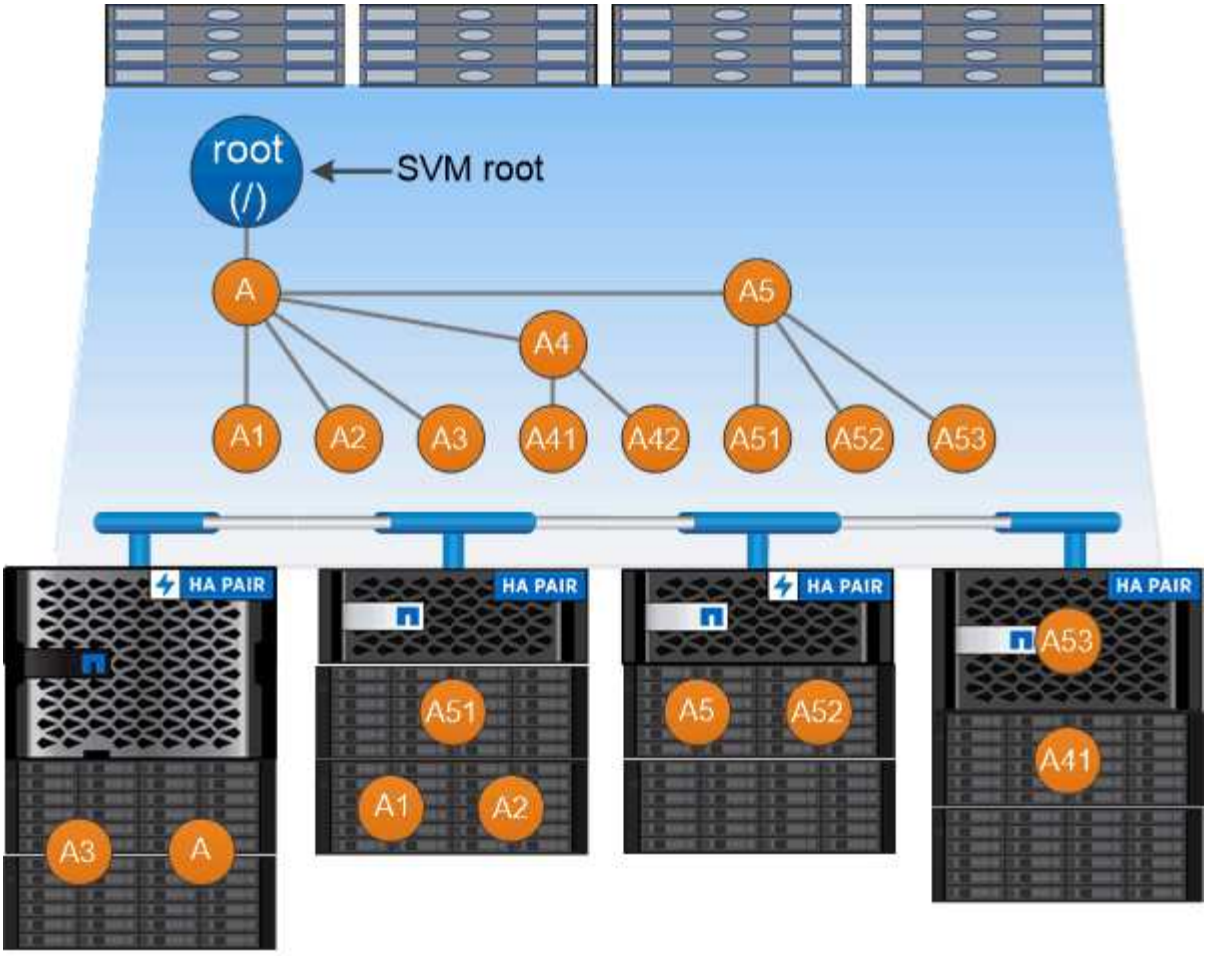
Un NAS *namespace* est un regroupement logique de volumes regroupés à *Junction points* pour créer une seule hiérarchie de système de fichiers. Un client disposant des autorisations suffisantes peut accéder aux fichiers dans l'espace de noms sans spécifier l'emplacement des fichiers dans le stockage. Des volumes regroupés dans le cluster peuvent se trouver n'importe où.

Plutôt que de monter chaque volume contenant un fichier d'intérêt, les clients NAS monter un NFS *export* ou accéder à un partage SMB._ l'exportation ou le partage représente l'intégralité de l'espace de noms ou un emplacement intermédiaire dans l'espace de noms. Le client n'accède qu'aux volumes montés sous son point d'accès.

Vous pouvez ajouter des volumes au namespace selon vos besoins. Vous pouvez créer des points de jonction directement en-dessous d'une jonction de volume parent ou sur un répertoire au sein d'un volume. Il se peut qu'un chemin vers une jonction de volume pour un volume nommé « vol3 » soit possible `/vol1/vol2/vol3`, ou `/vol1/dir2/vol3`, ou même `/dir1/dir2/vol3`. Le chemin est appelé *Junction path.*

Chaque SVM possède un espace de noms unique. Le volume root du SVM est le point d'entrée de la hiérarchie de l'espace de noms.

Pour garantir la disponibilité des données en cas de panne du nœud ou de basculement, vous devez créer une copie *load-sharing mirror* pour le volume root du SVM.



A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.

Exemple

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

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

En savoir plus sur les architectures d'espace de noms NAS ONTAP

Plusieurs architectures d'espace de noms NAS classiques peuvent être utilisées lors de la création d'un espace de noms de SVM. Vous pouvez choisir l'architecture d'espace de noms qui correspond le mieux à vos besoins métiers et de flux de travail.

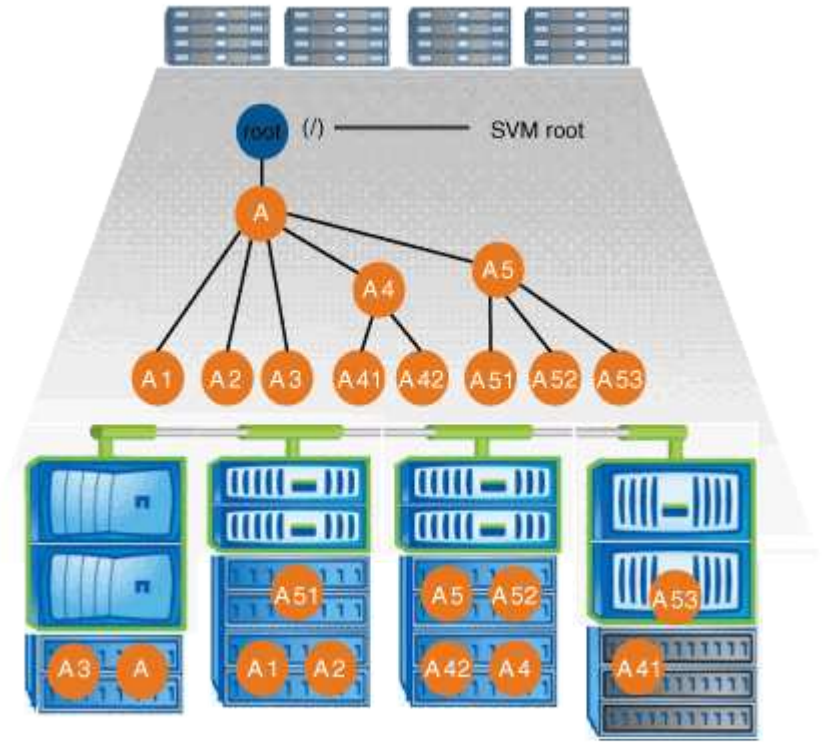
Le haut du namespace est toujours le volume root, représenté par une barre oblique (/). L'architecture d'espace de noms sous la racine se divise en trois catégories de base :

- Arbre branché unique, avec une seule jonction à la racine de l'espace de noms

- Plusieurs arborescences ramifiées, avec plusieurs points de jonction à la racine de l'espace de noms
- Plusieurs volumes autonomes, chacun avec un point de jonction séparé à la racine de l'espace de noms

Espace de noms avec une seule arborescence ramifiée

Une architecture avec une seule arborescence de branche possède un point d'insertion unique à la racine du namespace du SVM. Le point d'insertion unique peut être un volume relié par jonction ou un répertoire sous la racine. Tous les autres volumes sont montés aux points de jonction sous le point d'insertion unique (qui peut être un volume ou un répertoire).

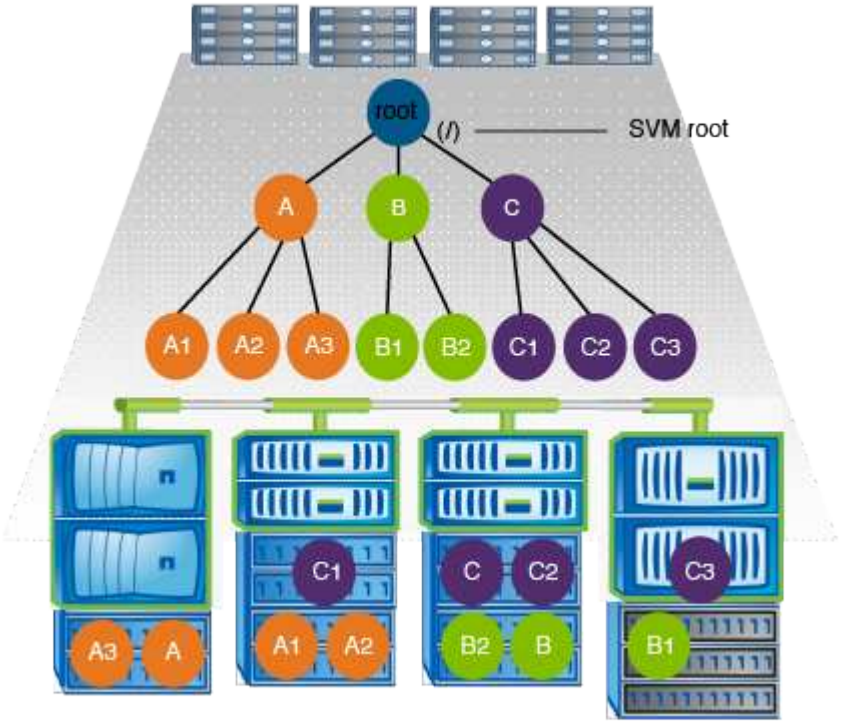


Par exemple, une configuration de jonction de volume typique avec l'architecture de namespace ci-dessus peut ressembler à la configuration suivante, où tous les volumes sont reliés sous le point d'insertion unique, qui est un répertoire nommé « `data' » :

```
                 Junction                       Junction
Vserver Volume   Active   Junction Path         Path Source
------- -------- -------- -------------------   -----------
vs1     corp1    true     /data/dir1/corp1      RW_volume
vs1     corp2    true     /data/dir1/corp2      RW_volume
vs1     data1    true     /data/data1           RW_volume
vs1     eng1     true     /data/data1/eng1      RW_volume
vs1     eng2     true     /data/data1/eng2      RW_volume
vs1     sales    true     /data/data1/sales     RW_volume
vs1     vol1     true     /data/vol1            RW_volume
vs1     vol2     true     /data/vol2            RW_volume
vs1     vol3     true     /data/vol3            RW_volume
vs1     vs1_root -        /                     -
```

Espace de noms avec plusieurs arborescences ramifiées

Une architecture avec plusieurs arbres ramifiés a plusieurs points d'insertion à la racine du namespace du SVM. Les points d'insertion peuvent être des volumes ou des répertoires sous la racine. Tous les autres volumes sont montés aux points de jonction sous les points d'insertion (qui peuvent être des volumes ou des répertoires).

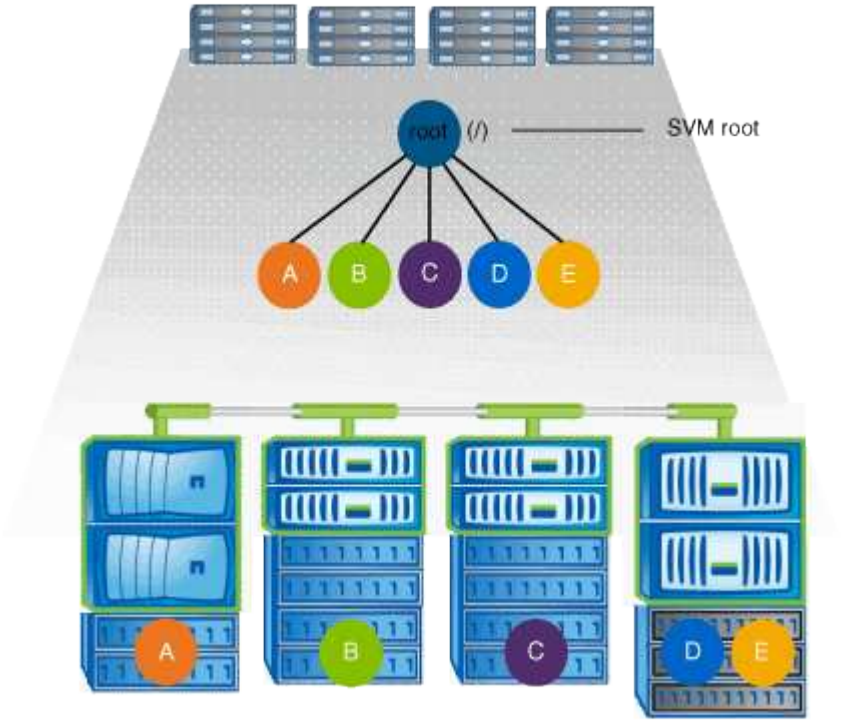


Par exemple, une configuration de jonction de volume standard avec l'architecture de namespace ci-dessus peut ressembler à la configuration suivante, où il existe trois points d'insertion pour le volume racine de la SVM. Deux points d'insertion sont des répertoires nommés "data" et "projets". Un point d'insertion est un volume relié par jonction nommé « audit » :

```
                    Junction                        Junction
Vserver Volume      Active   Junction Path          Path Source
------- ----------- -------- --------------------   -----------
vs1     audit       true     /audit                 RW_volume
vs1     audit_logs1 true     /audit/logs1           RW_volume
vs1     audit_logs2 true     /audit/logs2           RW_volume
vs1     audit_logs3 true     /audit/logs3           RW_volume
vs1     eng         true     /data/eng              RW_volume
vs1     mktg1       true     /data/mktg1            RW_volume
vs1     mktg2       true     /data/mktg2            RW_volume
vs1     project1    true     /projects/project1     RW_volume
vs1     project2    true     /projects/project2     RW_volume
vs1     vs1_root    -        /                      -
```

Espace de noms avec plusieurs volumes autonomes

Dans une architecture avec des volumes autonomes, chaque volume a un point d'insertion à la racine de l'espace de noms SVM ; cependant, le volume n'est pas relié par jonction sous un autre volume. Chaque volume a un chemin unique, avec une jonction directe sous la racine ou sous un répertoire sous la racine.



Par exemple, une configuration de jonction de volume standard avec l'architecture de l'espace de noms ci-dessus peut ressembler à la configuration suivante, où il existe cinq points d'insertion pour le volume racine de la SVM, avec chaque point d'insertion représentant un chemin vers un volume.

```
                    Junction                          Junction
Vserver Volume      Active   Junction Path            Path Source
------- ----------- -------- -------------------      -----------
vs1     eng         true     /eng                     RW_volume
vs1     mktg        true     /vol/mktg                RW_volume
vs1     project1    true     /project1                RW_volume
vs1     project2    true     /project2                RW_volume
vs1     sales       true     /sales                   RW_volume
vs1     vs1_root    -        /                        -
```

Comment ONTAP contrôle l'accès aux fichiers

En savoir plus sur le contrôle d'accès aux fichiers NAS ONTAP

ONTAP contrôle l'accès aux fichiers en fonction des restrictions basées sur l'authentification et les fichiers que vous avez spécifiées.

Lorsqu'un client se connecte au système de stockage pour accéder aux fichiers, ONTAP doit effectuer deux

tâches :

- Authentification

  ONTAP doit authentifier le client en vérifiant l'identité avec une source de confiance. De plus, le type d'authentification du client est une méthode qui peut être utilisée pour déterminer si un client peut accéder aux données lors de la configuration des export policies (facultatif pour CIFS).

- Autorisation

  ONTAP doit autoriser l'utilisateur en comparant les informations d'identification de l'utilisateur avec les autorisations configurées sur le fichier ou le répertoire et en déterminant le type d'accès à fournir, le cas échéant.

Pour gérer correctement le contrôle d'accès aux fichiers, ONTAP doit communiquer avec des services externes tels que des serveurs NIS, LDAP et Active Directory. La configuration d'un système de stockage pour l'accès aux fichiers via CIFS ou NFS nécessite la configuration des services appropriés, en fonction de votre environnement dans ONTAP.

En savoir plus sur les restrictions basées sur l'authentification pour les SVM NAS ONTAP

En cas de restrictions basées sur l'authentification, vous pouvez spécifier les ordinateurs clients et les utilisateurs autorisés à se connecter à la machine virtuelle de stockage (SVM).

ONTAP prend en charge l'authentification Kerberos depuis des serveurs UNIX et Windows.

En savoir plus sur les restrictions basées sur les fichiers pour les SVM NAS ONTAP

ONTAP évalue trois niveaux de sécurité pour déterminer si une entité est autorisée à effectuer une action demandée sur les fichiers et répertoires résidant sur une SVM. L'accès est déterminé par les autorisations effectives après évaluation des trois niveaux de sécurité.

Tout objet de stockage peut contenir jusqu'à trois types de couches de sécurité :

- Sécurité des exportations (NFS) et des partages (SMB)

  La sécurité des exportations et des partages s'applique à l'accès client à une exportation NFS ou à un partage SMB donné. Les utilisateurs disposant de privilèges d'administration peuvent gérer la sécurité au niveau de l'exportation et du partage à partir des clients SMB et NFS.

- Sécurité des fichiers et répertoires Access Guard du niveau de stockage

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

Si vous affichez les paramètres de sécurité d'un fichier ou d'un répertoire à partir d'un client NFS ou SMB, vous ne verrez pas la sécurité de Storage-Level Access Guard. La sécurité Access Guard au niveau du stockage ne peut pas être révoquée d'un client, même par un administrateur système (Windows ou UNIX).

- Sécurité native au niveau des fichiers NTFS, UNIX et NFSv4

  La sécurité native au niveau du fichier existe sur le fichier ou le répertoire qui représente l'objet de stockage. Vous pouvez définir la sécurité au niveau des fichiers à partir d'un client. Les autorisations liées aux fichiers sont efficaces, que SMB ou NFS soit utilisé pour accéder aux données.

Comment ONTAP gère l'authentification client NFS

En savoir plus sur l'authentification ONTAP pour les clients NAS

Les clients NFS doivent être authentifiés correctement avant que leur système puisse accéder aux données sur la SVM. ONTAP authentifie les clients en comparant leurs informations d'identification UNIX aux services de nom que vous configurez.

Lorsqu'un client NFS se connecte au SVM, ONTAP obtient les identifiants UNIX pour l'utilisateur en cochant différents services de noms selon la configuration des services de noms du SVM. ONTAP peut vérifier les informations d'identification des comptes UNIX locaux, des domaines NIS et des domaines LDAP. Au moins l'un d'entre eux doit être configuré de manière à ce que ONTAP puisse authentifier l'utilisateur avec succès. Vous pouvez spécifier plusieurs services de noms et l'ordre dans lequel ONTAP les recherche.

Dans un environnement NFS pur avec des styles de sécurité de volume UNIX, cette configuration suffit à authentifier et à fournir l'accès approprié aux fichiers pour un utilisateur connecté à partir d'un client NFS.

Si vous utilisez des styles de sécurité de volumes mixtes, NTFS ou Unified, ONTAP doit obtenir un nom d'utilisateur SMB pour l'utilisateur UNIX pour l'authentification avec un contrôleur de domaine Windows. Cela peut se produire soit en mappant des utilisateurs individuels à l'aide de comptes UNIX locaux ou de domaines LDAP, soit en utilisant un utilisateur SMB par défaut. Vous pouvez spécifier le nom des services que ONTAP recherche dans l'ordre ou spécifier un utilisateur SMB par défaut.

Découvrez comment ONTAP utilise les services de noms

ONTAP utilise les services de noms pour obtenir des informations sur les utilisateurs et les clients. ONTAP utilise ces informations pour authentifier les utilisateurs qui accèdent aux données sur ou administrent le système de stockage, et mapper les identifiants des utilisateurs dans un environnement mixte.

Lorsque vous configurez le système de stockage, vous devez spécifier les services de nom que vous souhaitez que ONTAP utilise pour obtenir les identifiants utilisateur pour l'authentification. ONTAP prend en charge les noms suivants :

- Utilisateurs locaux (fichier)
- Domaines NIS externes (NIS)
- Domaines LDAP externes (LDAP)

Vous utilisez le `vserver services name-service ns-switch` Famille de commandes afin de configurer les SVM avec les sources pour rechercher les informations relatives au réseau et l'ordre dans lequel les

rechercher. Ces commandes fournissent l'équivalent des fonctionnalités de `/etc/nsswitch.conf` Fichier sur les systèmes UNIX.

Lorsqu'un client NFS se connecte au SVM, ONTAP vérifie les services de nom spécifiés pour obtenir les informations d'identification UNIX pour l'utilisateur. Si les services de nom sont correctement configurés et que ONTAP peut obtenir les informations d'identification UNIX, ONTAP authentifie l'utilisateur avec succès.

Dans un environnement avec des styles de sécurité mixtes, ONTAP peut avoir à mapper les informations d'identification de l'utilisateur. Vous devez configurer les services de noms de manière appropriée pour votre environnement afin que ONTAP puisse correctement mapper les identifiants des utilisateurs.

ONTAP utilise également des services de noms pour l'authentification des comptes d'administrateur des SVM. Vous devez garder cela à l'esprit lors de la configuration ou de la modification du commutateur de service de nom afin d'éviter toute désactivation accidentelle de l'authentification pour les comptes d'administrateur SVM. Pour plus d'informations sur les utilisateurs d'administration des SVM, voir "Authentification de l'administrateur et RBAC".

Accorder l'accès aux fichiers SMB ONTAP à partir des clients NFS

ONTAP utilise la sémantique de sécurité du système de fichiers NTFS (Windows NT File System) pour déterminer si un utilisateur UNIX, sur un client NFS, a accès à un fichier avec des autorisations NTFS.

Pour ce faire, ONTAP convertit l'ID utilisateur UNIX (UID) de l'utilisateur en informations d'identification SMB, puis utilise les informations d'identification SMB pour vérifier que l'utilisateur dispose des droits d'accès au fichier. Un identifiant SMB se compose d'un identificateur de sécurité principal (SID), généralement le nom d'utilisateur Windows de l'utilisateur, et d'un ou plusieurs SID de groupe qui correspondent à des groupes Windows dont l'utilisateur est membre.

Le temps ONTAP nécessaire à la conversion de l'UID UNIX en identifiants SMB peut être de plusieurs dizaines de millisecondes à des centaines de millisecondes, car le processus implique de contacter un contrôleur de domaine. ONTAP mappe l'UID sur les identifiants SMB et entre le mappage dans un cache d'identifiants afin de réduire le temps de vérification provoqué par la conversion.

Comment fonctionne le cache d'informations d'identification NFS ONTAP

Lorsqu'un utilisateur NFS demande l'accès aux exports NFS sur le système de stockage, ONTAP doit récupérer les identifiants de l'utilisateur à partir de serveurs de noms externes ou de fichiers locaux afin de l'authentifier. ONTAP stocke ensuite ces informations d'identification dans un cache d'informations d'identification interne pour référence ultérieure. Il est donc essentiel de comprendre le fonctionnement des caches d'identifiants NFS pour gérer les problèmes de performance et d'accès qui peuvent survenir.

Sans le cache des informations d'identification, ONTAP devra interroger les services de noms chaque fois qu'un utilisateur NFS a demandé l'accès. Sur un système de stockage surchargé auquel de nombreux utilisateurs accèdent, cela peut rapidement entraîner des problèmes de performance graves, entraînant des retards non désirés ou même des dénis de l'accès client NFS.

Avec le cache des informations d'identification, ONTAP récupère les informations d'identification de l'utilisateur, puis les stocke pendant un délai prédéterminé pour un accès rapide et facile en cas d'envoi d'une autre demande par le client NFS. Cette méthode offre les avantages suivants :

- Il facilite la charge du système de stockage en gérant moins de requêtes vers des serveurs de noms externes (par exemple NIS ou LDAP).
- Il facilite la charge sur les serveurs de noms externes en leur envoyant moins de demandes.
- Il accélère l'accès des utilisateurs en éliminant le temps d'attente pour obtenir des informations d'identification de sources externes avant que l'utilisateur puisse être authentifié.

ONTAP stocke les informations d'identification positives et négatives dans le cache des informations d'identification. Des informations d'identification positives signifient que l'utilisateur a été authentifié et a accordé l'accès. Les identifiants négatifs signifient que l'utilisateur n'a pas été authentifié et a refusé l'accès.

Par défaut, ONTAP stocke des identifiants positifs pendant 24 heures. Ainsi, après l'authentification initiale d'un utilisateur, ONTAP utilise les identifiants mis en cache pour toutes les demandes d'accès de cet utilisateur pendant 24 heures. Si l'utilisateur demande l'accès après 24 heures, le cycle commence : ONTAP supprime les informations d'identification mises en cache et obtient à nouveau les informations d'identification à partir de la source de service de noms appropriée. Si les informations d'identification ont été modifiées sur le serveur de noms au cours des 24 dernières heures, ONTAP met en cache les informations d'identification mises à jour pour les 24 prochaines heures.

Par défaut, ONTAP stocke les informations d'identification négatives pendant deux heures. Ainsi, après avoir initialement refusé l'accès à un utilisateur, ONTAP continue à refuser toute demande d'accès à cet utilisateur pendant deux heures. Si l'utilisateur demande l'accès au bout de 2 heures, le cycle commence : ONTAP obtient à nouveau les informations d'identification à partir de la source de service de noms appropriée. Si les informations d'identification ont été modifiées sur le serveur de noms au cours des deux heures précédentes, ONTAP met en cache les informations d'identification mises à jour pour les deux heures suivantes.

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

Créer des volumes NAS ONTAP avec des points de jonction spécifiés

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

Avant de commencer

- L'agrégat dans lequel vous souhaitez créer le volume doit déjà exister.
- À partir de ONTAP 9.13.1, vous pouvez créer des volumes avec les fonctions d'analyse de la capacité et de suivi des activités activées. Pour activer le suivi de capacité ou d'activité, exécutez la `volume create` commande avec `-analytics-state` ou `-activity-tracking-state` définissez sur `on`.

  Pour en savoir plus sur l'analyse de la capacité et le suivi des activités, reportez-vous à la section "Activez l'analyse du système de fichiers". Pour en savoir plus, `volume create` consultez le "Référence de commande ONTAP".

> Les caractères suivants ne peuvent pas être utilisés dans le chemin de jonction : `* # " > < | ? \`

De plus, la longueur du chemin de jonction ne peut pas dépasser 255 caractères.

Étapes

1. Créer le volume avec un point de jonction :

```
volume create -vserver <vserver_name> -volume <volume_name> -aggregate
<aggregate_name> -size {integer[KB|MB|GB|TB|PB]} -security-style
{ntfs|unix|mixed} -junction-path <junction_path>
```

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

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

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

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

2. Vérifier que le volume a été créé avec le point de jonction souhaité :

```
volume show -vserver <vserver_name> -volume <volume_name> -junction
```

Exemple

L'exemple suivant crée un volume nommé `home4` situé sur le SVM vs1 qui a une Junction path `/eng/home`:

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

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

Créer des volumes NAS ONTAP sans points de jonction spécifiques

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

exportations NFS pour ce volume.

Avant de commencer

- L'agrégat dans lequel vous souhaitez créer le volume doit déjà exister.
- À partir de ONTAP 9.13.1, vous pouvez créer des volumes avec les fonctions d'analyse de la capacité et de suivi des activités activées. Pour activer le suivi de capacité ou d'activité, exécutez la `volume create` commande avec `-analytics-state` ou `-activity-tracking-state` définissez sur `on`.

  Pour en savoir plus sur l'analyse de la capacité et le suivi des activités, reportez-vous à la section "Activez l'analyse du système de fichiers". Pour en savoir plus, `volume create` consultez le "Référence de commande ONTAP".

Étapes

1. Créer le volume sans point de jonction en utilisant la commande suivante :

   ```
   volume create -vserver vserver_name -volume volume_name -aggregate
   aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style
   {ntfs|unix|mixed}
   ```

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

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

2. Vérifier que le volume a été créé sans point de jonction :

   ```
   volume show -vserver vserver_name -volume volume_name -junction
   ```

Exemple

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

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

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

Monter ou démonter des volumes ONTAP NFS dans l'espace de noms NAS

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

Description de la tâche

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

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

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

Étapes

1. Effectuez l'action souhaitée :

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

Les fonctions que vous recherchez…	Entrez les commandes…

Démonter un volume	`volume unmount -vserver svm_name -volume volume_name`
	
	`volume offline -vserver svm_name -volume volume_name`

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

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

Exemples

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

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

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

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

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

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

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

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

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

Vous pouvez afficher des informations sur les volumes montés pour les SVM et les points

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

Étape

1. Effectuez l'action souhaitée :

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

Exemples

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

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

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

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

Configurer les styles de sécurité

Comment les styles de sécurité affectent l'accès aux données

En savoir plus sur les styles de sécurité NAS ONTAP

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

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

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

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

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

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

Le `show-effective-permissions` paramètre avec le `vserver security file-directory` La commande vous permet d'afficher les autorisations effectives accordées à un utilisateur Windows ou UNIX sur le chemin de fichier ou de dossier spécifié. En outre, le paramètre facultatif `-share-name` vous permet d'afficher l'autorisation de partage effectif. Pour en savoir plus, `vserver security file-directory show-effective-permissions` consultez le "Référence de commande ONTAP".

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

Informations associées

- "Référence de commande ONTAP"

En savoir plus sur les styles de sécurité sur les volumes ONTAP NFS FlexVol

Les styles de sécurité peuvent être définis sur les volumes FlexVol (volumes root ou de

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

Décidez quel style de sécurité utiliser sur les SVM NAS ONTAP

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

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

Style de sécurité	Choisissez si…
UNIX	• Le système de fichiers est géré par un administrateur UNIX. • La plupart des utilisateurs sont des clients NFS. • Une application accédant aux données utilise un utilisateur UNIX comme compte de service.
NTFS	• Le système de fichiers est géré par un administrateur Windows. • La majorité des utilisateurs sont des clients SMB. • Une application accédant aux données utilise un utilisateur Windows comme compte de service.
Mixte	• Le système de fichiers est géré à la fois par les administrateurs et utilisateurs d'UNIX et de Windows, et il se compose de clients NFS et SMB.

En savoir plus sur l'héritage de style de sécurité NFS de ONTAP

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

Les styles de sécurité sont hérités de la manière suivante :

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

En savoir plus sur la préservation des autorisations ONTAP NFS 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.

Gérer les autorisations UNIX sur les SVM ONTAP NFS à l'aide de l'onglet Sécurité Windows

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

- Modification des autorisations UNIX

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

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

- Modification des autorisations UNIX en autorisations NTFS

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

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

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

Configurer les styles de sécurité sur les volumes racine ONTAP NFS SVM

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

Étapes

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

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

2. Afficher et vérifier la configuration, y compris le style de sécurité du volume root du SVM que vous avez créé :

   `vserver show -vserver vserver_name`

Configurer les styles de sécurité sur les volumes ONTAP NFS FlexVol

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

Étapes

1. Effectuez l'une des opérations suivantes :

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

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

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

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

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

   `volume show -volume volume_name -instance`

Configurer les styles de sécurité sur les qtrees ONTAP NFS

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

Étapes

1. Effectuez l'une des opérations suivantes :

Si le qtree…	Utilisez la commande…

N’existe pas encore	`volume qtree create` et inclure le `-security-style` paramètre pour spécifier le style de sécurité.
Existe déjà	`volume qtree modify` et inclure le `-security-style` paramètre pour spécifier le style de sécurité.

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

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

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

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

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

En savoir plus sur la configuration de l’accès aux fichiers NFS sur les SVM ONTAP

Vous devez suivre un certain nombre d’étapes pour permettre aux clients d’accéder aux fichiers sur des SVM (Storage Virtual machine) à l’aide de NFS. Certaines étapes supplémentaires sont facultatives en fonction de la configuration actuelle de votre environnement.

Pour que les clients puissent accéder aux fichiers sur des SVM via NFS, vous devez effectuer les tâches suivantes :

1. Activer le protocole NFS sur le SVM.

   On doit configurer le SVM de façon à permettre l’accès aux données des clients sur NFS.

2. Créer un serveur NFS sur le SVM.

   Un serveur NFS est une entité logique du SVM qui permet à la SVM de transmettre des fichiers via NFS. Vous devez créer le serveur NFS et spécifier les versions de protocole NFS que vous souhaitez autoriser.

3. Configurer les export policy sur le SVM.

   Vous devez configurer des règles d’exportation pour que les volumes et les qtrees soient disponibles pour les clients.

4. Configurez le serveur NFS avec les paramètres de sécurité appropriés et d’autres paramètres en fonction du réseau et de l’environnement de stockage.

   Cette étape peut inclure la configuration de Kerberos, LDAP, NIS, mappages de noms et utilisateurs locaux.

Sécurisation de l’accès NFS à l’aide de règles d’exportation

Comment les politiques d’exportation contrôlent l’accès des clients aux volumes NFS ou qtrees ONTAP

Les règles d’exportation contiennent une ou plusieurs *export rules* qui traitent chaque demande d’accès client. Le résultat du processus détermine si le client est refusé ou accordé et quel niveau d’accès. Un export policy avec règles d’export doit exister sur la machine virtuelle de stockage (SVM) afin que les clients puissent accéder aux données.

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

- Assigner différentes export policy à chaque volume ou qtree du SVM pour le contrôle d’accès client individuel à chaque volume ou qtree du SVM.
- Assigner la même export policy à plusieurs volumes ou qtree du SVM pour un contrôle d’accès client identique sans avoir à créer une nouvelle export policy pour chaque volume ou qtree.

Si un client effectue une demande d’accès qui n’est pas autorisée par la stratégie d’exportation applicable, la requête échoue et un message d’autorisation est refusé. Si un client ne correspond à aucune règle de l’export policy, l’accès est refusé. Si une export policy est vide, alors tous les accès sont implicitement refusés.

Vous pouvez modifier une export-policy de manière dynamique sur un système exécutant ONTAP.

Stratégies d’exportation par défaut pour les SVM NFS ONTAP

Chaque SVM dispose d’une export policy par défaut qui ne contient aucune règle. Un export policy avec règles doit exister pour que les clients puissent accéder aux données sur la SVM. Chaque volume FlexVol contenu au SVM doit être associé à une export policy.

Lorsque vous créez un SVM, le système de stockage crée automatiquement une export policy par défaut appelée `default` Pour le volume root du SVM. On doit créer une ou plusieurs règles pour l’export policy par défaut avant que les clients puissent accéder aux données sur la SVM. Vous pouvez également créer une export-policy personnalisée avec des règles. Vous pouvez modifier et renommer l’export policy par défaut, mais vous ne pouvez pas supprimer l’export policy par défaut.

Lorsque vous créez un volume FlexVol dans son SVM contenant, le système de stockage crée le volume et associe le volume avec la export policy par défaut pour le volume root du SVM. Par défaut, chaque volume créé au sein du SVM est associé à l’export policy par défaut pour le volume root. Vous pouvez utiliser l’export policy par défaut pour tous les volumes contenus dans le SVM, ou bien créer une export policy unique pour chaque volume. Vous pouvez associer plusieurs volumes à la même export policy.

Comment fonctionnent les règles d’exportation NFS ONTAP

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

Une export-policy doit contenir au moins une règle d’exportation pour permettre l’accès aux clients. Si une

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

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

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

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

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

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

> Depuis ONTAP 9.3, vous pouvez activer la vérification de la configuration des règles d'exportation en tant que tâche d'arrière-plan qui enregistre toutes les violations de règles dans une liste de règles d'erreur. Le `vserver export-policy config-checker` les commandes invoquent le vérificateur et affichent les résultats, que vous pouvez utiliser pour vérifier votre configuration et supprimer des règles erronées de la stratégie.
>
> Les commandes valident uniquement la configuration d'exportation pour les noms d'hôte, les groupes réseau et les utilisateurs anonymes.

Exemple

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

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

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

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

Exemple

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

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

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

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

Exemple

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

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

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

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

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

Gérer l'accès ONTAP SVM pour les clients NFS avec des types de sécurité non répertoriés

Lorsqu'un client se présente avec un type de sécurité qui n'est pas répertorié dans un paramètre d'accès d'une règle d'exportation, vous pouvez soit refuser l'accès au client, soit le mapper à l'ID utilisateur anonyme à la place de l'aide de l'option `none` dans le paramètre d'accès.

Un client peut se présenter avec un type de sécurité qui n'est pas répertorié dans un paramètre d'accès car il a été authentifié avec un type de sécurité différent ou n'a pas été authentifié du tout (type de sécurité AUTH_NONE). Par défaut, l'accès au client est automatiquement refusé. Toutefois, vous pouvez ajouter l'option `none` au paramètre d'accès. Par conséquent, les clients dont le style de sécurité n'est pas répertorié sont mappés sur l'ID utilisateur anonyme. Le `-anon` Paramètre détermine quel ID utilisateur est attribué à ces clients. ID utilisateur spécifié pour le `-anon` le paramètre doit être un utilisateur valide configuré avec des autorisations appropriées pour l'utilisateur anonyme.

Valeurs valides pour le `-anon` plage de paramètres de `0` à `65535`.

ID utilisateur attribué à `-anon`	**Traitement des demandes d'accès client résultant**
`0` - `65533`	La demande d'accès client est mappée à l'ID utilisateur anonyme et obtient l'accès en fonction des autorisations configurées pour cet utilisateur.

ID utilisateur attribué à `-anon`	Traitement des demandes d'accès client résultant
`65534`	La demande d'accès client est mappée à l'utilisateur personne et obtient l'accès en fonction des autorisations configurées pour cet utilisateur. Il s'agit de la valeur par défaut.
`65535`	La demande d'accès de n'importe quel client est refusée lorsqu'elle est mappée à cet ID et que le client se présente avec le type de sécurité AUTH_NONE. La demande d'accès des clients avec l'ID utilisateur 0 est refusée lorsqu'elle est mappée à cet ID et que le client se présente avec tout autre type de sécurité.

Lorsque vous utilisez l'option `none`, il est important de se rappeler que le paramètre lecture seule est traité en premier. Lors de la configuration des règles d'exportation pour les clients dont les types de sécurité ne sont pas répertoriés, prenez en compte les consignes suivantes :

La lecture seule inclut `none`	Lecture-écriture incluse `none`	Accès résultant pour les clients avec des types de sécurité non répertoriés
Non	Non	Refusée
Non	Oui.	Refusé car la lecture seule est traitée en premier
Oui.	Non	Lecture seule comme anonyme
Oui.	Oui.	Lecture-écriture comme anonyme

Exemple

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

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule any`
- `-anon 70`

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

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

Le client #3 a l'adresse IP 10.1.16.234, envoie une demande d'accès à l'aide du protocole NFSv3 et ne

s’authentifie pas (ce qui signifie le type de sécurité AUTH_NONE).

Le protocole d’accès client et l’adresse IP correspondent pour les trois clients. Le paramètre lecture seule permet l’accès en lecture seule aux clients avec leur propre ID utilisateur authentifié auprès de AUTH_SYS. Le paramètre lecture seule permet l’accès en lecture seule en tant qu’utilisateur anonyme avec l’ID utilisateur 70 aux clients authentifiés à l’aide de n’importe quel autre type de sécurité. Le paramètre lecture-écriture permet l’accès en lecture-écriture à n’importe quel type de sécurité, mais s’applique uniquement aux clients déjà filtrés par la règle en lecture seule.

Par conséquent, les clients n° 1 et n° 3 bénéficient de l’accès en lecture-écriture uniquement en tant qu’utilisateur anonyme avec l’ID utilisateur 70. Le client #2 obtient un accès en lecture-écriture avec son propre ID utilisateur.

Exemple

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

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule none`
- `-anon 70`

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

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

Le client #3 a l’adresse IP 10.1.16.234, envoie une demande d’accès à l’aide du protocole NFSv3 et ne s’authentifie pas (ce qui signifie le type de sécurité AUTH_NONE).

Le protocole d’accès client et l’adresse IP correspondent pour les trois clients. Le paramètre lecture seule permet l’accès en lecture seule aux clients avec leur propre ID utilisateur authentifié auprès de AUTH_SYS. Le paramètre lecture seule permet l’accès en lecture seule en tant qu’utilisateur anonyme avec l’ID utilisateur 70 aux clients authentifiés à l’aide de n’importe quel autre type de sécurité. Le paramètre lecture-écriture permet l’accès en lecture-écriture uniquement en tant qu’utilisateur anonyme.

Par conséquent, les clients #1 et le client #3 obtiennent un accès en lecture-écriture uniquement en tant qu’utilisateur anonyme avec l’ID utilisateur 70. Le client #2 obtient un accès en lecture seule avec son propre ID utilisateur, mais il est refusé l’accès en lecture-écriture.

Comment les types de sécurité ONTAP déterminent les niveaux d’accès des clients NFS

Le type de sécurité auquel le client s’est authentifié joue un rôle particulier dans les règles d’exportation. Vous devez comprendre la manière dont le type de sécurité détermine les niveaux d’accès du client à un volume ou à un qtree.

Les trois niveaux d’accès possibles sont les suivants :

1. Lecture seule
2. Lecture-écriture

3. Super-utilisateur (pour les clients ayant l'ID utilisateur 0)

Dans la mesure où le niveau d'accès par type de sécurité est évalué dans cet ordre, vous devez respecter les règles suivantes lors de la construction de paramètres de niveau d'accès dans les règles d'exportation :

Pour qu'un client puisse obtenir le niveau d'accès…	**Ces paramètres d'accès doivent correspondre au type de sécurité du client…**
Lecture seule normale par l'utilisateur	Lecture seule (`-rorule`)
Lecture-écriture utilisateur normale	Lecture seule (`-rorule`) et lecture-écriture (`-rwrule`)
Super-utilisateur en lecture seule	Lecture seule (`-rorule`) et `-superuser`
Super-utilisateur lecture-écriture	Lecture seule (`-rorule`) et lecture-écriture (`-rwrule`) et `-superuser`

Les types de sécurité suivants sont valides pour chacun de ces trois paramètres d'accès :

- `any`
- `none`
- `never`

  Ce type de sécurité n'est pas valide pour une utilisation avec `-superuser` paramètre.

- `krb5`
- `krb5i`
- `krb5p`
- `ntlm`
- `sys`

Lorsque vous faites correspondre le type de sécurité d'un client à chacun des trois paramètres d'accès, trois résultats sont possibles :

Si le type de sécurité du client…	**Ensuite, le client…**
Correspond à celui spécifié dans le paramètre d'accès.	Obtient l'accès à ce niveau avec son propre ID utilisateur.
Ne correspond pas à celui spécifié, mais le paramètre d'accès inclut l'option `none`.	Obtient l'accès pour ce niveau, mais en tant qu'utilisateur anonyme avec l'ID utilisateur spécifié par le `-anon` paramètre.

Si le type de sécurité du client…	Ensuite, le client…
Ne correspond pas à celui spécifié et le paramètre d'accès n'inclut pas l'option `none`.	Ne dispose d'aucun accès pour ce niveau.cela ne s'applique pas à l' `-superuser` paramètre car il inclut toujours `none` même si elle n'est pas spécifiée.

Exemple

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

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

Le client #1 a l'adresse IP 10.1.16.207, a l'ID utilisateur 0, envoie une demande d'accès à l'aide du protocole NFSv3 et authentifiée avec Kerberos v5.

Le client #2 a l'adresse IP 10.1.16.211, a l'ID utilisateur 0, envoie une demande d'accès à l'aide du protocole NFSv3 et authentifiée avec AUTH_SYS.

Le client #3 a l'adresse IP 10.1.16.234, a l'ID utilisateur 0, envoie une demande d'accès à l'aide du protocole NFSv3 et n'a pas authentifié (AUTH_NONE).

Le protocole d'accès client et l'adresse IP correspondent aux trois clients. Le paramètre lecture seule permet un accès en lecture seule à tous les clients, quel que soit leur type de sécurité. Le paramètre lecture-écriture permet l'accès en lecture-écriture aux clients avec leur propre ID utilisateur authentifié par AUTH_SYS ou Kerberos v5. Le paramètre superuser permet un accès superuser aux clients avec l'ID utilisateur 0 authentifié avec Kerberos v5.

Par conséquent, le client #1 obtient l'accès en lecture-écriture superutilisateur car il correspond aux trois paramètres d'accès. Le client #2 obtient un accès en lecture-écriture mais pas un accès super-utilisateur. Le client #3 obtient un accès en lecture seule mais pas un accès super-utilisateur.

En savoir plus sur la gestion des demandes d'accès superutilisateur ONTAP NFS

Lorsque vous configurez des stratégies d'exportation, vous devez tenir compte de ce que vous voulez faire si le système de stockage reçoit une demande d'accès client avec l'ID utilisateur 0, c'est-à-dire en tant que superutilisateur, et définir vos règles d'exportation en conséquence.

Dans le monde UNIX, un utilisateur avec l'ID utilisateur 0 est appelé superutilisateur, généralement appelé root, qui dispose de droits d'accès illimités sur un système. L'utilisation des privilèges de superutilisateur peut être dangereuse pour plusieurs raisons, y compris une violation du système et de la sécurité des données.

Par défaut, ONTAP mappe les clients présentant l'ID utilisateur 0 à l'utilisateur anonyme. Toutefois, vous pouvez spécifier le `-superuser` Paramètre dans les règles d'exportation pour déterminer comment gérer les clients présentant l'ID utilisateur 0 en fonction de leur type de sécurité. Les options suivantes sont valides pour le `-superuser` paramètre :

- any
- none

  Il s'agit du paramètre par défaut si vous ne spécifiez pas le -superuser paramètre.

- krb5
- ntlm
- sys

Il existe deux façons différentes de gérer les clients présentant l'ID utilisateur 0, selon le -superuser configuration des paramètres :

Si le -superuser et le type de sécurité du client…	Ensuite, le client…
Correspondance	Obtient l'accès superutilisateur avec l'ID utilisateur 0.
Ne correspondent pas	Obtient l'accès en tant qu'utilisateur anonyme avec l'ID utilisateur spécifié par le -anon paramètre et ses autorisations attribuées. Cette option est précise si le paramètre lecture seule ou lecture-écriture spécifie l'option none.

Si un client se présente avec l'ID utilisateur 0 pour accéder à un volume avec le style de sécurité NTFS et le -superuser le paramètre est défini sur none, ONTAP utilise le mappage de noms pour l'utilisateur anonyme afin d'obtenir les informations d'identification appropriées.

Exemple

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

- -protocol nfs3
- -clientmatch 10.1.16.0/255.255.255.0
- -rorule any
- -rwrule krb5,ntlm
- -anon 127

Le client n° 1 a l'adresse IP 10.1.16.207, a l'ID utilisateur 746, envoie une demande d'accès à l'aide du protocole NFSv3 et s'authentifie avec Kerberos v5.

Le client #2 a l'adresse IP 10.1.16.211, a l'ID utilisateur 0, envoie une demande d'accès à l'aide du protocole NFSv3 et authentifiée avec AUTH_SYS.

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

Le client #2 ne dispose pas d'un accès super-utilisateur. Au lieu de cela, il est mappé sur anonyme car le -superuser paramètre non spécifié. Cela signifie que la valeur par défaut est none Et mappe

automatiquement l'ID utilisateur 0 sur anonyme. Le client #2 obtient également un accès en lecture seule car son type de sécurité ne correspond pas au paramètre lecture-écriture.

Exemple

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

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-superuser krb5`
- `-anon 0`

Le client #1 a l'adresse IP 10.1.16.207, a l'ID utilisateur 0, envoie une demande d'accès à l'aide du protocole NFSv3 et authentifiée avec Kerberos v5.

Le client #2 a l'adresse IP 10.1.16.211, a l'ID utilisateur 0, envoie une demande d'accès à l'aide du protocole NFSv3 et authentifiée avec AUTH_SYS.

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

La règle d'exportation permet l'accès superutilisateur pour les clients avec l'ID utilisateur 0. Le client #1 obtient l'accès superutilisateur car il correspond à l'ID utilisateur et au type de sécurité pour la lecture seule et `-superuser` paramètres. Le client #2 ne dispose pas d'un accès en lecture-écriture ou super-utilisateur, car son type de sécurité ne correspond pas au paramètre en lecture-écriture ou au `-superuser` paramètre. Au lieu de cela, le client #2 est mappé à l'utilisateur anonyme, qui a dans ce cas l'ID utilisateur 0.

En savoir plus sur les caches de stratégie d'exportation NFS ONTAP

Pour améliorer les performances système, ONTAP utilise des caches locaux pour stocker des informations telles que les noms d'hôtes et les groupes de réseaux. Cela permet à ONTAP de traiter les règles des export-policy plus rapidement que de récupérer les informations à partir de sources externes. Comprendre ce qu'sont les caches et ce qu'ils font pour vous aider à résoudre les problèmes d'accès client.

Vous configurez les export policy pour contrôler l'accès client aux exports NFS. Chaque export policy contient des règles, et chaque règle contient des paramètres qui correspondent à la règle avec les clients demandant un accès. Certains de ces paramètres exigent que ONTAP contacte une source externe, telle que des serveurs DNS ou NIS, pour résoudre des objets tels que des noms de domaine, des noms d'hôtes ou des groupes réseau.

Ces communications avec des sources externes prennent peu de temps. Afin d'améliorer les performances, ONTAP réduit le temps nécessaire à la résolution des objets de règles d'exportation en stockant les informations localement sur chaque nœud dans plusieurs caches.

Nom du cache	Type d'information stockée
L'accès	Mise en correspondance des clients avec les règles d'exportation correspondantes
Nom	Mappage des noms d'utilisateur UNIX avec les ID utilisateur UNIX correspondants
ID	Mappage des ID utilisateur UNIX avec les ID utilisateur UNIX correspondants et les ID de groupe UNIX étendus
Hôte	Mappages de noms d'hôtes sur les adresses IP correspondantes
Groupe réseau	Mappages de groupes réseau aux adresses IP correspondantes des membres
Showmount	Liste des répertoires exportés depuis le namespace du SVM

Si vous modifiez les informations sur les serveurs de noms externes de votre environnement après la récupération et le stockage en local par ONTAP, les caches peuvent désormais contenir des informations obsolètes. Bien que les mises à jour ONTAP se placent automatiquement après certaines périodes, différents caches ont des temps d'expiration et d'actualisation et des algorithmes différents.

Une autre raison possible pour que les caches contiennent des informations obsolètes est le moment où ONTAP tente d'actualiser les informations en cache mais rencontre un échec lors de tentatives de communication avec des serveurs de noms. Dans ce cas, ONTAP continue d'utiliser les informations actuellement stockées dans les caches locaux pour éviter toute perturbation du client.

Par conséquent, les demandes d'accès des clients qui sont censées réussir risquent d'échouer et les demandes d'accès des clients qui sont censées échouer pourraient réussir. Vous pouvez afficher et vider manuellement certains caches de règles d'exportation lors du dépannage de tels problèmes d'accès client.

En savoir plus sur les caches d'accès NFS ONTAP

ONTAP utilise un cache d'accès pour stocker les résultats de l'évaluation de la règle d'export policy pour les opérations d'accès client à un volume ou à un qtree. Il en résulte une amélioration des performances, car les informations peuvent être récupérées beaucoup plus rapidement depuis le cache d'accès qu'un processus d'évaluation des règles d'export-policy à chaque fois qu'un client envoie une requête d'E/S.

Lorsqu'un client NFS envoie une requête d'E/S pour accéder aux données d'un volume ou qtree, ONTAP doit évaluer chaque demande d'E/S afin de déterminer s'il faut accorder ou refuser la demande d'E/S. Cette évaluation implique de vérifier chaque règle d'export policy de la export policy associée au volume ou à qtree. Si le chemin vers le volume ou qtree implique de franchir un ou plusieurs points de jonction, cette vérification peut s'avérer nécessaire pour rechercher plusieurs règles d'exportation le long du chemin.

Notez que cette évaluation est effectuée pour chaque demande d'E/S envoyée depuis un client NFS, par exemple pour la lecture, l'écriture, la liste, la copie et d'autres opérations. Il ne s'agit pas uniquement de

demandes de montage initiales.

Une fois que ONTAP a identifié les règles d'export policy applicables et a décidé d'autoriser ou de refuser la requête, ONTAP crée ensuite une entrée dans le cache d'accès pour stocker ces informations.

Lorsqu'un client NFS envoie une requête d'E/S, ONTAP note l'adresse IP du client, l'ID de la SVM et la export policy associée au volume cible ou au qtree, et recherche d'abord une entrée correspondante dans le cache d'accès. S'il existe une entrée correspondante dans le cache d'accès, ONTAP utilise les informations stockées pour autoriser ou refuser la demande d'E/S. Si aucune entrée correspondante n'existe, ONTAP passe par le processus normal d'évaluation de toutes les règles de politique applicables, comme expliqué ci-dessus.

Les entrées du cache d'accès qui ne sont pas utilisées activement ne sont pas actualisées. Cela permet de réduire les communications inutiles et inutiles avec des services de noms externes.

La récupération des informations à partir du cache d'accès est bien plus rapide qu'au cours de l'intégralité du processus d'évaluation des règles des règles d'export-policy pour chaque demande d'E/S. Par conséquent, l'utilisation du cache d'accès améliore nettement les performances en réduisant la surcharge liée aux vérifications d'accès client.

En savoir plus sur les paramètres du cache d'accès NFS ONTAP

Plusieurs paramètres contrôlent les périodes d'actualisation des entrées dans le cache d'accès. Le fonctionnement de ces paramètres vous permet de les modifier pour régler le cache d'accès et équilibrer les performances avec la récente information stockée.

Le cache d'accès stocke des entrées composées d'une ou plusieurs règles d'exportation qui s'appliquent aux clients qui essaient d'accéder aux volumes ou aux qtrees. Ces entrées sont stockées pendant un certain temps avant leur actualisation. La durée d'actualisation est déterminée par les paramètres du cache d'accès et dépend du type d'entrée du cache d'accès.

Vous pouvez spécifier les paramètres du cache d'accès pour chaque SVM. Cela permet aux paramètres de différer en fonction des exigences d'accès des SVM. Les entrées de cache d'accès qui ne sont pas utilisées activement ne sont pas réactualisées, ce qui réduit les communications inutiles et inutiles avec le nom externe sert.

Accès au type d'entrée du cache	Description	Période d'actualisation en secondes
Entrées positives	Les entrées du cache d'accès qui n'ont pas entraîné de refus d'accès aux clients.	Minimum: 300 Maximum : 86,400 Valeur par défaut : 3,600
Entrées négatives	Les entrées du cache d'accès qui ont entraîné un refus d'accès aux clients.	Minimum : 60 Maximum : 86,400 Valeur par défaut : 3,600

Exemple

Un client NFS tente d'accéder à un volume sur un cluster. ONTAP mappe le client sur une règle export policy et détermine que le client accède à cette règle en fonction de la configuration de la règle export policy. ONTAP

stocke la règle d'export policy dans le cache d'accès sous forme d'entrée positive. Par défaut, ONTAP conserve l'entrée positive dans le cache d'accès pendant une heure (3,600 secondes), puis actualise automatiquement l'entrée pour maintenir les informations à jour.

Pour éviter que le cache d'accès ne se remplit inutilement, il existe un paramètre supplémentaire pour effacer les entrées existantes du cache d'accès qui n'ont pas été utilisées pendant une certaine période pour décider de l'accès client. C'est ça `-harvest-timeout` le paramètre a une plage autorisée de 60 à 2,592,000 secondes et un réglage par défaut de 86,400 secondes.

Supprimer les politiques d'exportation des qtrees ONTAP NFS

Si vous décidez de ne plus vouloir attribuer une export policy spécifique à un qtree, vous pouvez supprimer la export policy en modifiant le qtree de manière à hériter de la export policy du volume contenant. Pour ce faire, utilisez le `volume qtree modify` commande avec `-export-policy` paramètre et chaîne de nom vide ("").

Étapes

1. Pour supprimer une export policy d'un qtree, entrez la commande suivante :

   ```
   volume qtree modify -vserver vserver_name -qtree-path
   /vol/volume_name/qtree_name -export-policy ""
   ```

2. Vérifier que le qtree a été modifié en conséquence :

   ```
   volume qtree show -qtree qtree_name -fields export-policy
   ```

Valider les identifiants qtree ONTAP NFS pour les opérations de fichiers qtree

ONTAP peut procéder à une validation supplémentaire facultative des ID de qtree. Cette validation garantit que les demandes d'opérations de fichiers client utilisent un ID qtree valide et que les clients ne peuvent déplacer que les fichiers au sein du même qtree. Vous pouvez activer ou désactiver cette validation en modifiant le `-validate-qtree -export` paramètre. Ce paramètre est activé par défaut.

Description de la tâche

Ce paramètre n'est efficace que lorsque vous avez attribué une export policy directement à un ou plusieurs qtrees sur la machine virtuelle de stockage (SVM).

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Effectuez l'une des opérations suivantes :

Pour que la validation de l'ID qtree soit…	Saisissez la commande suivante…
Activé	`vserver nfs modify -vserver vserver_name -validate-qtree-export enabled`

Pour que la validation de l'ID qtree soit…	Saisissez la commande suivante…
Désactivé	`vserver nfs modify -vserver vserver_name -validate-qtree-export disabled`

3. Retour au niveau de privilège admin :

   ```
   set -privilege admin
   ```

Restrictions de politique d'exportation et jonctions imbriquées pour les volumes ONTAP NFS FlexVol

Si vous avez configuré des stratégies d'exportation pour définir une stratégie moins restrictive sur une jonction imbriquée mais une règle plus restrictive sur une jonction de niveau supérieur, l'accès à la jonction de niveau inférieur peut échouer.

Vous devez vous assurer que les jonctions de niveau supérieur disposent de règles d'exportation moins restrictives que les jonctions de niveau inférieur.

Utilisation de Kerberos avec NFS pour une sécurité renforcée

Prise en charge ONTAP NFS pour Kerberos

Kerberos fournit une authentification sécurisée renforcée pour les applications client/Server. L'authentification permet de vérifier les identités des utilisateurs et des processus à un serveur. Dans l'environnement ONTAP, Kerberos assure une authentification entre les SVM (Storage Virtual machine) et les clients NFS.

Dans ONTAP 9, les fonctionnalités Kerberos suivantes sont prises en charge :

- Authentification Kerberos 5 avec contrôle d'intégrité (krb5i)

  Krb5i utilise des checksums pour vérifier l'intégrité de chaque message NFS transféré entre le client et le serveur. Cette fonction est utile pour des raisons de sécurité (par exemple pour s'assurer que les données n'ont pas été falsifiées) et pour des raisons d'intégrité des données (par exemple, pour empêcher la corruption des données lors de l'utilisation de NFS sur des réseaux non fiables).

- Authentification Kerberos 5 avec vérification de la confidentialité (krb5p)

  Krb5p utilise des checksums pour chiffrer l'ensemble du trafic entre le client et le serveur. Ceci est plus sûr et entraîne également plus de charge.

- Chiffrement AES 128 bits et 256 bits

  Advanced Encryption Standard (AES) est un algorithme de cryptage permettant de sécuriser les données électroniques. ONTAP prend en charge AES avec des clés 128 bits (AES-128) et AES avec des clés 256 bits (AES-256) pour Kerberos pour une sécurité renforcée.

- Les configurations de Royaume Kerberos au niveau du SVM

  Les administrateurs des SVM peuvent désormais créer des configurations de domaine Kerberos au niveau

du SVM. Les administrateurs des SVM n'ont plus besoin de se reposer sur l'administrateur du cluster pour la configuration des royaumes Kerberos. Ils peuvent donc créer des configurations de Royaume Kerberos individuelles dans un environnement mutualisé.

Conditions requises pour la configuration de Kerberos avec ONTAP NFS

Avant de configurer Kerberos avec NFS sur votre système, vous devez vérifier que certains éléments de votre réseau et de votre environnement de stockage sont correctement configurés.

> Les étapes de configuration de votre environnement dépendent de la version et du type du système d'exploitation client, du contrôleur de domaine, de Kerberos, DNS, etc. Que vous utilisez. La documentation de toutes ces variables dépasse le cadre de ce document. Pour plus d'informations, reportez-vous à la documentation correspondante pour chaque composant.
>
> Pour obtenir un exemple détaillé de la configuration de ONTAP et de Kerberos 5 avec NFSv3 et NFSv4 dans un environnement utilisant des hôtes Windows Server 2008 R2 Active Directory et Linux, consultez le rapport technique 4073.

Les éléments suivants doivent d'abord être configurés :

Conditions requises pour l'environnement réseau

- Kerberos

  Vous devez avoir une configuration Kerberos fonctionnant avec un centre de distribution de clés (KDC), tel que Windows Active Directory Based Kerberos ou MIT Kerberos.

  Les serveurs NFS doivent utiliser `nfs` en tant que composant principal de leur machine principale.

- Service d'annuaire

  Vous devez utiliser un service d'annuaire sécurisé dans votre environnement, tel qu'Active Directory ou OpenLDAP, configuré pour utiliser LDAP sur SSL/TLS.

- NTP

  Vous devez disposer d'un serveur de temps de travail exécutant NTP. Cette opération est nécessaire pour éviter l'échec de l'authentification Kerberos en raison de l'inclinaison du temps.

- Résolution des noms de domaine (DNS)

  Chaque client UNIX et chaque LIF de SVM doivent avoir un enregistrement de service (SRV) correct enregistré auprès du KDC dans des zones de recherche avant et arrière. Tous les participants doivent être résolus correctement via DNS.

- Comptes d'utilisateur

  Chaque client doit disposer d'un compte utilisateur dans le domaine Kerberos. Les serveurs NFS doivent utiliser « nfs » comme composant principal de leur machine principale.

Exigences du client NFS

- NFS

  Chaque client doit être correctement configuré pour communiquer sur le réseau en utilisant NFSv3 ou NFSv4.

  Les clients doivent prendre en charge les RFC1964 et RFC2203.

- Kerberos

  Chaque client doit être correctement configuré pour utiliser l'authentification Kerberos, avec les informations suivantes :

  - Le chiffrement pour les communications TGS est activé.

    AES-256 pour une sécurité optimale.

  - Le type de cryptage le plus sécurisé pour les communications TGT est activé.
  - Le domaine et le domaine Kerberos sont configurés correctement.
  - GSS est activé.

    Lors de l'utilisation des informations d'identification de la machine

  - Ne pas exécuter `gssd` avec le `-n` paramètre.
  - Ne pas exécuter `kinit` en tant qu'utilisateur root.
- Chaque client doit utiliser la version la plus récente et la plus récente du système d'exploitation.

  Cela offre la meilleure compatibilité et fiabilité pour le chiffrement AES avec Kerberos.

- DNS

  Chaque client doit être correctement configuré pour utiliser DNS pour la résolution correcte du nom.

- NTP

  Chaque client doit être en cours de synchronisation avec le serveur NTP.

- Informations sur l'hôte et le domaine

  Chaque client `/etc/hosts` et `/etc/resolv.conf` Les fichiers doivent contenir le nom d'hôte et les informations DNS correctes, respectivement.

- Fichiers keytab

  Chaque client doit avoir un fichier keytab du KDC. Le Royaume doit être en majuscules. Le type de chiffrement doit être AES-256 pour une sécurité optimale.

- Facultatif : pour des performances optimales, les clients bénéficient d'au moins deux interfaces réseau : l'une pour communiquer avec le réseau local et l'autre pour communiquer avec le réseau de stockage.

Configuration requise pour le système de stockage

- Licence NFS

Une licence NFS valide doit être installée sur le système de stockage.

- Licence CIFS

  La licence CIFS est facultative. Il n'est nécessaire de vérifier les informations d'identification Windows que lors de l'utilisation du mappage de noms multiprotocole. Elle n'est pas requise dans un environnement UNIX strict.

- SVM

  Au moins un SVM doit être configuré sur le système.

- DNS sur le SVM

  On doit avoir configuré DNS sur chaque SVM.

- Serveur NFS

  Vous devez avoir configuré NFS sur le SVM.

- Cryptage AES

  Pour une sécurité optimale, vous devez configurer le serveur NFS de sorte qu'il n'autorise que le chiffrement AES-256 pour Kerberos.

- Serveur SMB

  Si vous exécutez un environnement multiprotocole, vous devez avoir configuré SMB sur le SVM. Le serveur SMB est requis pour le mappage de noms multiprotocole.

- Volumes

  On doit disposer d'un volume root et d'au moins un volume de données configuré pour une utilisation par la SVM.

- Volume racine

  Le volume root du SVM doit avoir la configuration suivante :

Nom	Réglage
Style de sécurité	UNIX
UID	Racine ou ID 0
GIDS	Racine ou ID 0
Autorisations UNIX	776

  Contrairement au volume racine, les volumes de données peuvent avoir n'importe quel style de sécurité.

- Groupes UNIX

  La SVM doit avoir les groupes UNIX suivants configurés :

Nom du groupe	ID de groupe
démon	1
racine	0
pcuser	65534 (créé automatiquement par ONTAP lors de la création du SVM)

- Utilisateurs UNIX

  Le SVM doit avoir les utilisateurs UNIX suivants configurés :

Nom d'utilisateur	ID d'utilisateur	ID de groupe principal	Commentaire
nfs	500	0	Requis pour la phase INITIALE GSS Le premier composant de l'utilisateur client NFS SPN est utilisé comme utilisateur.
pcuser	65534	65534	Obligatoire pour une utilisation multiprotocole NFS et CIFS Créé et ajouté au groupe pcuser automatiquement par ONTAP lors de la création de la SVM.
racine	0	0	Nécessaire pour le montage

  L'utilisateur nfs n'est pas requis si un mappage de nom Kerberos-UNIX existe pour le SPN de l'utilisateur client NFS.

- Export-policies et rules

  Vous devez avoir configuré des export policy avec les règles d'exportation nécessaires pour les volumes root et de données et les qtrees. Si tous les volumes du SVM sont accessibles via Kerberos, vous pouvez définir les options des règles d'exportation `-rorule`, `-rwrule`, et `-superuser` pour le volume racine à `krb5` , `krb5i`, ou `krb5p`.

- Mapping de noms Kerberos-UNIX

  Si vous souhaitez que l'utilisateur identifié par l'utilisateur client NFS SPN dispose d'autorisations root, vous devez créer un mappage de nom à la racine.

Informations associées

"Rapport technique NetApp 4073 : authentification unifiée sécurisée"

"Matrice d'interopérabilité NetApp"

"Administration du système"

"Gestion du stockage logique"

Spécifiez le domaine d'ID utilisateur ONTAP pour NFSv4

Pour spécifier le domaine d'ID utilisateur, vous pouvez définir le `-v4-id-domain` option.

Description de la tâche

Par défaut, ONTAP utilise le domaine NIS pour le mappage d'ID utilisateur NFSv4, si un est défini. Si aucun domaine NIS n'est défini, le domaine DNS est utilisé. Vous devrez peut-être définir le domaine d'ID utilisateur si, par exemple, vous disposez de plusieurs domaines d'ID utilisateur. Le nom de domaine doit correspondre à la configuration de domaine sur le contrôleur de domaine. Elle n'est pas requise pour NFSv3.

Étape

1. Saisissez la commande suivante :

```
vserver nfs modify -vserver vserver_name -v4-id-domain NIS_domain_name
```

Configurer NAME-services

En savoir plus sur la configuration des commutateurs du service de nom NFS de ONTAP

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

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

Types de base de données

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

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

Type de base de données	Définit les sources de service de noms pour…	Les sources valides sont…
passwd	Recherche des informations utilisateur	fichiers, nis, ldap
groupe réseau	Recherche des informations de groupe réseau	fichiers, nis, ldap
carte de nom	Mappage des noms d'utilisateur	fichiers, ldap

Types de source

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

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

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

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

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

Protocoles utilisés pour accéder à des sources externes

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

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

Exemple

L'exemple suivant montre la configuration du switch de service de nom pour le SVM svm svm_1 :

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

Pour rechercher les adresses IP des hôtes, ONTAP consulte d'abord les fichiers source locaux. Si la requête ne renvoie aucun résultat, les serveurs DNS sont vérifiés ensuite.

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

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

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

Informations associées

"Rapport technique de NetApp 4668 : name Services Best Practices Guide (Guide des meilleures pratiques des services de noms)"

Utiliser LDAP

En savoir plus sur LDAP pour les SVM NFS ONTAP

Un serveur LDAP (Lightweight Directory Access Protocol) vous permet de gérer de manière centralisée les informations utilisateur. Si vous stockez votre base de données utilisateur sur un serveur LDAP dans votre environnement, vous pouvez configurer votre système de stockage pour rechercher les informations utilisateur dans votre base de données LDAP existante.

- Avant de configurer LDAP pour ONTAP, vérifiez que votre déploiement de site respecte les bonnes pratiques en matière de configuration de serveur LDAP et de client. En particulier, les conditions suivantes doivent être remplies :
  - Le nom de domaine du serveur LDAP doit correspondre à l'entrée du client LDAP.
  - Les types de hachage de mot de passe utilisateur LDAP pris en charge par le serveur LDAP doivent inclure ceux pris en charge par ONTAP :
    - CRYPT (tous types) et SHA-1 (SHA, SSHA).
    - Depuis ONTAP 9.8, des hachages SHA-2 (SHA-256, SSH-384, SHA-512, SSHA-256, SSHA-384 et SSHA-512) sont également pris en charge.
  - Si le serveur LDAP nécessite des mesures de sécurité de session, vous devez les configurer dans le client LDAP.

    Les options de sécurité de session suivantes sont disponibles :

    - La signature LDAP (fournit un contrôle de l'intégrité des données), la signature et le chiffrement LDAP (assure le contrôle de l'intégrité des données et le chiffrement)
    - DÉMARRER TLS
    - LDAPS (LDAP sur TLS ou SSL)
  - Pour activer les requêtes LDAP signées et scellées, les services suivants doivent être configurés :
    - Les serveurs LDAP doivent prendre en charge le mécanisme GSSAPI (Kerberos) SASL.
    - Les serveurs LDAP doivent avoir des enregistrements DNS A/AAAA ainsi que des enregistrements PTR configurés sur le serveur DNS.
    - Les serveurs Kerberos doivent contenir des enregistrements SRV sur le serveur DNS.
  - Pour activer START TLS ou LDAPS, les points suivants doivent être pris en compte.
    - Il s'agit d'une meilleure pratique NetApp d'utiliser Start TLS plutôt que LDAPS.
    - Si LDAPS est utilisé, le serveur LDAP doit être activé pour TLS ou pour SSL dans ONTAP 9.5 et versions ultérieures. SSL n'est pas pris en charge dans ONTAP 9.4 - 9.0.
    - Un serveur de certificats doit déjà être configuré dans le domaine.
  - Pour activer la recherche de recommandation LDAP (dans ONTAP 9.5 et versions ultérieures), les conditions suivantes doivent être remplies :
    - Les deux domaines doivent être configurés avec l'une des relations d'approbation suivantes :
      - Bidirectionnel
      - Aller simple, où le principal fait confiance au domaine de référence
      - Parent-enfant
    - Le DNS doit être configuré pour résoudre tous les noms de serveur mentionnés.
    - Les mots de passe du domaine doivent être identiques pour s'authentifier lorsque `--bind-as-cifs-server` défini sur vrai.

Les configurations suivantes ne sont pas prises en charge avec la recherche de références LDAP.

- Pour toutes les versions de ONTAP :
- Clients LDAP sur un SVM d'admin
- Pour ONTAP 9.8 et versions antérieures (ils sont pris en charge dans la version 9.9.1 et ultérieures) :
- Signature et chiffrement LDAP (le `-session-security` en option)
- Connexions TLS cryptées (`-use-start-tls` en option)
- Communications via le port LDAPS 636 (le `-use-ldaps-for-ad-ldap` en option)

- A partir de ONTAP 9.11.1, vous pouvez utiliser "Utilisez la liaison rapide LDAP pour l'authentification nsswitch pour les SVM ONTAP NFS."
- Vous devez entrer un schéma LDAP lors de la configuration du client LDAP sur le SVM.

  Dans la plupart des cas, l'un des schémas ONTAP par défaut sera approprié. Toutefois, si le schéma LDAP de votre environnement diffère de celui-ci, vous devez créer un nouveau schéma client LDAP pour ONTAP avant de créer le client LDAP. Consultez votre administrateur LDAP pour connaître les conditions requises pour votre environnement.

- L'utilisation de LDAP pour la résolution du nom d'hôte n'est pas prise en charge.

Pour plus d'informations, reportez-vous à la section "Rapport technique NetApp 4835 : comment configurer LDAP dans ONTAP".

En savoir plus sur la signature et le scellement LDAP pour les SVM NFS ONTAP

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 NFS sur la machine virtuelle de stockage (SVM) de manière à ce 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`. testez

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

En savoir plus sur LDAPS pour les SVM NFS ONTAP

Vous devez comprendre certains termes et concepts relatifs à la sécurisation de la communication LDAP par ONTAP. ONTAP peut utiliser START TLS ou LDAPS pour configurer des sessions authentifiées entre des serveurs LDAP intégrés à Active Directory ou des serveurs LDAP basés sur UNIX.

Terminologie

Il existe certains termes que vous devez comprendre sur la manière dont ONTAP utilise LDAPS pour sécuriser

les communications LDAP.

- **LDAP**

  (Lightweight Directory Access Protocol) Protocole permettant d'accéder aux répertoires d'informations et de les gérer. LDAP est utilisé comme répertoire d'informations pour le stockage d'objets tels que des utilisateurs, des groupes et des groupes réseau. LDAP fournit également des services d'annuaire qui gèrent ces objets et répondent aux demandes LDAP des clients LDAP.

- **SSL**

  (Secure Sockets Layer) Protocole développé pour envoyer des informations en toute sécurité via Internet. Le protocole SSL est pris en charge par ONTAP 9 et versions ultérieures, mais il est obsolète en faveur de TLS.

- **TLS**

  (Sécurité de la couche de transport) un protocole de suivi conforme aux normes IETF, basé sur les spécifications SSL précédentes. C'est le successeur de SSL. TLS est pris en charge par ONTAP 9.5 et versions ultérieures.

- **LDAPS (LDAP sur SSL ou TLS)**

  Protocole utilisant TLS ou SSL pour sécuriser la communication entre les clients LDAP et les serveurs LDAP. Les termes *LDAP sur SSL* et *LDAP sur TLS* sont parfois utilisés de manière interchangeable. LDAPS est pris en charge par ONTAP 9.5 et versions ultérieures.

  - Dans ONTAP 9.8-9.5, LDAPS ne peut être activé que sur le port 636. Pour ce faire, utilisez le `-use -ldaps-for-ad-ldap` paramètre avec le `vserver cifs security modify` commande.
  - À partir de ONTAP 9.9.1, LDAPS peut être activé sur n'importe quel port, bien que le port 636 reste le port par défaut. Pour ce faire, réglez le `-ldaps-enabled` paramètre sur `true` et spécifiez le paramètre souhaité `-port`. Pour en savoir plus, `vserver services name-service ldap client create` consultez le "Référence de commande ONTAP".

  > Il s'agit d'une meilleure pratique NetApp d'utiliser Start TLS plutôt que LDAPS.

- **Démarrer TLS**

  (Également appelé *start_tls*, *STARTTLS* et *StartTLS*) Un mécanisme de communication sécurisée à l'aide des protocoles TLS.

  ONTAP utilise STARTTLS pour sécuriser les communications LDAP et utilise le port LDAP par défaut (389) pour communiquer avec le serveur LDAP. Le serveur LDAP doit être configuré de manière à autoriser les connexions via le port LDAP 389 ; sinon, les connexions LDAP TLS du SVM vers le serveur LDAP échouent.

Comment ONTAP utilise LDAPS

ONTAP prend en charge l'authentification du serveur TLS qui permet au client SVM LDAP de confirmer l'identité du serveur LDAP lors de l'opération BIND. Les clients LDAP compatibles TLS peuvent utiliser des techniques standard de cryptographie à clé publique pour vérifier que le certificat et l'ID public d'un serveur sont valides et ont été émis par une autorité de certification (AC) répertoriée dans la liste des autorités de certification de confiance du client.

LDAP prend en charge STARTTLS pour crypter les communications à l'aide de TLS. STARTTLS commence comme une connexion texte clair sur le port LDAP standard (389), et cette connexion est ensuite mise à niveau vers TLS.

ONTAP supporte les éléments suivants :

- LDAPS pour le trafic lié au SMB entre les serveurs LDAP intégrés à Active Directory et le SVM
- LDAPS pour le trafic LDAP pour le mappage de noms et autres informations UNIX

  Les serveurs LDAP intégrés à Active Directory ou les serveurs LDAP basés sur UNIX peuvent être utilisés pour stocker des informations pour le mappage de noms LDAP et d'autres informations UNIX, telles que des utilisateurs, des groupes et des netgroups.

- Certificats CA racine auto-signés

  Lors de l'utilisation d'un LDAP intégré à Active-Directory, le certificat racine auto-signé est généré lorsque le service de certificat Windows Server est installé dans le domaine. Lors de l'utilisation d'un serveur LDAP UNIX pour le mappage de noms LDAP, le certificat racine auto-signé est généré et enregistré à l'aide de moyens appropriés à cette application LDAP.

Par défaut, LDAPS est désactivé.

Activer la prise en charge LDAP RFC2307bis pour les SVM ONTAP NFS

Si vous souhaitez utiliser LDAP et que vous avez besoin de la fonctionnalité supplémentaire d'utilisation des appartenances aux groupes imbriqués, vous pouvez configurer ONTAP pour activer la prise en charge de LDAP RFC2307bis.

Avant de commencer

Vous devez avoir créé une copie de l'un des schémas de client LDAP par défaut que vous souhaitez utiliser.

Description de la tâche

Dans les schémas client LDAP, les objets de groupe utilisent l'attribut memberUID. Cet attribut peut contenir plusieurs valeurs et répertorie les noms des utilisateurs appartenant à ce groupe. Dans les schémas de client LDAP compatibles avec RFC2307bis, les objets de groupe utilisent l'attribut uniqueMember. Cet attribut peut contenir le nom unique complet (DN) d'un autre objet dans le répertoire LDAP. Cela vous permet d'utiliser des groupes imbriqués car les groupes peuvent avoir d'autres groupes en tant que membres.

L'utilisateur ne doit pas être membre de plus de 256 groupes, y compris des groupes imbriqués. ONTAP ignore tous les groupes dépassant la limite de 256 groupes.

Par défaut, le support RFC2307bis est désactivé.

> La prise en charge RFC2307bis est activée automatiquement dans ONTAP lorsqu'un client LDAP est créé avec le schéma MS-AD-BIS.

Pour plus d'informations, reportez-vous à la section "Rapport technique NetApp 4835 : comment configurer LDAP dans ONTAP".

Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Modifiez le schéma de client LDAP RFC2307 copié pour activer la prise en charge de RFC2307bis :

```
vserver services name-service ldap client schema modify -vserver vserver_name
-schema schema-name -enable-rfc2307bis true
```

3. Modifiez le schéma pour qu'il corresponde à la classe d'objet prise en charge par le serveur LDAP :

```
vserver services name-service ldap client schema modify -vserver vserver-name
-schema schema_name -group-of-unique-names-object-class object_class
```

4. Modifiez le schéma pour qu'il corresponde au nom d'attribut pris en charge par le serveur LDAP :

```
vserver services name-service ldap client schema modify -vserver vserver-name
-schema schema_name -unique-member-attribute attribute_name
```

5. Retour au niveau de privilège admin :

```
set -privilege admin
```

Options de configuration ONTAP NFS pour les recherches dans l'annuaire LDAP

Vous pouvez optimiser les recherches d'annuaire LDAP, y compris les informations sur les utilisateurs, les groupes et les groupes réseau, en configurant le client LDAP ONTAP pour vous connecter aux serveurs LDAP de la manière la plus appropriée pour votre environnement. Vous devez savoir quand les valeurs de base LDAP et de recherche d'étendue par défaut sont suffisantes et quels paramètres doivent spécifier lorsque les valeurs personnalisées sont plus appropriées.

Les options de recherche du client LDAP pour les informations utilisateur, groupe et groupe réseau permettent d'éviter les requêtes LDAP échoués et, par conséquent, l'échec de l'accès du client aux systèmes de stockage. Ils permettent également de s'assurer que les recherches sont aussi efficaces que possible pour éviter les problèmes de performance du client.

Valeurs par défaut de recherche de base et de portée

La base LDAP est le DN de base par défaut utilisé par le client LDAP pour effectuer des requêtes LDAP. Toutes les recherches, y compris les recherches d'utilisateur, de groupe et de groupe réseau, sont effectuées à l'aide du DN de base. Cette option est appropriée lorsque votre répertoire LDAP est relativement petit et que toutes les entrées pertinentes se trouvent dans le même DN.

Si vous ne spécifiez pas de NA de base personnalisé, la valeur par défaut est `root`. Cela signifie que chaque requête recherche l'intégralité du répertoire. Bien que cela optimise les chances de réussite de la requête LDAP, elle peut être inefficace et entraîner une baisse significative des performances avec les grands répertoires LDAP.

L'étendue de base LDAP est l'étendue de recherche par défaut utilisée par le client LDAP pour effectuer des requêtes LDAP. Toutes les recherches, y compris les recherches d'utilisateur, de groupe et de groupe réseau, sont effectuées à l'aide de la portée de base. Elle détermine si la requête LDAP recherche uniquement l'entrée nommée, entre un niveau sous le DN ou l'ensemble de la sous-arborescence sous le DN.

Si vous ne spécifiez pas d'étendue de base personnalisée, la valeur par défaut est `subtree`. Cela signifie que chaque requête effectue une recherche dans toute la sous-arborescence située sous le nom unique. Bien que cela optimise les chances de réussite de la requête LDAP, elle peut être inefficace et entraîner une baisse significative des performances avec les grands répertoires LDAP.

Valeurs de base et d'étendue personnalisées

Vous pouvez éventuellement spécifier des valeurs de base et de portée distinctes pour les recherches utilisateur, groupe et groupe réseau. Limiter la base de recherche et l'étendue des requêtes de cette façon peut améliorer considérablement les performances car elle limite la recherche à une sous-section plus petite de l'annuaire LDAP.

Si vous spécifiez des valeurs de base et d'étendue personnalisées, elles remplacent la base de recherche générale par défaut et la portée pour les recherches utilisateur, groupe et groupe réseau. Les paramètres permettant de spécifier des valeurs de base et d'étendue personnalisées sont disponibles au niveau de privilège avancé.

Paramètre client LDAP…	Spécifie personnalisé…
`-base-dn`	Nom unique de base pour toutes les recherches LDAP. Plusieurs valeurs peuvent être saisies si nécessaire (par exemple, si la recherche de référence LDAP est activée dans ONTAP 9.5 et versions ultérieures).
`-base-scope`	Portée de base pour toutes les recherches LDAP.
`-user-dn`	Noms distinctifs de base pour toutes les recherches d'utilisateurs LDAP. Ce paramètre s'applique également aux recherches de mappage de noms d'utilisateurs.
`-user-scope`	Portée de base pour toutes les recherches d'utilisateurs LDAP. Ce paramètre s'applique également aux recherches de mappage de noms d'utilisateurs.
`-group-dn`	DN de base pour toutes les recherches de groupes LDAP.
`-group-scope`	Portée de base pour toutes les recherches de groupe LDAP.
`-netgroup-dn`	DN de base pour toutes les recherches de groupes réseau LDAP.
`-netgroup-scope`	Portée de base pour toutes les recherches de groupes réseau LDAP.

Plusieurs valeurs DN de base personnalisées

Si votre structure d'annuaire LDAP est plus complexe, vous devrez peut-être spécifier plusieurs DNS de base pour rechercher des informations dans plusieurs parties de votre annuaire LDAP. Vous pouvez spécifier plusieurs DNS pour les paramètres DN utilisateur, groupe et groupe réseau en les séparant par un point-virgule (;) et en enfermant toute la liste de recherche DN avec des guillemets doubles ("). Si un DN contient un point-virgule, vous devez ajouter un caractère d'échappement (\) immédiatement avant le point-virgule dans le DN.

Notez que le périmètre s'applique à la liste complète de DNS spécifiée pour le paramètre correspondant. Par exemple, si vous spécifiez une liste de trois noms d'utilisateur différents et de sous-arborescence pour l'étendue utilisateur, l'utilisateur LDAP recherche dans l'ensemble de la sous-arborescence pour chacun des trois DNS spécifiés.

Depuis ONTAP 9.5, vous pouvez également spécifier LDAP *recommandation traquer*, qui permet au client LDAP ONTAP de renvoyer des demandes de recherche à d'autres serveurs LDAP si une réponse de recommandation LDAP n'est pas renvoyée par le serveur LDAP principal. Le client utilise ces données de référence pour extraire l'objet cible du serveur décrit dans les données de référence. Pour rechercher des objets présents dans les serveurs LDAP désignés, le dn de base des objets désignés peut être ajouté au dn de base dans le cadre de la configuration du client LDAP. Cependant, les objets renvoyés ne sont examinés que lorsque la recherche de renvoi est activée (à l'aide du `-referral-enabled true`) lors de la création ou de la modification d'un client LDAP.

Filtres de recherche LDAP personnalisés

Vous pouvez utiliser le paramètre d'option de configuration LDAP pour créer un filtre de recherche personnalisé. Le `-group-membership-filter` paramètre spécifie le filtre de recherche à utiliser lors de la recherche de l'appartenance à un groupe à partir d'un serveur LDAP.

Voici un exemple de filtres valides :

```
(cn=*99), (cn=1*), (|(cn=*22)(cn=*33))
```

En savoir plus sur "Comment configurer LDAP dans ONTAP".

Améliorer les performances des recherches de groupe réseau par hôte dans l'annuaire LDAP pour les SVM NFS ONTAP

Si votre environnement LDAP est configuré pour permettre des recherches netgroup-par-hôte, vous pouvez configurer ONTAP pour en tirer parti et effectuer des recherches netgroup-par-hôte. Cela permet d'accélérer considérablement les recherches sur les groupes réseau et de réduire les problèmes d'accès aux clients NFS possibles en raison de la latence lors des recherches sur les groupes réseau.

Avant de commencer

Votre annuaire LDAP doit contenir un `netgroup.byhost` carte.

Vos serveurs DNS doivent contenir des enregistrements de recherche avant (A) et arrière (PTR) pour les clients NFS.

Lorsque vous spécifiez des adresses IPv6 dans les groupes réseau, vous devez toujours raccourcir et compresser chaque adresse comme spécifié dans RFC 5952.

Description de la tâche

Les serveurs NIS stockent les informations de groupe réseau sous trois cartes distinctes appelées `netgroup`, `netgroup.byuser`, et `netgroup.byhost`. Le but du `netgroup.byuser` et `netgroup.byhost` les cartes permettent d'accélérer la recherche de groupes réseau. ONTAP peut effectuer des recherches netgroup par hôte sur les serveurs NIS pour améliorer les temps de réponse de montage.

Par défaut, les répertoires LDAP ne possèdent pas ce type de `netgroup.byhost` Effectuez des mappes comme les serveurs NIS. Il est cependant possible, avec l'aide d'outils tiers, d'importer un NIS

`netgroup.byhost` Effectuez un mappage vers des répertoires LDAP pour permettre des recherches réseau par hôte rapides. Si vous avez configuré votre environnement LDAP pour autoriser des recherches netgroup-par-hôte, vous pouvez configurer le client LDAP ONTAP avec le système `netgroup.byhost` Nom de mappage, DN et étendue de recherche pour des recherches plus rapides avec netgroup par hôte.

La réception plus rapide des résultats de recherches netgroup par hôte permet à ONTAP de traiter les règles d'exportation plus rapidement lorsque les clients NFS demandent un accès aux exportations. Cela permet de réduire les risques de retard d'accès en raison des problèmes de latence de recherche de groupe réseau.

Étapes

1. Obtenir le nom distinctif complet exact du NIS `netgroup.byhost` Mapper que vous avez importé dans votre répertoire LDAP.

   Le NA de carte peut varier en fonction de l'outil tiers utilisé pour l'importation. Pour des performances optimales, vous devez spécifier le NA correspondant exact.

2. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
3. Activer les recherches netgroup-by-host dans la configuration client LDAP de la machine virtuelle de stockage (SVM) : `vserver services name-service ldap client modify -vserver vserver_name -client-config config_name -is-netgroup-byhost-enabled true -netgroup-byhost-dn netgroup-by-host_map_distinguished_name -netgroup-byhost -scope netgroup-by-host_search_scope`

   `-is-netgroup-byhost-enabled` {`true` `false`} Active ou désactive la recherche netgroup-par-hôte pour les répertoires LDAP. La valeur par défaut est `false`.

   `-netgroup-byhost-dn` `netgroup-by-host_map_distinguished_name` spécifie le nom distinctif du `netgroup.byhost` Mapper dans le répertoire LDAP. Il remplace le DN de base pour les recherches netgroup-par-hôte. Si vous ne spécifiez pas ce paramètre, ONTAP utilise plutôt le DN de base.

   `-netgroup-byhost-scope` {`base`|`onelevel` `subtree`} spécifie l'étendue de recherche pour les recherches netgroup-par-hôte. Si vous ne spécifiez pas ce paramètre, le paramètre par défaut est `subtree`.

   Si la configuration client LDAP n'existe pas encore, vous pouvez activer les recherches netgroup-par-hôte en spécifiant ces paramètres lors de la création d'une nouvelle configuration client LDAP à l'aide de l' `vserver services name-service ldap client create` commande.

   > Le `-ldap-servers` le champ remplace le `-servers` champ. Vous pouvez utiliser le `-ldap-servers` champ pour spécifier soit un nom d'hôte soit une adresse IP pour le serveur LDAP.

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

Exemple

La commande suivante modifie la configuration du client LDAP existante nommée « ldap_corp » pour activer les recherches netgroup par hôte à l'aide de l' `netgroup.byhost` Carte nommée ""nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com" et champ de recherche par défaut `subtree`:

```
cluster1::*> vserver services name-service ldap client modify -vserver vs1
-client-config ldap_corp -is-netgroup-byhost-enabled true -netgroup-byhost
-dn nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com
```

Une fois que vous avez terminé

Le `netgroup.byhost` et `netgroup` les cartes du répertoire doivent être synchronisées en permanence pour éviter tout problème d'accès client.

Informations associées

"IETF RFC 5952 : une recommandation pour la représentation texte de l'adresse IPv6"

Utiliser la liaison rapide LDAP pour l'authentification nsswitch pour les SVM NFS ONTAP

Depuis ONTAP 9.11.1, vous pouvez bénéficier de la fonctionnalité LDAP *FAST bind* (également appelée *bind* simultanée) pour des requêtes d'authentification client plus rapides et plus simples. Pour utiliser cette fonctionnalité, le serveur LDAP doit prendre en charge la fonctionnalité de liaison rapide.

Description de la tâche

Sans liaison rapide, ONTAP utilise LDAP simple BIND pour authentifier les utilisateurs admin avec le serveur LDAP. Avec cette méthode d'authentification, ONTAP envoie un nom d'utilisateur ou de groupe au serveur LDAP, reçoit le mot de passe de hachage stocké et compare le code de hachage du serveur avec le code de hachage généré localement à partir du mot de passe de l'utilisateur. S'ils sont identiques, ONTAP accorde l'autorisation de connexion.

Grâce à la fonctionnalité de liaison rapide, ONTAP n'envoie que les informations d'identification de l'utilisateur (nom d'utilisateur et mot de passe) au serveur LDAP via une connexion sécurisée. Le serveur LDAP valide ensuite ces informations d'identification et demande à ONTAP d'accorder des autorisations de connexion.

L'un des avantages de Fast bind est qu'il n'est pas nécessaire que ONTAP prenne en charge chaque nouvel algorithme de hachage pris en charge par les serveurs LDAP, car le hachage du mot de passe est effectué par le serveur LDAP.

"En savoir plus sur l'utilisation de FAST BIND."

Vous pouvez utiliser les configurations client LDAP existantes pour la liaison rapide LDAP. Cependant, il est fortement recommandé de configurer le client LDAP pour TLS ou LDAPS ; dans le cas contraire, le mot de passe est envoyé sur le réseau en texte brut.

Pour activer la liaison rapide LDAP dans un environnement ONTAP, vous devez répondre aux exigences suivantes :

- Les utilisateurs admin ONTAP doivent être configurés sur un serveur LDAP qui prend en charge la liaison rapide.
- Le SVM ONTAP doit être configuré pour LDAP dans la base de données du switch des services de noms (nsswitch).
- Les comptes utilisateur et groupe admin ONTAP doivent être configurés pour l'authentification nsswitch avec le bind rapide.

Étapes

1. Vérifiez auprès de votre administrateur LDAP que la liaison rapide LDAP est prise en charge sur le serveur LDAP.
2. Assurez-vous que les informations d'identification de l'utilisateur administrateur ONTAP sont configurées sur le serveur LDAP.
3. Vérifier que le SVM admin ou données est configuré correctement pour LDAP FAST BIND.

   a. Pour confirmer que le serveur LDAP FAST BIND est répertorié dans la configuration du client LDAP, entrez :

      `vserver services name-service ldap client show`

      "En savoir plus sur la configuration du client LDAP."

   b. Pour le confirmer `ldap` est l'une des sources configurées pour le nsswitch `passwd` base de données, entrez :

      `vserver services name-service ns-switch show`

   "Découvrez la configuration nsswitch."

4. Assurez-vous que les utilisateurs admin s'authentifient auprès de nsswitch et que l'authentification LDAP FAST BIND est activée dans leurs comptes.

   ◦ Pour les utilisateurs existants, entrez `security login modify` et vérifiez les paramètres suivants :

      `-authentication-method nsswitch`

      `-is-ldap-fastbind true`

   Pour en savoir plus, `security login modify` consultez le "Référence de commande ONTAP".

   ◦ Pour les nouveaux utilisateurs admin, voir "Activez l'accès au compte ONTAP LDAP ou NIS".

Afficher les statistiques LDAP pour les SVM ONTAP NFS

Vous pouvez afficher les statistiques LDAP pour les machines virtuelles de stockage (SVM) sur un système de stockage pour surveiller les performances et diagnostiquer les problèmes.

Avant de commencer

- Vous devez avoir configuré un client LDAP sur la SVM.
- Vous devez avoir identifié des objets LDAP à partir desquels vous pouvez afficher des données.

Étape

1. Afficher les données de performance des objets compteur :

   `statistics show`

Exemples

L'exemple suivant affiche les statistiques de l'échantillon nommé **smpl_1** pour les compteurs : avg_processor_Busy et cpu_Busy

```
cluster1::*> statistics start -object system -counter
avg_processor_busy|cpu_busy -sample-id smpl_1
Statistics collection is being started for Sample-id: smpl_1

cluster1::*> statistics stop -sample-id smpl_1
Statistics collection is being stopped for Sample-id: smpl_1

cluster1::*> statistics show -sample-id smpl_1
Object: system
Instance: cluster
Start-time: 8/2/2012 18:27:53
End-time: 8/2/2012 18:27:56
Cluster: cluster1
   Counter                                                     Value
   -------------------------------- --------------------------------
   avg_processor_busy                                             6%
   cpu_busy
```

Informations associées

- "les statistiques montrent"
- "les statistiques commencent"
- "les statistiques s'arrêtent"

Configurez les mappages de noms

En savoir plus sur la configuration du mappage de noms pour les SVM NAS ONTAP

ONTAP utilise le mappage de noms pour mapper les identités SMB aux identités UNIX, aux identités Kerberos aux identités UNIX et aux identités UNIX aux identités SMB. Il a besoin de ces informations pour obtenir les informations d'identification des utilisateurs et fournir un accès approprié aux fichiers, qu'ils se connectent depuis un client NFS ou un client SMB.

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

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

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

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

Toutefois, vous pouvez mapper un groupe d'utilisateurs individuels à un utilisateur spécifique. Par exemple, vous pouvez mapper tous les utilisateurs AD qui commencent ou se terminent par le mot VENTES à un utilisateur UNIX spécifique et à l'UID de l'utilisateur.

En savoir plus sur les mappages de noms pour les SVM NAS ONTAP

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

- Pour le mappage Windows à UNIX

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

- Pour le mappage d'UNIX à Windows

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

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

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

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

Recherches multidomaines pour les mappages de noms d'utilisateur UNIX vers Windows sur les SVM NAS ONTAP

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

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

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

- *Confiance bidirectionnelle*

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

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

- *Confiance sortante*

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

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

- *Confiance entrante*

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

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

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

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

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

Motif	Remplacement	Résultat
*	{astérisque}\\{asterslash}*	Les utilisateurs UNIX valides sont mappés aux utilisateurs Windows correspondants. Tous les domaines approuvés sont recherchés dans l'ordre jusqu'à ce que le premier utilisateur correspondant à ce nom soit trouvé. Le motif {astérisque}\\{Astersl ash} est valable uniquement pour le mappage de noms d'UNIX à Windows, pas l'inverse.

Mode d'exécution des recherches sur plusieurs noms de domaine

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

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

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

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

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

Règles de conversion de mappage de noms pour les SVM NAS ONTAP

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

Créer des mappages de noms pour les SVM NAS ONTAP

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

Description de la tâche

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

Étape

1. Créer un mappage de noms :

```
vserver name-mapping create -vserver vserver_name -direction {krb-unix|win-unix|unix-win} -position integer -pattern text -replacement text
```

> Les `-pattern` instructions et `-replacement` peuvent être formulées en tant qu'expressions régulières. Vous pouvez également utiliser l'`-replacement`instruction pour refuser explicitement un mappage à l'utilisateur en utilisant la chaîne de remplacement NULL `" "` (caractère d'espace). Pour en savoir plus, `vserver name-mapping create` consultez le "Référence de commande ONTAP".

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

Exemples

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

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

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

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

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

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

Configurer l'utilisateur par défaut pour les SVM NAS ONTAP

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

Description de la tâche

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

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

Étape

1. Effectuez l'une des opérations suivantes :

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

Commandes ONTAP pour la gestion des mappages de noms NFS

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

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

Échange de la position de deux mappages de noms REMARQUE : un échange n'est pas autorisé lorsque le mappage-noms est configuré avec une entrée de qualificatif-ip.	`vserver name-mapping swap`
Modifier un mappage de noms	`vserver name-mapping modify`
Supprime un mappage de noms	`vserver name-mapping delete`
Valider le mappage de nom correct	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

Pour en savoir plus, `vserver name-mapping` consultez le "Référence de commande ONTAP".

Activer l'accès des clients Windows NFS pour les SVM ONTAP

ONTAP prend en charge l'accès aux fichiers à partir de clients Windows NFSv3. Cela signifie que les clients exécutant des systèmes d'exploitation Windows avec prise en charge de NFSv3 peuvent accéder aux fichiers lors des exports NFSv3 sur le cluster. Pour utiliser correctement cette fonctionnalité, vous devez configurer correctement le serveur virtuel de stockage (SVM) et connaître certaines exigences et limites.

Description de la tâche

Par défaut, la prise en charge du client Windows NFSv3 est désactivée.

Avant de commencer

NFSv3 doit être activé sur le SVM.

Étapes

1. Activer la prise en charge des clients Windows NFSv3 :

   ```
   vserver nfs modify -vserver svm_name -v3-ms-dos-client enabled -mount-rootonly disabled
   ```

2. Sur tous les SVM qui prennent en charge les clients Windows NFSv3, désactivez le `-enable-ejukebox` et `-v3-connection-drop` paramètres :

   ```
   vserver nfs modify -vserver vserver_name -enable-ejukebox false -v3-connection-drop disabled
   ```

   Les clients Windows NFSv3 peuvent désormais monter des exportations sur le système de stockage.

3. Assurez-vous que chaque client Windows NFSv3 utilise des montages durs en spécifiant le `-o mtype=hard` option.

   Ceci est nécessaire pour garantir la fiabilité des supports.

```
mount -o mtype=hard \\10.53.33.10\vol\vol1 z:\
```

Activer l’affichage des exportations sur les clients NFS pour les SVM ONTAP

Les clients NFS peuvent utiliser le `showmount -e` Commande pour afficher la liste des exportations disponibles à partir d’un serveur NFS ONTAP. Cela peut aider les utilisateurs à identifier le système de fichiers qu’ils souhaitent monter.

ONTAP permet aux clients NFS d’afficher la liste d’exportation par défaut. Dans les versions précédentes, l' `showmount`option de la `vserver nfs modify` commande doit être activée explicitement. Pour afficher la liste d’export, NFSv3 doit être activé sur le SVM.

Exemple

La commande suivante présente la fonctionnalité showmount sur le SVM nommé vs1 :

```
clusterl : : > vserver nfs show -vserver vs1 -fields showmount
vserver showmount
------- ---------
vs1    enabled
```

La commande suivante exécutée sur un client NFS affiche la liste des exportations sur un serveur NFS avec l’adresse IP 10.63.21.9 :

```
showmount -e 10.63.21.9
Export list for 10.63.21.9:
/unix         (everyone)
/unix/unixl   (everyone)
/unix/unix2   (everyone)
/             (everyone)
```

Gérer l’accès aux fichiers à l’aide de NFS

Activer ou désactiver NFSv3 pour les SVM ONTAP

Vous pouvez activer ou désactiver NFSv3 en modifiant le `-v3` option. Cette fonctionnalité permet aux clients d’accéder aux fichiers via le protocole NFSv3. NFSv3 est activé par défaut.

Étape

1. Effectuez l’une des opérations suivantes :

Les fonctions que vous recherchez…	Entrez la commande…

Activez NFSv3	`vserver nfs modify -vserver vserver_name -v3 enabled`
Désactiver NFSv3	`vserver nfs modify -vserver vserver_name -v3 disabled`

Activer ou désactiver NFSv4.0 pour les SVM ONTAP

Vous pouvez activer ou désactiver NFSv4.0 en modifiant le `-v4.0` option. Cela permet d'accéder aux fichiers pour les clients utilisant le protocole NFSv4.0. Dans ONTAP 9.9.1, NFSv4.0 est activé par défaut ; dans les versions antérieures, il est désactivé par défaut.

Étape

1. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Saisissez la commande suivante…
Activer NFSv4.0	`vserver nfs modify -vserver vserver_name -v4.0 enabled`
Désactivez NFSv4.0	`vserver nfs modify -vserver vserver_name -v4.0 disabled`

Activer ou désactiver NFSv4.1 pour les SVM ONTAP

Vous pouvez activer ou désactiver NFSv4.1 en modifiant `-v4.1` option. Ainsi, les clients bénéficient d'un accès aux fichiers à l'aide du protocole NFSv4.1. Dans ONTAP 9.9.1, NFSv4.1 est activé par défaut. Dans les versions antérieures, il est désactivé par défaut.

Étape

1. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Saisissez la commande suivante…
Activation de NFSv4.1	`vserver nfs modify -vserver vserver_name -v4.1 enabled`
Désactiver NFSv4.1	`vserver nfs modify -vserver vserver_name -v4.1 disabled`

Gérer les limites du pool de stockage ONTAP NFSv4

À partir de ONTAP 9.13, les administrateurs peuvent activer leurs serveurs NFSv4 pour refuser des ressources aux clients NFSv4 lorsqu'ils ont atteint les limites de ressources de pool de stockage par client. Lorsque les clients consomment trop de ressources de pool de stockage NFSv4, cela peut entraîner le blocage d'autres clients NFSv4 en raison

de l’indisponibilité des ressources de pool de stockage NFSv4.

L’activation de cette fonction permet également aux clients d’afficher la consommation de ressources du pool de stockage actif par chaque client. Cela facilite l’identification des clients qui épuise les ressources système et permet d’imposer des limites de ressources par client.

Afficher les ressources de pool de stockage consommées

Le `vserver nfs storepool show` affiche le nombre de ressources de pool de stockage utilisées. Un pool de stockage est un pool de ressources utilisé par les clients NFSv4.

Étape

1. En tant qu’administrateur, exécutez `vserver nfs storepool show` Commande permettant d’afficher les informations de réserve des clients NFSv4.

Exemple

Cet exemple affiche les informations relatives au pool de stockage des clients NFSv4.

```
cluster1::*> vserver nfs storepool show

Node: node1

Vserver: vs1

Data-Ip: 10.0.1.1

Client-Ip Protocol IsTrunked OwnerCount OpenCount DelegCount LockCount

-------------- --------- --------- ---------- ---------- ----------
---------

10.0.2.1          nfs4.1     true    2 1 0 4

10.0.2.2          nfs4.2     true    2 1 0 4

2 entries were displayed.
```

Activer ou désactiver les contrôles de limite de pool de stockage

Les administrateurs peuvent utiliser les commandes suivantes pour activer ou désactiver les contrôles de limite de pool de stockage.

Étape

1. En tant qu’administrateur, effectuez l’une des opérations suivantes :

Les fonctions que vous recherchez…	Saisissez la commande suivante…
Activer les contrôles de limite de pool de stockage	`vserver nfs storepool config modify -limit-enforce enabled`
Désactiver les contrôles de limite de pool de stockage	`vserver nfs storepool config modify -limit-enforce disabled`

Afficher la liste des clients bloqués

Si la limite de réserve est activée, les administrateurs peuvent voir quels clients ont été bloqués lorsqu'ils ont atteint leur seuil de ressources par client. Les administrateurs peuvent utiliser la commande suivante pour voir quels clients ont été marqués comme des clients bloqués.

Étapes

1. Utilisez le `vserver nfs storepool blocked-client show` Commande permettant d'afficher la liste des clients bloqués par NFSv4.

Supprimer un client de la liste des clients bloqués

Les clients qui atteignent leur seuil par client seront déconnectés et ajoutés au cache client-bloc. Les administrateurs peuvent utiliser la commande suivante pour supprimer le client du cache du client de bloc. Cela permettra au client de se connecter au serveur ONTAP NFSV4.

Étapes

1. Utilisez le `vserver nfs storepool blocked-client flush -client-ip <ip address>` commande permettant de vider le cache client bloqué du pool de stockage.
2. Utilisez le `vserver nfs storepool blocked-client show` commande permettant de vérifier que le client a été supprimé du cache du client en mode bloc.

Exemple

Cet exemple affiche un client bloqué dont l'adresse IP "10.2.1.1" est vidée de tous les nœuds.

```
cluster1::*>vserver nfs storepool blocked-client flush -client-ip 10.2.1.1

cluster1::*>vserver nfs storepool blocked-client show

Node: node1

Client IP
----------
10.1.1.1

1 entries were displayed.
```

Activer ou désactiver pNFS pour les SVM ONTAP

PNFS améliore les performances en permettant aux clients NFS d'effectuer des opérations de lecture/écriture sur les périphériques de stockage directement et en parallèle, en contournant le serveur NFS comme un goulot d'étranglement potentiel. Pour activer ou désactiver pNFS (Parallel NFS), vous pouvez modifier le `-v4.1-pnfs` option.

Si la version de ONTAP est…	La norme pNFS par défaut est…
9.8 ou ultérieure	désactivé
9.7 ou antérieure	activé

Avant de commencer

La prise en charge de NFSv4.1 est requise pour pouvoir utiliser pNFS.

Si vous souhaitez activer pNFS, vous devez d'abord désactiver les référencements NFS. Les deux ne peuvent pas être activées en même temps.

Si vous utilisez pNFS avec Kerberos sur des SVM, il faut activer Kerberos sur chaque LIF de la SVM.

Étape

1. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Entrez la commande…
Activez pNFS	`vserver nfs modify -vserver vserver_name -v4.1-pnfs enabled`
Désactiver pNFS	`vserver nfs modify -vserver vserver_name -v4.1-pnfs disabled`

Informations associées

- Présentation de l'agrégation NFS

Contrôler l'accès NFS via TCP et UDP pour les SVM ONTAP

Vous pouvez activer ou désactiver l'accès NFS aux serveurs virtuels de stockage (SVM) via TCP et UDP en modifiant le `-tcp` et `-udp` paramètres, respectivement. Vous pouvez ainsi contrôler l'accès des clients NFS aux données via TCP ou UDP dans votre environnement.

Description de la tâche

Ces paramètres s'appliquent uniquement à NFS. Ils n'affectent pas les protocoles auxiliaires. Par exemple, si NFS sur TCP est désactivé, les opérations de montage sur TCP ont toujours réussi. Pour bloquer complètement le trafic TCP ou UDP, vous pouvez utiliser des règles d'export-policy.

Vous devez désactiver le serveur RPC SnapDiff avant de désactiver TCP pour NFS pour éviter une erreur de commande. Vous pouvez désactiver TCP en utilisant la commande `vserver snapdiff-rpc-server off -vserver vserver name`.

Étape

1. Effectuez l'une des opérations suivantes :

Si vous souhaitez obtenir un accès NFS…	Entrez la commande…
Activé sur TCP	`vserver nfs modify -vserver vserver_name -tcp enabled`
Désactivé sur TCP	`vserver nfs modify -vserver vserver_name -tcp disabled`
Activé sur UDP	`vserver nfs modify -vserver vserver_name -udp enabled`
Désactivé sur UDP	`vserver nfs modify -vserver vserver_name -udp disabled`

Contrôler les requêtes NFS à partir de ports non réservés pour les SVM ONTAP

Vous pouvez rejeter les demandes de montage NFS à partir de ports non réservés en activant le `-mount-rootonly` option. Pour rejeter toutes les demandes NFS de ports non réservés, vous pouvez activer le `-nfs-rootonly` option.

Description de la tâche

Par défaut, l'option `-mount-rootonly` est `enabled`.

Par défaut, l'option `-nfs-rootonly` est `disabled`.

Ces options ne s'appliquent pas à la procédure NULL.

Étape

1. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Entrez la commande…
Autoriser les demandes de montage NFS à partir de ports non réservés	`vserver nfs modify -vserver vserver_name -mount -rootonly disabled`
Rejeter les demandes de montage NFS à partir de ports non réservés	`vserver nfs modify -vserver vserver_name -mount -rootonly enabled`
Autoriser toutes les demandes NFS à partir de ports non réservés	`vserver nfs modify -vserver vserver_name -nfs -rootonly disabled`

Rejeter toutes les demandes NFS de ports non réservés	`vserver nfs modify -vserver vserver_name -nfs -rootonly enabled`

Gérer l'accès NFS aux volumes ONTAP NTFS ou aux qtrees pour les utilisateurs UNIX inconnus

Si ONTAP ne peut pas identifier les utilisateurs UNIX qui tentent de se connecter à des volumes ou des qtrees avec le style de sécurité NTFS, il ne peut donc pas mapper l'utilisateur de façon explicite à un utilisateur Windows. Vous pouvez configurer ONTAP de manière à refuser l'accès à ces utilisateurs pour une sécurité plus stricte ou les mapper à un utilisateur Windows par défaut afin d'assurer un niveau d'accès minimum pour tous les utilisateurs.

Avant de commencer

Un utilisateur Windows par défaut doit être configuré si vous souhaitez activer cette option.

Description de la tâche

Si un utilisateur UNIX tente d'accéder aux volumes ou aux qtrees avec un style de sécurité NTFS, l'utilisateur UNIX doit d'abord être mappé à un utilisateur Windows afin que ONTAP puisse correctement évaluer les autorisations NTFS. Cependant, si ONTAP ne peut pas rechercher le nom de l'utilisateur UNIX dans les sources de service de nom d'informations utilisateur configurées, il ne peut pas explicitement mapper l'utilisateur UNIX à un utilisateur Windows spécifique. Vous pouvez décider comment gérer ces utilisateurs UNIX inconnus de la manière suivante :

- Refuser l'accès aux utilisateurs UNIX inconnus.

  Ceci met en œuvre une sécurité plus stricte en nécessitant un mappage explicite pour tous les utilisateurs UNIX afin d'accéder aux volumes ou aux qtrees NTFS.

- Mapper des utilisateurs UNIX inconnus à un utilisateur Windows par défaut.

  Cette fonctionnalité offre moins de sécurité et davantage de commodité, en veillant à ce que tous les utilisateurs aient un niveau d'accès minimal aux volumes NTFS ou aux qtrees par l'intermédiaire d'un utilisateur Windows par défaut.

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Effectuez l'une des opérations suivantes :

Si vous voulez que l'utilisateur Windows par défaut pour les utilisateurs UNIX inconnus…	Entrez la commande…
Activé	`vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user enabled`

Désactivé	`vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user disabled`

3. Retour au niveau de privilège admin :

```
set -privilege admin
```

Considérations pour les clients qui montent des exportations NFS ONTAP sur des ports non réservés

Le `-mount-rootonly` L'option doit être désactivée sur un système de stockage qui doit prendre en charge les clients qui montent des exportations NFS à l'aide d'un port non réservé, même lorsque l'utilisateur est connecté en tant que root. Ces clients comprennent les clients Hummingbird et les clients Solaris NFS/IPv6.

Si le `-mount-rootonly` ONTAP n'autorise pas les clients NFS utilisant des ports non réservés. Ainsi, les ports dont les numéros sont supérieurs à 1,023, ne permettent pas le montage des exports NFS.

Effectuez une vérification d'accès plus stricte pour les groupes réseau en vérifiant les domaines pour les SVM NFS ONTAP

Par défaut, ONTAP effectue une vérification supplémentaire lors de l'évaluation de l'accès client pour un groupe réseau. Cette vérification supplémentaire garantit que le domaine du client correspond à la configuration de domaine de la machine virtuelle de stockage (SVM). Sinon, ONTAP refuse l'accès client.

Description de la tâche

Lorsque ONTAP évalue les règles d'export policy pour l'accès client et qu'une règle d'export policy contient un netgroup, ONTAP doit déterminer si l'adresse IP d'un client appartient au netgroup. Pour ce faire, ONTAP convertit l'adresse IP du client en un nom d'hôte à l'aide du DNS et obtient un nom de domaine complet (FQDN).

Si le fichier netgroup répertorie uniquement un nom court pour l'hôte et que le nom court de l'hôte existe dans plusieurs domaines, il est possible qu'un client d'un domaine différent obtienne un accès sans cette vérification.

Pour empêcher cela, ONTAP compare le domaine renvoyé par DNS pour l'hôte avec la liste des noms de domaine DNS configurés pour le SVM. Si la correspondance correspond, l'accès est autorisé. Si ce n'est pas le cas, l'accès est refusé.

Cette vérification est activée par défaut. Vous pouvez le gérer en modifiant le `-netgroup-dns-domain -search` paramètre, disponible au niveau de privilège avancé.

Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Effectuez l'action souhaitée :

Si vous voulez que la vérification de domaine pour les groupes réseau soit…	Entrer…
Activé	`vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search enabled`
Désactivé	`vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search disabled`

3. Définissez le niveau de privilège sur admin :

   ```
   set -privilege admin
   ```

Modifier les ports utilisés pour les services NFSv3 pour les SVM ONTAP

Le serveur NFS du système de stockage utilise des services tels que le démon de montage et Network Lock Manager pour communiquer avec les clients NFS sur des ports réseau par défaut spécifiques. Dans la plupart des environnements NFS, les ports par défaut fonctionnent correctement et ne nécessitent pas de modification, mais si vous souhaitez utiliser différents ports réseau NFS dans votre environnement NFSv3, vous pouvez le faire.

Avant de commencer

La modification des ports NFS sur le système de stockage requiert que tous les clients NFS se connectent au système. Il est donc important de communiquer ces informations aux utilisateurs avant de faire la modification.

Description de la tâche

Vous pouvez définir les ports utilisés par les services du démon de montage NFS, Network Lock Manager, Network Status Monitor et NFS quota daemon pour chaque machine virtuelle de stockage (SVM). La modification du numéro de port affecte l'accès des clients NFS aux données via TCP et UDP.

Les ports pour NFSv4 et NFSv4.1 ne peuvent pas être modifiés.

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Désactivation de l'accès à NFS :

   ```
   vserver nfs modify -vserver vserver_name -access false
   ```

3. Définissez le port NFS pour le service NFS spécifique :

   ```
   vserver nfs modify -vserver vserver_namenfs_port_parameterport_number
   ```

Paramètre du port NFS	Description	Port par défaut
`-mountd-port`	Démon de montage NFS	658
`-nlm-port`	Gestionnaire de verrouillage réseau	4045
`-nsm-port`	Moniteur d'état du réseau	4046
`-rquotad-port`	Démon de quota NFS	4049

Outre le port par défaut, la plage autorisée de numéros de port est comprise entre 1024 et 65535. Chaque service NFS doit utiliser un port unique.

4. Activation de l'accès au NFS :

   ```
   vserver nfs modify -vserver vserver_name -access true
   ```

5. Utilisez le `network connections listening show` pour vérifier que le numéro de port change.

   Pour en savoir plus, `network connections listening show` consultez le "Référence de commande ONTAP".

6. Retour au niveau de privilège admin :

   ```
   set -privilege admin
   ```

Exemple

Les commandes suivantes définissent le port NFS Mount Daemon sur 1113 sur le SVM nommé vs1 :

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
         them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -access false

vs1::*> vserver nfs modify -vserver vs1 -mountd-port 1113

vs1::*> vserver nfs modify -vserver vs1 -access true

vs1::*> network connections listening show
Vserver Name     Interface Name:Local Port        Protocol/Service
---------------- -------------------------------  ----------------
Node: cluster1-01
Cluster          cluster1-01_clus_1:7700          TCP/ctlopcp
vs1              data1:4046                       TCP/sm
vs1              data1:4046                       UDP/sm
vs1              data1:4045                       TCP/nlm-v4
vs1              data1:4045                       UDP/nlm-v4
vs1              data1:1113                       TCP/mount
vs1              data1:1113                       UDP/mount
...
vs1::*> set -privilege admin
```

Commandes ONTAP pour la gestion des serveurs NFS

Il existe des commandes ONTAP spécifiques pour gérer les serveurs NFS.

Les fonctions que vous recherchez…	Utilisez cette commande…
Créez un serveur NFS	`vserver nfs create`
Affichez les serveurs NFS	`vserver nfs show`
Modifier un serveur NFS	`vserver nfs modify`
Supprimer un serveur NFS	`vserver nfs delete`

Masquer le `.snapshot` Liste de répertoires sous points de montage NFSv3 Accès explicite au `.snapshot` le répertoire reste autorisé même si l'option est activée.	`vserver nfs` commandes avec le `-v3-hide-snapshot` option activée

Pour en savoir plus, `vserver nfs` consultez le "Référence de commande ONTAP".

Résoudre les problèmes de service de noms pour les SVM NAS ONTAP

Lorsque les clients rencontrent des échecs d'accès en raison de problèmes de service de nom, vous pouvez utiliser le `vserver services name-service getxxbyyy` famille de commandes pour effectuer manuellement différentes recherches de services de noms et examiner les détails et les résultats de la recherche pour faciliter le dépannage.

Description de la tâche

- Pour chaque commande, vous pouvez spécifier les éléments suivants :
  - Nom du nœud ou de la machine virtuelle de stockage (SVM) à effectuer la recherche.

    Cela vous permet de tester les recherches de service de noms pour un nœud ou un SVM spécifique afin de limiter la recherche de problèmes potentiels de configuration du service de noms.

  - Indique si la source utilisée pour la recherche doit être utilisée.

    Cela vous permet de vérifier si la source correcte a été utilisée.
- ONTAP sélectionne le service pour effectuer la recherche en fonction de l'ordre de commutation de service de noms configuré.
- Ces commandes sont disponibles au niveau de privilège avancé.

Étapes

1. Effectuez l'une des opérations suivantes :

Pour récupérer…	Utilisez la commande…
Adresse IP d'un nom d'hôte	`vserver services name-service getxxbyyy getaddrinfo` `vserver services name-service getxxbyyy gethostbyname` (Adresses IPv4 uniquement)
Membres d'un groupe par ID de groupe	`vserver services name-service getxxbyyy getgrbygid`

Membres d'un groupe par nom de groupe	`vserver services name-service getxxbyyy getgrbyname`
Liste des groupes auxquels un utilisateur appartient	`vserver services name-service getxxbyyy getgrlist`
Nom d'hôte d'une adresse IP	`vserver services name-service getxxbyyy getnameinfo` `vserver services name-service getxxbyyy gethostbyaddr` (Adresses IPv4 uniquement)
Informations sur l'utilisateur par nom d'utilisateur	`vserver services name-service getxxbyyy getpwbyname` Vous pouvez tester la résolution des noms des utilisateurs RBAC en spécifiant le `-use -rbac` ens. paramètre `true`.
Informations utilisateur par ID utilisateur	`vserver services name-service getxxbyyy getpwbyuid` Vous pouvez tester la résolution des noms des utilisateurs RBAC en spécifiant le `-use-rbac` ens. paramètre `true`.
Appartenance au groupe réseau d'un client	`vserver services name-service getxxbyyy netgrp`
Appartenance à un groupe réseau d'un client à l'aide de la recherche netgroup par hôte	`vserver services name-service getxxbyyy netgrpbyhost`

L'exemple suivant montre un test de recherche DNS pour le SVM vs1 en essayant d'obtenir l'adresse IP pour l'hôte acast1.eng.example.com :

```
cluster1::*> vserver services name-service getxxbyyy getaddrinfo -vserver
vs1 -hostname acast1.eng.example.com -address-family all -show-source true
Source used for lookup: DNS
Host name: acast1.eng.example.com
Canonical Name: acast1.eng.example.com
IPv4: 10.72.8.29
```

L'exemple suivant montre un test de recherche NIS pour le SVM vs1 en essayant de récupérer les informations utilisateur pour un utilisateur avec l'UID 501768 :

```
cluster1::*> vserver services name-service getxxbyyy getpwbyuid -vserver
vs1 -userID 501768 -show-source true
Source used for lookup: NIS
pw_name: jsmith
pw_passwd: $1$y8rA4XX7$/DDOXAvc2PC/IsNFozfIN0
pw_uid: 501768
pw_gid: 501768
pw_gecos:
pw_dir: /home/jsmith
pw_shell: /bin/bash
```

L'exemple suivant montre un test de recherche LDAP pour le SVM vs1 en tentant de récupérer les informations utilisateur d'un utilisateur portant le nom ldap1 :

```
cluster1::*> vserver services name-service getxxbyyy getpwbyname -vserver
vs1 -username ldap1 -use-rbac false -show-source true
Source used for lookup: LDAP
pw_name: ldap1
pw_passwd: {crypt}JSPM6yc/ilIX6
pw_uid: 10001
pw_gid: 3333
pw_gecos: ldap1 user
pw_dir: /u/ldap1
pw_shell: /bin/csh
```

L'exemple suivant montre un test de recherche de groupe réseau pour le SVM vs1 en essayant de déterminer si le client dnshost0 est membre du groupe netgroup136 :

```
cluster1::*> vserver services name-service getxxbyyy netgrp -vserver vs1
-netgroup lnetgroup136 -client dnshost0 -show-source true
Source used for lookup: LDAP
dnshost0 is a member of lnetgroup136
```

1. Analysez les résultats du test que vous avez effectué et prenez les mesures nécessaires.

Si…	Vérifiez le…
La recherche de nom d'hôte ou d'adresse IP a échoué ou a produit des résultats incorrects	Configuration DNS
Recherche interrogea une source incorrecte	Nommer la configuration du commutateur de service

Si…	Vérifiez le…
La recherche d'utilisateur ou de groupe a échoué ou a produit des résultats incorrects	• Nommer la configuration du commutateur de service • Configuration source (fichiers locaux, domaine NIS, client LDAP) • Configuration du réseau (par exemple, LIFs et routes)
La recherche de nom d'hôte a échoué ou a expiré et le serveur DNS ne résout pas les noms courts DNS (par exemple, host1).	Configuration DNS pour les requêtes de domaine de premier niveau (TLD). Vous pouvez désactiver les requêtes TLD à l'aide du `-is-tld-query -enabled false` à la `vserver services name-service dns modify` commande.

Informations associées

"Rapport technique de NetApp 4668 : name Services Best Practices Guide (Guide des meilleures pratiques des services de noms)"

Vérifier les connexions au service de noms pour les SVM NAS ONTAP

Vous pouvez vérifier les serveurs de noms DNS et Lightweight Directory Access Protocol (LDAP) pour vérifier qu'ils sont connectés à ONTAP. Ces commandes sont disponibles au niveau de privilège admin.

Description de la tâche

Vous pouvez vérifier que la configuration du service de noms DNS ou LDAP est valide selon les besoins à l'aide du vérificateur de configuration du service de noms. Cette vérification de validation peut être lancée en ligne de commande ou dans System Manager.

Pour les configurations DNS, tous les serveurs sont testés et doivent fonctionner pour que la configuration soit considérée comme valide. Pour les configurations LDAP, tant qu'un serveur est en service, la configuration est valide. Les commandes name service appliquent le vérificateur de configuration sauf `skip-config-validation` le champ est vrai (la valeur par défaut est faux).

Étape

1. Utiliser la commande appropriée pour vérifier la configuration du service de noms. L'interface utilisateur affiche l'état des serveurs configurés.

Pour vérifier…	Utilisez cette commande…
État de la configuration DNS	`vserver services name-service dns check`
État de la configuration LDAP	`vserver services name-service ldap check`

```
cluster1::> vserver services name-service dns check -vserver vs0

Vserver         Name Server     Status  Status Details
--------------  --------------- ------- -------------------------
 vs0            10.11.12.13     up      Response time (msec): 55
 vs0            10.11.12.14     up      Response time (msec): 70
 vs0            10.11.12.15     down    Connection refused.
+---------------------------------------------------------------+
```

```
cluster1::> vserver services name-service ldap check -vserver vs0

| Vserver: vs0                                                 |
| Client Configuration Name: c1                                |
| LDAP Status: up                                              |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                                 |
```

La validation de la configuration est réussie si au moins un des serveurs configurés (name-Server/ldap-servers) est accessible et fournit le service. Un avertissement est affiché si certains serveurs sont inaccessibles.

Commandes ONTAP pour la gestion des entrées de commutateur de service de noms NAS

Vous pouvez gérer les entrées de commutateur de service de noms en les créant, en les affichant, en les modifiant et en les supprimant.

Les fonctions que vous recherchez…	Utilisez cette commande…
Créer une entrée de commutateur de service de nom	`vserver services name-service ns-switch create`
Afficher les entrées du commutateur d'entretien du nom	`vserver services name-service ns-switch show`
Modifier une entrée de commutateur de service de nom	`vserver services name-service ns-switch modify`
Supprimer une entrée de commutateur de service de nom	`vserver services name-service ns-switch delete`

Pour en savoir plus, `vserver services name-service ns-switch` consultez le "Référence de commande ONTAP".

Informations associées

"Rapport technique de NetApp 4668 : name Services Best Practices Guide (Guide des meilleures pratiques des services de noms)"

Commandes ONTAP pour la gestion du cache du service de noms NAS

Vous pouvez gérer le cache du service de noms en modifiant la valeur TTL (Time to live). La valeur TTL détermine la persistance des informations de service de noms longs dans le cache.

Si vous souhaitez modifier la valeur TTL pour…	Utilisez cette commande…
Utilisateurs UNIX	`vserver services name-service cache unix-user settings`
Groupes UNIX	`vserver services name-service cache unix-group settings`
Netgroups UNIX	`vserver services name-service cache netgroups settings`
Hôtes	`vserver services name-service cache hosts settings`
Appartenance à un groupe	`vserver services name-service cache group-membership settings`

Informations associées

"Référence de commande ONTAP"

Commandes ONTAP pour la gestion des mappages de noms NFS

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

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

Échange de la position de deux mappages de noms REMARQUE : un échange n'est pas autorisé lorsque le mappage-noms est configuré avec une entrée de qualificatif-ip.	`vserver name-mapping swap`
Modifier un mappage de noms	`vserver name-mapping modify`
Supprime un mappage de noms	`vserver name-mapping delete`
Valider le mappage de nom correct	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

Pour en savoir plus, `vserver name-mapping` consultez le "Référence de commande ONTAP".

Commandes ONTAP pour la gestion des utilisateurs UNIX locaux NAS

Il existe des commandes ONTAP spécifiques pour gérer les utilisateurs UNIX locaux.

Les fonctions que vous recherchez…	Utilisez cette commande…
Créez un utilisateur UNIX local	`vserver services name-service unix-user create`
Chargement des utilisateurs UNIX locaux à partir d'un URI	`vserver services name-service unix-user load-from-uri`
Afficher les utilisateurs UNIX locaux	`vserver services name-service unix-user show`
Modifier un utilisateur UNIX local	`vserver services name-service unix-user modify`
Supprimer un utilisateur UNIX local	`vserver services name-service unix-user delete`

Pour en savoir plus, `vserver services name-service unix-user` consultez le "Référence de commande ONTAP".

Commandes ONTAP pour la gestion des groupes UNIX locaux NAS

Il existe des commandes ONTAP spécifiques pour gérer les groupes UNIX locaux.

Les fonctions que vous recherchez…	Utilisez cette commande…
Créer un groupe UNIX local	`vserver services name-service unix-group create`

Ajouter un utilisateur à un groupe UNIX local	`vserver services name-service unix-group adduser`
Chargement des groupes UNIX locaux à partir d'un URI	`vserver services name-service unix-group load-from-uri`
Afficher les groupes UNIX locaux	`vserver services name-service unix-group show`
Modifier un groupe UNIX local	`vserver services name-service unix-group modify`
Supprimer un utilisateur d'un groupe UNIX local	`vserver services name-service unix-group deluser`
Supprimer un groupe UNIX local	`vserver services name-service unix-group delete`

Pour en savoir plus, `vserver services name-service unix-group` consultez le "Référence de commande ONTAP".

Limites pour les utilisateurs, groupes et membres de groupe UNIX locaux pour les SVM NFS ONTAP

ONTAP a introduit des limites au nombre maximal d'utilisateurs et de groupes UNIX dans le cluster, et des commandes pour gérer ces limites. Ces limites peuvent aider à éviter les problèmes de performances en empêchant les administrateurs de créer un trop grand nombre d'utilisateurs et de groupes UNIX locaux au sein du cluster.

Il existe une limite pour le nombre combiné de groupes d'utilisateurs UNIX locaux et de membres de groupe. Il existe une limite distincte pour les utilisateurs UNIX locaux. Les limites portent à l'échelle du cluster. Chacune de ces nouvelles limites est définie sur une valeur par défaut que vous pouvez modifier jusqu'à une limite stricte préaffectée.

Base de données	Limite par défaut	Limitation stricte
Utilisateurs UNIX locaux	32,768	65,536
Groupes UNIX locaux et membres de groupes	32,768	65,536

Gérer les limites des utilisateurs et groupes UNIX locaux pour les SVM ONTAP NFS

Il existe des commandes ONTAP spécifiques permettant de gérer les limites des utilisateurs et groupes UNIX locaux. Les administrateurs du cluster peuvent utiliser ces commandes pour résoudre les problèmes de performances qui, selon eux, seraient liés à un nombre excessif d'utilisateurs et de groupes UNIX locaux.

Description de la tâche

Ces commandes sont disponibles pour l'administrateur du cluster au niveau de privilège avancé.

Étape

1. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Utilisez la commande…
Affiche des informations sur les limites des utilisateurs UNIX locaux	`vserver services unix-user max-limit show`
Affiche des informations sur les limites de groupe UNIX locales	`vserver services unix-group max-limit show`
Modifier les limites des utilisateurs UNIX locaux	`vserver services unix-user max-limit modify`
Modifier les limites du groupe UNIX local	`vserver services unix-group max-limit modify`

Pour en savoir plus, `vserver services unix` consultez le "Référence de commande ONTAP".

Commandes ONTAP pour la gestion des groupes de réseaux locaux NFS

Vous pouvez gérer les groupes réseau locaux en les chargeant à partir d'un URI, en vérifiant leur état sur les nœuds, en les affichant et en les supprimant.

Les fonctions que vous recherchez…	Utilisez la commande…
Charger des groupes réseau à partir d'un URI	`vserver services name-service netgroup load`
Vérifiez l'état des groupes réseau sur les nœuds	`vserver services name-service netgroup status` Disponible au niveau de privilège avancé et au niveau supérieur.
Afficher les groupes réseau locaux	`vserver services name-service netgroup file show`
Supprimer un groupe réseau local	`vserver services name-service netgroup file delete`

Pour en savoir plus, `vserver services name-service netgroup file` consultez le "Référence de commande ONTAP".

Commandes ONTAP pour la gestion des configurations de domaine NFS NIS

Il existe des commandes ONTAP spécifiques pour gérer les configurations de domaine NIS.

Les fonctions que vous recherchez…	Utilisez cette commande…
Créez une configuration de domaine NIS	`vserver services name-service nis-domain create`
Affiche les configurations de domaine NIS	`vserver services name-service nis-domain show`
Affiche l'état de liaison d'une configuration de domaine NIS	`vserver services name-service nis-domain show-bound`
Affiche les statistiques NIS	`vserver services name-service nis-domain show-statistics` Disponible au niveau de privilège avancé et au niveau supérieur.
Effacer les statistiques NIS	`vserver services name-service nis-domain clear-statistics` Disponible au niveau de privilège avancé et au niveau supérieur.
Modifier une configuration de domaine NIS	`vserver services name-service nis-domain modify`
Supprimer une configuration de domaine NIS	`vserver services name-service nis-domain delete`
Activer la mise en cache pour les recherches netgroup-par-hôte	`vserver services name-service nis-domain netgroup-database config modify` Disponible au niveau de privilège avancé et au niveau supérieur.

Pour en savoir plus, `vserver services name-service nis-domain` consultez le "Référence de commande ONTAP".

Commandes ONTAP pour la gestion des configurations client NFS LDAP

Il existe des commandes ONTAP spécifiques pour gérer les configurations du client LDAP.

> Les administrateurs du SVM ne peuvent ni modifier ni supprimer les configurations du client LDAP créées par les administrateurs du cluster.

Les fonctions que vous recherchez…	Utilisez cette commande…
Créez une configuration client LDAP	`vserver services name-service ldap client create`
Affiche les configurations du client LDAP	`vserver services name-service ldap client show`

Modifier une configuration client LDAP	`vserver services name-service ldap client modify`
Modifiez le mot de passe DE LIAISON du client LDAP	`vserver services name-service ldap client modify-bind-password`
Supprimez une configuration client LDAP	`vserver services name-service ldap client delete`

Pour en savoir plus, `vserver services name-service ldap client` consultez le "Référence de commande ONTAP".

Commandes ONTAP pour la gestion des configurations LDAP NFS

Il existe des commandes ONTAP spécifiques pour gérer les configurations LDAP.

Les fonctions que vous recherchez…	Utilisez cette commande…
Créez une configuration LDAP	`vserver services name-service ldap create`
Afficher les configurations LDAP	`vserver services name-service ldap show`
Modifier une configuration LDAP	`vserver services name-service ldap modify`
Supprimez une configuration LDAP	`vserver services name-service ldap delete`

Pour en savoir plus, `vserver services name-service ldap` consultez le "Référence de commande ONTAP".

Commandes ONTAP pour la gestion des modèles de schéma client LDAP NFS

Il existe des commandes ONTAP spécifiques pour gérer les modèles de schéma client LDAP.

> Les administrateurs SVM ne peuvent ni modifier ni supprimer les schémas des clients LDAP qui ont été créés par les administrateurs du cluster.

Les fonctions que vous recherchez…	Utilisez cette commande…
Copier un modèle de schéma LDAP existant	`vserver services name-service ldap client schema copy` Disponible au niveau de privilège avancé et au niveau supérieur.
Afficher les modèles de schéma LDAP	`vserver services name-service ldap client schema show`

Modifier un modèle de schéma LDAP	`vserver services name-service ldap client schema modify` Disponible au niveau de privilège avancé et au niveau supérieur.
Supprimer un modèle de schéma LDAP	`vserver services name-service ldap client schema delete` Disponible au niveau de privilège avancé et au niveau supérieur.

Pour en savoir plus, `vserver services name-service ldap client schema` consultez le "Référence de commande ONTAP".

Commandes ONTAP pour la gestion des configurations d'interface NFS Kerberos

Il existe des commandes ONTAP spécifiques pour gérer les configurations de l'interface Kerberos NFS.

Les fonctions que vous recherchez…	Utilisez cette commande…
Activez NFS Kerberos sur une LIF	`vserver nfs kerberos interface enable`
Affiche les configurations de l'interface Kerberos NFS	`vserver nfs kerberos interface show`
Modifiez une configuration d'interface Kerberos NFS	`vserver nfs kerberos interface modify`
Désactivation de NFS Kerberos sur une LIF	`vserver nfs kerberos interface disable`

Pour en savoir plus, `vserver nfs kerberos interface` consultez le "Référence de commande ONTAP".

Commandes ONTAP pour la gestion des configurations de domaine NFS Kerberos

Il existe des commandes ONTAP spécifiques pour gérer les configurations de Royaume Kerberos NFS.

Les fonctions que vous recherchez…	**Utilisez cette commande…**
Créez une configuration de domaine NFS Kerberos	`vserver nfs kerberos realm create`
Affiche les configurations de domaine NFS Kerberos	`vserver nfs kerberos realm show`
Modifiez une configuration de domaine NFS Kerberos	`vserver nfs kerberos realm modify`

Les fonctions que vous recherchez…	Utilisez cette commande…
Supprimez une configuration de domaine NFS Kerberos	`vserver nfs kerberos realm delete`

Pour en savoir plus, `vserver nfs kerberos realm` consultez le "Référence de commande ONTAP".

Commandes ONTAP pour la gestion des politiques d'exportation

Il existe des commandes ONTAP spécifiques pour gérer les export-policies.

Les fonctions que vous recherchez…	Utilisez cette commande…
Affiche des informations sur les export-policy	`vserver export-policy show`
Renommez une export-policy	`vserver export-policy rename`
Copier une export-policy	`vserver export-policy copy`
Supprime une export-policy	`vserver export-policy delete`

Pour en savoir plus, `vserver export-policy` consultez le "Référence de commande ONTAP".

Commandes ONTAP pour la gestion des règles d'exportation

Il existe des commandes ONTAP spécifiques pour gérer les règles d'exportation.

Les fonctions que vous recherchez…	Utilisez cette commande…
Créer une règle d'exportation	`vserver export-policy rule create`
Affiche des informations sur les règles d'exportation	`vserver export-policy rule show`
Modifier une règle d'exportation	`vserver export-policy rule modify`
Supprimer une règle d'exportation	`vserver export-policy rule delete`

Si vous avez configuré plusieurs règles d'exportation identiques correspondant à différents clients, veillez à les garder synchronisées lors de la gestion des règles d'exportation.

Pour en savoir plus, `vserver export-policy` consultez le "Référence de commande ONTAP".

Configurez le cache des informations d'identification NFS

Raisons de la modification de la durée de vie du cache d'informations d'identification NFS pour les SVM ONTAP

ONTAP utilise un cache d'identifiants pour stocker les informations nécessaires à l'authentification utilisateur pour l'accès aux exportations NFS afin d'accélérer l'accès et d'améliorer les performances. Vous pouvez configurer la durée de stockage des informations d'identification dans le cache des informations d'identification pour les personnaliser en fonction de votre environnement.

La modification du TTL (Time-to-Live) du cache d'identifiants NFS permet de résoudre certains problèmes. Vous devez comprendre ce que sont ces scénarios ainsi que les conséquences de ces modifications.

Raisons

Envisagez de modifier le TTL par défaut dans les cas suivants :

Problème	Action corrective
Les noms de serveurs de votre environnement subissent une dégradation des performances en raison d'une charge élevée de requêtes de ONTAP.	Augmentez le TTL des identifiants positifs et négatifs en cache afin de réduire le nombre de requêtes de ONTAP vers les serveurs de noms.
L'administrateur du serveur de noms a apporté des modifications pour autoriser l'accès aux utilisateurs NFS qui étaient précédemment refusés.	Réduisez le TTL des identifiants négatifs en cache afin de réduire le temps que les utilisateurs NFS doivent attendre que ONTAP demande de nouvelles informations d'identification à partir de serveurs de noms externes afin qu'ils puissent obtenir un accès.
L'administrateur du serveur de noms a apporté des modifications pour refuser l'accès aux utilisateurs NFS précédemment autorisés.	Réduisez le TTL des identifiants positifs qui ont été mis en cache afin de réduire le temps avant que ONTAP ne demande de nouvelles informations d'identification auprès de serveurs de noms externes, de sorte que les utilisateurs NFS ne puissent plus accéder à ces derniers.

Conséquences

Vous pouvez modifier la durée individuellement pour la mise en cache des informations d'identification positives et négatives. Cependant, vous devriez être conscient à la fois des avantages et des inconvénients de le faire.

Si…	L'avantage, c'est…	L'inconvénient est…
Augmenter la durée du cache des informations d'identification positives	ONTAP envoie moins souvent des demandes d'informations d'identification pour nommer des serveurs, ce qui réduit la charge sur les serveurs de noms.	Il faut plus de temps pour refuser l'accès aux utilisateurs NFS, mais qui étaient auparavant autorisés à y accéder.

Si…	L’avantage, c’est…	L’inconvénient est…
Réduisez la durée du cache des informations d’identification positives	Le refus d’accès aux utilisateurs NFS, qui étaient auparavant autorisés, prend moins de temps.	ONTAP envoie plus fréquemment des demandes d’informations d’identification pour nommer des serveurs, ce qui augmente la charge sur les serveurs de noms.
Augmenter la durée du cache des informations d’identification négatives	ONTAP envoie moins souvent des demandes d’informations d’identification pour nommer des serveurs, ce qui réduit la charge sur les serveurs de noms.	Il faut plus de temps pour accorder l’accès aux utilisateurs NFS qui n’étaient auparavant pas autorisés mais qui le sont maintenant.
Réduisez le temps négatif du cache des informations d’identification	Il faut moins de temps pour accorder l’accès aux utilisateurs NFS qui n’étaient auparavant pas autorisés mais qui le sont maintenant.	ONTAP envoie plus fréquemment des demandes d’informations d’identification pour nommer des serveurs, ce qui augmente la charge sur les serveurs de noms.

Configurer la durée de vie des informations d’identification utilisateur NFS mises en cache pour les SVM ONTAP

Vous pouvez configurer la durée pendant laquelle ONTAP stocke les identifiants des utilisateurs NFS dans son cache interne (TTL ou délai avant activation) en modifiant le serveur NFS de la machine virtuelle de stockage (SVM). Vous pourrez ainsi remédier à certains problèmes liés à une charge élevée sur les serveurs de noms ou à des modifications d’identifiants qui affectent l’accès des utilisateurs NFS.

Description de la tâche

Ces paramètres sont disponibles au niveau de privilège avancé.

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Effectuez l’action souhaitée :

Si vous souhaitez modifier le TTL pour le cache…	Utilisez la commande…

Références positives	`vserver nfs modify -vserver vserver_name -cached -cred-positive-ttl time_to_live` Le TTL est mesuré en millisecondes. À partir de ONTAP 9.10.1 et versions ultérieures, la valeur par défaut est 1 heure (3,600,000 millisecondes). Dans ONTAP 9.9.1 et les versions antérieures, la valeur par défaut est de 24 heures (86,400,000 millisecondes). La plage autorisée pour cette valeur est de 1 minute (60000 millisecondes) à 7 jours (604,800,000 millisecondes).
Références négatives	`vserver nfs modify -vserver vserver_name -cached -cred-negative-ttl time_to_live` Le TTL est mesuré en millisecondes. La valeur par défaut est 2 heures (7,200,000 millisecondes). La plage autorisée pour cette valeur est de 1 minute (60000 millisecondes) à 7 jours (604,800,000 millisecondes).

3. Retour au niveau de privilège admin :

   `set -privilege admin`

Gestion des caches de règles d'exportation

Vider les caches de politique d'exportation pour les SVM NAS ONTAP

ONTAP utilise plusieurs caches de règles d'exportation pour stocker les informations relatives aux règles d'exportation afin d'accélérer les accès. Vidage manuel des caches des règles d'exportation (`vserver export-policy cache flush`) Supprime les informations potentiellement obsolètes et force ONTAP à extraire les informations actuelles des ressources externes appropriées. Cela peut aider à résoudre de nombreux problèmes liés à l'accès client aux exportations NFS.

Description de la tâche

Les informations du cache de la politique d'exportation peuvent être obsolètes pour les raisons suivantes :

- Modification récente des règles d'export-policy
- Modification récente des enregistrements de nom d'hôte dans les serveurs de noms
- Modification récente des entrées de groupe réseau dans les serveurs de noms
- Récupération suite à une panne réseau qui a empêché le chargement complet des groupes réseau

Étapes

1. Si le cache du service de noms n'est pas activé, effectuez l'une des opérations suivantes en mode privilèges avancés :

Si vous voulez rincer…	Entrez la commande…
Tous les caches des règles d'exportation (sauf showmount)	`vserver export-policy cache flush -vserver vserver_name`
Cache d'accès aux règles export-policy	`vserver export-policy cache flush -vserver vserver_name -cache access` Vous pouvez inclure l'option `-node` paramètre pour spécifier le nœud sur lequel vous souhaitez vider le cache d'accès.
Cache de nom d'hôte	`vserver export-policy cache flush -vserver vserver_name -cache host`
Le cache netgroup	`vserver export-policy cache flush -vserver vserver_name -cache netgroup` Le traitement des groupes réseau est intensif en ressources. Vous ne devez vider le cache netgroup que si vous essayez de résoudre un problème d'accès client causé par un groupe réseau obsolète.
Le cache showmount	`vserver export-policy cache flush -vserver vserver_name -cache showmount`

2. Si le cache du service de nom est activé, effectuez l'une des opérations suivantes :

Si vous voulez rincer…	Entrez la commande…
Cache d'accès aux règles export-policy	`vserver export-policy cache flush -vserver vserver_name -cache access` Vous pouvez inclure l'option `-node` paramètre pour spécifier le nœud sur lequel vous souhaitez vider le cache d'accès.
Cache de nom d'hôte	`vserver services name-service cache hosts forward-lookup delete-all`
Le cache netgroup	`vserver services name-service cache netgroups ip-to-netgroup delete-all vserver services name-service cache netgroups members delete-all` Le traitement des groupes réseau est intensif en ressources. Vous ne devez vider le cache netgroup que si vous essayez de résoudre un problème d'accès client causé par un groupe réseau obsolète.
Le cache showmount	`vserver export-policy cache flush -vserver vserver_name -cache showmount`

Afficher la file d'attente et le cache du groupe réseau de la politique d'exportation pour les SVM NFS ONTAP

ONTAP utilise la file d'attente du groupe réseau lors de l'importation et de la résolution des groupes réseau et utilise le cache du groupe réseau pour stocker les informations obtenues. Lors de la résolution des problèmes liés à la stratégie d'exportation netgroup, vous pouvez utiliser le `vserver export-policy netgroup queue show` et `vserver export-policy netgroup cache show` commandes permettant d'afficher l'état de la file d'attente netgroup et le contenu du cache netgroup.

Étape

1. Effectuez l'une des opérations suivantes :

Pour afficher le groupe réseau de la export policy…	Entrez la commande…
File d'attente	`vserver export-policy netgroup queue show`
Cache	`vserver export-policy netgroup cache show -vserver vserver_name`

Pour en savoir plus, `vserver export-policy netgroup` consultez le "Référence de commande ONTAP".

Vérifiez si une adresse IP client est membre d'un groupe réseau ONTAP NFS

Lors du dépannage des problèmes d'accès client NFS liés aux netgroups, vous pouvez utiliser le `vserver export-policy netgroup check-membership` Commande permettant de déterminer si une adresse IP client est membre d'un certain groupe réseau.

Description de la tâche

La vérification de l'appartenance à un groupe réseau vous permet de déterminer si ONTAP est conscient qu'un client est ou non membre d'un groupe réseau. Il vous permet également de savoir si le cache ONTAP netgroup est à l'état transitoire lors de l'actualisation des informations de groupe réseau. Ces informations peuvent vous aider à comprendre pourquoi un client peut être accordé ou refusé de façon inattendue.

Étape

1. Vérifiez l'appartenance d'un groupe réseau à une adresse IP client : `vserver export-policy netgroup check-membership -vserver vserver_name -netgroup netgroup_name -client-ip client_ip`

   La commande peut renvoyer les résultats suivants :

   - Le client est membre du groupe réseau.

     Cette opération a été confirmée par une analyse de recherche inversée ou une recherche netgroup-par-hôte.

- Le client est membre du groupe réseau.

  Elle a été trouvée dans le cache du groupe réseau ONTAP.

- Le client n'est pas membre du groupe réseau.
- L'appartenance du client ne peut pas encore être déterminée car ONTAP actualisant actuellement la mémoire cache du groupe réseau.

  Jusqu'à ce que cela soit fait, l'adhésion ne peut être explicitement exclue. Utilisez le `vserver export-policy netgroup queue show` commande permettant de surveiller le chargement du groupe réseau et de relancer la vérification une fois la vérification terminée.

Exemple

L'exemple suivant vérifie si un client avec l'adresse IP 172.17.16.72 est membre du netgroup Mercury sur la SVM vs1 :

```
 cluster1::> vserver export-policy netgroup check-membership -vserver vs1
-netgroup  mercury -client-ip 172.17.16.72
```

Optimiser les performances du cache d'accès pour les SVM ONTAP NFS

Vous pouvez configurer plusieurs paramètres afin d'optimiser le cache d'accès et trouver le juste équilibre entre les performances et la mise à jour des informations stockées dans le cache d'accès.

Description de la tâche

Lorsque vous configurez les périodes d'actualisation du cache d'accès, gardez les éléments suivants à l'esprit :

- Des valeurs plus élevées signifient que les entrées restent plus longues dans le cache d'accès.

  Ses performances sont meilleures, car ONTAP consacre moins de ressources à l'actualisation des entrées du cache d'accès. L'inconvénient est que si les règles d'export-policy changent et que les entrées de cache d'accès deviennent obsolètes, il faut donc plus de temps pour les mettre à jour. Par conséquent, il est possible que les clients qui devraient obtenir un accès soient refusés et que les clients qui devraient en être refusés aient un accès.

- Les valeurs faibles signifient que ONTAP actualise les entrées du cache d'accès plus souvent.

  L'avantage est que les entrées sont plus récentes et que les clients sont plus susceptibles d'obtenir correctement ou de refuser l'accès. L'inconvénient est que les performances sont diminueraient, car ONTAP dépense davantage de ressources lors de la mise à jour des entrées du cache d'accès.

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Effectuez l'action souhaitée :

Pour modifier…	Entrer…
Actualiser la période pour les entrées positives	`vserver export-policy access-cache config modify-all-vservers -refresh -period-positive timeout_value`
Actualiser la période pour les entrées négatives	`vserver export-policy access-cache config modify-all-vservers -refresh -period-negative timeout_value`
Délai d'expiration pour les anciennes entrées	`vserver export-policy access-cache config modify-all-vservers -harvest -timeout timeout_value`

3. Vérifiez les nouveaux paramètres :

   ```
   vserver export-policy access-cache config show-all-vservers
   ```

4. Retour au niveau de privilège admin :

   ```
   set -privilege admin
   ```

Gérer les verrous de fichier

En savoir plus sur le verrouillage des fichiers entre les protocoles pour les SVM ONTAP NFS

Le verrouillage de fichier est une méthode utilisée par les applications client pour empêcher un utilisateur d'accéder à un fichier précédemment ouvert par un autre utilisateur. Le mode de verrouillage des fichiers par ONTAP dépend du protocole du client.

Si le client est un client NFS, les verrouillages sont consultatifs ; si le client est un client SMB, les verrous sont obligatoires.

En raison des différences entre les verrouillages de fichiers NFS et SMB, un client NFS peut ne pas accéder à un fichier précédemment ouvert par une application SMB.

Ce qui suit se produit lorsqu'un client NFS tente d'accéder à un fichier verrouillé par une application SMB :

- Dans les volumes mixtes ou NTFS, les opérations de manipulation de fichiers telles que `rm`, `rmdir`, et `mv` Peut entraîner l'échec de l'application NFS.
- Les opérations de lecture et d'écriture NFS sont refusées par les modes SMB Deny-read et deny-write open, respectivement.
- Les opérations d'écriture NFS échouent lorsque la plage d'écriture du fichier est verrouillée par un bytelock SMB exclusif.

Dans les volumes de style de sécurité UNIX, les opérations de dissociation NFS et de renommage ignorent l'état du verrouillage SMB et permettent l'accès au fichier. Toutes les autres opérations NFS sur des volumes de type sécurité UNIX respectent l'état de verrouillage SMB.

En savoir plus sur les bits en lecture seule pour les SVM ONTAP NFS

Le bit de lecture seule est défini fichier par fichier pour indiquer si un fichier est inscriptible (désactivé) ou en lecture seule (activé).

Les clients SMB qui utilisent Windows peuvent définir un bit en lecture seule par fichier. Les clients NFS ne définissent pas de bit en lecture seule par fichier, car les clients NFS ne disposent d'aucune opération de protocole utilisant un bit en lecture seule par fichier.

ONTAP peut définir un bit en lecture seule sur un fichier lorsqu'un client SMB utilisant Windows crée ce fichier. ONTAP peut également définir un bit en lecture seule lorsqu'un fichier est partagé entre les clients NFS et les clients SMB. Certains logiciels, lorsqu'ils sont utilisés par des clients NFS et SMB, nécessitent l'activation du bit en lecture seule.

Pour que ONTAP garde les autorisations appropriées en lecture et écriture sur un fichier partagé entre les clients NFS et les clients SMB, il traite le bit en lecture seule conformément aux règles suivantes :

- NFS traite tous les fichiers dont le bit de lecture seule est activé comme s'il n'a pas de bits d'autorisation d'écriture activés.
- Si un client NFS désactive tous les bits d'autorisation d'écriture et qu'au moins un de ces bits avait été précédemment activé, ONTAP active le bit en lecture seule pour ce fichier.
- Si un client NFS active un bit d'autorisation d'écriture, ONTAP désactive le bit en lecture seule pour ce fichier.
- Si le bit de lecture seule d'un fichier est activé et qu'un client NFS tente de détecter les autorisations pour le fichier, les bits d'autorisation du fichier ne sont pas envoyés au client NFS. ONTAP envoie les bits d'autorisation au client NFS avec les bits d'autorisation d'écriture masqués.
- Si le bit de lecture seule d'un fichier est activé et qu'un client SMB désactive le bit de lecture seule, ONTAP active le bit d'autorisation d'écriture du propriétaire pour le fichier.
- Les fichiers dont le bit de lecture seule est activé sont accessibles en écriture uniquement par root.

Le bit en lecture seule interagit avec les bits de mode ACL et Unix des manières suivantes :

Lorsque le bit de lecture seule est défini sur un fichier :

- Aucune modification n'est apportée à la liste de contrôle d'accès (ACL) pour ce fichier. Les clients NFS verront la même liste de contrôle d'accès qu'avant la définition du bit de lecture seule.
- Tous les bits du mode Unix qui autorisent l'accès en écriture au fichier sont ignorés.
- Les clients NFS et SMB peuvent lire le fichier, mais ils ne peuvent pas le modifier.
- Les ACL et les bits du mode UNIX sont ignorés au profit du bit de lecture seule. Cela signifie que même si l'ACL autorise l'accès en écriture, le bit de lecture seule empêche toute modification.

Lorsque le bit de lecture seule n'est pas défini sur un fichier :

- ONTAP détermine l'accès en fonction des bits de mode ACL et UNIX.
  - Si l'ACL ou les bits du mode UNIX refusent l'accès en écriture, les clients NFS et SMB ne peuvent pas modifier le fichier.
  - Si ni les bits de mode ACL ni les bits de mode UNIX ne refusent l'accès en écriture, les clients NFS et SMB peuvent modifier le fichier.

Les modifications des autorisations liées aux fichiers sont immédiatement appliquées aux clients SMB, mais elles peuvent ne pas être immédiatement appliquées aux clients NFS si le client NFS active la mise en cache des attributs.

Découvrez en quoi ONTAP NFS et Windows diffèrent dans la gestion des verrous sur les composants du chemin de partage

Contrairement à Windows, ONTAP ne verrouille pas chaque composant du chemin d'accès à un fichier ouvert lorsque le fichier est ouvert. Ce comportement affecte également les chemins de partage SMB.

Étant donné que ONTAP ne verrouille pas chaque composant du chemin d'accès, il est possible de renommer un composant de chemin au-dessus du fichier ou du partage ouvert, ce qui peut causer des problèmes pour certaines applications ou peut rendre le chemin de partage dans la configuration SMB invalide. Cela peut rendre le partage inaccessible.

Pour éviter les problèmes causés par le changement de nom des composants du chemin d'accès, vous pouvez appliquer des paramètres de sécurité de la liste de contrôle d'accès Windows (ACL) qui empêchent les utilisateurs ou les applications de renommer les répertoires critiques.

En savoir plus sur "Comment empêcher le changement de nom des répertoires lorsque les clients y accèdent".

Afficher des informations sur les verrous pour les SVM ONTAP NFS

Vous pouvez afficher des informations sur les verrous de fichier en cours, y compris les types de verrous qui sont conservés et l'état de verrouillage, les détails sur les verrous de plage d'octets, les modes de verrouillage de sharelock, les verrous de délégation et les verrous opportunistes, et si les verrous sont ouverts avec des poignées durables ou persistantes.

Description de la tâche

L'adresse IP du client ne peut pas être affichée pour les verrouillages établis via NFS V4 ou NFS v4.1.

Par défaut, la commande affiche des informations relatives à tous les verrouillages. Vous pouvez utiliser les paramètres de la commande pour afficher des informations sur les verrous d'une machine virtuelle de stockage (SVM) spécifique ou pour filtrer les résultats de la commande par d'autres critères.

Le `vserver locks show` la commande affiche des informations sur quatre types de verrous :

- Les verrous de plage d'octets, qui verrouillent uniquement une partie d'un fichier.
- Verrous de partage, qui verrouillent les fichiers ouverts.
- Verrouillages opportunistes, qui contrôlent la mise en cache côté client sur SMB.
- Des délégations qui contrôlent la mise en cache côté client sur NFSv4.x.

En spécifiant des paramètres facultatifs, vous pouvez déterminer des informations importantes sur chaque type de verrou. Pour en savoir plus, `vserver locks show` consultez le "Référence de commande ONTAP".

Étape

1. Affiche des informations sur les verrous à l'aide de `vserver locks show` commande.

Exemples

L'exemple suivant présente un récapitulatif des informations relatives à un verrouillage NFSv4 sur un fichier avec le chemin d'accès `/vol1/file1`. Le mode d'accès de sharelock est Write-deny_none et le verrou a été accordé avec la délégation d'écriture :

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path               LIF         Protocol  Lock Type   Client
------- ------------------------- ----------- --------- -----------
-------
vol1    /vol1/file1               lif1        nfsv4     share-level -
              Sharelock Mode: write-deny_none
                                                        delegation  -
              Delegation Type: write
```

L'exemple suivant affiche des informations détaillées sur le verrou SMB d'un fichier avec le chemin d'accès `/data2/data2_2/intro.pptx`. Un descripteur durable est accordé sur le fichier avec un mode d'accès à verrouillage de partage Write-Deny_none à un client dont l'adresse IP est 10.3.1.3. Un oplock de location est accordé avec un niveau de oplock de lot :

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

                    Vserver: vs1
                     Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/intro.pptx
                  Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
              Lock Protocol: cifs
                  Lock Type: share-level
   Node Holding Lock State: node3
                 Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
              SMB Open Type: durable
         SMB Connect State: connected
SMB Expiration Time (Secs): -
```

```
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                   Vserver: vs1
                    Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/test.pptx
                  Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
              Lock Protocol: cifs
                  Lock Type: op-lock
   Node Holding Lock State: node3
                 Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

Briser les verrous de fichiers pour les SVM NFS ONTAP

Lorsque des verrous de fichier empêchent l'accès client aux fichiers, vous pouvez afficher des informations sur les verrous actuellement mis en attente, puis interrompre des verrous spécifiques. Les applications de débogage sont des exemples de scénarios dans lesquels vous devrez peut-être interrompre les verrous.

Description de la tâche

`vserver locks break`La commande n'est disponible qu'au niveau de privilège avancé et supérieur. Pour en savoir plus, `vserver locks break` consultez le link:https://docs.netapp.com/us-en/ontap-cli/vserver-locks-break.html["Référence de commande ONTAP"^].

Étapes

1. Pour trouver les informations dont vous avez besoin pour interrompre un verrouillage, utilisez le `vserver locks show` commande.

Pour en savoir plus, `vserver locks show` consultez le "Référence de commande ONTAP".

2. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

3. Effectuez l'une des opérations suivantes :

Si vous voulez rompre un verrou en spécifiant…	Entrez la commande…
Le nom du SVM, le nom du volume, le nom de la LIF et le chemin de fichier	`vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif`
L'ID de verrouillage	`vserver locks break -lockid UUID`

4. Retour au niveau de privilège admin :

   ```
   set -privilege admin
   ```

Découvrez comment les filtres de première lecture et de première écriture ONTAP FPolicy fonctionnent avec NFS

Les clients NFS bénéficient d'un temps de réponse élevé lors du trafic important de requêtes en lecture/écriture lorsque FPolicy est activé à l'aide d'un serveur FPolicy externe avec des opérations de lecture/écriture sous forme d'événements surveillés. Pour les clients NFS, l'utilisation de filtres de première lecture et de première écriture dans FPolicy réduit le nombre de notifications FPolicy et améliore les performances.

Dans NFS, le client effectue des E/S sur un fichier en récupérant son descripteur. Cet descripteur peut rester valide entre les redémarrages du serveur et du client. Par conséquent, le client est libre de mettre en cache le descripteur et d'y envoyer des requêtes sans récupérer de nouveau les poignées. Dans une session ordinaire, un grand nombre de requêtes de lecture/écriture sont envoyées au serveur de fichiers. Si des notifications sont générées pour toutes ces demandes, cela peut entraîner les problèmes suivants :

- Une charge plus importante grâce à un traitement supplémentaire des notifications et des temps de réponse plus courts.
- Envoi de nombreuses notifications au serveur FPolicy même si toutes les notifications ne sont pas affectées.

Après réception de la première demande de lecture/écriture d'un client pour un fichier particulier, une entrée de cache est créée et le nombre de lectures/écritures est incrémenté. Cette requête est marquée comme opération de première lecture/écriture et un événement FPolicy est généré. Avant de planifier et de créer les filtres FPolicy pour un client NFS, il est important de connaître les principes de base du fonctionnement des filtres FPolicy.

- Première lecture : filtre les demandes de lecture du client pour la première lecture.

  Lorsque ce filtre est utilisé pour les événements NFS, le `-file-session-io-grouping-count` et

`-file-session-io-grouping-duration` Les paramètres déterminent la demande de première lecture pour laquelle FPolicy est traité.

- Première écriture : filtre les demandes d'écriture du client pour la première écriture.

  Lorsque ce filtre est utilisé pour les événements NFS, le `-file-session-io-grouping-count` et `-file-session-io-grouping-duration` Les paramètres déterminent la première requête d'écriture pour laquelle FPolicy a traité.

Les options suivantes sont ajoutées dans la base de données des serveurs NFS.

```
file-session-io-grouping-count: Number of I/O Ops on a File to Be Clubbed
and Considered as One Session
for Event Generation
file-session-io-grouping-duration: Duration for Which I/O Ops on a File to
Be Clubbed and Considered as
One Session for Event Generation
```

Modifier l'ID d'implémentation du serveur NFSv4.1 pour les SVM ONTAP

Le protocole NFSv4.1 inclut un ID de mise en œuvre du serveur qui documente le domaine, le nom et la date du serveur. Vous pouvez modifier les valeurs par défaut de l'ID d'implémentation du serveur. La modification des valeurs par défaut peut être utile, par exemple, lors de la collecte des statistiques d'utilisation ou de la résolution des problèmes d'interopérabilité. Pour plus d'informations, consultez RFC 5661.

Description de la tâche

Les valeurs par défaut des trois options sont les suivantes :

Option	Nom de l'option	Valeur par défaut
Domaine d'ID d'implémentation NFSv4.1	`-v4.1-implementation -domain`	netapp.com
Nom de l'ID de mise en œuvre NFSv4.1	`-v4.1-implementation-name`	Nom de version du cluster
Date ID mise en œuvre NFSv4.1	`-v4.1-implementation-date`	Date de version du cluster

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Effectuez l'une des opérations suivantes :

Si vous voulez modifier l'ID d'implémentation NFSv4.1…	Entrez la commande…
Domaine	`vserver nfs modify -v4.1 -implementation-domain domain`
Nom	`vserver nfs modify -v4.1 -implementation-name name`
Date	`vserver nfs modify -v4.1 -implementation-date date`

3. Retour au niveau de privilège admin :

   ```
   set -privilege admin
   ```

Gérer les listes de contrôle d'accès NFSv4

Découvrez les avantages de l'activation des ACL NFSv4 pour les SVM ONTAP

Il existe de nombreux avantages pour activer les listes de contrôle d'accès NFSv4.

Voici quelques-uns des avantages majeurs apportés par les ACL NFSv4 :

- Contrôle plus précis de l'accès des utilisateurs aux fichiers et aux répertoires
- Sécurité NFS renforcée
- Interopérabilité accrue avec CIFS
- Suppression de la limitation NFS de 16 groupes par utilisateur

En savoir plus sur les ACL NFSv4 pour les SVM ONTAP

Un client utilisant des listes de contrôle d'accès NFSv4 peut définir et afficher des listes de contrôle d'accès sur les fichiers et les répertoires du système. Lorsqu'un nouveau fichier ou sous-répertoire est créé dans un répertoire contenant une liste de contrôle d'accès, le nouveau fichier ou sous-répertoire hérite de toutes les entrées de contrôle d'accès (ACE) de la liste de contrôle d'accès qui ont été marquées avec les indicateurs d'héritage appropriés.

Lorsqu'un fichier ou un répertoire est créé à la suite d'une requête NFSv4, l'ACL du fichier ou répertoire résultant dépend du fait que la demande de création de fichier inclut une ACL ou uniquement les autorisations d'accès aux fichiers UNIX standard, et si le répertoire parent possède une ACL :

- Si la requête inclut une liste de contrôle d'accès, cette liste de contrôle d'accès est utilisée.
- Si la demande comprend uniquement des autorisations d'accès aux fichiers UNIX standard mais que le répertoire parent possède une ACL, les ACE de l'ACL du répertoire parent sont hérités par le nouveau fichier ou répertoire tant que les ACE ont été balisés avec les indicateurs d'héritage appropriés.

Une ACL parent est héritée même si `-v4.0-acl` est défini sur `off`.

- Si la requête inclut uniquement les autorisations d'accès aux fichiers UNIX standard et que le répertoire parent ne dispose pas d'ACL, le mode fichier client est utilisé pour définir les autorisations d'accès aux fichiers UNIX standard.
- Si la requête inclut uniquement les autorisations d'accès aux fichiers UNIX standard et que le répertoire parent dispose d'une ACL non héritable, le nouvel objet est créé uniquement avec des bits de mode.

Si le `-chown-mode` paramètre a été défini sur `restricted` avec des commandes dans les `vserver nfs` familles ou `vserver export-policy rule`, la propriété du fichier ne peut être modifiée que par le superutilisateur, même si les autorisations sur disque définies avec les listes de contrôle d'accès NFSv4 permettent à un utilisateur non root de modifier la propriété du fichier. Pour en savoir plus sur les commandes décrites dans cette procédure"Référence de commande ONTAP", reportez-vous à la .

Activer ou désactiver la modification de l'ACL NFSv4 pour les SVM ONTAP

Lorsque ONTAP reçoit un `chmod` Commande pour un fichier ou un répertoire avec une liste de contrôle d'accès, la liste de contrôle d'accès est par défaut conservée et modifiée pour refléter le changement de bit de mode. Vous pouvez désactiver le `-v4-acl -preserve` Paramètre pour modifier le comportement si vous souhaitez que la liste de contrôle d'accès soit supprimée.

Description de la tâche

Lors de l'utilisation d'un style de sécurité unifié, ce paramètre indique également si les autorisations de fichier NTFS sont conservées ou supprimées lorsqu'un client envoie une commande chmod, chgroup ou chown pour un fichier ou un répertoire.

La valeur par défaut de ce paramètre est activée.

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Saisissez la commande suivante…
Activer la conservation et la modification des listes de contrôle d'accès NFSv4 existantes (par défaut)	`vserver nfs modify -vserver vserver_name -v4-acl -preserve enabled`
Désactivez la conservation et déposez les ACL NFSv4 lors du changement de bits de mode	`vserver nfs modify -vserver vserver_name -v4-acl -preserve disabled`

3. Retour au niveau de privilège admin :

```
set -privilege admin
```

Découvrez comment ONTAP utilise les ACL NFSv4 pour déterminer s'il peut supprimer des fichiers

Pour déterminer s'il peut supprimer un fichier, ONTAP utilise une combinaison du bit DE SUPPRESSION du fichier et du bit DE SUPPRESSION_ENFANT du répertoire contenant. Pour plus d'informations, consultez le document NFS 4.1 RFC 5661.

Activer ou désactiver les ACL NFSv4 pour les SVM ONTAP

Pour activer ou désactiver les ACL NFSv4, vous pouvez modifier le `-v4.0-acl` et `-v4.1-acl` options. Ces options sont désactivées par défaut.

Description de la tâche

Le `-v4.0-acl` ou `-v4.1-acl` Option contrôle la définition et l'affichage des ACL NFSv4 ; elle ne contrôle pas l'application de ces listes de contrôle d'accès pour la vérification de l'accès.

Étape

1. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Alors…
Activez les listes de contrôle d'accès NFSv4.0	Saisissez la commande suivante : `vserver nfs modify -vserver vserver_name -v4.0-acl enabled`
Désactivez les listes de contrôle d'accès NFSv4.0	Saisissez la commande suivante : `vserver nfs modify -vserver vserver_name -v4.0-acl disabled`
Activer les ACL NFSv4.1	Saisissez la commande suivante : `vserver nfs modify -vserver vserver_name -v4.1-acl enabled`
Désactiver les listes de contrôle d'accès NFSv4.1	Saisissez la commande suivante : `vserver nfs modify -vserver vserver_name -v4.1-acl disabled`

Modifier la limite ACE maximale pour les ACL NFSv4 pour les SVM ONTAP

Vous pouvez modifier le nombre maximal d'ACE autorisés pour chaque ACL NFSv4 en

modifiant le paramètre `-v4-acl-max-aces`. Par défaut, la limite est définie sur 400 ACE pour chaque ACL. L'augmentation de cette limite peut permettre de réussir la migration des données avec des listes de contrôle d'accès contenant plus de 400 ACE vers les systèmes de stockage exécutant ONTAP.

Description de la tâche

L'augmentation de cette limite peut avoir un impact sur les performances des clients accédant aux fichiers avec des listes de contrôle d'accès NFSv4.

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Modifier la limite ACE maximale pour les listes de contrôle d'accès NFSv4 :

   ```
   vserver nfs modify -v4-acl-max-aces max_ace_limit
   ```

   Plage valide de

   `max_ace_limit` est `192` à `1024`.

3. Retour au niveau de privilège admin :

   ```
   set -privilege admin
   ```

Gérer les délégations de fichiers NFSv4

Activer ou désactiver les délégations de fichiers de lecture NFSv4 pour les SVM ONTAP

Pour activer ou désactiver les délégations de fichiers en lecture NFSv4, vous pouvez modifier `-v4.0-read-delegation`ou option. En activant les délégations de fichiers de lecture, vous pouvez éliminer une grande partie de la surcharge de messages associée à l'ouverture et à la fermeture des fichiers.

Description de la tâche

Par défaut, les délégations des fichiers lus sont désactivées.

L'inconvénient de l'activation des délégations de fichiers en lecture est que le serveur et ses clients doivent restaurer des délégations après le redémarrage ou le redémarrage du serveur, qu'un client redémarre ou qu'une partition réseau se produit.

Étape

1. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Alors…

Activer les délégations des fichiers lus NFSv4	Saisissez la commande suivante : `vserver nfs modify -vserver vserver_name -v4.0 -read-delegation enabled`
Activer les délégations des fichiers de lecture NFSv4.1	Saisissez la commande suivante : + `vserver nfs modify -vserver vserver_name -v4.1 -read-delegation enabled`
Désactiver les délégations des fichiers de lecture NFSv4	Saisissez la commande suivante : `vserver nfs modify -vserver vserver_name -v4.0 -read-delegation disabled`
Désactiver les délégations de fichiers de lecture NFSv4.1	Saisissez la commande suivante : `vserver nfs modify -vserver vserver_name -v4.1 -read-delegation disabled`

Résultat

Les options de délégation de fichiers prennent effet dès qu'elles sont modifiées. Il n'est pas nécessaire de redémarrer ou de redémarrer NFS.

Activer ou désactiver les délégations de fichiers d'écriture NFSv4 pour les SVM ONTAP

Pour activer ou désactiver les délégations de fichiers d'écriture, vous pouvez modifier le `-v4.0-write-delegation`ou option. En activant les délégations de fichiers d'écriture, vous pouvez éliminer la majeure partie des surcharges de messages associées au verrouillage des fichiers et des enregistrements, en plus de l'ouverture et de la fermeture des fichiers.

Description de la tâche

Par défaut, les délégations des fichiers d'écriture sont désactivées.

L'inconvénient de l'activation des délégations de fichiers d'écriture est que le serveur et ses clients doivent effectuer des tâches supplémentaires pour restaurer des délégations après le redémarrage ou le redémarrage du serveur, qu'un client redémarre ou qu'une partition réseau se produit.

Étape

1. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Alors…
Activer les délégations des fichiers d'écriture NFSv4	Saisissez la commande suivante : `vserver nfs modify -vserver vserver_name -v4.0 -write-delegation enabled`

Les fonctions que vous recherchez…	Alors…
Activer les délégations de fichiers d'écriture NFSv4.1	Saisissez la commande suivante : `vserver nfs modify -vserver vserver_name -v4.1 -write-delegation enabled`
Désactiver les délégations des fichiers d'écriture NFSv4	Saisissez la commande suivante : `vserver nfs modify -vserver vserver_name -v4.0 -write-delegation disabled`
Désactiver les délégations de fichiers d'écriture NFSv4.1	Saisissez la commande suivante : `vserver nfs modify -vserver vserver_name -v4.1 -write-delegation disabled`

Résultat

Les options de délégation de fichiers prennent effet dès qu'elles sont modifiées. Il n'est pas nécessaire de redémarrer ou de redémarrer NFS.

Configurez le verrouillage des fichiers NFSv4 et des enregistrements

En savoir plus sur le verrouillage des fichiers et des enregistrements NFSv4 pour les SVM ONTAP

Pour les clients NFSv4, ONTAP supporte le mécanisme de verrouillage des fichiers NFSv4, tout en conservant l'état de tous les verrouillages de fichiers sous un modèle basé sur la location.

"Rapport technique NetApp 3580 : Guide des améliorations et des meilleures pratiques NFSv4 implémentation d'Data ONTAP"

Spécifier la période de bail de verrouillage NFSv4 pour les SVM ONTAP

Pour spécifier la période de verrouillage NFSv4 (c'est-à-dire la période pendant laquelle ONTAP accorde irrévocablement un verrouillage à un client), vous pouvez modifier le `-v4-lease-seconds` option. Des délais de location plus courts accélèrent la restauration des serveurs, tandis que des périodes de location plus longues sont avantageuses pour les serveurs qui gèrent un nombre très important de clients.

Description de la tâche

Par défaut, cette option est définie sur `30`. La valeur minimale de cette option est `10`. La valeur maximale pour cette option est le délai de grâce de verrouillage, que vous pouvez définir avec l' `locking.lease_seconds` option.

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Saisissez la commande suivante :

```
vserver nfs modify -vserver vserver_name -v4-lease-seconds number_of_seconds
```

3. Retour au niveau de privilège admin :

```
set -privilege admin
```

Spécifier la période de grâce de verrouillage NFSv4 pour les SVM ONTAP

Pour spécifier la période de grâce de verrouillage NFSv4 (c'est-à-dire le délai durant lequel les clients tentent de récupérer leur état de verrouillage à partir de ONTAP lors de la restauration du serveur), vous pouvez modifier le `-v4-grace-seconds` option.

Description de la tâche

Par défaut, cette option est définie sur `45`.

Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Saisissez la commande suivante :

```
vserver nfs modify -vserver vserver_name -v4-grace-seconds number_of_seconds
```

3. Retour au niveau de privilège admin :

```
set -privilege admin
```

En savoir plus sur les références NFSv4 pour les SVM ONTAP

Lorsque vous activez les référencements NFSv4, ONTAP fournit des référencements « intra-SVM » aux clients NFSv4. La référence intra-SVM est utilisée lorsqu'un nœud de cluster recevant la requête NFSv4 fait référence au client NFSv4 à une autre interface logique (LIF) sur la machine virtuelle de stockage (SVM).

Le client NFSv4 doit accéder au chemin qui a reçu la recommandation au niveau du LIF cible à partir de ce point. Le nœud de cluster d'origine fournit une telle recommandation lorsqu'il détermine qu'il existe une LIF dans le SVM qui réside sur le nœud de cluster sur lequel réside le volume de données, ce qui permet aux clients d'accéder plus rapidement aux données et d'éviter toute communication supplémentaire du cluster.

Activer ou désactiver les références NFSv4 pour les SVM ONTAP

Vous pouvez activer les référencements NFSv4 sur les machines virtuelles de stockage (SVM) en activant les options `-v4-fsid-change` et `-v4.0-referrals`ou. L'activation des référencements NFSV4 peut entraîner un accès plus rapide aux données pour les clients NFSv4 qui prennent en charge cette fonctionnalité.

Avant de commencer

Si vous souhaitez activer les référencements NFS, vous devez d'abord désactiver Parallel NFS. Vous ne

pouvez pas activer les deux en même temps.

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Entrez la commande…
Activez les référencements NFSv4	`vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.0-referrals enabled`
Désactiver les référencements NFSv4	`vserver nfs modify -vserver vserver_name -v4.0 -referrals disabled`
Activer les référencements NFSv4.1	`vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.1-referrals enabled`
Désactiver les référencements NFSv4.1	`vserver nfs modify -vserver vserver_name -v4.1 -referrals disabled`

3. Retour au niveau de privilège admin :

   ```
   set -privilege admin
   ```

Afficher les statistiques pour les SVM ONTAP NFS

Pour surveiller les performances et diagnostiquer les problèmes, vous pouvez afficher les statistiques NFS des serveurs virtuels de stockage (SVM) sur le système de stockage.

Étapes

1. Utilisez le `statistics catalog object show` Commande permettant d'identifier les objets NFS à partir desquels vous pouvez afficher les données.

   ```
   statistics catalog object show -object nfs*
   ```

2. Utilisez le `statistics start` et en option `statistics stop` commandes permettant de collecter un échantillon de données à partir d'un ou de plusieurs objets.
3. Utilisez le `statistics show` commande pour afficher les exemples de données.

Exemple : contrôle des performances NFSv3

L'exemple suivant montre les données de performances pour le protocole NFSv3.

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

```
vs1::> statistics start -object nfsv3 -sample-id nfs_sample
```

La commande suivante affiche les données de l'échantillon en spécifiant des compteurs qui indiquent le nombre de demandes de lecture et d'écriture réussies par rapport au nombre total de demandes de lecture et d'écriture :

```
vs1::> statistics show -sample-id nfs_sample -counter
read_total|write_total|read_success|write_success

Object: nfsv3
Instance: vs1
Start-time: 2/11/2013 15:38:29
End-time: 2/11/2013 15:38:41
Cluster: cluster1

    Counter                                     Value
    --------------------------- ----------------------------
    read_success                                  40042
    read_total                                    40042
    write_success                               1492052
    write_total                                 1492052
```

Informations associées

- "Configuration du contrôle des performances"
- "objet de catalogue de statistiques afficher"
- "les statistiques montrent"
- "les statistiques commencent"
- "les statistiques s'arrêtent"

Afficher les statistiques DNS pour les SVM ONTAP NFS

Vous pouvez afficher les statistiques DNS des ordinateurs virtuels de stockage (SVM) sur le système de stockage afin de surveiller les performances et de diagnostiquer les problèmes.

Étapes

1. Utilisez le `statistics catalog object show` Commande permettant d'identifier les objets DNS à partir desquels vous pouvez afficher les données.

   ```
   statistics catalog object show -object external_service_op*
   ```

2. Utilisez le `statistics start` et `statistics stop` commandes permettant de collecter un échantillon de données à partir d'un ou de plusieurs objets.
3. Utilisez le `statistics show` commande pour afficher les exemples de données.

Surveillance des statistiques DNS

Les exemples suivants présentent les données de performances des requêtes DNS. Les commandes suivantes permettent de lancer la collecte de données pour un nouvel échantillon :

```
vs1::*> statistics start -object external_service_op -sample-id
dns_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
dns_sample2
```

La commande suivante affiche les données de l'échantillon en spécifiant des compteurs qui affichent le nombre de requêtes DNS envoyées par rapport au nombre de requêtes DNS reçues, échouées ou expirées :

```
vs1::*> statistics show -sample-id dns_sample1 -counter
num_requests_sent|num_responses_received|num_successful_responses|num_time
outs|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:DNS:Query:10.72.219.109
Start-time: 3/8/2016 11:15:21
End-time: 3/8/2016 11:16:52
Elapsed-time: 91s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    num_not_found_responses                                         0
    num_request_failures                                            0
    num_requests_sent                                               1
    num_responses_received                                          1
    num_successful_responses                                        1
    num_timeouts                                                    0
6 entries were displayed.
```

La commande suivante affiche les données de l'échantillon en spécifiant des compteurs qui affichent le nombre de fois qu'une erreur spécifique a été reçue pour une requête DNS sur le serveur particulier :

```
vs1::*> statistics show -sample-id dns_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:DNS:Query:NXDOMAIN:10.72.219.109
Start-time: 3/8/2016 11:23:21
End-time: 3/8/2016 11:24:25
Elapsed-time: 64s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    count                                                           1
    error_string                                             NXDOMAIN
    server_ip_address                                   10.72.219.109
3 entries were displayed.
```

Informations associées

- "Configuration du contrôle des performances"
- "objet de catalogue de statistiques afficher"
- "les statistiques montrent"
- "les statistiques commencent"
- "les statistiques s'arrêtent"

Afficher les statistiques NIS pour les SVM ONTAP NFS

Pour surveiller les performances et diagnostiquer les problèmes, vous pouvez afficher les statistiques NIS des machines virtuelles de stockage (SVM) sur le système de stockage.

Étapes

1. Utilisez le `statistics catalog object show` Pour identifier les objets NIS à partir desquels vous pouvez afficher des données.

   ```
   statistics catalog object show -object external_service_op*
   ```

2. Utilisez le `statistics start` et `statistics stop` commandes permettant de collecter un échantillon de données à partir d'un ou de plusieurs objets.
3. Utilisez le `statistics show` commande pour afficher les exemples de données.

Surveillance des statistiques NIS

Les exemples suivants affichent des données de performances pour les requêtes NIS. Les commandes suivantes permettent de lancer la collecte de données pour un nouvel échantillon :

```
vs1::*> statistics start -object external_service_op -sample-id
nis_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
nis_sample2
```

La commande suivante affiche les données de l'échantillon en spécifiant des compteurs indiquant le nombre de requêtes NIS envoyées par rapport au nombre de requêtes NIS reçues, en échec ou en expiration :

```
vs1::*> statistics show -sample-id nis_sample1 -counter
instance|num_requests_sent|num_responses_received|num_successful_responses
|num_timeouts|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:NIS:Query:10.227.13.221
Start-time: 3/8/2016 11:27:39
End-time: 3/8/2016 11:27:56
Elapsed-time: 17s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    num_not_found_responses                                         0
    num_request_failures                                            1
    num_requests_sent                                               2
    num_responses_received                                          1
    num_successful_responses                                        1
    num_timeouts                                                    0
6 entries were displayed.
```

La commande suivante affiche les données de l'échantillon en spécifiant des compteurs indiquant le nombre de fois où une erreur spécifique a été reçue pour une requête NIS sur le serveur particulier :

```
vs1::*> statistics show -sample-id nis_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:NIS:Query:YP_NOTFOUND:10.227.13.221
Start-time: 3/8/2016 11:33:05
End-time: 3/8/2016 11:33:10
Elapsed-time: 5s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    count                                                           1
    error_string                                           YP_NOTFOUND
    server_ip_address                                    10.227.13.221
3 entries were displayed.
```

Informations associées

- "Configuration du contrôle des performances"
- "objet de catalogue de statistiques afficher"
- "les statistiques montrent"
- "les statistiques commencent"
- "les statistiques s'arrêtent"

En savoir plus sur la prise en charge de VMware vStorage sur ONTAP NFS

ONTAP prend en charge certaines fonctionnalités VMware vStorage APIs for Array Integration (VAAI) dans un environnement NFS.

Fonctionnalités prises en charge

Les fonctionnalités suivantes sont prises en charge :

- Copie auxiliaire

  Permet à un hôte ESXi de copier des machines virtuelles ou des disques de machines virtuelles directement entre les emplacements de datastore source et de destination sans impliquer l'hôte. Cela permet d'économiser les cycles du processeur de l'hôte ESXi et la bande passante du réseau. Le déchargement des copies préserve l'efficacité de l'espace si le volume source est faible.

- Réservation d'espace

  Garantit l'espace de stockage d'un fichier VMDK en réservant de l'espace pour celui-ci.

Limites

VMware vStorage over NFS présente les limites suivantes :

- Les opérations de déchargement des copies peuvent échouer dans les scénarios suivants :
  - Lors de l'exécution de waffer sur le volume source ou de destination, car il met temporairement le volume hors ligne
  - Pendant le déplacement du volume source ou de destination
  - Lors du déplacement de LIF source ou de destination
  - Lors des opérations de basculement ou de rétablissement
  - Lors des opérations de basculement ou de rétablissement
- La copie côté serveur peut échouer en raison des différences de format de descripteur de fichier dans le scénario suivant :

  Tentative de copie des données à partir des SVM dont les qtrees n'ont pas encore été exportés vers des SVM, ou qui ont déjà été exportés. Pour contourner cette limitation, vous pouvez exporter au moins un qtree sur le SVM de destination.

Informations associées

"Quelles opérations VAAI Offloaded sont prises en charge par Data ONTAP ?"

Activer ou désactiver VMware vStorage sur ONTAP NFS

Vous pouvez activer ou désactiver la prise en charge de VMware vStorage sur NFS sur des SVM (Storage Virtual machines) à l'aide du `vserver nfs modify` commande.

Description de la tâche

Par défaut, la prise en charge de VMware vStorage over NFS est désactivée.

Étapes

1. Afficher l'état actuel de la prise en charge de vStorage pour les SVM :

   ```
   vserver nfs show -vserver vserver_name -instance
   ```

2. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Saisissez la commande suivante…
Prise en charge de VMware vStorage	`vserver nfs modify -vserver vserver_name -vstorage enabled`
Désactivez la prise en charge de VMware vStorage	`vserver nfs modify -vserver vserver_name -vstorage disabled`

Une fois que vous avez terminé

Vous devez installer le plug-in NFS pour VMware VAAI avant de pouvoir utiliser cette fonctionnalité. Pour plus d'informations, consultez *installation du plug-in NetApp NFS pour VMware VAAI*.

Informations associées

"Documentation NetApp : plug-in NetApp NFS pour VMware VAAI"

Activer ou désactiver la prise en charge de rquota sur les SVM NFS ONTAP

Le protocole de quota distant (rquota) permet aux clients NFS d'obtenir des informations de quota pour les utilisateurs à partir d'une machine distante. La prise en charge des versions de rquota varie en fonction de votre version de ONTAP.

- Rquota v1 est pris en charge dans ONTAP 9 et les versions ultérieures.
- Rquota v2 est pris en charge dans ONTAP 9.12.1 et les versions ultérieures.

  Si vous effectuez une mise à niveau de rquota v1 vers rquota v2, vous remarquerez peut-être un changement inattendu dans votre limite de quota utilisateur. Ce changement est dû à la différence dans la façon dont le quota est calculé entre rquota v1 et rquota v2. Pour plus d'informations, consultez le"Base de connaissances NetApp : Pourquoi la limite de quota utilisateur a-t-elle changé de manière inattendue ?" .

Description de la tâche

Par défaut, rquota est désactivé.

Étape

1. Activer ou désactiver rquota :

Les fonctions que vous recherchez…	Saisissez la commande suivante…
Activer la prise en charge de rquota pour les SVM	`vserver nfs modify -vserver vserver_name -rquota enable`
Désactiver la prise en charge de rquota pour les SVM	`vserver nfs modify -vserver vserver_name -rquota disable`

Pour plus d'informations sur les quotas, reportez-vous à la section "Gestion du stockage logique".

Découvrez les améliorations des performances NFSv3 et NFSv4 et la taille de transfert TCP pour les SVM ONTAP

Vous pouvez améliorer les performances des clients NFSv3 et NFSv4 qui se connectent aux systèmes de stockage sur un réseau à latence élevée en modifiant la taille maximale du transfert TCP.

Lorsque les clients accèdent aux systèmes de stockage sur un réseau à latence élevée, tel qu'un réseau WAN (Wide Area Network) ou un réseau MAN (Metro Area Network) avec une latence supérieure à 10 millisecondes, vous pouvez améliorer les performances de connexion en modifiant la taille maximale du transfert TCP. Les clients qui accèdent aux systèmes de stockage dans un réseau à faible latence, tel qu'un réseau local (LAN), ne peuvent guère bénéficier de la modification de ces paramètres. Si l'amélioration du

débit ne l'emporte pas sur l'impact sur la latence, vous ne devez pas utiliser ces paramètres.

Pour déterminer si votre environnement de stockage peut tirer parti de la modification de ces paramètres, vous devez d'abord effectuer une évaluation complète des performances d'un client NFS peu performant. Vérifiez si les faibles performances sont à cause d'une latence aller-retour excessive et d'une petite demande sur le client. Dans ces conditions, le client et le serveur ne peuvent pas utiliser pleinement la bande passante disponible parce qu'ils passent la majorité de leurs cycles de service en attente de petites demandes et réponses à transmettre par le biais de la connexion.

En augmentant la taille des requêtes NFSv3 et NFSv4, le client et le serveur peuvent utiliser la bande passante disponible plus efficacement pour déplacer plus de données par unité de temps, ce qui accroît l'efficacité globale de la connexion.

N'oubliez pas que la configuration entre le système de stockage et le client peut varier. Le système de stockage et le client prennent en charge une taille maximale de 1 Mo pour les opérations de transfert. Cependant, si vous configurez le système de stockage pour prendre en charge une taille de transfert maximale de 1 Mo mais que le client ne prend en charge que 64 Ko, la taille de transfert de montage est limitée à 64 Ko ou moins.

Avant de modifier ces paramètres, notez qu'il entraîne une consommation de mémoire supplémentaire sur le système de stockage pendant la durée nécessaire à l'assemblage et à la transmission d'une réponse importante. Plus les connexions à latence élevée sont nombreuses, plus la consommation de mémoire supplémentaire augmente. Les systèmes de stockage dont la capacité de mémoire est élevée ne subissent que très peu d'effet. Les systèmes de stockage dont la capacité de mémoire est faible peuvent constater une dégradation notable des performances.

La réussite de l'utilisation de ces paramètres repose sur la capacité à récupérer les données provenant de plusieurs nœuds d'un cluster. La latence inhérente au réseau du cluster peut augmenter la latence globale de la réponse. La latence globale a tendance à augmenter lors de l'utilisation de ces paramètres. Ainsi, les charges de travail sensibles à la latence peuvent avoir un impact négatif.

Modifier la taille de transfert maximale TCP NFSv3 et NFSv4 pour les SVM ONTAP

Vous pouvez modifier le `-tcp-max-xfer-size` Option permettant de configurer les tailles de transfert maximales pour toutes les connexions TCP en utilisant les protocoles NFSv3 et NFSv4.x.

Description de la tâche

Vous pouvez modifier ces options individuellement pour chaque serveur virtuel de stockage (SVM).

À partir de ONTAP 9, le `v3-tcp-max-read-size` et `v3-tcp-max-write-size` les options sont obsolètes. Vous devez utiliser le `-tcp-max-xfer-size` à la place.

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Entrez la commande…
Modifier la taille maximale du transfert TCP NFSv3 ou NFSv4	`vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer_max_xfer_size`

Option	Gamme	Valeur par défaut
`-tcp-max-xfer-size`	8192 à 1048576 octets	65536 octets

> La taille de transfert maximale que vous saisissez doit être un multiple de 4 Ko (4096 octets). Les demandes qui ne sont pas correctement alignées ont un impact négatif sur les performances.

3. Utilisez le `vserver nfs show -fields tcp-max-xfer-size` pour vérifier les modifications.
4. Si des clients utilisent des montages statiques, démontez et remontez la nouvelle taille de paramètre pour prendre effet.

Exemple

La commande suivante définit la taille maximale du transfert NFSv3 et NFSv4.x TCP à 1048576 octets sur le SVM nommé vs1 :

```
vs1::> vserver nfs modify -vserver vs1 -tcp-max-xfer-size 1048576
```

Configurer le nombre d'ID de groupe autorisés pour les utilisateurs NFS pour les SVM ONTAP

Par défaut, ONTAP prend en charge jusqu'à 32 ID de groupe lors du traitement des informations d'identification des utilisateurs NFS à l'aide de l'authentification Kerberos (RPCSEC_GSS). Lors de l'utilisation de l'authentification AUTH_SYS, le nombre maximal par défaut d'ID de groupe est de 16, comme défini dans RFC 5531. Vous pouvez augmenter le maximum jusqu'à 1,024 si vous avez des utilisateurs qui sont membres de plus que le nombre par défaut de groupes.

Description de la tâche

Si un utilisateur a plus que le nombre par défaut d'ID de groupe dans ses informations d'identification, les ID de groupe restants sont tronqués et l'utilisateur peut recevoir des erreurs lorsqu'il tente d'accéder aux fichiers du système de stockage. Vous devez définir le nombre maximal de groupes par SVM sur un nombre qui représente le maximum de groupes dans votre environnement.

> Pour comprendre les conditions préalables d'authentification AUTH_SYS pour l'activation des groupes étendus(`-auth-sys-extended-groups`) qui utilisent des identifiants de groupe au-delà du maximum par défaut de 16, reportez-vous à la"Base de connaissances NetApp : Quelles sont les conditions préalables à l'activation de auth-sys-extended-groups ?"

Le tableau suivant montre les deux paramètres du `vserver nfs modify` Commande qui détermine le

nombre maximal d'ID de groupe dans trois exemples de configuration :

Paramètres	Paramètres	Limite des ID de groupe résultant

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`32`
	
	`disabled`
	
	Il s'agit des paramètres par défaut.
		RPCSEC_GSS : 32
		
		AUTH_SYS : 16

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`256`
	
	`disabled`
		RPCSEC_GSS : 256
		
		AUTH_SYS : 16

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`512`
	
	`enabled`
		RPCSEC_GSS : 512
		
		AUTH_SYS : 512

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Effectuez l'action souhaitée :

Si vous souhaitez définir le nombre maximum de groupes auxiliaires autorisés…	Entrez la commande…
Uniquement pour RPCSEC_GSS et laisser AUTH_SYS à la valeur par défaut 16	`vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups disabled`
Pour RPCSEC_GSS et AUTH_SYS	`vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups enabled`

3. Vérifiez le `-extended-groups-limit` Et vérifier si AUTH_SYS utilise des groupes étendus : `vserver nfs show -vserver vserver_name -fields auth-sys-extended-groups,extended-groups-limit`
4. Retour au niveau de privilège admin :

   ```
   set -privilege admin
   ```

Exemple

L'exemple suivant active les groupes étendus pour l'authentification AUTH_SYS et définit le nombre maximal

de groupes étendus sur 512 pour l'authentification AUTH_SYS et RPCSEC_GSS. Ces modifications sont effectuées uniquement pour les clients qui accèdent à la SVM nommée vs1 :

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
         them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -auth-sys-extended-groups enabled
-extended-groups-limit 512

vs1::*> vserver nfs show -vserver vs1 -fields auth-sys-extended-
groups,extended-groups-limit
vserver auth-sys-extended-groups extended-groups-limit
------- ------------------------ --------------------
vs1     enabled                  512

vs1::*> set -privilege admin
```

Informations associées

- "Base de connaissances NetApp : Modifications des groupes étendus AUTH_SYS pour l'authentification NFS pour ONTAP 9"

Contrôler l'accès des utilisateurs root aux données de style sécurité NTFS pour les SVM ONTAP

Vous pouvez configurer ONTAP de manière à permettre aux clients NFS d'accéder aux données de type sécurité NTFS et aux clients NTFS pour accéder aux données de type sécurité NFS. Lorsque vous utilisez le style de sécurité NTFS dans un magasin de données NFS, vous devez décider comment traiter l'accès par l'utilisateur root et configurer la machine virtuelle de stockage (SVM) en conséquence.

Description de la tâche

Lorsqu'un utilisateur root accède aux données de style de sécurité NTFS, vous disposez de deux options :

- Mappez l'utilisateur root à un utilisateur Windows comme tout autre utilisateur NFS et gérez l'accès en fonction des listes de contrôle d'accès NTFS.
- Ignorez les listes de contrôle d'accès NTFS et offrez un accès complet à la racine.

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Effectuez l'action souhaitée :

Si vous voulez que l'utilisateur root…	Entrez la commande…
Être mappé à un utilisateur Windows	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root disabled`
Ignorer la vérification de la liste de contrôle d'accès NT	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root enabled`

Par défaut, ce paramètre est désactivé.

Si ce paramètre est activé mais qu'il n'y a pas de mappage de noms pour l'utilisateur root, ONTAP utilise les informations d'identification d'administrateur SMB par défaut pour l'audit.

3. Retour au niveau de privilège admin :

```
set -privilege admin
```

Versions NFS et clients pris en charge

En savoir plus sur les versions et les clients ONTAP NFS pris en charge

Avant d'utiliser NFS dans votre réseau, vous devez connaître les versions NFS et les clients pris en charge par ONTAP.

Ce tableau indique lorsque des versions majeures et mineures des protocoles NFS sont prises en charge par défaut dans ONTAP. Par défaut, la prise en charge n'indique pas qu'il s'agit de la version la plus ancienne de ONTAP prenant en charge ce protocole NFS.

Version	Pris en charge	Introduction
NFSv3	Oui.	Toutes les versions de ONTAP
NFSv4.0	Oui.	ONTAP 8
NFSv4.1	Oui.	ONTAP 8,1
NFSv4.2	Oui.	ONTAP 9.8
PNFS	Oui.	ONTAP 8,1

Pour obtenir les dernières informations sur les clients NFS pris en charge par ONTAP, consultez la matrice d'interopérabilité.

"Matrice d'interopérabilité NetApp"

En savoir plus sur la prise en charge ONTAP pour la fonctionnalité NFSv4.0

ONTAP prend en charge toutes les fonctionnalités obligatoires dans NFSv4.0, à l'exception des mécanismes de sécurité SPKM3 et LIPKEY.

Les fonctionnalités NFSV4 suivantes sont prises en charge :

- **COMPOSÉ**

  Permet à un client de demander plusieurs opérations de fichier dans une seule demande RPC (Remote Procedure Call).

- **Délégation de fichiers**

  Permet au serveur de déléguer le contrôle de fichiers à certains types de clients pour l'accès en lecture et en écriture.

- **Pseudo-fs**

  Utilisé par les serveurs NFSv4 pour déterminer les points de montage sur le système de stockage. Il n'y a pas de protocole de montage dans NFSv4.

- **Verrouillage**

  Basé sur la location. Il n'existe pas de protocoles NLM (Network Lock Manager) ou NSM (Network Status Monitor) distincts dans NFSv4.

Pour plus d'informations sur le protocole NFSv4.0, voir RFC 3530.

En savoir plus sur les limitations de prise en charge ONTAP pour NFSv4

Vous devez tenir compte de plusieurs restrictions liées à la prise en charge de ONTAP pour NFSv4.

- La fonction de délégation n'est pas prise en charge par tous les types de clients.
- Dans ONTAP 9.4 et versions antérieures, le système de stockage rejette les noms comportant des caractères non ASCII sur des volumes autres que les volumes UTF8.

  Dans ONTAP 9.5 et versions ultérieures, les volumes créés avec le paramètre de langue utf8mb4 et montés via NFS v4 ne sont plus soumis à cette restriction.

- Tous les descripteurs de fichier sont persistants ; le serveur ne fournit pas de descripteurs de fichier volatiles.
- La migration et la réplication ne sont pas prises en charge.
- Les clients NFSv4 ne sont pas pris en charge par les miroirs de partage de charge en lecture seule.

  ONTAP achemine les clients NFSv4 vers la source du miroir de partage de charge pour un accès en lecture et en écriture directs.

- Les attributs nommés ne sont pas pris en charge.
- Tous les attributs recommandés sont pris en charge, à l'exception des éléments suivants :

- archive
- hidden
- homogeneous
- mimetype
- quota_avail_hard
- quota_avail_soft
- quota_used
- system
- time_backup

> Même s'il ne prend pas en charge le `quota*` Attributs, ONTAP prend en charge les quotas d'utilisateurs et de groupes via le protocole de bande latérale RQUOTA.

En savoir plus sur la prise en charge ONTAP pour NFSv4.1

Depuis ONTAP 9.8, la fonctionnalité nconnect est disponible par défaut lorsque NFSv4.1 est activé.

Les implémentations de clients NFS antérieures n'utilisent qu'une connexion TCP unique avec un montage. En ONTAP, une connexion TCP unique peut former un goulot d'étranglement lorsque le nombre d'IOPS augmente.

nconnect améliore les performances du client NFS en autorisant plusieurs connexions TCP (jusqu'à 16) pour un seul montage, ce qui permet de surmonter le goulot d'étranglement des performances qui peut survenir avec une seule connexion TCP lorsque les IOPS augmentent.

NFSv4.1 est activé par défaut dans ONTAP 9.9.1 et versions ultérieures. Dans les versions antérieures, vous pouvez l'activer en spécifiant le `-v4.1` et le définir sur `enabled` Lors de la création d'un serveur NFS sur la machine virtuelle de stockage (SVM).

ONTAP ne prend pas en charge les délégations au niveau des fichiers et des répertoires NFSv4.1.

Informations associées

"Découvrez nconnect pour optimiser les performances NFS".

En savoir plus sur la prise en charge ONTAP pour NFSv4.2

À partir de ONTAP 9.8, ONTAP prend en charge le protocole NFSv4.2 pour permettre l'accès aux clients compatibles NFSv4.2.

NFSv4.2 est activé par défaut dans ONTAP 9.9.1 et versions ultérieures. Dans ONTAP 9.8, il est nécessaire d'activer manuellement la version 4.2 en spécifiant le `-v4.2` option et la paramétrer `enabled` lors de la création d'un serveur NFS sur la machine virtuelle de stockage (SVM). L'activation de NFSv4.1 permet également aux clients d'utiliser les fonctionnalités NFSv4.1 même lorsqu'il est monté en tant que v4.2.

Les versions successives de ONTAP étendent la prise en charge des fonctionnalités facultatives NFSv4.2.

À commencer par…	NFSv4.2 fonctionnalités facultatives comprennent …
ONTAP 9.12.1	• Attributs étendus NFS • Fichiers épars • Réservations d'espace
ONTAP 9.9.1	Contrôle d'accès obligatoire (MAC) nommé NFS

Étiquettes de sécurité NFS v4.2

Depuis ONTAP 9.9.1, les étiquettes de sécurité NFS peuvent être activées. Ils sont désactivés par défaut.

Avec les étiquettes de sécurité NFS v4.2, les serveurs NFS ONTAP prennent en charge le contrôle d'accès obligatoire (MAC), en stockant et en récupérant les attributs sec_label envoyés par les clients.

Pour plus d'informations, voir "RFC 7240".

Depuis la version ONTAP 9.12.1, les étiquettes de sécurité NFS v4.2 sont prises en charge pour les opérations de dump NDMP. Si des étiquettes de sécurité sont rencontrées sur des fichiers ou des répertoires dans des versions antérieures, le vidage échoue.

Étapes

1. Modifiez le paramètre de privilège sur avancé :

```
set -privilege advanced
```

2. Activer les étiquettes de sécurité :

```
vserver nfs modify -vserver <svm_name> -v4.2-seclabel enabled
```

Attributs étendus NFS

Depuis ONTAP 9.12.1, les attributs étendus NFS (xattrs) sont activés par défaut.

Les attributs étendus sont des attributs NFS standard définis par "RFC 8276" Et compatible avec les clients NFS modernes. Elles peuvent servir à associer des métadonnées définies par l'utilisateur à des objets de système de fichiers et présentent un intérêt dans des déploiements de sécurité avancés.

Les attributs étendus NFS ne sont actuellement pas pris en charge pour les opérations de dump NDMP. Si des attributs étendus sont rencontrés sur des fichiers ou des répertoires, le vidage procède mais ne sauvegarde pas les attributs étendus sur ces fichiers ou répertoires.

Si vous devez désactiver les attributs étendus, utilisez le `vserver nfs modify -v4.2-xattrs disabled` commande.

Découvrez nconnect pour optimiser les performances NFS

À partir d' ONTAP 9.8, la fonctionnalité nconnect est disponible par défaut lorsque NFSv4.1 est activé. nconnect améliore les performances du client NFS en autorisant plusieurs connexions TCP pour un même montage.

Comment fonctionne nconnect

Les implémentations de clients NFS antérieures n'utilisent qu'une connexion TCP unique avec un montage. En ONTAP, une connexion TCP unique peut former un goulot d'étranglement lorsque le nombre d'IOPS augmente.

Un client compatible avec nconnect peut avoir plusieurs connexions TCP (jusqu'à 16) associées à un seul montage NFS. nconnect utilise une seule adresse IP et établit plusieurs connexions TCP via cette adresse IP unique pour monter le partage NFS. Le client NFS répartit les opérations sur les fichiers sur plusieurs connexions TCP selon un principe de round-robin, obtenant ainsi un débit plus élevé à partir de la bande passante réseau disponible.

Versions NFS prises en charge

- nconnect est recommandé pour les montages NFSv3, NFSv4.2 et NFSv4.1.
- nconnect n'est *pas* recommandé pour les montages NFSv4.0.

> Pour des performances optimales, NetApp recommande d'utiliser NFSv4.1 avec nconnect au lieu de NFSv4.0. Alors que NFSv4.0 prend en charge plusieurs connexions, NFSv4.1 avec nconnect offre une meilleure répartition de la charge et un débit amélioré.

Assistance clientèle

Consultez la documentation de votre client NFS pour vérifier si nconnect est pris en charge dans la version de votre client.

Informations associées

- "En savoir plus sur la prise en charge ONTAP pour NFSv4.1"
- "En savoir plus sur la prise en charge ONTAP pour NFSv4.2"

En savoir plus sur la prise en charge ONTAP pour NFS parallèle

ONTAP prend en charge Parallel NFS (pNFS). Le protocole pNFS améliore les performances en offrant aux clients un accès direct aux données d'un ensemble de fichiers distribués sur plusieurs nœuds d'un cluster. Elle aide les clients à trouver le chemin optimal vers un volume.

En savoir plus sur les montages matériels ONTAP NFS

Lors du dépannage des problèmes de montage, veillez à utiliser le type de montage approprié. NFS prend en charge deux types de montage : les montages souples et les montages durs. Pour des raisons de fiabilité, n'utilisez que des supports durs.

Vous ne devez pas utiliser de montages souples, en particulier en cas de retards NFS fréquents. Ces délais peuvent entraîner la corruption des données.

Dépendances de nommage des fichiers et des répertoires NFS et SMB

En savoir plus sur les dépendances de nommage des fichiers et des répertoires ONTAP NFS et SMB

Les conventions d'appellation des fichiers et des répertoires dépendent à la fois des systèmes d'exploitation des clients réseau et des protocoles de partage de fichiers, en plus des paramètres de langue sur le cluster ONTAP et les clients.

Le système d'exploitation et les protocoles de partage de fichiers déterminent ce qui suit :

- Caractères un nom de fichier peut utiliser
- Sensibilité à la casse d'un nom de fichier

ONTAP prend en charge les caractères multi-octets dans les noms de fichier, de répertoire et de qtree, en fonction de la version de ONTAP utilisée.

Découvrez les caractères valides dans différents systèmes d'exploitation pour les SVM ONTAP NFS

Si vous accédez à un fichier ou à un répertoire à partir de clients ayant différents systèmes d'exploitation, vous devez utiliser des caractères valides dans les deux systèmes d'exploitation.

Par exemple, si vous utilisez UNIX pour créer un fichier ou un répertoire, n'utilisez pas de deux-points (:) dans le nom car le deux-points n'est pas autorisé dans les noms de fichiers ou de répertoires MS-DOS. Comme les restrictions sur les caractères valides varient d'un système d'exploitation à l'autre, consultez la documentation de votre système d'exploitation client pour plus d'informations sur les caractères interdits.

En savoir plus sur la sensibilité à la casse des noms de fichiers et de répertoires dans un environnement multiprotocole ONTAP NFS

Les noms de fichiers et de répertoires sont sensibles à la casse pour les clients NFS et non sensibles à la casse, mais ils préservent la casse pour les clients SMB. Vous devez comprendre les implications dans un environnement multiprotocole et les actions nécessaires lorsque vous spécifiez le chemin lors de la création des partages SMB et lors de l'accès aux données au sein des partages.

Si un client SMB crée un répertoire nommé `testdir`, Les clients SMB et NFS affichent le nom de fichier comme `testdir`. Toutefois, si un utilisateur SMB tente par la suite de créer un nom de répertoire `TESTDIR`, Le nom n'est pas autorisé car, pour le client SMB, ce nom existe actuellement. Si un utilisateur NFS crée par la suite un répertoire nommé `TESTDIR`, Les clients NFS et SMB affichent le nom du répertoire différemment, comme suit :

- Sur les clients NFS, vous voyez les deux noms de répertoire tels qu'ils ont été créés, par exemple

`testdir` et `TESTDIR`, car les noms de répertoire sont sensibles à la casse.

- Les clients SMB utilisent les 8.3 noms pour faire la distinction entre les deux répertoires. Un répertoire porte le nom du fichier de base. Un nom de fichier 8.3 est attribué aux répertoires supplémentaires.
  - Sur les clients SMB, vous voyez `testdir` et `TESTDI~1`.
  - ONTAP crée le `TESTDI~1` nom du répertoire pour différencier les deux répertoires.

    Dans ce cas, vous devez utiliser le nom 8.3 lorsque vous spécifiez un chemin de partage lors de la création ou de la modification d'un partage sur un SVM (Storage Virtual machine).

De la même manière pour les fichiers, si un client SMB crée `test.txt`, Les clients SMB et NFS affichent le nom de fichier comme `text.txt`. Toutefois, si un utilisateur SMB tente par la suite de le créer `Test.txt`, Le nom n'est pas autorisé car, pour le client SMB, ce nom existe actuellement. Si un utilisateur NFS crée par la suite un fichier nommé `Test.txt`, Les clients NFS et SMB affichent le nom de fichier différemment, comme suit :

- Sur les clients NFS, les deux noms de fichiers sont ceux qu'ils ont créés, `test.txt` et `Test.txt`, car les noms de fichiers sont sensibles à la casse.
- Les clients SMB utilisent les 8.3 noms pour distinguer les deux fichiers. Un fichier porte le nom du fichier de base. Un nom de fichier 8.3 est attribué aux fichiers supplémentaires.
  - Sur les clients SMB, vous voyez `test.txt` et `TEST~1.TXT`.
  - ONTAP crée le `TEST~1.TXT` nom de fichier pour différencier les deux fichiers.

> Si un mappage de caractères a été créé à l'aide des commandes de mappage de caractères CIFS du Vserver, une recherche Windows qui ne serait normalement pas sensible à la casse peut être sensible à la casse. Cela signifie que les recherches de nom de fichier ne seront sensibles à la casse que si le mappage de caractères a été créé et que le nom de fichier utilise ce mappage de caractères.

En savoir plus sur la création de noms de fichiers et de répertoires ONTAP NFS

ONTAP crée et conserve deux noms pour les fichiers ou les répertoires de tout répertoire ayant accès à partir d'un client SMB : le nom long et le nom d'origine au format 8.3.

Pour les noms de fichier ou de répertoire dépassant le nom de huit caractères ou la limite d'extension de trois caractères (pour les fichiers), ONTAP génère un nom de format 8.3 comme suit :

- Il tronque le nom de fichier ou de répertoire d'origine à six caractères, si le nom dépasse six caractères.
- Il ajoute un tilde (~) et un nombre, un à cinq, aux noms de fichier ou de répertoire qui ne sont plus uniques après être tronqués.

  S'il manque des nombres parce qu'il y a plus de cinq noms similaires, il crée un nom unique qui n'a aucune relation avec le nom original.

- Dans le cas des fichiers, il tronque l'extension du nom de fichier à trois caractères.

Par exemple, si un client NFS crée un fichier nommé `specifications.html`, Le nom de fichier au format 8.3 créé par ONTAP est `specif~1.htm`. Si ce nom existe déjà, ONTAP utilise un numéro différent à la fin du nom du fichier. Par exemple, si un client NFS crée un autre fichier nommé `specifications_new.html`, le format 8.3 de `specifications_new.html` est `specif~2.htm`.

En savoir plus sur la gestion ONTAP NFS des noms de fichiers, de répertoires et de qtree multi-octets

À partir de ONTAP 9.5, la prise en charge des noms codés UTF-8 de 4 octets permet la création et l'affichage des noms de fichier, de répertoire et d'arborescence qui incluent des caractères supplémentaires Unicode à l'extérieur du plan multilingue de base (BMP). Dans les versions précédentes, ces caractères supplémentaires ne s'affichent pas correctement dans les environnements multiprotocoles.

Pour activer la prise en charge des noms codés UTF-8 à 4 octets, un nouveau code de langue *utf8mb4* est disponible pour l' `vserver` et `volume` familles de commandement.

- Vous devez créer un volume de l'une des manières suivantes :
- Réglage du volume `-language` explicitement option :

  ```
  volume create -language utf8mb4 {…}
  ```

- Hériter du volume `-language` Option d'un SVM qui a été créé avec ou modifié pour l'option :

  ```
  vserver [create|modify] -language utf8mb4 {…}``volume create {…}
  ```

- Si vous utilisez ONTAP 9.6 et des versions antérieures, vous ne pouvez pas modifier les volumes existants pour le support utf8mb4 ; vous devez créer un nouveau volume prêt à utf8mb4, puis migrer les données à l'aide d'outils de copie basés sur le client.

  Si vous utilisez ONTAP 9.7P1 ou une version ultérieure, vous pouvez modifier les volumes existants pour utf8mb4 avec une demande de support. Pour plus d'informations, voir "Est-il possible de modifier la langue du volume après sa création dans ONTAP ?".

  Vous pouvez mettre à jour les SVM pour la prise en charge de utf8mb4, mais les volumes existants conservent leurs codes de langue d'origine.

  > Les noms de LUN portant des caractères UTF-8 de 4 octets ne sont pas pris en charge actuellement.

- Les données de caractères Unicode sont généralement représentées dans les applications de systèmes de fichiers Windows utilisant le format de transformation Unicode 16 bits (UTF-16) et dans les systèmes de fichiers NFS utilisant le format de transformation Unicode 8 bits (UTF-8).

  Dans les versions antérieures à ONTAP 9.5, les noms, y compris les caractères supplémentaires UTF-16 créés par les clients Windows, étaient correctement affichés sur d'autres clients Windows mais n'étaient pas traduits correctement en UTF-8 pour les clients NFS. De même, les noms comportant des caractères supplémentaires UTF-8 par les clients NFS créés n'ont pas été correctement traduits en UTF-16 pour les clients Windows.

- Lorsque vous créez des noms de fichier sur des systèmes exécutant ONTAP 9.4 ou une version antérieure contenant des caractères supplémentaires valides ou non valides, ONTAP rejette le nom de fichier et renvoie une erreur de nom de fichier non valide.

  Pour éviter ce problème, utilisez uniquement des caractères BMP dans les noms de fichiers et évitez d'utiliser des caractères supplémentaires, ou mettez à niveau vers ONTAP 9.5 ou version ultérieure.

Les caractères Unicode sont autorisés dans les noms de qtree.

- Vous pouvez utiliser le `volume qtree` Famille de commandes ou System Manager pour définir ou modifier les noms des qtree.
- Les noms des qtrees peuvent inclure des caractères multi-octets au format Unicode, comme les caractères japonais et chinois.
- Dans les versions antérieures à ONTAP 9.5, seuls les caractères BMP (c'est-à-dire ceux qui pouvaient être représentés en 3 octets) étaient pris en charge.

> Dans les versions antérieures à ONTAP 9.5, le Junction-path du volume parent du qtree peut contenir des noms de qtree et de répertoire avec des caractères Unicode. Le `volume show` La commande affiche ces noms correctement lorsque le volume parent a un paramètre de langue UTF-8. Cependant, si la langue du volume parent n'est pas l'un des paramètres de langue UTF-8, certaines parties du chemin de jonction sont affichées à l'aide d'un nom de remplacement NFS numérique.

- Dans les versions 9.5 et ultérieures, les noms des qtree prennent en charge des caractères de 4 octets, à condition que le qtree se trouve dans un volume activé pour utf8m4.

Configurer le mappage de caractères pour la traduction des noms de fichiers SMB sur les volumes ONTAP NFS

Les clients NFS peuvent créer des noms de fichiers contenant des caractères non valides pour les clients SMB et certaines applications Windows. Vous pouvez configurer le mappage de caractères pour la conversion de noms de fichiers sur des volumes pour permettre aux clients SMB d'accéder aux fichiers avec des noms NFS qui ne seraient autrement pas valides.

Description de la tâche

Lorsque les fichiers créés par des clients NFS sont accessibles par des clients SMB, ONTAP recherche le nom du fichier. Si le nom n'est pas un nom de fichier SMB valide (par exemple, s'il comporte un caractère «`:`") inclus, ONTAP renvoie le nom de fichier 8.3 qui est conservé pour chaque fichier. Cependant, cela cause des problèmes pour les applications qui codent des informations importantes dans des noms de fichiers longs.

Par conséquent, si vous partagez un fichier entre des clients sur des systèmes d'exploitation différents, vous devez utiliser des caractères dans les noms de fichiers valides dans les deux systèmes d'exploitation.

Cependant, si vous avez des clients NFS qui créent des noms de fichier contenant des caractères qui ne sont pas des noms de fichier valides pour les clients SMB, vous pouvez définir une carte qui convertit les caractères NFS non valides en caractères Unicode acceptés par SMB et certaines applications Windows. Par exemple, cette fonctionnalité prend en charge les applications CATIA MCAD et Mathematica, ainsi que d'autres applications qui ont cette exigence.

Vous pouvez configurer le mappage de caractères sur une base volume par volume.

Lors de la configuration du mappage de caractères sur un volume, vous devez garder à l'esprit les éléments suivants :

- Le mappage de caractères n'est pas appliqué à travers les points de jonction.

  Vous devez configurer explicitement le mappage de caractères pour chaque volume de jonction.

- Vous devez vous assurer que les caractères Unicode utilisés pour représenter des caractères non valides ou illégaux sont des caractères qui n'apparaissent normalement pas dans les noms de fichiers ; sinon, des mappages indésirables se produisent.

  Par exemple, si vous essayez de mapper un deux-points (:) à un tiret (-) mais que le tiret (-) a été utilisé correctement dans le nom de fichier, un client Windows essayant d'accéder à un fichier nommé ""a-b" aurait sa demande mappée au nom NFS de ""a:b" (pas le résultat souhaité).

- Après l'application du mappage de caractères, si le mappage contient toujours un caractère Windows non valide, ONTAP revient aux noms de fichier Windows 8.3.
- Dans les notifications FPolicy, les journaux d'audit NAS et les messages de suivi de sécurité, les noms de fichiers mappés sont affichés.
- Lors de la création d'une relation SnapMirror de type DP, le mappage de caractères du volume source n'est pas répliqué sur le volume DP de destination.
- Sensibilité à la casse : comme les noms Windows mappés se transforment en noms NFS, la recherche des noms suit la sémantique NFS. Ainsi, les recherches NFS sont sensibles à la casse. Cela signifie que les applications qui accèdent aux partages mappés ne doivent pas se fier au comportement non sensible à la casse de Windows. Cependant, le nom 8.3 est disponible, et cela n'est pas sensible à la casse.
- Mappages partiels ou non valides : après le mappage d'un nom pour revenir aux clients faisant une énumération de répertoire (« dir »), le nom Unicode obtenu est vérifié pour la validité de Windows. Si ce nom contient toujours des caractères non valides ou s'il n'est pas valide pour Windows (par exemple, il se termine par "." ou vierge), le nom 8.3 est renvoyé à la place du nom non valide.

Étape

1. Configurer le mappage de caractères :

   ```
   vserver cifs character-mapping create -vserver vserver_name -volume
   volume_name -mapping mapping_text, ...
   ```

   Le mappage se compose d'une liste de paires de caractères source-cible séparées par «»:». Les caractères sont des caractères Unicode saisis à l'aide de chiffres hexadécimaux. Par exemple : 3C:E03C.

   La première valeur de chaque `mapping_text` La paire séparée par deux-points est la valeur hexadécimale du caractère NFS que vous souhaitez traduire, et la seconde est la valeur Unicode utilisée par SMB. Les paires de mappage doivent être uniques (un mappage un-à-un doit exister).

   - Mappage de source

     Le tableau suivant montre le jeu de caractères Unicode autorisé pour le mappage de source :

Caractère Unicode	Caractère imprimé	Description
0x01-0x19	Sans objet	Caractères de contrôle sans impression
0x5C	\	Barre oblique inversée
0x3A	:	Deux-points
0x2A	*	Astérisque

0x3F	?	Point d'interrogation
0x22	«	Devis
0x3C	<	Inférieur à
0x3E	>	Supérieur à
0x7C		
Ligne verticale	0xb1	±

◦ Mappage de cible

Vous pouvez spécifier des caractères cibles dans la « zone d'utilisation privée » d'Unicode dans la plage suivante : U+E0000…U+F8FF.

Exemple

La commande suivante crée un mappage de caractères pour un volume nommé « `dates' » sur la machine virtuelle de stockage (SVM) vs1 :

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show

Vserver         Volume Name  Character Mapping
--------------  -----------  -----------------------------------------
vs1             data         3c:e17c, 3e:f17d, 2a:f745
```

Commandes ONTAP NFS pour la gestion des mappages de caractères pour la traduction des noms de fichiers SMB

Vous pouvez gérer le mappage de caractères en créant, en modifiant, en affichant des informations sur et en supprimant des mappages de caractères de fichiers utilisés pour la conversion de noms de fichiers SMB sur des volumes FlexVol.

Les fonctions que vous recherchez…	Utilisez cette commande…
Créer de nouveaux mappages de caractères de fichier	`vserver cifs character-mapping create`
Affiche des informations sur les mappages de caractères de fichier	`vserver cifs character-mapping show`

Modifier les mappages de caractères de fichier existants	`vserver cifs character-mapping modify`
Supprimer les mappages de caractères de fichier	`vserver cifs character-mapping delete`

Pour en savoir plus, `vserver cifs character-mapping` consultez le "Référence de commande ONTAP".

Informations sur le copyright

Informations sur les marques commerciales