Aggiungere capacità di storage a una SVM abilitata per NFS

ONTAP 9

NetApp
April 24, 2024

Sommario

Aggiungere capacità di storage a una SVM abilitata per NFS

Aggiunta di capacità di storage a una panoramica SVM abilitata per NFS

Per aggiungere capacità di storage a una SVM abilitata per NFS, è necessario creare un volume o un qtree per fornire un container di storage e creare o modificare un criterio di esportazione per tale container. È quindi possibile verificare l'accesso del client NFS dal cluster e verificare l'accesso dai sistemi client.

Di cosa hai bisogno

- NFS deve essere completamente configurato su SVM.
- Il criterio di esportazione predefinito del volume root SVM deve contenere una regola che consenta l'accesso a tutti i client.
- Tutti gli aggiornamenti della configurazione dei name service devono essere completi.
- Eventuali aggiunte o modifiche a una configurazione Kerberos devono essere completate.

Creare una policy di esportazione

Prima di creare regole di esportazione, è necessario creare un criterio di esportazione per conservarle. È possibile utilizzare `vserver export-policy create` per creare un criterio di esportazione.

Fasi

1. Creare una policy di esportazione:

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

   Il nome del criterio può contenere fino a 256 caratteri.

2. Verificare che il criterio di esportazione sia stato creato:

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

Esempio

I seguenti comandi creano e verificano la creazione di una policy di esportazione denominata exp1 sulla SVM denominata vs1:

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

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

Aggiungere una regola a un criterio di esportazione

Senza regole, i criteri di esportazione non possono fornire l'accesso client ai dati. Per creare una nuova regola di esportazione, è necessario identificare i client e selezionare un formato di corrispondenza client, selezionare i tipi di accesso e di sicurezza, specificare un mapping anonimo dell'ID utente, selezionare un numero di indice della regola e selezionare il protocollo di accesso. È quindi possibile utilizzare `vserver export-policy rule create` per aggiungere la nuova regola a un criterio di esportazione.

Di cosa hai bisogno

- Il criterio di esportazione a cui si desidera aggiungere le regole di esportazione deve già esistere.
- Il DNS deve essere configurato correttamente sui dati SVM e i server DNS devono avere le voci corrette per i client NFS.

  Questo perché ONTAP esegue ricerche DNS utilizzando la configurazione DNS dei dati SVM per determinati formati di corrispondenza client, e gli errori nella corrispondenza delle regole dei criteri di esportazione possono impedire l'accesso ai dati del client.

- Se si esegue l'autenticazione con Kerberos, è necessario determinare quale dei seguenti metodi di protezione viene utilizzato sui client NFS:
  - `krb5` (Protocollo Kerberos V5)
  - `krb5i` (Protocollo Kerberos V5 con controllo dell'integrità mediante checksum)
  - `krb5p` (Protocollo Kerberos V5 con servizio di privacy)

A proposito di questa attività

Non è necessario creare una nuova regola se una regola esistente in un criterio di esportazione copre i requisiti di accesso e corrispondenza del client.

Se si esegue l'autenticazione con Kerberos e si accede a tutti i volumi della SVM tramite Kerberos, è possibile impostare le opzioni della regola di esportazione `-rorule`, `-rwrule`, e. `-superuser` per il volume root a. `krb5`, `krb5i`, o. `krb5p`.

Fasi

1. Identificare i client e il formato di corrispondenza del client per la nuova regola.

   Il `-clientmatch` option specifica i client a cui si applica la regola. È possibile specificare valori di corrispondenza client singoli o multipli; le specifiche di valori multipli devono essere separate da virgole. È possibile specificare la corrispondenza in uno dei seguenti formati:

Formato di corrispondenza del client	Esempio
Nome di dominio preceduto da "." carattere	`.example.com` oppure `.example.com,.example.net,...`
Nome host	`host1` oppure `host1,host2, ...`
Indirizzo IPv4	`10.1.12.24` oppure `10.1.12.24,10.1.12.25, ...`
Indirizzo IPv4 con una subnet mask espressa come numero di bit	`10.1.12.10/4` oppure `10.1.12.10/4,10.1.12.11/4,...`
Indirizzo IPv4 con una maschera di rete	`10.1.16.0/255.255.255.0` oppure `10.1.16.0/255.255.255.0,10.1.17.0/255.255.255.0,...`
Indirizzo IPv6 in formato punteggiato	`::1.2.3.4` oppure `::1.2.3.4,::1.2.3.5,...`
Indirizzo IPv6 con una subnet mask espressa come numero di bit	`ff::00/32` oppure `ff::00/32,ff::01/32,...`
Un singolo netgroup con il nome del netgroup preceduto dal carattere @	`@netgroup1` oppure `@netgroup1,@netgroup2,...`

È inoltre possibile combinare tipi di definizioni client, ad esempio `.example.com,@netgroup1`.

Quando si specificano gli indirizzi IP, tenere presente quanto segue:

- Non è consentito inserire un intervallo di indirizzi IP, ad esempio 10.1.12.10-10.1.12.70.

  Le voci in questo formato vengono interpretate come una stringa di testo e trattate come nome host.

- Quando si specificano singoli indirizzi IP nelle regole di esportazione per la gestione granulare dell'accesso client, non specificare gli indirizzi IP assegnati in modo dinamico (ad esempio DHCP) o temporaneo (ad esempio IPv6).

  In caso contrario, il client perde l'accesso quando cambia l'indirizzo IP.

- Non è consentito inserire un indirizzo IPv6 con una maschera di rete, ad esempio ff::12/ff::00.

2. Selezionare i tipi di accesso e di sicurezza per le corrispondenze dei client.

   È possibile specificare una o più delle seguenti modalità di accesso per i client che eseguono l'autenticazione con i tipi di protezione specificati:

   - `-rorule` (accesso di sola lettura)
   - `-rwrule` (accesso di lettura/scrittura)
   - `-superuser` (accesso root)

> Un client può ottenere l'accesso in lettura/scrittura solo per un tipo di protezione specifico se la regola di esportazione consente l'accesso in sola lettura anche per quel tipo di protezione. Se il parametro di sola lettura è più restrittivo per un tipo di protezione rispetto al parametro di lettura/scrittura, il client potrebbe non ottenere l'accesso di lettura/scrittura. Lo stesso vale per l'accesso dei superutenti.

È possibile specificare un elenco separato da virgole di più tipi di protezione per una regola. Se si specifica il tipo di protezione come `any` oppure `never`, non specificare altri tipi di protezione. Scegliere tra i seguenti tipi di protezione validi:

Quando il tipo di protezione è impostato su…	Un client corrispondente può accedere ai dati esportati…
`any`	Sempre, indipendentemente dal tipo di sicurezza in entrata.
`none`	Se elencati da soli, ai client con qualsiasi tipo di protezione viene concesso l'accesso come anonimo. Se elencato con altri tipi di protezione, ai client con un tipo di protezione specificato viene concesso l'accesso e ai client con qualsiasi altro tipo di protezione viene concesso l'accesso come anonimo.
`never`	Mai, indipendentemente dal tipo di sicurezza in entrata.
`krb5`	Se autenticato da Kerberos 5. Authentication Only (solo autenticazione): L'intestazione di ogni richiesta e risposta viene firmata.
`krb5i`	Se autenticato da Kerberos 5i. Autenticazione e integrità: L'intestazione e il corpo di ogni richiesta e risposta vengono firmati.
`krb5p`	Se autenticato da Kerberos 5p. Autenticazione, integrità e privacy: L'intestazione e il corpo di ogni richiesta e risposta vengono firmati e il payload dei dati NFS viene crittografato.
`ntlm`	Se autenticato da CIFS NTLM.
`sys`	Se autenticato da NFS AUTH_SYS.

Il tipo di protezione consigliato è `sys`Oppure, se si utilizza Kerberos, `krb5, krb5i, o. `krb5p`.

Se si utilizza Kerberos con NFSv3, la regola dei criteri di esportazione deve consentire `-rorule` e. `-rwrule` accesso a. `sys` oltre a `krb5`. Ciò è dovuto alla necessità di consentire l'accesso NLM (Network Lock Manager) all'esportazione.

3. Specificare un mapping anonimo dell'ID utente.

   Il `-anon` L'opzione specifica un ID utente UNIX o un nome utente mappato alle richieste del client che arrivano con un ID utente 0 (zero), che in genere è associato al nome utente root. Il valore predefinito è `65534`. I client NFS in genere associano l'ID utente 65534 con il nome utente nessuno (noto anche come *root squashing*). In ONTAP, questo ID utente è associato all'utente pcuser. Per disattivare l'accesso da parte di qualsiasi client con un ID utente pari a 0, specificare un valore di `65535`.

4. Selezionare l'ordine di indice della regola.

   Il `-ruleindex` option specifica il numero di indice per la regola. Le regole vengono valutate in base al loro ordine nell'elenco dei numeri di indice; le regole con numeri di indice inferiori vengono valutate per prime. Ad esempio, la regola con indice numero 1 viene valutata prima della regola con indice numero 2.

Se si desidera aggiungere…	Quindi…
La prima regola per un criterio di esportazione	Invio `1`.
Regole aggiuntive per una policy di esportazione	a. Visualizzare le regole esistenti nel criterio: `vserver export-policy rule show -instance -policyname` *`your_policy`* b. Selezionare un numero di indice per la nuova regola in base all'ordine in cui deve essere valutata.

5. Selezionare il valore di accesso NFS applicabile: {`nfs`|`nfs3`|`nfs4`}.

   `nfs` corrisponde a qualsiasi versione, `nfs3` e. `nfs4` associare solo le versioni specifiche.

6. Creare la regola di esportazione e aggiungerla a un criterio di esportazione esistente:

   ```
   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. Visualizzare le regole per il criterio di esportazione per verificare la presenza della nuova regola:

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

   Il comando visualizza un riepilogo per il criterio di esportazione, incluso un elenco di regole applicate a tale criterio. ONTAP assegna a ogni regola un numero di indice della regola. Una volta conosciuto il numero di indice della regola, è possibile utilizzarlo per visualizzare informazioni dettagliate sulla regola di esportazione specificata.

8. Verificare che le regole applicate ai criteri di esportazione siano configurate correttamente:

   ```
   vserver export-policy rule show -policyname policy_name -vserver vserver_name
   -ruleindex integer
   ```

Esempi

I seguenti comandi creano e verificano la creazione di una regola di esportazione su SVM denominata vs1 in un criterio di esportazione denominato rs1. La regola ha il numero di indice 1. La regola corrisponde a qualsiasi client nel dominio eng.company.com e al netgroup @netgroup1. La regola attiva tutti gli accessi NFS. Consente l'accesso in sola lettura e in lettura/scrittura agli utenti autenticati con AUTH_SYS. I client con ID utente UNIX 0 (zero) vengono anonimizzati a meno che non vengano autenticati con 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
```

I seguenti comandi creano e verificano la creazione di una regola di esportazione su SVM denominata vs2 in un criterio di esportazione denominato expol2. La regola ha il numero di indice 21. La regola consente di confrontare i client con i membri del netgroup dev_netgroup_main. La regola attiva tutti gli accessi NFS. Consente l'accesso in sola lettura per gli utenti autenticati con AUTH_SYS e richiede l'autenticazione Kerberos per l'accesso in lettura-scrittura e root. Ai client con ID utente UNIX 0 (zero) viene negato l'accesso root a meno che non vengano autenticati con 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
```

Creare un volume o un contenitore di storage qtree

Creare un volume

È possibile creare un volume e specificarne il punto di giunzione e altre proprietà utilizzando `volume create` comando.

A proposito di questa attività

Un volume deve includere un *percorso di giunzione* per rendere i dati disponibili ai client. È possibile specificare il percorso di giunzione quando si crea un nuovo volume. Se si crea un volume senza specificare un percorso di giunzione, è necessario *montare* il volume nello spazio dei nomi SVM utilizzando `volume mount` comando.

Prima di iniziare

- NFS deve essere configurato e in esecuzione.
- Lo stile di sicurezza SVM deve essere UNIX.
- A partire da ONTAP 9.13.1, puoi creare volumi con l'analisi della capacità e il monitoraggio delle attività abilitati. Per attivare il monitoraggio della capacità o dell'attività, eseguire il `volume create` comando con

`-analytics-state` oppure `-activity-tracking-state` impostare su `on`.

Per ulteriori informazioni sull'analisi della capacità e sul monitoraggio delle attività, consulta Abilita analisi del file system.

Fasi

1. Creare il volume con un punto di giunzione:

   ```
   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]
   ```

   Le scelte per `-junction-path` sono i seguenti:

   - Direttamente sotto root, ad esempio `/new_vol`

     È possibile creare un nuovo volume e specificarne il montaggio direttamente nel volume root SVM.

   - In una directory esistente, ad esempio `/existing_dir/new_vol`

     È possibile creare un nuovo volume e specificarne il montaggio in un volume esistente (in una gerarchia esistente), espresso come directory.

     Se si desidera creare un volume in una nuova directory (in una nuova gerarchia sotto un nuovo volume), ad esempio, `/new_dir/new_vol`, Quindi, è necessario creare prima un nuovo volume padre che sia congiunto al volume root SVM. Creare quindi il nuovo volume figlio nel percorso di giunzione del nuovo volume padre (nuova directory).

   + se si intende utilizzare un criterio di esportazione esistente, è possibile specificarlo al momento della creazione del volume. È inoltre possibile aggiungere un criterio di esportazione in un secondo momento con `volume modify` comando.

2. Verificare che il volume sia stato creato con il punto di giunzione desiderato:

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

Esempi

Il seguente comando crea un nuovo volume denominato users1 su SVM vs1.example.com e sull'aggregato aggr1. Il nuovo volume è disponibile all'indirizzo `/users`. Il volume ha una dimensione di 750 GB e la relativa garanzia è di tipo volume (per impostazione predefinita).

```
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
```

Il seguente comando crea un nuovo volume denominato "home4" su SVM "vs1.example.com" e l'aggregato "aggr1". La directory `/eng/` Esiste già nello spazio dei nomi per vs1 SVM e il nuovo volume è disponibile all'indirizzo `/eng/home`, che diventa la home directory di `/eng/` namespace. Il volume è di 750 GB e la relativa garanzia è di tipo `volume` (per impostazione predefinita).

```
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
```

Creare un qtree

È possibile creare un qtree per contenere i dati e specificarne le proprietà utilizzando `volume qtree create` comando.

Di cosa hai bisogno

- La SVM e il volume che conterrà il nuovo qtree devono già esistere.
- Lo stile di sicurezza SVM deve essere UNIX e NFS deve essere configurato e in esecuzione.

Fasi

1. Creare il qtree:

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

   È possibile specificare il volume e il qtree come argomenti separati o specificare l'argomento del percorso qtree nel formato `/vol/`*`volume_name/_qtree_name`*.

   Per impostazione predefinita, i qtree ereditano i criteri di esportazione del volume principale, ma possono essere configurati per l'utilizzo dei propri. Se si intende utilizzare un criterio di esportazione esistente, è

possibile specificarlo al momento della creazione del qtree. È inoltre possibile aggiungere un criterio di esportazione in un secondo momento con `volume qtree modify` comando.

2. Verificare che il qtree sia stato creato con il percorso di giunzione desiderato:

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

Esempio

Nell'esempio seguente viene creato un qtree chiamato qt01 situato su SVM vs1.example.com che ha un percorso di giunzione `/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
```

Accesso sicuro a NFS tramite policy di esportazione

Accesso sicuro a NFS tramite policy di esportazione

È possibile utilizzare policy di esportazione per limitare l'accesso NFS a volumi o qtree a client che corrispondono a parametri specifici. Quando si effettua il provisioning di nuovo storage, è possibile utilizzare policy e regole esistenti, aggiungere regole a policy esistenti o creare nuove policy e regole. È inoltre possibile verificare la configurazione dei criteri di esportazione

A partire da ONTAP 9.3, è possibile attivare il controllo della configurazione dei criteri di esportazione come processo in background che registra eventuali violazioni delle regole in un elenco di regole di errore. Il `vserver export-policy config-checker` I comandi richiamano il controllo e visualizzano i risultati, che è possibile utilizzare per verificare la configurazione ed eliminare le regole errate dal criterio.i comandi convalidano solo la configurazione di esportazione per i nomi host, i netgroup e gli utenti anonimi.

Gestire l'ordine di elaborazione delle regole di esportazione

È possibile utilizzare `vserver export-policy rule setindex` per impostare manualmente il numero di indice di una regola di esportazione esistente. In questo modo è possibile specificare la precedenza con cui ONTAP applica le regole di esportazione alle richieste del client.

A proposito di questa attività

Se il nuovo numero di indice è già in uso, il comando inserisce la regola nel punto specificato e riordina l'elenco di conseguenza.

Fase

1. Modificare il numero di indice di una regola di esportazione specificata:

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

Esempio

Il seguente comando modifica il numero di indice di una regola di esportazione al numero di indice 3 in quello 2 in una policy di esportazione denominata rs1 sulla SVM denominata vs1:

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

Assegnare un criterio di esportazione a un volume

Ogni volume contenuto nella SVM deve essere associato a un criterio di esportazione che contenga regole di esportazione per consentire ai client di accedere ai dati nel volume.

A proposito di questa attività

È possibile associare un criterio di esportazione a un volume quando si crea il volume o in qualsiasi momento dopo averlo creato. È possibile associare un criterio di esportazione al volume, anche se un criterio può essere associato a più volumi.

Fasi

1. Se non è stato specificato un criterio di esportazione al momento della creazione del volume, assegnare un criterio di esportazione al volume:

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

2. Verificare che il criterio sia stato assegnato al volume:

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

Esempio

I seguenti comandi assegnano il criterio di esportazione nfs_policy al volume vol1 su SVM vs1 e ne verificano l'assegnazione:

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

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

Assegnare un criterio di esportazione a un qtree

Invece di esportare un intero volume, è possibile esportare un qtree specifico su un volume per renderlo direttamente accessibile ai client. È possibile esportare un qtree assegnandogli un criterio di esportazione. È possibile assegnare il criterio di esportazione quando si crea un nuovo qtree o modificando un qtree esistente.

Di cosa hai bisogno

Il criterio di esportazione deve esistere.

A proposito di questa attività

Per impostazione predefinita, i qtree ereditano il criterio di esportazione padre del volume contenente, se non diversamente specificato al momento della creazione.

È possibile associare un criterio di esportazione a un qtree quando si crea il qtree o in qualsiasi momento dopo la creazione del qtree. È possibile associare un criterio di esportazione al qtree, anche se un criterio può essere associato a molti qtree.

Fasi

1. Se non è stato specificato un criterio di esportazione al momento della creazione del qtree, assegnare un criterio di esportazione al qtree:

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

2. Verificare che il criterio sia stato assegnato al qtree:

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

Esempio

I seguenti comandi assegnano il criterio di esportazione nfs_policy al qtree qt1 su SVM vs1 e ne verificano l'assegnazione:

```
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
```

Verificare l'accesso del client NFS dal cluster

È possibile consentire ai client selezionati di accedere alla condivisione impostando le autorizzazioni per i file UNIX su un host di amministrazione UNIX. È possibile controllare l'accesso del client utilizzando `vserver export-policy check-access` , regolando le regole di esportazione secondo necessità.

Fasi

1. Nel cluster, controllare l'accesso del client alle esportazioni utilizzando `vserver export-policy check-access` comando.

   Il seguente comando controlla l'accesso in lettura/scrittura per un client NFSv3 con l'indirizzo IP 1.2.3.4 nel volume home2. L'output del comando indica che il volume utilizza il criterio di esportazione `exp-home-dir` e che l'accesso è negato.

   ```
   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. Esaminare l'output per determinare se il criterio di esportazione funziona come previsto e se l'accesso client si comporta come previsto.

   In particolare, è necessario verificare quali criteri di esportazione vengono utilizzati dal volume o dal qtree e il tipo di accesso che ne deriva dal client.

3. Se necessario, riconfigurare le regole dei criteri di esportazione.

Verificare l’accesso NFS dai sistemi client

Dopo aver verificato l’accesso NFS al nuovo oggetto storage, è necessario verificare la configurazione accedendo a un host di amministrazione NFS e leggendo i dati da e scrivendo i dati su SVM. Ripetere il processo come utente non root su un sistema client.

Di cosa hai bisogno

- Il sistema client deve disporre di un indirizzo IP consentito dalla regola di esportazione specificata in precedenza.
- È necessario disporre delle informazioni di accesso per l’utente root.

Fasi

1. Sul cluster, verificare l’indirizzo IP della LIF che ospita il nuovo volume:

   `network interface show –vserver svm_name`

2. Accedere come utente root al sistema client host di amministrazione.
3. Modificare la directory nella cartella mount:

   `cd /mnt/`

4. Creare e montare una nuova cartella utilizzando l’indirizzo IP di SVM:

   a. Creare una nuova cartella:
   `mkdir /mnt/folder`

   b. Montare il nuovo volume in questa nuova directory:
   `mount -t nfs -o hard IPAddress:/volume_name /mnt/folder`

   c. Modificare la directory nella nuova cartella:
   `cd folder`

   I seguenti comandi creano una cartella denominata test1, montano il volume vol1 all’indirizzo IP 192.0.2.130 sulla cartella di montaggio test1 e cambiano nella nuova directory test1:

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

5. Creare un nuovo file, verificarne l’esistenza e scriverne del testo:

   a. Creare un file di test:
   `touch filename`

   b. Verificare che il file esista.:
   `ls -l filename`

   c. Immettere:
   `cat > filename`

   Digitare del testo, quindi premere Ctrl+D per scrivere il testo nel file di prova.

d. Visualizzare il contenuto del file di test.
`cat filename`

e. Rimuovere il file di test:
`rm filename`

f. Tornare alla directory principale:
`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. Come root, impostare la proprietà e le autorizzazioni UNIX desiderate sul volume montato.
7. Su un sistema client UNIX identificato nelle regole di esportazione, accedere come uno degli utenti autorizzati che ora ha accesso al nuovo volume e ripetere le procedure descritte nei passaggi da 3 a 5 per verificare che sia possibile montare il volume e creare un file.