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

ONTAP 9

NetApp
April 24, 2024

Sommaire

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

Activer ou désactiver NFSv3

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`

Activez ou désactivez NFSv4.0

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

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`

Gestion des limites des pools de stockage 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

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

Ce dont vous avez besoin

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

Contrôle de l'accès NFS sur TCP et UDP

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`

Contrôlez les demandes NFS à partir de ports non réservés

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 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.

Ce dont vous avez besoin

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 relatives aux clients qui montent des exportations NFS à l'aide d'un port non réservé

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.

Effectuer des contrôles d’accès plus stricts pour les groupes réseau en vérifiant les domaines

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

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.

Ce dont vous avez besoin

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.
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 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

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

Résoudre les problèmes de service de noms

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)"

Vérifiez le nom des connexions de service

Depuis ONTAP 9.2, vous pouvez vérifier les serveurs de noms DNS et LDAP pour vous assurer 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 permettant de gérer les entrées des commutateurs de service de noms

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`

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

Informations associées

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

Commandes permettant de gérer le cache du service de noms

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

"Commandes de ONTAP 9"

Commandes permettant de gérer les mappages de noms

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

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

Échangez la position de deux mappages de noms REMARQUE : un échange n'est pas autorisé lorsque le mappage de 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`

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

Commandes permettant de gérer les utilisateurs UNIX locaux

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`

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

Commandes permettant de gérer les groupes UNIX locaux

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`

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

Limites pour les utilisateurs, groupes et membres UNIX locaux

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

Gérez les limites des utilisateurs et groupes UNIX locaux

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`

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

Commandes de gestion des groupes réseau locaux

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`

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

Commandes pour la gestion des configurations de domaine 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.

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

Commandes permettant de gérer les configurations du client 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`

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

Commandes pour la gestion des configurations LDAP

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`

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

Commandes de gestion des modèles de schéma client LDAP

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.

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

Commandes permettant de gérer les configurations de l'interface Kerberos NFS

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`

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

Commandes de 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`

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

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

Commandes permettant de gérer les export-policies

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`

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

Commandes permettant de gérer les 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.

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

Configurez le cache des informations d’identification NFS

Raisons de la modification du temps de mise en cache des identifiants NFS

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.
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.

Configurez le délai de mise en service pour les informations d'identification de l'utilisateur NFS en cache

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 des règles d’exportation

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`

Affiche la file d'attente et le cache de groupe réseau de la politique d'export

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`

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

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

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
```

Optimisez les performances du cache d'accès

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

A propos du verrouillage de fichier entre les protocoles

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

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

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

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

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

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

Comment ONTAP traite les bits en lecture seule

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

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

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

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

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

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

La différence entre ONTAP et Windows en ce qui concerne la gestion des verrous sur les composants de chemin de partage

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

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

Pour éviter les problèmes causés par 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".

Affiche des informations sur les verrous

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

Description de la tâche

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

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

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

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

En spécifiant des paramètres facultatifs, vous pouvez déterminer des informations importantes sur chaque type de verrou. Consultez la page man pour la commande pour plus d'informations.

Étape

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

Exemples

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

```
cluster1::> vserver locks show

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

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

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

                   Vserver: vs1
                    Volume: data2_2
        Logical Interface: lif2
              Object Path: /data2/data2_2/intro.pptx
                Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
            Lock Protocol: cifs
                Lock Type: share-level
   Node Holding Lock State: node3
               Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: durable
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                   Vserver: vs1
                    Volume: data2_2
        Logical Interface: lif2
              Object Path: /data2/data2_2/test.pptx
                Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
            Lock Protocol: cifs
                Lock Type: op-lock
   Node Holding Lock State: node3
               Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
```

```
        Shared Lock is Soft: -
            Delegation Type: -
             Client Address: 10.3.1.3
              SMB Open Type: -
          SMB Connect State: connected
SMB Expiration Time (Secs): -
          SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

Serrures de sécurité

Lorsque des verrous de fichier empêchent l'accès client aux fichiers, vous pouvez afficher des informations sur les verrous actuellement mis en attente, puis interrompre des verrous spécifiques. Les applications de débogage sont des exemples de scénarios dans lesquels vous devrez peut-être interrompre les verrous.

Description de la tâche

Le `vserver locks break` la commande n'est disponible que au niveau de privilège avancé et supérieur. La page man de la commande contient des informations détaillées.

Étapes

1. Pour trouver les informations dont vous avez besoin pour interrompre un verrouillage, utilisez le `vserver locks show` commande.

   La page man de la commande contient des informations détaillées.

2. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

3. Effectuez l'une des opérations suivantes :

Si vous voulez rompre un verrou en spécifiant…	Entrez la commande…
Le nom du SVM, le nom du volume, le nom de la LIF et le chemin de fichier	`vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif`
L'ID de verrouillage	`vserver locks break -lockid UUID`

4. Retour au niveau de privilège admin :

   ```
   set -privilege admin
   ```

Fonctionnement des filtres FPolicy de première lecture et de première écriture 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

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

Avantages des listes de contrôle d'accès NFSv4

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

Fonctionnement des listes de contrôle d'accès NFSv4

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 comportant une liste de contrôle d'accès, le nouveau fichier ou sous-répertoire hérite de toutes les entrées ACL (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` le paramètre a été défini sur `restricted` à l'aide des commandes dans `vserver nfs` ou `vserver export-policy rule` Familles, la propriété des fichiers ne peut être modifiée que par le superutilisateur, même si les autorisations sur disque définies avec les ACL NFSv4 permettent à un utilisateur non-root de modifier la propriété des fichiers. Pour plus d'informations, consultez les pages de manuel correspondantes.

Activer ou désactiver la modification des listes de contrôle d'accès NFSv4

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
   ```

Comment ONTAP utilise les listes de contrôle d'accès NFSv4 pour déterminer si elles peuvent supprimer un fichier

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 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 listes de contrôle d'accès NFSv4

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 des fichiers de lecture NFSv4

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 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`
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

À propos du verrouillage des fichiers et des enregistrements NFSv4

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 du verrouillage NFSv4

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 du verrouillage NFSv4

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
```

Fonctionnement des référencements NFSv4

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.

Activez ou désactivez les référencements NFSv4

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.

Ce dont vous avez besoin

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
   ```

Affiche les statistiques 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"

Affiche les statistiques DNS

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"

Affiche les statistiques NIS

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"

Prise en charge de VMware vStorage over 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 ?"

Activation ou désactivation de VMware vStorage sur 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

ONTAP supporte le protocole de quota distant version 1 (rquota v1). Le protocole rquota permet aux clients NFS d'obtenir des informations de quotas pour les utilisateurs à partir d'une machine distante. Vous pouvez activer rquota sur des machines virtuelles de stockage (SVM) à l'aide du `vserver nfs modify` commande.

Description de la tâche

Par défaut, rquota est désactivé.

Étape

1. Effectuez l'une des opérations suivantes :

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".

Amélioration des performances de NFSv3 et NFSv4 en modifiant la taille du transfert TCP

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 maximale du transfert TCP NFSv3 et NFSv4

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
```

Configurez le nombre d'ID de groupe autorisé pour les utilisateurs NFS

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.

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
```

Contrôler l'accès utilisateur root aux données de style de sécurité NTFS

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
```