Ajout de capacité de stockage à un SVM compatible NFS

ONTAP 9

NetApp
April 24, 2024

Sommaire

Ajout de capacité de stockage à un SVM compatible NFS

Ajoutez de la capacité de stockage à une présentation de SVM compatible NFS

Pour ajouter de la capacité de stockage à un SVM compatible NFS, vous devez créer un volume ou qtree pour fournir un conteneur de stockage, et créer ou modifier une export policy pour ce conteneur. Vous pouvez ensuite vérifier l'accès client NFS depuis le cluster et tester l'accès depuis les systèmes client.

Ce dont vous avez besoin

- NFS doit être entièrement configuré sur le SVM.
- La export policy default du volume root du SVM doit contenir une règle qui permet d'accéder à tous les clients.
- Toute mise à jour de la configuration des services de noms doit être terminée.
- Tout ajout ou modification d'une configuration Kerberos doit être effectué.

Créer une export-policy

Avant de créer des règles d'exportation, vous devez créer une export-policy pour les tenir. Vous pouvez utiliser le `vserver export-policy create` commande pour créer une export policy.

Étapes

1. Créer une export-policy :

   ```
   vserver export-policy create -vserver vserver_name -policyname policy_name
   ```

   Le nom de la stratégie peut comporter jusqu'à 256 caractères.

2. Vérifier que l'export policy a été créée :

   ```
   vserver export-policy show -policyname policy_name
   ```

Exemple

Les commandes suivantes créent et vérifient la création d'une export policy nommée exp1 sur le SVM nommé vs1:

```
vs1::> vserver export-policy create -vserver vs1 -policyname exp1

vs1::> vserver export-policy show -policyname exp1
Vserver          Policy Name
---------------  -------------------
vs1              exp1
```

Ajouter une règle à une export-policy

Sans règles, l'export policy ne peut pas fournir aux clients l'accès aux données. Pour créer une nouvelle règle d'exportation, vous devez identifier les clients et sélectionner un format de correspondance client, sélectionner les types d'accès et de sécurité, spécifier un mappage d'ID utilisateur anonyme, sélectionner un numéro d'index de règle et sélectionner le protocole d'accès. Vous pouvez ensuite utiliser le `vserver export-policy rule create` commande pour ajouter la nouvelle règle à une export-policy.

Ce dont vous avez besoin

- L'export policy à laquelle vous souhaitez ajouter les règles d'exportation doit déjà exister.
- Le DNS doit être correctement configuré sur le SVM de données et les serveurs DNS doivent avoir des entrées correctes pour les clients NFS.

  En effet, ONTAP effectue des recherches DNS en utilisant la configuration DNS du SVM de données pour certains formats de correspondance client, et les échecs de mise en correspondance de règles d'export peuvent empêcher l'accès aux données client.

- Si vous authentifiez avec Kerberos, vous devez avoir déterminé les méthodes de sécurité suivantes utilisées sur vos clients NFS :
  - `krb5` (Protocole Kerberos V5)
  - `krb5i` (Protocole Kerberos V5 avec contrôle d'intégrité à l'aide de checksums)
  - `krb5p` (Protocole Kerberos V5 avec service de confidentialité)

Description de la tâche

Il n'est pas nécessaire de créer une nouvelle règle si une règle existante d'une stratégie d'exportation couvre la correspondance de vos clients et les exigences d'accès.

Si vous authentifiez avec Kerberos et si tous les volumes du SVM sont accessibles via Kerberos, vous pouvez définir les options des règles d'exportation `-rorule`, `-rwrule`, et `-superuser` pour le volume racine à `krb5`, `krb5i`, ou `krb5p`.

Étapes

1. Identifiez les clients et le format de correspondance client pour la nouvelle règle.

   Le `-clientmatch` spécifie les clients auxquels la règle s'applique. Des valeurs de correspondance client uniques ou multiples peuvent être spécifiées ; les spécifications de valeurs multiples doivent être séparées par des virgules. Vous pouvez spécifier la correspondance dans l'un des formats suivants :

Format de correspondance client	Exemple
Nom de domaine précédé du caractère "."	`.example.com` ou `.example.com,.example.net,...`
Nom d'hôte	`host1` ou `host1,host2, ...`
Adresse IPv4	`10.1.12.24` ou `10.1.12.24,10.1.12.25, ...`
Adresse IPv4 avec un masque de sous-réseau exprimé en nombre de bits	`10.1.12.10/4` ou `10.1.12.10/4,10.1.12.11/4,...`
Adresse IPv4 avec un masque de réseau	`10.1.16.0/255.255.255.0` ou `10.1.16.0/255.255.255.0,10.1.17.0/255.255.255.0,...`
Adresse IPv6 en format pointillé	`::1.2.3.4` ou `::1.2.3.4,::1.2.3.5,...`
Adresse IPv6 avec un masque de sous-réseau exprimé en nombre de bits	`ff::00/32` ou `ff::00/32,ff::01/32,...`
Un seul groupe de réseau avec le nom de groupe de réseau précédé du caractère @	`@netgroup1` ou `@netgroup1,@netgroup2,...`

Vous pouvez également combiner des types de définitions de client, par exemple, `.example.com,@netgroup1`.

Lors de la définition des adresses IP, notez les éléments suivants :

- La saisie d'une plage d'adresses IP, par exemple 10.1.12.10-10.1.12.70, n'est pas autorisée.

  Les entrées de ce format sont interprétées comme une chaîne de texte et sont traitées comme un nom d'hôte.

- Lors de la spécification d'adresses IP individuelles dans des règles d'exportation pour la gestion granulaire de l'accès client, ne spécifiez pas d'adresses IP dynamiquement (par exemple, DHCP) ou temporairement (par exemple, IPv6) attribuées.

  Sinon, le client perd l'accès lorsque son adresse IP change.

- La saisie d'une adresse IPv6 avec un masque de réseau, par exemple ff::12/ff::00, n'est pas autorisée.

2. Sélectionnez les types d'accès et de sécurité pour les correspondances client.

   Vous pouvez spécifier un ou plusieurs des modes d'accès suivants aux clients qui s'authentifient avec les types de sécurité spécifiés :

   - `-rorule` (accès en lecture seule)
   - `-rwrule` (accès en lecture/écriture)

- `-superuser` (accès racine)

> Un client peut uniquement obtenir un accès en lecture/écriture pour un type de sécurité spécifique si la règle d'exportation autorise également un accès en lecture seule pour ce type de sécurité. Si le paramètre lecture seule est plus restrictif pour un type de sécurité que le paramètre lecture-écriture, il se peut que le client n'ait pas accès en lecture-écriture. Il en va de même pour l'accès superutilisateur.

Vous pouvez spécifier une liste de plusieurs types de sécurité séparés par des virgules pour une règle. Si vous spécifiez le type de sécurité comme `any` ou `never`, ne spécifiez aucun autre type de sécurité. Choisissez parmi les types de sécurité valides suivants :

Lorsque le type de sécurité est défini sur…	Un client correspondant peut accéder aux données exportées…
`any`	Toujours, quel que soit le type de sécurité entrant.
`none`	S'ils sont répertoriés seuls, l'accès des clients possédant n'importe quel type de sécurité est accordé en tant qu'anonyme. Si elle est répertoriée avec d'autres types de sécurité, les clients avec un type de sécurité spécifié bénéficient d'un accès et les clients avec un autre type de sécurité bénéficient d'un accès anonyme.
`never`	Jamais, quel que soit le type de sécurité entrant.
`krb5`	S'il est authentifié par Kerberos 5. Authentification uniquement : l'en-tête de chaque requête et réponse est signé.
`krb5i`	S'il est authentifié par Kerberos 5i. Authentification et intégrité : l'en-tête et le corps de chaque requête et réponse sont signés.
`krb5p`	S'il est authentifié par Kerberos 5p. Authentification, intégrité et confidentialité : l'en-tête et le corps de chaque requête et réponse sont signés, et la charge utile des données NFS est chiffrée.
`ntlm`	S'il est authentifié par CIFS NTLM.
`sys`	S'il est authentifié par NFS AUTH_SYS.

Le type de sécurité recommandé est `sys`, Ou si Kerberos est utilisé, `krb5`, `krb5i`, ou `krb5p`.

Si vous utilisez Kerberos avec NFSv3, la règle de export policy doit autoriser `-rorule` et `-rwrule` accès à `sys` en plus de `krb5`. Ceci est dû au besoin d'autoriser l'accès à Network Lock Manager (NLM) pour

l'exportation.

3. Spécifiez un mappage d'ID utilisateur anonyme.

   Le `-anon` Option spécifie un ID utilisateur ou un nom d'utilisateur UNIX qui est mappé aux demandes client qui arrivent avec un ID utilisateur de 0 (zéro), généralement associé à la racine du nom d'utilisateur. La valeur par défaut est `65534`. Les clients NFS associent généralement l'ID utilisateur 65534 au nom d'utilisateur personne (également appelé *root scaling*). Dans ONTAP, cet ID utilisateur est associé à l'utilisateur pcuser. Pour désactiver l'accès par tout client ayant un ID utilisateur de 0, spécifiez une valeur de `65535`.

4. Sélectionnez l'ordre d'index des règles.

   Le `-ruleindex` option spécifie le numéro d'index de la règle. Les règles sont évaluées en fonction de leur ordre dans la liste des numéros d'index ; les règles avec des numéros d'index inférieurs sont évaluées en premier. Par exemple, la règle avec l'index numéro 1 est évaluée avant la règle avec l'index numéro 2.

Si vous ajoutez…	**Alors…**
La première règle vers une export-policy	Entrez `1`.
Règles supplémentaires à une export-policy	a. Afficher les règles existantes dans la stratégie : `vserver export-policy rule show -instance -policyname` *`your_policy`* b. Sélectionnez un numéro d'index pour la nouvelle règle en fonction de l'ordre dans lequel elle doit être évaluée.

5. Sélectionnez la valeur d'accès NFS applicable : {`nfs`|`nfs3`|`nfs4`}.

   `nfs` correspond à n'importe quelle version, `nfs3` et `nfs4` correspondent uniquement à ces versions spécifiques.

6. Créer la règle d'exportation et l'ajouter à une export policy existante :

   `vserver export-policy rule create -vserver` *`vserver_name`* `-policyname` *`policy_name`* `-ruleindex` *`integer`* `-protocol {nfs|nfs3|nfs4} -clientmatch { text |` *`"text,text,…"`* `} -rorule` *`security_type`* `-rwrule` *`security_type`* `-superuser` *`security_type`* `-anon` *`user_ID`*

7. Afficher les règles pour l'export policy pour vérifier que la nouvelle règle est présente :

   `vserver export-policy rule show -policyname` *`policy_name`*

   La commande affiche un récapitulatif de cette export policy, y compris une liste des règles appliquées à cette policy. ONTAP attribue à chaque règle un numéro d'index de règle. Après avoir connu le numéro d'index de la règle, vous pouvez l'utiliser pour afficher des informations détaillées sur la règle d'exportation spécifiée.

8. Vérifiez que les règles appliquées à l'export policy sont configurées correctement :

   `vserver export-policy rule show -policyname` *`policy_name`* `-vserver` *`vserver_name`*

```
-ruleindex integer
```

Exemples

Les commandes suivantes créent et vérifient la création d'une règle d'exportation sur le SVM nommé vs1 dans une export policy nommée rs1. La règle a l'index numéro 1. La règle correspond à n'importe quel client du domaine eng.company.com et au groupe réseau @netgroup1. La règle active tous les accès NFS. Il active l'accès en lecture seule et en lecture-écriture aux utilisateurs authentifiés avec AUTH_SYS. Les clients possédant l'ID utilisateur UNIX 0 (zéro) sont anonymisés sauf s'ils sont authentifiés avec Kerberos.

```
vs1::> vserver export-policy rule create -vserver vs1 -policyname exp1
-ruleindex 1 -protocol nfs
-clientmatch .eng.company.com,@netgoup1 -rorule sys -rwrule sys -anon
65534 -superuser krb5

vs1::> vserver export-policy rule show -policyname nfs_policy
Virtual      Policy         Rule    Access    Client           RO
Server       Name           Index   Protocol  Match            Rule
------------ -------------- ------  --------  ---------------- ------
vs1          exp1           1       nfs       eng.company.com, sys
                                              @netgroup1

vs1::> vserver export-policy rule show -policyname exp1 -vserver vs1
-ruleindex 1

                                   Vserver: vs1
                               Policy Name: exp1
                                Rule Index: 1
                            Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
eng.company.com,@netgroup1
                             RO Access Rule: sys
                             RW Access Rule: sys
User ID To Which Anonymous Users Are Mapped: 65534
                    Superuser Security Types: krb5
                Honor SetUID Bits in SETATTR: true
                   Allow Creation of Devices: true
```

Les commandes suivantes créent et vérifient la création d'une règle d'export sur le SVM nommé vs2 dans une export policy nommée expol2. La règle a le numéro d'index 21. La règle correspond aux clients aux membres du groupe réseau dev_netgroup_main. La règle active tous les accès NFS. Il active un accès en lecture seule pour les utilisateurs authentifiés avec AUTH_SYS et nécessite une authentification Kerberos pour l'accès en lecture-écriture et racine. Les clients possédant l'ID utilisateur UNIX 0 (zéro) se voient refuser l'accès racine sauf s'ils sont authentifiés avec Kerberos.

```
vs2::> vserver export-policy rule create -vserver vs2 -policyname expol2
-ruleindex 21 -protocol nfs
-clientmatch @dev_netgroup_main -rorule sys -rwrule krb5 -anon 65535
-superuser krb5

vs2::> vserver export-policy rule show -policyname nfs_policy
Virtual  Policy       Rule    Access    Client              RO
Server   Name         Index   Protocol  Match               Rule
-------- ------------ ------  --------  ------------------  ------
vs2      expol2       21       nfs      @dev_netgroup_main  sys

vs2::> vserver export-policy rule show -policyname expol2 -vserver vs1
-ruleindex 21

                                   Vserver: vs2
                               Policy Name: expol2
                                Rule Index: 21
                           Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
                                            @dev_netgroup_main
                            RO Access Rule: sys
                            RW Access Rule: krb5
User ID To Which Anonymous Users Are Mapped: 65535
                   Superuser Security Types: krb5
               Honor SetUID Bits in SETATTR: true
                  Allow Creation of Devices: true
```

Créer un volume ou un conteneur de stockage qtree

Créer un volume

Vous pouvez créer un volume et spécifier son point de jonction et d'autres propriétés en utilisant le `volume create` commande.

Description de la tâche

Un volume doit inclure une *Junction path* pour que ses données soient mises à disposition des clients. Vous pouvez spécifier le chemin de jonction lorsque vous créez un nouveau volume. Si vous créez un volume sans spécifier un chemin de jonction, vous devez *mount* le volume du namespace du SVM à l'aide de `volume mount` commande.

Avant de commencer

- NFS doit être configuré et exécuté.
- La sécurité du SVM doit être de style UNIX.
- À partir de ONTAP 9.13.1, vous pouvez créer des volumes dont l'analyse de la capacité et le suivi des activités sont activés. Pour activer le suivi de la capacité ou des activités, exécutez le `volume create`

commande avec `-analytics-state` ou `-activity-tracking-state` réglez sur `on`.

Pour en savoir plus sur l'analyse de la capacité et le suivi des activités, reportez-vous à la section Activez l'analyse du système de fichiers.

Étapes

1. Créer le volume avec un point de jonction :

   ```
   volume create -vserver svm_name -volume volume_name -aggregate aggregate_name
   -size {integer[KB|MB|GB|TB|PB]} -security-style unix -user user_name_or_number
   -group group_name_or_number -junction-path junction_path [-policy
   export_policy_name]
   ```

   Les choix pour `-junction-path` sont les suivants :

   - Directement sous la racine, par exemple, `/new_vol`

     Vous pouvez créer un nouveau volume et préciser qu'il peut être monté directement sur le volume root du SVM.

   - Sous un répertoire existant, par exemple, `/existing_dir/new_vol`

     Vous pouvez créer un nouveau volume et spécifier qu'il doit être monté sur un volume existant (dans une hiérarchie existante), exprimé en tant que répertoire.

     Si vous souhaitez créer un volume dans un nouveau répertoire (dans une nouvelle hiérarchie sous un nouveau volume), par exemple, `/new_dir/new_vol`, Ensuite, vous devez d'abord créer un nouveau volume parent qui est relié par une jonction au volume racine de la SVM. Vous devez ensuite créer le nouveau volume enfant dans la Junction path du nouveau volume parent (nouveau répertoire).

     Si vous prévoyez d'utiliser une export policy existante, vous pouvez la spécifier lors de la création du volume. Vous pouvez également ajouter une export-policy plus tard avec le `volume modify` commande.

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

   ```
   volume show -vserver svm_name -volume volume_name -junction
   ```

Exemples

La commande suivante crée un nouveau volume nommé users1 sur le SVM vs1.example.com et l'agrégat aggr1. Le nouveau volume est disponible sur le site `/users`. Le volume a une taille de 750 Go et sa garantie de volume est de type volume (par défaut).

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction
                          Junction                 Junction
Vserver           Volume  Active   Junction Path   Path Source
----------------- ------- -------- --------------- -----------
vs1.example.com   users1  true     /users          RW_volume
```

La commande suivante crée un nouveau volume nommé « home4 » sur le SVM « vs1.example.com » et l'agrégat « aggr1 ». Le répertoire `/eng/` Existe déjà dans l'espace de nommage de la SVM vs1, et le nouveau volume est mis à disposition à `/eng/home`, qui devient le répertoire de base de l' `/eng/` espace de noms. Le volume a une taille de 750 Go et sa garantie de volume est de type `volume` (par défaut).

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

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

Créer un qtree

Vous pouvez créer un qtree pour contenir vos données et spécifier ses propriétés en utilisant le `volume qtree create` commande.

Ce dont vous avez besoin

- La SVM et le volume qui contiendra le nouveau qtree doivent déjà exister.
- La méthode de sécurité SVM doit être UNIX et NFS doit être configuré et en cours d'exécution.

Étapes

1. Créer le qtree :

   `volume qtree create -vserver` *`vserver_name`* `{ -volume` *`volume_name`* `-qtree` *`qtree_name`* `| -qtree-path` *`qtree path`* `} -security-style unix [-policy` *`export_policy_name`*`]`

   Vous pouvez spécifier le volume et qtree en tant qu'arguments distincts ou spécifier l'argument du chemin qtree au format `/vol/`*`volume_name/_qtree_name`*.

   Par défaut, les qtrees héritent des règles d'exportation du volume parent, mais ils peuvent être configurés pour leur propre volume. Si vous prévoyez d'utiliser une export policy existante, vous pouvez l'indiquer lors

de la création du qtree. Vous pouvez également ajouter une export-policy plus tard avec le `volume qtree modify` commande.

2. Vérifier que le qtree a été créé avec le chemin de jonction souhaité :

   `volume qtree show -vserver` *`vserver_name`* `{ -volume` *`volume_name`* `-qtree` *`qtree_name`* `| -qtree-path` *`qtree path`* `}`

Exemple

L'exemple suivant crée un qtree nommé qt01 situé sur le SVM vs1.example.com qui dispose d'un chemin de jonction `/vol/data1`:

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path
/vol/data1/qt01 -security-style unix
[Job 1642] Job succeeded: Successful

cluster1::> volume qtree show -vserver vs1.example.com -qtree-path
/vol/data1/qt01

                      Vserver Name: vs1.example.com
                       Volume Name: data1
                        Qtree Name: qt01
  Actual (Non-Junction) Qtree Path: /vol/data1/qt01
                    Security Style: unix
                       Oplock Mode: enable
                  Unix Permissions: ---rwxr-xr-x
                          Qtree Id: 2
                      Qtree Status: normal
                     Export Policy: default
        Is Export Policy Inherited: true
```

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

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

Vous pouvez utiliser des règles d'exportation pour restreindre l'accès NFS aux volumes ou aux qtrees aux clients correspondant à des paramètres spécifiques. Lorsque vous provisionnez un nouveau stockage, vous pouvez utiliser une stratégie et des règles existantes, ajouter des règles à une stratégie existante, ou créer une nouvelle règle et de nouvelles règles. Vous pouvez également vérifier la configuration des export-policies

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

Gérer l'ordre de traitement des règles d'exportation

Vous pouvez utiliser le `vserver export-policy rule setindex` commande permettant de définir manuellement le numéro d'index d'une règle d'exportation existante. Cela vous permet de spécifier la priorité selon laquelle ONTAP applique des règles d'exportation aux requêtes client.

Description de la tâche

Si le nouveau numéro d'index est déjà utilisé, la commande insère la règle au point spécifié et réorganise la liste en conséquence.

Étape

1. Modifier le numéro d'index d'une règle d'exportation spécifiée :

   `vserver export-policy rule setindex -vserver` *`virtual_server_name`* `-policyname` *`policy_name`* `-ruleindex` *`integer`* `-newruleindex` *`integer`*

Exemple

La commande suivante modifie l'index numéro d'une règle d'exportation au niveau de l'index numéro 3 en index numéro 2 dans une export policy nommée rs1 sur le SVM nommée vs1 :

```
vs1::> vserver export-policy rule setindex -vserver vs1
-policyname rs1 -ruleindex 3 -newruleindex 2
```

Affectation d'une export-policy à un volume

Chaque volume contenu au SVM doit être associé à une export policy qui contient les export rules auxquelles les clients ont accès les données au sein du volume.

Description de la tâche

Vous pouvez associer une export policy à un volume lors de la création du volume ou à tout moment après sa création. Vous pouvez associer une export policy au volume, bien qu'une seule policy puisse être associée à de nombreux volumes.

Étapes

1. Si une export policy n'a pas été spécifiée lors de la création du volume, affectez une export policy au volume :

   `volume modify -vserver` *`vserver_name`* `-volume` *`volume_name`* `-policy` *`export_policy_name`*

2. Vérifiez que la policy a été assignée au volume :

   ```
   volume show -volume volume_name -fields policy
   ```

Exemple

Les commandes suivantes affectent l'export policy nfs_policy vers le volume vol1 sur le SVM vs1 et vérifient l'affectation :

```
cluster::> volume modify -v1server vs1 -volume vol1 -policy nfs_policy

cluster::>volume show -volume vol -fields policy
vserver volume       policy
------- ------------ ----------------
vs1     vol1         nfs_policy
```

Affecter une export policy à un qtree

Au lieu d'exporter un volume entier, vous pouvez également exporter un qtree spécifique sur un volume afin de le rendre directement accessible aux clients. Vous pouvez exporter un qtree en lui attribuant une export policy. Vous pouvez affecter la export policy lorsque vous créez un qtree ou en modifiant un qtree existant.

Ce dont vous avez besoin

La export policy doit exister.

Description de la tâche

Par défaut, les qtrees héritent de la politique d'exportation parent du volume contenant, si elle n'est pas spécifiée au moment de la création.

Vous pouvez associer une export policy à un qtree lors de la création du qtree ou à tout moment après la création du qtree. Vous pouvez associer une export policy au qtree, bien qu'une seule règle puisse être associée à de nombreux qtrees.

Étapes

1. Si une export policy n'a pas été spécifiée lors de la création du qtree, assigner une export policy au qtree :

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

2. Vérifier que la règle a été attribuée au qtree :

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

Exemple

Les commandes suivantes affectent l'export policy nfs_policy au qtree qt1 sur le SVM vs1 et vérifient l'affectation :

```
cluster::> volume modify -v1server vs1 -qtree-path /vol/vol1/qt1 -policy
nfs_policy

cluster::>volume qtree show -volume vol1 -fields export-policy
vserver volume qtree export-policy
------- ------ ----- -------------
vs1     data1  qt01  nfs_policy
```

Vérifiez l'accès client NFS depuis le cluster

Vous pouvez donner à certains clients l'accès au partage en définissant les autorisations de fichier UNIX sur un hôte d'administration UNIX. Vous pouvez vérifier l'accès client à l'aide de `vserver export-policy check-access` commande, en ajustant les règles d'exportation si nécessaire.

Étapes

1. Sur le cluster, vérifiez l'accès des clients aux exportations à l'aide de `vserver export-policy check-access` commande.

   La commande suivante vérifie l'accès en lecture/écriture pour un client NFSv3 avec l'adresse IP 1.2.3.4 vers la commande volume home2. La sortie de la commande indique que le volume utilise la export policy `exp-home-dir` et cet accès est refusé.

   ```
   cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
   1.2.3.4 -volume home2 -authentication-method sys -protocol nfs3 -access
   -type read-write
                                          Policy    Policy     Rule
   Path                     Policy        Owner     Owner Type Index  Access
   ------------------------ ------------- --------- ---------- ------
   ----------
   /                        default       vs1_root  volume          1 read
   /eng                     default       vs1_root  volume          1 read
   /eng/home2               exp-home-dir  home2     volume          1 denied

   3 entries were displayed.
   ```

2. Examinez la sortie pour déterminer si l'export policy fonctionne comme prévu et si l'accès client se comporte comme prévu.

   Plus précisément, vous devez vérifier quelles export policy est utilisée par le volume ou qtree et ce type d'accès par le client.

3. Si nécessaire, reconfigurer les règles d'export policy.

Testez l'accès NFS à partir des systèmes client

Après avoir vérifié l'accès NFS au nouvel objet de stockage, il est important de tester la configuration en vous connectant à un hôte d'administration NFS et en lisant les données à partir de et en écrivant les données sur la SVM. Vous devez ensuite répéter le processus en tant qu'utilisateur non-root sur un système client.

Ce dont vous avez besoin

- Le système client doit disposer d'une adresse IP autorisée par la règle d'exportation que vous avez spécifiée précédemment.
- Vous devez disposer des informations de connexion pour l'utilisateur root.

Étapes

1. Sur le cluster, vérifier l'adresse IP de la LIF qui héberge le nouveau volume :

   `network interface show –vserver svm_name`

2. Connectez-vous en tant qu'utilisateur racine au système client hôte d'administration.
3. Changez le répertoire pour le dossier de montage :

   `cd /mnt/`

4. Créer et monter un nouveau dossier en utilisant l'adresse IP de la SVM :

   a. Créer un nouveau dossier :
   `mkdir /mnt/folder`

   b. Montez le nouveau volume dans ce nouveau répertoire :
   `mount -t nfs -o hard IPAddress:/volume_name /mnt/folder`

   c. Changez le répertoire pour le nouveau dossier :
   `cd folder`

   Les commandes suivantes créent un dossier nommé test1, montent le volume vol1 à l'adresse IP 192.0.2.130 du dossier de montage tes1 et changent dans le nouveau répertoire tes1 :

```
host# mkdir /mnt/test1
host# mount -t nfs -o hard 192.0.2.130:/vol1 /mnt/test1
host# cd /mnt/test1
```

5. Créez un nouveau fichier, vérifiez qu'il existe et écrivez du texte :

   a. Créer un fichier de test :
   `touch filename`

   b. Vérifiez que le fichier existe :
   `ls -l filename`

   c. Entrez :
   `cat > filename`

Tapez du texte, puis appuyez sur Ctrl+D pour écrire du texte dans le fichier test.

d. Afficher le contenu du fichier de test.
`cat filename`

e. Supprimez le fichier de test :
`rm filename`

f. Retour au répertoire parent :
`cd ..`

```
host# touch myfile1
host# ls -l myfile1
-rw-r--r-- 1 root root 0 Sep 18 15:58 myfile1
host# cat >myfile1
This text inside the first file
host# cat myfile1
This text inside the first file
host# rm -r myfile1
host# cd ..
```

6. En tant que root, définissez les droits de propriété et les autorisations UNIX souhaités sur le volume monté.
7. Sur un système client UNIX identifié dans vos règles d'exportation, connectez-vous en tant qu'un des utilisateurs autorisés qui ont désormais accès au nouveau volume, puis répétez les procédures des étapes 3 à 5 pour vérifier que vous pouvez monter le volume et créer un fichier.