Gestire l'accesso ai file con NFS

ONTAP 9

NetApp
April 24, 2024

Sommario

Gestire l’accesso ai file con NFS

Attivare o disattivare NFSv3

È possibile attivare o disattivare NFSv3 modificando il `-v3` opzione. Ciò consente l’accesso ai file per i client che utilizzano il protocollo NFSv3. Per impostazione predefinita, NFSv3 è attivato.

Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera…	Immettere il comando…
Abilitare NFSv3	`vserver nfs modify -vserver vserver_name -v3 enabled`
Disattiva NFSv3	`vserver nfs modify -vserver vserver_name -v3 disabled`

Attivare o disattivare NFSv4.0

È possibile attivare o disattivare NFSv4.0 modificando il `-v4.0` opzione. Questo consente l’accesso al file per i client che utilizzano il protocollo NFSv4.0. In ONTAP 9.9.1, NFSv4.0 è attivato per impostazione predefinita; nelle versioni precedenti, è disattivato per impostazione predefinita.

Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera…	**Immettere il seguente comando…**
Abilitare NFSv4.0	`vserver nfs modify -vserver vserver_name -v4.0 enabled`
Disattiva NFSv4.0	`vserver nfs modify -vserver vserver_name -v4.0 disabled`

Attivare o disattivare NFSv4.1

È possibile attivare o disattivare NFSv4.1 modificando il `-v4.1` opzione. Ciò consente l’accesso ai file per i client che utilizzano il protocollo NFSv4.1. In ONTAP 9.9.1, NFSv4.1 è attivato per impostazione predefinita; nelle versioni precedenti, è disattivato per impostazione predefinita.

Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera…	Immettere il seguente comando…
Abilitare NFSv4.1	`vserver nfs modify -vserver vserver_name -v4.1 enabled`
Disattiva NFSv4.1	`vserver nfs modify -vserver vserver_name -v4.1 disabled`

Gestire i limiti dello storepool di NFSv4

A partire da ONTAP 9.13, gli amministratori possono consentire ai server NFSv4 di negare le risorse ai client NFSv4 quando raggiungono i limiti di risorse dello storepool per client. Quando i client consumano troppe risorse dello storepool NFSv4, questo può causare il blocco di altri client NFSv4 a causa della mancata disponibilità delle risorse dello storepool NFSv4.

L'attivazione di questa funzionalità consente inoltre ai clienti di visualizzare il consumo attivo delle risorse dello storepool da parte di ciascun client. Ciò semplifica l'identificazione dei client che esauriscono le risorse di sistema e consente di imporre limiti di risorse per client.

Visualizza le risorse dello storepool consumate

Il `vserver nfs storepool show` il comando mostra il numero di risorse dello storepool utilizzate. Uno storepool è un pool di risorse utilizzate dai client NFSv4.

Fase

1. In qualità di amministratore, eseguire `vserver nfs storepool show` Per visualizzare le informazioni sullo storepool dei client NFSv4.

Esempio

In questo esempio vengono visualizzate le informazioni sullo storepool dei client 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.
```

Attiva o disattiva i controlli dei limiti dello storepool

Gli amministratori possono utilizzare i seguenti comandi per attivare o disattivare i controlli dei limiti dello storepool.

Fase

1. In qualità di amministratore, eseguire una delle seguenti operazioni:

Se si desidera…	Immettere il seguente comando…
Abilitare i controlli dei limiti dello storepool	`vserver nfs storepool config modify -limit-enforce enabled`
Disattiva i controlli dei limiti di storepool	`vserver nfs storepool config modify -limit-enforce disabled`

Visualizzare un elenco di client bloccati

Se il limite di storepool è attivato, gli amministratori possono vedere quali client sono stati bloccati al raggiungimento della soglia di risorse per client. Gli amministratori possono utilizzare il seguente comando per vedere quali client sono stati contrassegnati come client bloccati.

Fasi

1. Utilizzare `vserver nfs storepool blocked-client show` Per visualizzare l'elenco dei client NFSv4 bloccati.

Rimuovere un client dall'elenco dei client bloccati

I client che raggiungono la soglia per client verranno disconnessi e aggiunti alla cache del client a blocchi. Gli amministratori possono utilizzare il seguente comando per rimuovere il client dalla cache del client a blocchi. In questo modo, il client potrà connettersi al server NFSV4 di ONTAP.

Fasi

1. Utilizzare `vserver nfs storepool blocked-client flush -client-ip <ip address>` comando per svuotare la cache del client bloccato nello storepool.
2. Utilizzare `vserver nfs storepool blocked-client show` comando per verificare che il client sia stato rimosso dalla cache del client a blocchi.

Esempio

In questo esempio viene visualizzato un client bloccato con l'indirizzo IP "10.2.1.1" che viene liberato da tutti i nodi.

```
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.
```

Abilitare o disabilitare pNFS

PNFS migliora le performance consentendo ai client NFS di eseguire operazioni di lettura/scrittura direttamente e in parallelo sui dispositivi di storage, ignorando il server NFS come potenziale collo di bottiglia. Per attivare o disattivare pNFS (Parallel NFS), è possibile modificare `-v4.1-pnfs` opzione.

Se la versione di ONTAP è…	Il valore predefinito di pNFS è…
9.8 o versione successiva	disattivato
9.7 o versioni precedenti	attivato

Di cosa hai bisogno

Il supporto di NFSv4.1 è necessario per poter utilizzare pNFS.

Se si desidera attivare pNFS, è necessario prima disattivare i riferimenti NFS. Non è possibile abilitare entrambi contemporaneamente.

Se si utilizza pNFS con Kerberos su SVM, è necessario attivare Kerberos su ogni LIF su SVM.

Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera…	Immettere il comando…
Abilitare pNFS	`vserver nfs modify -vserver vserver_name -v4.1-pnfs enabled`
Disattiva pNFS	`vserver nfs modify -vserver vserver_name -v4.1-pnfs disabled`

Informazioni correlate

- Panoramica del trunking NFS

Controlla l'accesso NFS su TCP e UDP

È possibile attivare o disattivare l'accesso NFS alle macchine virtuali di storage (SVM) su TCP e UDP modificando il `-tcp` e. `-udp` parametri, rispettivamente. In questo modo è possibile controllare se i client NFS possono accedere ai dati tramite TCP o UDP nel proprio ambiente.

A proposito di questa attività

Questi parametri si applicano solo a NFS. Non influiscono sui protocolli ausiliari. Ad esempio, se NFS su TCP è disattivato, le operazioni di montaggio su TCP continuano a avere successo. Per bloccare completamente il traffico TCP o UDP, è possibile utilizzare le regole dei criteri di esportazione.

> È necessario disattivare SnapDiff RPC Server prima di disattivare TCP per NFS per evitare un errore di comando non riuscito. È possibile disattivare il protocollo TCP utilizzando il comando `vserver snapdiff-rpc-server off -vserver vserver name`.

Fase

1. Eseguire una delle seguenti operazioni:

Se vuoi che l'accesso NFS sia…	Immettere il comando…
Abilitato su TCP	`vserver nfs modify -vserver vserver_name -tcp enabled`
Disattivato su TCP	`vserver nfs modify -vserver vserver_name -tcp disabled`
Abilitato su UDP	`vserver nfs modify -vserver vserver_name -udp enabled`
Disattivato su UDP	`vserver nfs modify -vserver vserver_name -udp disabled`

Controllo delle richieste NFS da porte non riservate

È possibile rifiutare le richieste di montaggio NFS da porte non riservate attivando `-mount-rootonly` opzione. Per rifiutare tutte le richieste NFS da porte non riservate, è possibile attivare `-nfs-rootonly` opzione.

A proposito di questa attività

Per impostazione predefinita, l'opzione `-mount-rootonly` è `enabled`.

Per impostazione predefinita, l'opzione `-nfs-rootonly` è `disabled`.

Queste opzioni non si applicano alla procedura NULL.

Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera…	Immettere il comando…
Consenti richieste di montaggio NFS da porte non riservate	`vserver nfs modify -vserver vserver_name -mount -rootonly disabled`
Rifiutare le richieste di montaggio NFS da porte non riservate	`vserver nfs modify -vserver vserver_name -mount -rootonly enabled`
Consenti tutte le richieste NFS da porte non riservate	`vserver nfs modify -vserver vserver_name -nfs -rootonly disabled`
Rifiutare tutte le richieste NFS da porte non riservate	`vserver nfs modify -vserver vserver_name -nfs -rootonly enabled`

Gestire l'accesso NFS a volumi NTFS o qtree per utenti UNIX sconosciuti

Se ONTAP non riesce a identificare gli utenti UNIX che tentano di connettersi a volumi o qtree con lo stile di protezione NTFS, non può quindi mappare esplicitamente l'utente a un utente Windows. È possibile configurare ONTAP in modo che neghi l'accesso a tali utenti per una protezione più rigorosa oppure mapparli a un utente Windows predefinito per garantire un livello minimo di accesso a tutti gli utenti.

Di cosa hai bisogno

Se si desidera attivare questa opzione, è necessario configurare un utente Windows predefinito.

A proposito di questa attività

Se un utente UNIX tenta di accedere a volumi o qtree con uno stile di protezione NTFS, l'utente UNIX deve prima essere mappato a un utente Windows in modo che ONTAP possa valutare correttamente le autorizzazioni NTFS. Tuttavia, se ONTAP non riesce a cercare il nome dell'utente UNIX nelle origini del

servizio nome informazioni utente configurate, non può eseguire il mapping esplicito dell'utente UNIX a un utente Windows specifico. È possibile decidere come gestire tali utenti UNIX sconosciuti nei seguenti modi:

- Negare l'accesso a utenti UNIX sconosciuti.

  In questo modo viene garantita una sicurezza più rigorosa, richiedendo il mapping esplicito per tutti gli utenti UNIX per ottenere l'accesso ai volumi NTFS o ai qtree.

- Associare utenti UNIX sconosciuti a un utente Windows predefinito.

  In questo modo si ottiene meno sicurezza, ma maggiore praticità, garantendo a tutti gli utenti un livello minimo di accesso ai volumi NTFS o ai qtree tramite un utente Windows predefinito.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

   ```
   set -privilege advanced
   ```

2. Eseguire una delle seguenti operazioni:

Se si desidera utilizzare l'utente Windows predefinito per utenti UNIX sconosciuti…	Immettere il comando…
Attivato	`vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user enabled`
Disattivato	`vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user disabled`

3. Tornare al livello di privilegio admin:

   ```
   set -privilege admin
   ```

Considerazioni per i client che montano le esportazioni NFS utilizzando una porta non riservata

Il `-mount-rootonly` L'opzione deve essere disattivata su un sistema storage che deve supportare i client che montano le esportazioni NFS utilizzando una porta non riservata anche quando l'utente è connesso come root. Tali client includono i client Hummingbird e i client NFS/IPv6 di Solaris.

Se il `-mount-rootonly` ONTAP non consente ai client NFS che utilizzano porte non riservate, ovvero porte con numeri superiori a 1,023, di montare le esportazioni NFS.

Eseguire un controllo degli accessi più rigoroso per i netgroup verificando i domini

Per impostazione predefinita, ONTAP esegue un'ulteriore verifica quando valuta l'accesso client per un netgroup. Il controllo aggiuntivo garantisce che il dominio del client corrisponda alla configurazione di dominio della macchina virtuale di storage (SVM). In caso contrario, ONTAP nega l'accesso al client.

A proposito di questa attività

Quando ONTAP valuta le regole dei criteri di esportazione per l'accesso client e una regola dei criteri di esportazione contiene un netgroup, ONTAP deve determinare se l'indirizzo IP di un client appartiene al netgroup. A tale scopo, ONTAP converte l'indirizzo IP del client in un nome host utilizzando DNS e ottiene un nome di dominio completo (FQDN).

Se il file netgroup elenca solo un nome breve per l'host e il nome breve per l'host esiste in più domini, è possibile che un client di un dominio diverso ottenga l'accesso senza questo controllo.

Per evitare che ciò accada, ONTAP confronta il dominio restituito dal DNS per l'host con l'elenco dei nomi di dominio DNS configurati per la SVM. Se corrisponde, l'accesso è consentito. Se non corrisponde, l'accesso viene negato.

Questa verifica è attivata per impostazione predefinita. È possibile gestirlo modificando il `-netgroup-dns -domain-search` che è disponibile al livello di privilegio avanzato.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

   ```
   set -privilege advanced
   ```

2. Eseguire l'azione desiderata:

Se si desidera che la verifica del dominio per i netgroup sia…	Inserisci…
Attivato	`vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search enabled`
Disattivato	`vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search disabled`

3. Impostare il livello di privilegio su admin:

   ```
   set -privilege admin
   ```

Modificare le porte utilizzate per i servizi NFSv3

Il server NFS sul sistema di storage utilizza servizi come mount daemon e Network Lock

Manager per comunicare con i client NFS su porte di rete predefinite specifiche. Nella maggior parte degli ambienti NFS, le porte predefinite funzionano correttamente e non richiedono modifiche, ma se si desidera utilizzare diverse porte di rete NFS nell'ambiente NFSv3, è possibile farlo.

Di cosa hai bisogno

La modifica delle porte NFS sul sistema di storage richiede che tutti i client NFS si riconnettano al sistema, pertanto è necessario comunicare queste informazioni agli utenti prima di apportare la modifica.

A proposito di questa attività

È possibile impostare le porte utilizzate dai servizi NFS mount daemon, Network Lock Manager, Network Status Monitor e NFS quota daemon per ciascuna macchina virtuale di storage (SVM). La modifica del numero di porta influisce sull'accesso dei client NFS ai dati sia su TCP che su UDP.

Le porte per NFSv4 e NFSv4.1 non possono essere modificate.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

   ```
   set -privilege advanced
   ```

2. Disattivare l'accesso a NFS:

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

3. Impostare la porta NFS per il servizio NFS specifico:

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

Parametro della porta NFS	Descrizione	Porta predefinita
`-mountd-port`	Daemon di montaggio NFS	635
`-nlm-port`	Network Lock Manager	4045
`-nsm-port`	Network Status Monitor (Monitor di stato della rete	4046
`-rquotad-port`	Daemon quota NFS	4049

   Oltre alla porta predefinita, l'intervallo consentito di numeri di porta è compreso tra 1024 e 65535. Ogni servizio NFS deve utilizzare una porta univoca.

4. Abilitare l'accesso a NFS:

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

5. Utilizzare `network connections listening show` per verificare che il numero di porta cambi.
6. Tornare al livello di privilegio admin:

```
set -privilege admin
```

Esempio

I seguenti comandi impostano la porta NFS Mount Daemon su 1113 sulla SVM denominata 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
```

Comandi per la gestione dei server NFS

Esistono comandi ONTAP specifici per la gestione dei server NFS.

Se si desidera…	Utilizzare questo comando…
Creare un server NFS	`vserver nfs create`
Visualizzare i server NFS	`vserver nfs show`
Modificare un server NFS	`vserver nfs modify`
Eliminare un server NFS	`vserver nfs delete`

Nascondere `.snapshot` Elenco di directory sotto i punti di montaggio NFSv3 Accesso esplicito a `.snapshot` la directory sarà comunque consentita anche se l'opzione è attivata.	`vserver nfs` comandi con `-v3-hide-snapshot` opzione attivata

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

Risolvere i problemi di name service

Quando i client riscontrano errori di accesso dovuti a problemi di name service, è possibile utilizzare `vserver services name-service getxxbyyy` famiglia di comandi per eseguire manualmente varie ricerche dei name service ed esaminare i dettagli e i risultati della ricerca per agevolare la risoluzione dei problemi.

A proposito di questa attività

- Per ciascun comando, è possibile specificare quanto segue:
  - Nome del nodo o della SVM (Storage Virtual Machine) su cui eseguire la ricerca.

    In questo modo è possibile verificare le ricerche name service per un nodo o una SVM specifico per limitare la ricerca di un potenziale problema di configurazione del name service.

  - Se visualizzare l'origine utilizzata per la ricerca.

    In questo modo è possibile verificare se è stata utilizzata la sorgente corretta.

- ONTAP seleziona il servizio per l'esecuzione della ricerca in base all'ordine di switch name service configurato.
- Questi comandi sono disponibili a livello di privilegio avanzato.

Fasi

1. Eseguire una delle seguenti operazioni:

Per recuperare…	Utilizzare il comando…
Indirizzo IP di un nome host	`vserver services name-service getxxbyyy getaddrinfo` `vserver services name-service getxxbyyy gethostbyname` (Solo indirizzi IPv4)
Membri di un gruppo per ID gruppo	`vserver services name-service getxxbyyy getgrbygid`

Membri di un gruppo in base al nome del gruppo	`vserver services name-service getxxbyyy getgrbyname`
Elenco dei gruppi a cui appartiene un utente	`vserver services name-service getxxbyyy getgrlist`
Nome host di un indirizzo IP	`vserver services name-service getxxbyyy getnameinfo` `vserver services name-service getxxbyyy gethostbyaddr` (Solo indirizzi IPv4)
Informazioni utente per nome utente	`vserver services name-service getxxbyyy getpwbyname` È possibile verificare la risoluzione dei nomi degli utenti RBAC specificando `-use-rbac` parametro as `true`.
Informazioni utente per ID utente	`vserver services name-service getxxbyyy getpwbyuid`È possibile verificare la risoluzione dei nomi degli utenti RBAC specificando `-use-rbac` parametro as `true`.
Appartenenza a netgroup di un client	`vserver services name-service getxxbyyy netgrp`
Appartenenza a netgroup di un client mediante la ricerca netgroup-by-host	`vserver services name-service getxxbyyy netgrpbyhost`

L'esempio seguente mostra un test di ricerca DNS per SVM vs1 tentando di ottenere l'indirizzo IP per l'host 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'esempio seguente mostra un test di ricerca NIS per SVM vs1 tentando di recuperare le informazioni utente per un utente con 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'esempio seguente mostra un test di ricerca LDAP per SVM vs1 tentando di recuperare le informazioni utente per un utente con il nome 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'esempio seguente mostra un test di ricerca di netgroup per SVM vs1 cercando di scoprire se il client dnshost0 è un membro del netgroup lnetgroup136:

```
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. Analizzare i risultati del test eseguito e intraprendere le azioni necessarie.

Se…	**Controllare…**
La ricerca del nome host o dell'indirizzo IP non è riuscita o ha dato risultati errati	Configurazione DNS
La ricerca ha richiesto un'origine errata	Configurazione dello switch name service

Se…	Controllare…
La ricerca di utenti o gruppi non è riuscita o ha prodotto risultati errati	• Configurazione dello switch name service • Configurazione di origine (file locali, dominio NIS, client LDAP) • Configurazione di rete (ad esempio, LIF e route)
Ricerca nome host non riuscita o scaduta e il server DNS non risolve i nomi brevi DNS (ad esempio, host1)	Configurazione DNS per query TLD (Top-Level Domain). È possibile disattivare le query TLD utilizzando `-is-tld-query-enabled false` al `vserver services name-service dns modify` comando.

Informazioni correlate

"Report tecnico di NetApp 4668: Guida alle Best practice per i servizi di nome"

Verificare le connessioni name service

A partire da ONTAP 9.2, è possibile controllare i server dei nomi DNS e LDAP per verificare che siano connessi a ONTAP. Questi comandi sono disponibili a livello di privilegi di amministratore.

A proposito di questa attività

È possibile verificare la presenza di una configurazione DNS o LDAP name service valida in base alle necessità utilizzando il controllo della configurazione del name service. Questo controllo di convalida può essere avviato dalla riga di comando o in System Manager.

Per le configurazioni DNS, tutti i server sono testati e devono funzionare perché la configurazione sia considerata valida. Per le configurazioni LDAP, se un server è attivo, la configurazione è valida. I comandi name service applicano il controllo della configurazione, a meno che non lo sia `skip-config-validation` il campo è true (il valore predefinito è false).

Fase

1. Utilizzare il comando appropriato per controllare la configurazione di un name service. L'interfaccia utente visualizza lo stato dei server configurati.

Per verificare…	Utilizzare questo comando…
Stato della configurazione DNS	`vserver services name-service dns check`
Stato della configurazione 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 convalida della configurazione ha esito positivo se almeno uno dei server configurati (name-server/ldap-server) è raggiungibile e fornisce il servizio. Se alcuni server non sono raggiungibili, viene visualizzato un avviso.

Comandi per la gestione delle voci di switch name service

È possibile gestire le voci di name service switch creandole, visualizzandole, modificandole ed eliminandole.

Se si desidera…	Utilizzare questo comando…
Creare una voce name service switch	`vserver services name-service ns-switch create`
Nome visualizzato voci switch servizio	`vserver services name-service ns-switch show`
Modificare una voce di name service switch	`vserver services name-service ns-switch modify`
Consente di eliminare una voce di switch name service	`vserver services name-service ns-switch delete`

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

Informazioni correlate

"Report tecnico di NetApp 4668: Guida alle Best practice per i servizi di nome"

Comandi per la gestione della cache del name service

È possibile gestire la cache del name service modificando il valore TTL (Time To Live). Il valore TTL determina per quanto tempo le informazioni del servizio dei nomi sono persistenti nella cache.

Se si desidera modificare il valore TTL per…	Utilizzare questo comando…
Utenti UNIX	`vserver services name-service cache unix-user settings`
Gruppi UNIX	`vserver services name-service cache unix-group settings`
Netgroup UNIX	`vserver services name-service cache netgroups settings`
Host	`vserver services name-service cache hosts settings`
Appartenenza al gruppo	`vserver services name-service cache group-membership settings`

Informazioni correlate

"Comandi di ONTAP 9"

Comandi per la gestione delle mappature dei nomi

Esistono comandi ONTAP specifici per la gestione delle mappature dei nomi.

Se si desidera…	Utilizzare questo comando…
Creare una mappatura dei nomi	`vserver name-mapping create`
Inserire una mappatura dei nomi in una posizione specifica	`vserver name-mapping insert`
Visualizza mappature dei nomi	`vserver name-mapping show`
Scambiare la posizione di due mappature dei nomi NOTA: Non è consentito eseguire uno swap quando la mappatura dei nomi è configurata con una voce di qualificatore ip.	`vserver name-mapping swap`

Modificare una mappatura dei nomi	`vserver name-mapping modify`
Eliminare una mappatura dei nomi	`vserver name-mapping delete`
Convalidare la corretta mappatura dei nomi	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

Comandi per la gestione degli utenti UNIX locali

Esistono comandi ONTAP specifici per la gestione degli utenti UNIX locali.

Se si desidera…	Utilizzare questo comando…
Creare un utente UNIX locale	`vserver services name-service unix-user create`
Caricare utenti UNIX locali da un URI	`vserver services name-service unix-user load-from-uri`
Visualizzare gli utenti UNIX locali	`vserver services name-service unix-user show`
Modificare un utente UNIX locale	`vserver services name-service unix-user modify`
Eliminare un utente UNIX locale	`vserver services name-service unix-user delete`

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

Comandi per la gestione di gruppi UNIX locali

Esistono comandi ONTAP specifici per la gestione dei gruppi UNIX locali.

Se si desidera…	Utilizzare questo comando…
Creare un gruppo UNIX locale	`vserver services name-service unix-group create`
Aggiungere un utente a un gruppo UNIX locale	`vserver services name-service unix-group adduser`
Caricare i gruppi UNIX locali da un URI	`vserver services name-service unix-group load-from-uri`
Visualizzare i gruppi UNIX locali	`vserver services name-service unix-group show`

Modificare un gruppo UNIX locale	`vserver services name-service unix-group modify`
Eliminare un utente da un gruppo UNIX locale	`vserver services name-service unix-group deluser`
Eliminare un gruppo UNIX locale	`vserver services name-service unix-group delete`

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

Limiti per utenti UNIX locali, gruppi e membri del gruppo

ONTAP ha introdotto limiti per il numero massimo di utenti e gruppi UNIX nel cluster e comandi per gestire questi limiti. Questi limiti possono aiutare a evitare problemi di performance impedendo agli amministratori di creare troppi utenti e gruppi UNIX locali nel cluster.

Esiste un limite per il numero combinato di gruppi di utenti UNIX locali e di membri del gruppo. Esiste un limite separato per gli utenti UNIX locali. I limiti sono a livello di cluster. Ciascuno di questi nuovi limiti viene impostato su un valore predefinito che è possibile modificare fino a un limite massimo preassegnato.

Database	Limite predefinito	Limite massimo
Utenti UNIX locali	32,768	65,536
Gruppi UNIX locali e membri del gruppo	32,768	65,536

Gestire i limiti per utenti e gruppi UNIX locali

Esistono comandi ONTAP specifici per la gestione dei limiti per utenti e gruppi UNIX locali. Gli amministratori dei cluster possono utilizzare questi comandi per risolvere i problemi di performance nel cluster che si ritiene siano correlati a un numero eccessivo di utenti e gruppi UNIX locali.

A proposito di questa attività

Questi comandi sono disponibili per l'amministratore del cluster a livello di privilegi avanzati.

Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera…	Utilizzare il comando…
Visualizza informazioni sui limiti utente UNIX locali	`vserver services unix-user max-limit show`

Se si desidera…	Utilizzare il comando…
Visualizza informazioni sui limiti dei gruppi UNIX locali	`vserver services unix-group max-limit show`
Modificare i limiti utente UNIX locali	`vserver services unix-user max-limit modify`
Modificare i limiti dei gruppi UNIX locali	`vserver services unix-group max-limit modify`

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

Comandi per la gestione dei netgroup locali

È possibile gestire i netgroup locali caricandoli da un URI, verificandone lo stato tra i nodi, visualizzandoli ed eliminandoli.

Se si desidera…	Utilizzare il comando…
Caricare i netgroup da un URI	`vserver services name-service netgroup load`
Verificare lo stato dei netgroup nei nodi	`vserver services name-service netgroup status` Disponibile a un livello di privilegio avanzato e superiore.
Visualizzare i netgroup locali	`vserver services name-service netgroup file show`
Eliminare un netgroup locale	`vserver services name-service netgroup file delete`

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

Comandi per la gestione delle configurazioni di dominio NIS

Esistono comandi ONTAP specifici per la gestione delle configurazioni di dominio NIS.

Se si desidera…	Utilizzare questo comando…
Creare una configurazione di dominio NIS	`vserver services name-service nis-domain create`
Visualizzare le configurazioni di dominio NIS	`vserver services name-service nis-domain show`

Visualizza lo stato di binding di una configurazione di dominio NIS	`vserver services name-service nis-domain show-bound`
Visualizzare le statistiche NIS	`vserver services name-service nis-domain show-statistics` Disponibile a un livello di privilegio avanzato e superiore.
Cancellare le statistiche NIS	`vserver services name-service nis-domain clear-statistics` Disponibile a un livello di privilegio avanzato e superiore.
Modificare una configurazione di dominio NIS	`vserver services name-service nis-domain modify`
Eliminare una configurazione di dominio NIS	`vserver services name-service nis-domain delete`
Abilitare il caching per le ricerche netgroup-by-host	`vserver services name-service nis-domain netgroup-database config modify` Disponibile a un livello di privilegio avanzato e superiore.

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

Comandi per la gestione delle configurazioni del client LDAP

Esistono comandi ONTAP specifici per la gestione delle configurazioni del client LDAP.

> Gli amministratori SVM non possono modificare o eliminare le configurazioni client LDAP create dagli amministratori del cluster.

Se si desidera…	Utilizzare questo comando…
Creare una configurazione del client LDAP	`vserver services name-service ldap client create`
Visualizzare le configurazioni del client LDAP	`vserver services name-service ldap client show`
Modificare una configurazione del client LDAP	`vserver services name-service ldap client modify`
Modificare la password BIND del client LDAP	`vserver services name-service ldap client modify-bind-password`
Eliminare una configurazione del client LDAP	`vserver services name-service ldap client delete`

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

Comandi per la gestione delle configurazioni LDAP

Esistono comandi ONTAP specifici per la gestione delle configurazioni LDAP.

Se si desidera…	Utilizzare questo comando…
Creare una configurazione LDAP	`vserver services name-service ldap create`
Visualizzare le configurazioni LDAP	`vserver services name-service ldap show`
Modificare una configurazione LDAP	`vserver services name-service ldap modify`
Eliminare una configurazione LDAP	`vserver services name-service ldap delete`

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

Comandi per la gestione dei modelli di schema del client LDAP

Esistono comandi ONTAP specifici per la gestione dei modelli di schema del client LDAP.

> Gli amministratori di SVM non possono modificare o eliminare gli schemi client LDAP creati dagli amministratori del cluster.

Se si desidera…	Utilizzare questo comando…
Copiare un modello di schema LDAP esistente	`vserver services name-service ldap client schema copy` Disponibile a un livello di privilegio avanzato e superiore.
Visualizzare i modelli di schema LDAP	`vserver services name-service ldap client schema show`
Modificare un modello di schema LDAP	`vserver services name-service ldap client schema modify` Disponibile a un livello di privilegio avanzato e superiore.
Eliminare un modello di schema LDAP	`vserver services name-service ldap client schema delete` Disponibile a un livello di privilegio avanzato e superiore.

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

Comandi per la gestione delle configurazioni dell'interfaccia Kerberos NFS

Esistono comandi ONTAP specifici per la gestione delle configurazioni dell'interfaccia Kerberos NFS.

Se si desidera…	Utilizzare questo comando…
Abilitare NFS Kerberos su una LIF	`vserver nfs kerberos interface enable`
Visualizzare le configurazioni dell'interfaccia Kerberos NFS	`vserver nfs kerberos interface show`
Modificare una configurazione dell'interfaccia Kerberos NFS	`vserver nfs kerberos interface modify`
Disattiva NFS Kerberos su LIF	`vserver nfs kerberos interface disable`

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

Comandi per la gestione delle configurazioni del realm Kerberos NFS

Esistono comandi ONTAP specifici per la gestione delle configurazioni di autenticazione Kerberos NFS.

Se si desidera…	**Utilizzare questo comando…**
Creare una configurazione di autenticazione Kerberos NFS	`vserver nfs kerberos realm create`
Visualizzare le configurazioni del realm Kerberos NFS	`vserver nfs kerberos realm show`
Modificare la configurazione di un realm Kerberos NFS	`vserver nfs kerberos realm modify`
Eliminare una configurazione di autenticazione Kerberos NFS	`vserver nfs kerberos realm delete`

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

Comandi per la gestione delle policy di esportazione

Esistono comandi ONTAP specifici per la gestione delle policy di esportazione.

Se si desidera…	Utilizzare questo comando…
Visualizza informazioni sui criteri di esportazione	`vserver export-policy show`
Rinominare un criterio di esportazione	`vserver export-policy rename`
Copiare una policy di esportazione	`vserver export-policy copy`
Eliminare una policy di esportazione	`vserver export-policy delete`

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

Comandi per la gestione delle regole di esportazione

Esistono comandi ONTAP specifici per la gestione delle regole di esportazione.

Se si desidera…	Utilizzare questo comando…
Creare una regola di esportazione	`vserver export-policy rule create`
Visualizza le informazioni sulle regole di esportazione	`vserver export-policy rule show`
Modificare una regola di esportazione	`vserver export-policy rule modify`
Eliminare una regola di esportazione	`vserver export-policy rule delete`

Se sono state configurate più regole di esportazione identiche corrispondenti a client diversi, assicurarsi di mantenerle sincronizzate durante la gestione delle regole di esportazione.

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

Configurare la cache delle credenziali NFS

Motivi per modificare il time-to-live della cache delle credenziali NFS

ONTAP utilizza una cache delle credenziali per memorizzare le informazioni necessarie per l'autenticazione dell'utente per l'accesso all'esportazione NFS, in modo da fornire un accesso più rapido e migliorare le performance. È possibile configurare per quanto tempo le informazioni vengono memorizzate nella cache delle credenziali per personalizzarle in base all'ambiente in uso.

La modifica del TTL (Time-to-live) della cache delle credenziali NFS può aiutare a risolvere i problemi in diversi

scenari. È necessario comprendere quali sono questi scenari e le conseguenze di tali modifiche.

Motivi

Modificare il TTL predefinito nei seguenti casi:

Problema	Azione correttiva
I name server nel tuo ambiente stanno riscontrando un peggioramento delle performance dovuto a un elevato carico di richieste da parte di ONTAP.	Aumentare il TTL per le credenziali positive e negative memorizzate nella cache per ridurre il numero di richieste da ONTAP ai server dei nomi.
L'amministratore del name server ha apportato delle modifiche per consentire l'accesso agli utenti NFS precedentemente rifiutati.	Ridurre il TTL per le credenziali negative memorizzate nella cache per ridurre il tempo di attesa che gli utenti NFS debbano attendere che ONTAP richieda nuove credenziali ai server dei nomi esterni in modo che possano accedervi.
L'amministratore del name server ha apportato delle modifiche per negare l'accesso agli utenti NFS precedentemente autorizzati.	Riduci il TTL per le credenziali positive memorizzate nella cache per ridurre il tempo prima che ONTAP richieda nuove credenziali ai server dei nomi esterni, in modo che gli utenti NFS non possano accedere.

Conseguenze

È possibile modificare la durata del tempo singolarmente per il caching delle credenziali positive e negative. Tuttavia, è necessario essere consapevoli dei vantaggi e degli svantaggi di tale operazione.

Se…	Il vantaggio è…	Lo svantaggio è…
Aumentare il tempo di cache delle credenziali positive	ONTAP invia le richieste di credenziali ai server dei nomi con minore frequenza, riducendo il carico sui server dei nomi.	Ci vuole più tempo per negare l'accesso agli utenti NFS a cui in precedenza era consentito l'accesso ma che non sono più disponibili.
Ridurre il tempo di cache delle credenziali positive	È necessario meno tempo per negare l'accesso agli utenti NFS a cui in precedenza era consentito l'accesso ma che non sono più disponibili.	ONTAP invia più frequentemente richieste di credenziali ai server dei nomi, aumentando il carico sui server dei nomi.
Aumentare il tempo di cache delle credenziali negative	ONTAP invia le richieste di credenziali ai server dei nomi con minore frequenza, riducendo il carico sui server dei nomi.	Occorre più tempo per concedere l'accesso agli utenti NFS che in precedenza non avevano accesso, ma che ora lo sono.

Se…	Il vantaggio è…	Lo svantaggio è…
Ridurre il tempo di cache delle credenziali negative	Occorrono meno tempo per concedere l'accesso agli utenti NFS che in precedenza non avevano accesso, ma che ora lo sono.	ONTAP invia più frequentemente richieste di credenziali ai server dei nomi, aumentando il carico sui server dei nomi.

Configurare il time-to-live per le credenziali utente NFS memorizzate nella cache

È possibile configurare il periodo di tempo in cui ONTAP memorizza le credenziali degli utenti NFS nella cache interna (time-to-live o TTL) modificando il server NFS della macchina virtuale di storage (SVM). In questo modo è possibile ridurre alcuni problemi legati all'elevato carico sui server dei nomi o alle modifiche delle credenziali che influiscono sull'accesso degli utenti NFS.

A proposito di questa attività

Questi parametri sono disponibili a livello di privilegio avanzato.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

   ```
   set -privilege advanced
   ```

2. Eseguire l'azione desiderata:

Se si desidera modificare il TTL per la cache…	Utilizzare il comando…
Credenziali positive	`vserver nfs modify -vserver vserver_name -cached -cred-positive-ttl time_to_live` Il TTL viene misurato in millisecondi. A partire da ONTAP 9.10.1 e versioni successive, il valore predefinito è 1 ora (3.600.000 millisecondi). In ONTAP 9.9.1 e versioni precedenti, il valore predefinito è 24 ore (86.400.000 millisecondi). L'intervallo consentito per questo valore è compreso tra 1 minuto (60000 millisecondi) e 7 giorni (604,800,000 millisecondi).
Credenziali negative	`vserver nfs modify -vserver vserver_name -cached -cred-negative-ttl time_to_live` Il TTL viene misurato in millisecondi. L'impostazione predefinita è 2 ore (7,200,000 millisecondi). L'intervallo consentito per questo valore è compreso tra 1 minuto (60000 millisecondi) e 7 giorni (604,800,000 millisecondi).

3. Tornare al livello di privilegio admin:

   ```
   set -privilege admin
   ```

Gestire le cache delle policy di esportazione

Svuotare le cache delle policy di esportazione

ONTAP utilizza diverse cache delle policy di esportazione per memorizzare le informazioni relative alle policy di esportazione per un accesso più rapido. L'operazione di cancellazione della policy di esportazione viene eseguita manualmente nella cache (`vserver export-policy cache flush`) Rimuove le informazioni potenzialmente obsolete e costringe ONTAP a recuperare le informazioni correnti dalle risorse esterne appropriate. Questo può aiutare a risolvere una serie di problemi relativi all'accesso client alle esportazioni NFS.

A proposito di questa attività

Le informazioni della cache delle policy di esportazione potrebbero essere obsolete a causa dei seguenti motivi:

- Una recente modifica alle regole dei criteri di esportazione
- Una recente modifica ai record dei nomi host nei server dei nomi
- Una recente modifica alle voci di netgroup nei server dei nomi
- Ripristino da un'interruzione di rete che ha impedito il caricamento completo dei netgroup

Fasi

1. Se la cache del servizio nomi non è attivata, eseguire una delle seguenti operazioni in modalità privilegio avanzato:

Se si desidera eseguire il lavaggio…	Immettere il comando…
Tutte le cache delle policy di esportazione (ad eccezione di showmount)	`vserver export-policy cache flush -vserver vserver_name`
La policy di esportazione regola l'accesso alla cache	`vserver export-policy cache flush -vserver vserver_name -cache access` È possibile includere il opzionale `-node` parametro per specificare il nodo su cui si desidera svuotare la cache di accesso.
La cache dei nomi host	`vserver export-policy cache flush -vserver vserver_name -cache host`
La cache del netgroup	`vserver export-policy cache flush -vserver vserver_name -cache netgroup` L'elaborazione dei netgroup richiede un uso intensivo delle risorse. È necessario svuotare la cache del netgroup solo se si tenta di risolvere un problema di accesso client causato da un netgroup obsoleto.

Se si desidera eseguire il lavaggio…	Immettere il comando…
La cache di showmount	`vserver export-policy cache flush -vserver vserver_name -cache showmount`

2. Se la cache del name service è attivata, eseguire una delle seguenti operazioni:

Se si desidera eseguire il lavaggio…	Immettere il comando…
La policy di esportazione regola l'accesso alla cache	`vserver export-policy cache flush -vserver vserver_name -cache access` È possibile includere il opzionale `-node` parametro per specificare il nodo su cui si desidera svuotare la cache di accesso.
La cache dei nomi host	`vserver services name-service cache hosts forward-lookup delete-all`
La cache del netgroup	`vserver services name-service cache netgroups ip-to-netgroup delete-all` `vserver services name-service cache netgroups members delete-all` L'elaborazione dei netgroup richiede un uso intensivo delle risorse. È necessario svuotare la cache del netgroup solo se si tenta di risolvere un problema di accesso client causato da un netgroup obsoleto.
La cache di showmount	`vserver export-policy cache flush -vserver vserver_name -cache showmount`

Visualizza la coda e la cache del netgroup dei criteri di esportazione

ONTAP utilizza la coda netgroup per importare e risolvere i netgroup e la cache netgroup per memorizzare le informazioni risultanti. Durante la risoluzione dei problemi relativi ai netgroup di policy di esportazione, è possibile utilizzare `vserver export-policy netgroup queue show` e. `vserver export-policy netgroup cache show` comandi per visualizzare lo stato della coda netgroup e il contenuto della cache netgroup.

Fase

1. Eseguire una delle seguenti operazioni:

Per visualizzare il netgroup dei criteri di esportazione…	Immettere il comando…
Coda	`vserver export-policy netgroup queue show`

Cache	`vserver export-policy netgroup cache show -vserver vserver_name`

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

Verificare se un indirizzo IP del client è membro di un netgroup

Durante la risoluzione dei problemi di accesso al client NFS relativi ai netgroup, è possibile utilizzare `vserver export-policy netgroup check-membership` Per determinare se un IP client è membro di un determinato netgroup.

A proposito di questa attività

La verifica dell'appartenenza a netgroup consente di determinare se ONTAP è consapevole che un client è o meno membro di un netgroup. Consente inoltre di sapere se la cache del netgroup ONTAP si trova in uno stato transitorio durante l'aggiornamento delle informazioni del netgroup. Queste informazioni possono aiutarti a capire perché a un client potrebbe essere concesso o negato l'accesso in modo imprevisto.

Fase

1. Verificare l'appartenenza al netgroup di un indirizzo IP client: `vserver export-policy netgroup check-membership -vserver vserver_name -netgroup netgroup_name -client-ip client_ip`

   Il comando può restituire i seguenti risultati:

   - Il client è membro del netgroup.

     Ciò è stato confermato mediante una ricerca inversa o una ricerca netgroup-by-host.

   - Il client è membro del netgroup.

     È stato trovato nella cache del netgroup di ONTAP.

   - Il client non è membro del netgroup.
   - L'appartenenza del client non può ancora essere determinata perché ONTAP sta aggiornando la cache del netgroup.

     Fino a quando ciò non viene fatto, l'appartenenza non può essere esplicitamente esclusa o esclusa. Utilizzare `vserver export-policy netgroup queue show` comando per monitorare il caricamento del netgroup e riprovare il controllo al termine.

Esempio

Nell'esempio seguente viene verificato se un client con l'indirizzo IP 172.17.16.72 è membro del netgroup Mercury su SVM vs1:

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

Ottimizza le performance della cache di accesso

È possibile configurare diversi parametri per ottimizzare la cache di accesso e trovare il giusto equilibrio tra le prestazioni e la corrente delle informazioni memorizzate nella cache di accesso.

A proposito di questa attività

Quando si configurano i periodi di aggiornamento della cache di accesso, tenere presente quanto segue:

- Valori più elevati significano che le voci rimangono più lunghe nella cache di accesso.

  Il vantaggio è rappresentato dalle performance migliori, in quanto ONTAP spende meno risorse per il refresh delle voci della cache di accesso. Lo svantaggio è che se le regole dei criteri di esportazione cambiano e le voci della cache di accesso diventano obsolete, l'aggiornamento richiede più tempo. Di conseguenza, i client che dovrebbero ottenere l'accesso potrebbero essere rifiutati e i client che dovrebbero ottenere l'accesso potrebbero ottenere l'accesso.

- Valori più bassi significano che ONTAP aggiorna più spesso le voci della cache di accesso.

  Il vantaggio è che le voci sono più aggiornate e i client hanno maggiori probabilità di ottenere o negare l'accesso correttamente. Lo svantaggio è una diminuzione delle performance perché ONTAP spende più risorse per aggiornare le voci della cache di accesso.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

   ```
   set -privilege advanced
   ```

2. Eseguire l'azione desiderata:

Per modificare…	Inserisci…
Periodo di refresh per voci positive	`vserver export-policy access-cache config modify-all-vservers -refresh -period-positive timeout_value`
Periodo di refresh per le voci negative	`vserver export-policy access-cache config modify-all-vservers -refresh -period-negative timeout_value`
Periodo di timeout per le voci precedenti	`vserver export-policy access-cache config modify-all-vservers -harvest -timeout timeout_value`

3. Verificare le nuove impostazioni dei parametri:

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

4. Tornare al livello di privilegio admin:

   ```
   set -privilege admin
   ```

Gestire i blocchi dei file

Informazioni sul blocco dei file tra protocolli

Il blocco dei file è un metodo utilizzato dalle applicazioni client per impedire a un utente di accedere a un file precedentemente aperto da un altro utente. Il modo in cui ONTAP blocca i file dipende dal protocollo del client.

Se il client è un client NFS, i blocchi sono avvisi; se il client è un client SMB, i blocchi sono obbligatori.

A causa delle differenze tra i blocchi di file NFS e SMB, un client NFS potrebbe non riuscire ad accedere a un file precedentemente aperto da un'applicazione SMB.

Quando un client NFS tenta di accedere a un file bloccato da un'applicazione SMB, si verifica quanto segue:

- In volumi misti o NTFS, operazioni di manipolazione dei file come `rm`, `rmdir`, e. `mv` Può causare il malfunzionamento dell'applicazione NFS.
- Le operazioni di lettura e scrittura NFS sono negate rispettivamente dalle modalità aperta di negazione-lettura e di negazione-scrittura di SMB.
- Le operazioni di scrittura NFS non riescono quando l'intervallo scritto del file è bloccato con un esclusivo bytelock SMB.

Nei volumi UNIX di sicurezza, le operazioni di sconnessione e ridenominazione NFS ignorano lo stato di blocco SMB e consentono l'accesso al file. Tutte le altre operazioni NFS sui volumi UNIX di sicurezza rispettano lo stato di blocco SMB.

Come ONTAP tratta i bit di sola lettura

Il bit di sola lettura viene impostato file per file per indicare se un file è scrivibile (disattivato) o di sola lettura (abilitato).

I client SMB che utilizzano Windows possono impostare un bit di sola lettura per ogni file. I client NFS non impostano un bit di sola lettura per ogni file perché i client NFS non eseguono operazioni di protocollo che utilizzano un bit di sola lettura per ogni file.

ONTAP può impostare un bit di sola lettura su un file quando un client SMB che utilizza Windows crea tale file. ONTAP può anche impostare un bit di sola lettura quando un file viene condiviso tra client NFS e client SMB. Alcuni software, se utilizzati dai client NFS e dai client SMB, richiedono l'abilitazione del bit di sola lettura.

Affinché ONTAP mantenga le autorizzazioni di lettura e scrittura appropriate su un file condiviso tra client NFS e client SMB, tratta il bit di sola lettura in base alle seguenti regole:

- NFS considera qualsiasi file con il bit di sola lettura abilitato come se non abbia alcun bit di permesso di scrittura abilitato.
- Se un client NFS disattiva tutti i bit di permesso di scrittura e almeno uno di questi bit era stato precedentemente attivato, ONTAP attiva il bit di sola lettura per quel file.
- Se un client NFS attiva qualsiasi bit di autorizzazione di scrittura, ONTAP disattiva il bit di sola lettura per quel file.
- Se il bit di sola lettura per un file è attivato e un client NFS tenta di rilevare le autorizzazioni per il file, i bit di autorizzazione per il file non vengono inviati al client NFS; invece, ONTAP invia i bit di autorizzazione al client NFS con i bit di autorizzazione di scrittura mascherati.

- Se il bit di sola lettura per un file è attivato e un client SMB disattiva il bit di sola lettura, ONTAP attiva il bit di autorizzazione di scrittura del proprietario per il file.
- I file con il bit di sola lettura abilitato sono scrivibili solo da root.

> Le modifiche alle autorizzazioni dei file hanno effetto immediato sui client SMB, ma potrebbero non avere effetto immediato sui client NFS se il client NFS attiva il caching degli attributi.

In che modo ONTAP si differenzia da Windows per la gestione dei blocchi sui componenti del percorso di condivisione

A differenza di Windows, ONTAP non blocca ogni componente del percorso di un file aperto mentre il file è aperto. Questo comportamento influisce anche sui percorsi di condivisione SMB.

Poiché ONTAP non blocca ogni componente del percorso, è possibile rinominare un componente del percorso sopra il file aperto o la condivisione, che può causare problemi per alcune applicazioni o causare l'invalidità del percorso di condivisione nella configurazione SMB. Questo può rendere la condivisione inaccessibile.

Per evitare problemi causati dalla ridenominazione dei componenti del percorso, è possibile applicare le impostazioni di protezione dell'elenco di controllo di accesso Windows (ACL) che impediscono agli utenti o alle applicazioni di rinominare le directory critiche.

Scopri di più "Come impedire che le directory vengano rinominate mentre i client le accedono".

Visualizza informazioni sui blocchi

È possibile visualizzare informazioni sui blocchi di file correnti, inclusi i tipi di blocchi che vengono conservati e lo stato di blocco, i dettagli sui blocchi dell'intervallo di byte, le modalità sharelock, i blocchi di delega e i blocchi opportunistici e se i blocchi vengono aperti con handle durevoli o persistenti.

A proposito di questa attività

L'indirizzo IP del client non può essere visualizzato per i blocchi stabiliti tramite NFSv4 o NFSv4.1.

Per impostazione predefinita, il comando visualizza le informazioni relative a tutti i blocchi. È possibile utilizzare i parametri dei comandi per visualizzare informazioni sui blocchi di una specifica macchina virtuale di storage (SVM) o per filtrare l'output del comando in base ad altri criteri.

Il `vserver locks show` il comando visualizza informazioni su quattro tipi di blocchi:

- Blocchi byte-range, che bloccano solo una parte di un file.
- Blocchi di condivisione che bloccano i file aperti.
- Blocchi opportunistici, che controllano il caching lato client su SMB.
- Deleghe, che controllano il caching lato client su NFSv4.x.

Specificando i parametri opzionali, è possibile determinare informazioni importanti su ciascun tipo di blocco. Per ulteriori informazioni, vedere la pagina man per il comando.

Fase

1. Visualizzare le informazioni sui blocchi utilizzando `vserver locks show` comando.

Esempi

Nell'esempio riportato di seguito vengono visualizzate informazioni riepilogative per un blocco NFSv4 su un file con il percorso `/vol1/file1`. La modalità di accesso sharelock è write-deny_none e il blocco è stato concesso con delega di scrittura:

```
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
```

Nell'esempio riportato di seguito vengono visualizzate informazioni dettagliate sull'oplock e sullo sharlock relative al blocco SMB in un file con il percorso `/data2/data2_2/intro.pptx`. Un handle durevole viene concesso sul file con una modalità di accesso con blocco della condivisione write-deny_none a un client con un indirizzo IP 10.3.1.3. Un oplock di leasing viene concesso con un livello di oplock batch:

```
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
```

Blocchi di rottura

Quando i blocchi di file impediscono l'accesso dei client ai file, è possibile visualizzare le informazioni sui blocchi attualmente in attesa e quindi interrompere blocchi specifici. Esempi di scenari in cui potrebbe essere necessario interrompere i blocchi includono il debug delle applicazioni.

A proposito di questa attività

Il `vserver locks break` il comando è disponibile solo a un livello di privilegio avanzato e superiore. La pagina man del comando contiene informazioni dettagliate.

Fasi

1. Per trovare le informazioni necessarie per interrompere un blocco, utilizzare `vserver locks show` comando.

   La pagina man del comando contiene informazioni dettagliate.

2. Impostare il livello di privilegio su Advanced (avanzato):

   ```
   set -privilege advanced
   ```

3. Eseguire una delle seguenti operazioni:

Se si desidera interrompere un blocco specificando…	Immettere il comando…
Il nome SVM, il nome del volume, il nome LIF e il percorso del file	`vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif`
L'ID blocco	`vserver locks break -lockid UUID`

4. Tornare al livello di privilegio admin:

   ```
   set -privilege admin
   ```

Come funzionano i filtri FPolicy first-Read e first-write con NFS

I client NFS sperimentano tempi di risposta elevati durante il traffico elevato delle richieste di lettura/scrittura quando FPolicy viene abilitato utilizzando un server FPolicy esterno con operazioni di lettura/scrittura come eventi monitorati. Per i client NFS, l'utilizzo di filtri di prima lettura e prima scrittura in FPolicy riduce il numero di notifiche FPolicy e migliora le performance.

In NFS, il client esegue l'i/o su un file mediante il recupero dell'handle. Questo handle potrebbe rimanere valido per i riavvii del server e del client. Pertanto, il client è libero di memorizzare nella cache l'handle e di inviarne le richieste senza dover recuperare nuovamente gli handle. In una sessione regolare, molte richieste di lettura/scrittura vengono inviate al file server. Se vengono generate notifiche per tutte queste richieste, potrebbero verificarsi i seguenti problemi:

- Un carico maggiore grazie all'elaborazione aggiuntiva delle notifiche e a tempi di risposta più elevati.
- Un gran numero di notifiche inviate al server FPolicy anche se il server non è interessato da tutte le notifiche.

Dopo aver ricevuto la prima richiesta di lettura/scrittura da un client per un determinato file, viene creata una voce della cache e il conteggio di lettura/scrittura viene incrementato. Questa richiesta viene contrassegnata come prima operazione di lettura/scrittura e viene generato un evento FPolicy. Prima di pianificare e creare i filtri FPolicy per un client NFS, è necessario comprendere le nozioni di base sul funzionamento dei filtri FPolicy.

- First-Read (prima lettura): Filtra le richieste di lettura del client per la prima lettura.

  Quando questo filtro viene utilizzato per gli eventi NFS, il `-file-session-io-grouping-count` e. `-file-session-io-grouping-duration` Le impostazioni determinano la richiesta di prima lettura per la quale viene elaborato FPolicy.

- First-write: Filtra le richieste di scrittura del client per la first-write.

Quando questo filtro viene utilizzato per gli eventi NFS, il `-file-session-io-grouping-count` e. `-file-session-io-grouping-duration` Le impostazioni determinano la richiesta di prima scrittura per la quale FPolicy ha elaborato.

Le seguenti opzioni vengono aggiunte nel database dei server 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
```

Modificare l'ID di implementazione del server NFSv4.1

Il protocollo NFSv4.1 include un ID di implementazione del server che documenta il dominio, il nome e la data del server. È possibile modificare i valori predefiniti dell'ID di implementazione del server. La modifica dei valori predefiniti può essere utile, ad esempio, per la raccolta di statistiche di utilizzo o la risoluzione dei problemi di interoperabilità. Per ulteriori informazioni, vedere RFC 5661.

A proposito di questa attività

I valori predefiniti per le tre opzioni sono i seguenti:

Opzione	Nome dell'opzione	Valore predefinito
Dominio ID implementazione NFSv4.1	`-v4.1-implementation -domain`	netapp.com
Nome ID implementazione NFSv4.1	`-v4.1-implementation-name`	Nome della versione del cluster
Data ID implementazione NFSv4.1	`-v4.1-implementation-date`	Data di versione del cluster

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

   ```
   set -privilege advanced
   ```

2. Eseguire una delle seguenti operazioni:

Se si desidera modificare l'ID di implementazione NFSv4.1…	Immettere il comando…
Dominio	`vserver nfs modify -v4.1 -implementation-domain domain`

Se si desidera modificare l'ID di implementazione NFSv4.1…	Immettere il comando…
Nome	`vserver nfs modify -v4.1 -implementation-name name`
Data	`vserver nfs modify -v4.1 -implementation-date date`

3. Tornare al livello di privilegio admin:

   ```
   set -privilege admin
   ```

Gestire gli ACL NFSv4

Vantaggi dell'abilitazione degli ACL NFSv4

L'abilitazione degli ACL NFSv4 offre numerosi vantaggi.

I vantaggi derivanti dall'abilitazione degli ACL NFSv4 includono:

- Controllo più dettagliato dell'accesso degli utenti per file e directory
- Maggiore sicurezza NFS
- Maggiore interoperabilità con CIFS
- Rimozione del limite NFS di 16 gruppi per utente

Come funzionano gli ACL NFSv4

Un client che utilizza ACL NFSv4 può impostare e visualizzare ACL su file e directory del sistema. Quando viene creato un nuovo file o sottodirectory in una directory che dispone di un ACL, il nuovo file o sottodirectory eredita tutte le voci ACL (ACL) nell'ACL contrassegnate con gli indicatori di ereditarietà appropriati.

Quando viene creato un file o una directory come risultato di una richiesta NFSv4, l'ACL del file o della directory risultante dipende dal fatto che la richiesta di creazione del file includa un ACL o solo permessi di accesso ai file UNIX standard e se la directory principale dispone di un ACL:

- Se la richiesta include un ACL, viene utilizzato tale ACL.
- Se la richiesta include solo autorizzazioni di accesso ai file UNIX standard ma la directory principale dispone di un ACL, le ACE nell'ACL della directory principale vengono ereditate dal nuovo file o directory, purché le ACE siano state contrassegnate con gli indicatori di ereditarietà appropriati.

  > Un ACL padre viene ereditato anche se `-v4.0-acl` è impostato su `off`.

- Se la richiesta include solo le autorizzazioni di accesso ai file UNIX standard e la directory principale non dispone di un ACL, la modalità file client viene utilizzata per impostare le autorizzazioni di accesso ai file UNIX standard.

- Se la richiesta include solo le autorizzazioni di accesso ai file UNIX standard e la directory principale dispone di un ACL non ereditabile, il nuovo oggetto viene creato solo con i bit di modalità.

> Se il `-chown-mode` il parametro è stato impostato su `restricted` con i comandi in `vserver nfs` oppure `vserver export-policy rule` Famiglie, la proprietà del file può essere modificata solo dal superutente, anche se le autorizzazioni su disco impostate con gli ACL NFSv4 consentono a un utente non root di modificare la proprietà del file. Per ulteriori informazioni, consulta le relative pagine man.

Attiva o disattiva la modifica degli ACL NFSv4

Quando ONTAP riceve un `chmod` Per un file o una directory con un ACL, per impostazione predefinita l'ACL viene conservato e modificato per riflettere la modifica del bit di modalità. È possibile disattivare `-v4-acl-preserve` Parametro per modificare il comportamento se si desidera che l'ACL venga eliminato.

A proposito di questa attività

Quando si utilizza uno stile di sicurezza unificato, questo parametro specifica anche se le autorizzazioni del file NTFS vengono mantenute o interrotte quando un client invia un comando chmod, chgroup o chown per un file o una directory.

L'impostazione predefinita per questo parametro è Enabled (attivato).

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

   ```
   set -privilege advanced
   ```

2. Eseguire una delle seguenti operazioni:

Se si desidera…	Immettere il seguente comando…
Attiva conservazione e modifica degli ACL NFSv4 esistenti (impostazione predefinita)	`vserver nfs modify -vserver vserver_name -v4-acl -preserve enabled`
Disattiva la conservazione e disattiva gli ACL NFSv4 quando si modificano i bit di modalità	`vserver nfs modify -vserver vserver_name -v4-acl -preserve disabled`

3. Tornare al livello di privilegio admin:

   ```
   set -privilege admin
   ```

Come ONTAP utilizza gli ACL NFSv4 per determinare se è in grado di eliminare un file

Per determinare se è possibile eliminare un file, ONTAP utilizza una combinazione del bit DELETE del file e del bit DELETE_CHILD della directory contenente. Per ulteriori

informazioni, vedere NFS 4.1 RFC 5661.

Attivare o disattivare gli ACL NFSv4

Per attivare o disattivare gli ACL NFSv4, è possibile modificare `-v4.0-acl` e. `-v4.1 -acl` opzioni. Queste opzioni sono disattivate per impostazione predefinita.

A proposito di questa attività

Il `-v4.0-acl` oppure `-v4.1-acl` L'opzione controlla l'impostazione e la visualizzazione degli ACL NFSv4; non controlla l'applicazione di questi ACL per il controllo degli accessi.

Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera…	Quindi…
Abilitare gli ACL NFSv4.0	Immettere il seguente comando: `vserver nfs modify -vserver vserver_name -v4.0-acl enabled`
Disattivare gli ACL NFSv4.0	Immettere il seguente comando: `vserver nfs modify -vserver vserver_name -v4.0-acl disabled`
Abilitare gli ACL NFSv4.1	Immettere il seguente comando: `vserver nfs modify -vserver vserver_name -v4.1-acl enabled`
Disattivare gli ACL NFSv4.1	Immettere il seguente comando: `vserver nfs modify -vserver vserver_name -v4.1-acl disabled`

Modificare il limite massimo ACE per gli ACL NFSv4

È possibile modificare il numero massimo di ACE consentiti per ogni ACL NFSv4 modificando il parametro `-v4-acl-max-aces`. Per impostazione predefinita, il limite è impostato su 400 ACE per ogni ACL. L'aumento di questo limite può contribuire a garantire una migrazione corretta dei dati con ACL contenenti oltre 400 ACE nei sistemi storage che eseguono ONTAP.

A proposito di questa attività

L'aumento di questo limite potrebbe influire sulle performance dei client che accedono ai file con ACL NFSv4.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

   ```
   set -privilege advanced
   ```

2. Modificare il limite massimo ACE per gli ACL NFSv4:

   ```
   vserver nfs modify -v4-acl-max-aces max_ace_limit
   ```

   L'intervallo valido di

   `max_ace_limit` è `192` a. `1024.`

3. Tornare al livello di privilegio admin:

   ```
   set -privilege admin
   ```

Gestire le deleghe dei file NFSv4

Attivare o disattivare le deleghe dei file di lettura NFSv4

Per attivare o disattivare le deleghe dei file di lettura NFSv4, è possibile modificare `-v4.0-read-delegation`oppure opzione. Attivando le deleghe dei file di lettura, è possibile eliminare gran parte dell'overhead dei messaggi associato all'apertura e alla chiusura dei file.

A proposito di questa attività

Per impostazione predefinita, le deleghe dei file di lettura sono disattivate.

Lo svantaggio dell'abilitazione delle deleghe dei file in lettura consiste nel fatto che il server e i suoi client devono ripristinare le deleghe dopo il riavvio o il riavvio del server, il riavvio o il riavvio di un client o la creazione di una partizione di rete.

Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera…	Quindi…
Abilitare le deleghe dei file di lettura NFSv4	Immettere il seguente comando: `vserver nfs modify -vserver vserver_name -v4.0 -read-delegation enabled`
Abilitare le deleghe dei file di lettura NFSv4.1	Immettere il seguente comando: + `vserver nfs modify -vserver vserver_name -v4.1 -read-delegation enabled`

Disattiva le deleghe dei file di lettura NFSv4	Immettere il seguente comando: `vserver nfs modify -vserver vserver_name -v4.0 -read-delegation disabled`
Disattiva le deleghe dei file di lettura NFSv4.1	Immettere il seguente comando: `vserver nfs modify -vserver vserver_name -v4.1 -read-delegation disabled`

Risultato

Le opzioni di delega dei file diventano effettive non appena vengono modificate. Non è necessario riavviare NFS.

Attivare o disattivare le deleghe dei file di scrittura NFSv4

Per attivare o disattivare le deleghe dei file di scrittura, è possibile modificare `-v4.0 -write-delegation`oppure opzione. Attivando le deleghe di scrittura dei file, è possibile eliminare gran parte dell'overhead dei messaggi associato al blocco di file e record, oltre all'apertura e alla chiusura dei file.

A proposito di questa attività

Per impostazione predefinita, le deleghe dei file di scrittura sono disattivate.

Lo svantaggio di abilitare le deleghe dei file di scrittura è che il server e i relativi client devono eseguire attività aggiuntive per ripristinare le deleghe dopo il riavvio o il riavvio del server, il riavvio o il riavvio di un client o la creazione di una partizione di rete.

Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera…	Quindi…
Abilitare le deleghe dei file di scrittura NFSv4	Immettere il seguente comando: `vserver nfs modify -vserver vserver_name -v4.0 -write-delegation enabled`
Abilitare le deleghe dei file di scrittura NFSv4.1	Immettere il seguente comando: `vserver nfs modify -vserver vserver_name -v4.1 -write-delegation enabled`
Disattiva le deleghe dei file di scrittura NFSv4	Immettere il seguente comando: `vserver nfs modify -vserver vserver_name -v4.0 -write-delegation disabled`

Se si desidera…	Quindi…
Disattivare le deleghe dei file di scrittura NFSv4.1	Immettere il seguente comando: `vserver nfs modify -vserver vserver_name -v4.1 -write-delegation disabled`

Risultato

Le opzioni di delega dei file diventano effettive non appena vengono modificate. Non è necessario riavviare NFS.

Configurare il blocco di file e record NFSv4

Informazioni sul blocco di file e record NFSv4

Per i client NFSv4, ONTAP supporta il meccanismo di blocco dei file NFSv4, mantenendo lo stato di tutti i blocchi dei file in un modello basato sul lease.

"Report tecnico di NetApp 3580: Guida ai miglioramenti e alle Best practice di NFSv4 per l'implementazione di Data ONTAP"

Specificare il periodo di lease di blocco NFSv4

Per specificare il periodo di leasing di blocco NFSv4 (ovvero, il periodo di tempo in cui ONTAP concede irrevocabilmente un blocco a un client), è possibile modificare `-v4 -lease-seconds` opzione. I periodi di leasing più brevi accelerano il ripristino dei server, mentre i periodi di leasing più lunghi sono vantaggiosi per i server che gestiscono un numero molto elevato di client.

A proposito di questa attività

Per impostazione predefinita, questa opzione è impostata su `30`. Il valore minimo per questa opzione è `10`. Il valore massimo per questa opzione è il periodo di tolleranza di blocco, che è possibile impostare con `locking.lease_seconds` opzione.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

   ```
   set -privilege advanced
   ```

2. Immettere il seguente comando:

   ```
   vserver nfs modify -vserver vserver_name -v4-lease-seconds number_of_seconds
   ```

3. Tornare al livello di privilegio admin:

   ```
   set -privilege admin
   ```

Specificare il periodo di tolleranza del blocco NFSv4

Per specificare il periodo di tolleranza del blocco NFSv4 (ovvero il periodo di tempo in cui i client tentano di recuperare il proprio stato di blocco da ONTAP durante il ripristino del server), è possibile modificare `-v4-grace-seconds` opzione.

A proposito di questa attività

Per impostazione predefinita, questa opzione è impostata su `45`.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

   ```
   set -privilege advanced
   ```

2. Immettere il seguente comando:

   ```
   vserver nfs modify -vserver vserver_name -v4-grace-seconds number_of_seconds
   ```

3. Tornare al livello di privilegio admin:

   ```
   set -privilege admin
   ```

Come funzionano i referral NFSv4

Quando si abilitano i riferimenti NFSv4, ONTAP fornisce i riferimenti “intra-SVM” ai client NFSv4. Il riferimento intra-SVM avviene quando un nodo del cluster che riceve la richiesta NFSv4 fa riferimento al client NFSv4 a un’altra interfaccia logica (LIF) sulla macchina virtuale di storage (SVM).

Il client NFSv4 deve accedere al percorso che ha ricevuto il riferimento alla LIF di destinazione da quel momento in poi. Il nodo del cluster originale fornisce tale riferimento quando determina l’esistenza di una LIF nella SVM residente sul nodo del cluster su cui risiede il volume di dati, consentendo ai client un accesso più rapido ai dati ed evitando comunicazioni del cluster aggiuntive.

Attiva o disattiva i riferimenti NFSv4

È possibile attivare i riferimenti NFSv4 sulle macchine virtuali di storage (SVM) attivando le opzioni `-v4-fsid-change` e. `-v4.0-referrals`oppure. L’attivazione dei riferimenti NFSV4 può accelerare l’accesso ai dati per i client NFSv4 che supportano questa funzionalità.

Di cosa hai bisogno

Se si desidera attivare i riferimenti NFS, è necessario prima disattivare Parallel NFS. Non è possibile attivare entrambi contemporaneamente.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

   ```
   set -privilege advanced
   ```

2. Eseguire una delle seguenti operazioni:

Se si desidera…	Immettere il comando…
Abilitare i riferimenti NFSv4	`vserver nfs modify -vserver vserver_name -v4-fsid -change enabled` `vserver nfs modify -vserver vserver_name -v4.0-referrals enabled`
Disattiva i riferimenti NFSv4	`vserver nfs modify -vserver vserver_name -v4.0 -referrals disabled`
Abilitare i riferimenti NFSv4.1	`vserver nfs modify -vserver vserver_name -v4-fsid -change enabled` `vserver nfs modify -vserver vserver_name -v4.1-referrals enabled`
Disattiva i riferimenti NFSv4.1	`vserver nfs modify -vserver vserver_name -v4.1 -referrals disabled`

3. Tornare al livello di privilegio admin:

   ```
   set -privilege admin
   ```

Visualizzare le statistiche NFS

È possibile visualizzare le statistiche NFS per le macchine virtuali di storage (SVM) sul sistema storage per monitorare le performance e diagnosticare i problemi.

Fasi

1. Utilizzare `statistics catalog object show` Per identificare gli oggetti NFS da cui è possibile visualizzare i dati.

   ```
   statistics catalog object show -object nfs*
   ```

2. Utilizzare `statistics start` e opzionale `statistics stop` comandi per raccogliere un campione di dati da uno o più oggetti.
3. Utilizzare `statistics show` per visualizzare i dati di esempio.

Esempio: Monitoraggio delle performance di NFSv3

L'esempio seguente mostra i dati relativi alle prestazioni per il protocollo NFSv3.

Il seguente comando avvia la raccolta dati per un nuovo campione:

```
vs1::> statistics start -object nfsv3 -sample-id nfs_sample
```

Il comando seguente mostra i dati dell'esempio specificando i contatori che mostrano il numero di richieste di lettura e scrittura riuscite rispetto al numero totale di richieste di lettura e scrittura:

```
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
```

Informazioni correlate

"Configurazione del monitoraggio delle performance"

Visualizzare le statistiche DNS

È possibile visualizzare le statistiche DNS per le macchine virtuali di storage (SVM) sul sistema di storage per monitorare le performance e diagnosticare i problemi.

Fasi

1. Utilizzare `statistics catalog object show` Per identificare gli oggetti DNS da cui è possibile visualizzare i dati.

   ```
   statistics catalog object show -object external_service_op*
   ```

2. Utilizzare `statistics start` e. `statistics stop` comandi per raccogliere un campione di dati da uno o più oggetti.
3. Utilizzare `statistics show` per visualizzare i dati di esempio.

Monitoraggio delle statistiche DNS

I seguenti esempi mostrano i dati relativi alle prestazioni per le query DNS. I seguenti comandi avviano la raccolta di dati per un nuovo campione:

```
vs1::*> statistics start -object external_service_op -sample-id
dns_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
dns_sample2
```

Il seguente comando visualizza i dati dell'esempio specificando i contatori che visualizzano il numero di query

DNS inviate rispetto al numero di query DNS ricevute, non riuscite o in timeout:

```
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.
```

Il seguente comando visualizza i dati dell'esempio specificando i contatori che visualizzano il numero di volte in cui è stato ricevuto un errore specifico per una query DNS sul server specifico:

```
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.
```

Informazioni correlate

"Configurazione del monitoraggio delle performance"

Visualizzare le statistiche NIS

È possibile visualizzare le statistiche NIS per le macchine virtuali di storage (SVM) sul sistema storage per monitorare le performance e diagnosticare i problemi.

Fasi

1. Utilizzare `statistics catalog object show` Per identificare gli oggetti NIS da cui è possibile visualizzare i dati.

   `statistics catalog object show -object external_service_op*`

2. Utilizzare `statistics start` e. `statistics stop` comandi per raccogliere un campione di dati da uno o più oggetti.
3. Utilizzare `statistics show` per visualizzare i dati di esempio.

Monitoraggio delle statistiche NIS

I seguenti esempi mostrano i dati relativi alle prestazioni per le query NIS. I seguenti comandi avviano la raccolta di dati per un nuovo campione:

```
vs1::*> statistics start -object external_service_op -sample-id
nis_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
nis_sample2
```

Il seguente comando visualizza i dati dell'esempio specificando i contatori che mostrano il numero di query NIS inviate rispetto al numero di query NIS ricevute, non riuscite o in timeout:

```
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.
```

Il seguente comando visualizza i dati dell'esempio specificando i contatori che indicano il numero di volte in cui è stato ricevuto un errore specifico per una query NIS sul server specifico:

```
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.
```

Informazioni correlate

"Configurazione del monitoraggio delle performance"

Supporto per VMware vStorage su NFS

ONTAP supporta alcune API vStorage VMware per l'integrazione degli array (VAAI) in un ambiente NFS.

Funzionalità supportate

Sono supportate le seguenti funzioni:

- Offload delle copie

  Consente a un host ESXi di copiare macchine virtuali o dischi di macchine virtuali (VMDK) direttamente tra la posizione dell'archivio dati di origine e di destinazione senza coinvolgere l'host. In questo modo si preservano i cicli della CPU host ESXi e la larghezza di banda della rete. L'offload delle copie preserva l'efficienza dello spazio se il volume di origine è sparso.

- Prenotazione di spazio

  Garantisce lo spazio di storage per un file VMDK riservando spazio all'IT.

Limitazioni

VMware vStorage su NFS presenta le seguenti limitazioni:

- Le operazioni di offload della copia possono avere esito negativo nei seguenti scenari:
  - Durante l'esecuzione di wafliron sul volume di origine o di destinazione, in quanto il volume viene temporaneamente disattivato
  - Durante lo spostamento del volume di origine o di destinazione
  - Durante lo spostamento della LIF di origine o di destinazione
  - Durante l'esecuzione di operazioni di Takeover o giveback
  - Durante le operazioni di switchover o switchback
- La copia lato server potrebbe non riuscire a causa delle differenze di formato del file handle nel seguente scenario:

  Si tenta di copiare i dati dalle SVM che hanno attualmente o precedentemente esportato qtree in SVM che non hanno mai esportato qtree. Per aggirare questo limite, è possibile esportare almeno un qtree sulla SVM di destinazione.

Informazioni correlate

"Quali operazioni VAAI offloaded sono supportate da Data ONTAP?"

Abilitare o disabilitare VMware vStorage su NFS

È possibile attivare o disattivare il supporto per VMware vStorage su NFS su macchine virtuali di storage (SVM) utilizzando `vserver nfs modify` comando.

A proposito di questa attività

Per impostazione predefinita, il supporto di VMware vStorage su NFS è disattivato.

Fasi

1. Visualizzare lo stato corrente del supporto vStorage per le SVM:

```
vserver nfs show -vserver vserver_name -instance
```

2. Eseguire una delle seguenti operazioni:

Se si desidera…	Immettere il seguente comando…
Abilitare il supporto di VMware vStorage	`vserver nfs modify -vserver vserver_name -vstorage enabled`
Disattivare il supporto di VMware vStorage	`vserver nfs modify -vserver vserver_name -vstorage disabled`

Al termine

Prima di utilizzare questa funzionalità, è necessario installare il plug-in NFS per VMware VAAI. Per ulteriori informazioni, consulta la sezione *Installazione del plug-in NetApp NFS per VMware VAAI*.

Informazioni correlate

"Documentazione NetApp: Plug-in NetApp NFS per VMware VAAI"

Attiva o disattiva il supporto rquota

ONTAP supporta il protocollo di quota remota versione 1 (rquota v1). Il protocollo rquota consente ai client NFS di ottenere informazioni sulle quote per gli utenti da un computer remoto. È possibile attivare rquota su macchine virtuali storage (SVM) utilizzando `vserver nfs modify` comando.

A proposito di questa attività

Per impostazione predefinita, rquota è disattivato.

Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera…	Immettere il seguente comando…
Abilitare il supporto rquota per le SVM	`vserver nfs modify -vserver vserver_name -rquota enable`
Disattiva il supporto rquota per le SVM	`vserver nfs modify -vserver vserver_name -rquota disable`

Per ulteriori informazioni sulle quote, vedere "Gestione dello storage logico".

Miglioramento delle performance di NFSv3 e NFSv4 modificando le dimensioni del trasferimento TCP

È possibile migliorare le prestazioni dei client NFSv3 e NFSv4 che si connettono ai sistemi storage su una rete ad alta latenza modificando le dimensioni massime di trasferimento TCP.

Quando i client accedono ai sistemi storage su una rete ad alta latenza, ad esempio WAN (Wide Area Network) o MAN (Metro Area Network) con una latenza superiore a 10 millisecondi, è possibile migliorare le prestazioni di connessione modificando le dimensioni massime di trasferimento TCP. I client che accedono a sistemi storage in una rete a bassa latenza, come una LAN (Local Area Network), possono aspettarsi pochi benefici dalla modifica di questi parametri. Se il miglioramento del throughput non supera l'impatto della latenza, non utilizzare questi parametri.

Per determinare se il tuo ambiente di storage potrebbe trarre beneficio dalla modifica di questi parametri, devi prima eseguire una valutazione completa delle performance di un client NFS dalle performance scarse. Verificare se le performance ridotte sono dovute a un'eccessiva latenza di round trip e a una piccola richiesta sul client. In queste condizioni, il client e il server non possono utilizzare completamente la larghezza di banda disponibile perché trascorrono la maggior parte dei loro cicli di lavoro in attesa di piccole richieste e risposte da trasmettere sulla connessione.

Aumentando le dimensioni delle richieste NFSv3 e NFSv4, il client e il server possono utilizzare la larghezza di banda disponibile in modo più efficace per spostare più dati per unità di tempo, aumentando quindi l'efficienza complessiva della connessione.

Tenere presente che la configurazione tra il sistema storage e il client potrebbe variare. Il sistema storage e il client supportano una dimensione massima di 1 MB per le operazioni di trasferimento. Tuttavia, se si configura il sistema di storage in modo che supporti le dimensioni massime di trasferimento di 1 MB ma il client supporta solo 64 KB, la dimensione di trasferimento del mount è limitata a 64 KB o meno.

Prima di modificare questi parametri, è necessario tenere presente che questo comporta un consumo di memoria aggiuntivo nel sistema di storage per il periodo di tempo necessario per assemblare e trasmettere una risposta elevata. Maggiore è la latenza elevata delle connessioni al sistema storage, maggiore è il consumo di memoria aggiuntivo. I sistemi storage con elevata capacità di memoria potrebbero avere un effetto molto ridotto da questo cambiamento. I sistemi storage con capacità di memoria bassa potrebbero riscontrare un notevole peggioramento delle performance.

Il corretto utilizzo di questi parametri dipende dalla capacità di recuperare i dati da più nodi di un cluster. La latenza intrinseca della rete del cluster potrebbe aumentare la latenza complessiva della risposta. La latenza complessiva tende ad aumentare quando si utilizzano questi parametri. Di conseguenza, i carichi di lavoro sensibili alla latenza potrebbero avere un impatto negativo.

Modificare le dimensioni massime di trasferimento TCP NFSv3 e NFSv4

È possibile modificare `-tcp-max-xfer-size` Opzione per configurare le dimensioni massime di trasferimento per tutte le connessioni TCP utilizzando i protocolli NFSv3 e NFSv4.x.

A proposito di questa attività

È possibile modificare queste opzioni singolarmente per ciascuna macchina virtuale di storage (SVM).

A partire da ONTAP 9 `v3-tcp-max-read-size` e. `v3-tcp-max-write-size` le opzioni sono obsolete. È necessario utilizzare `-tcp-max-xfer-size` invece.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

   ```
   set -privilege advanced
   ```

2. Eseguire una delle seguenti operazioni:

Se si desidera…	Immettere il comando…
Modificare le dimensioni massime di trasferimento TCP NFSv3 o NFSv4	`vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer_max_xfer_size`

Opzione	Raggio d'azione	Predefinito
`-tcp-max-xfer-size`	da 8192 a 1048576 byte	65536 byte

> La dimensione massima di trasferimento immessa deve essere un multiplo di 4 KB (4096 byte). Le richieste non allineate correttamente influiscono negativamente sulle performance.

3. Utilizzare `vserver nfs show -fields tcp-max-xfer-size` per verificare le modifiche.
4. Se alcuni client utilizzano i mount statici, smontare e rimontare per rendere effettive le nuove dimensioni dei parametri.

Esempio

Il seguente comando imposta le dimensioni massime di trasferimento TCP NFSv3 e NFSv4.x su 1048576 byte sulla SVM denominata vs1:

```
vs1::> vserver nfs modify -vserver vs1 -tcp-max-xfer-size 1048576
```

Configurare il numero di ID di gruppo consentiti per gli utenti NFS

Per impostazione predefinita, ONTAP supporta fino a 32 ID di gruppo quando gestisce le credenziali utente NFS utilizzando l'autenticazione Kerberos (RPCSEC_GSS). Quando si utilizza l'autenticazione AUTH_SYS, il numero massimo predefinito di ID gruppo è 16, come definito in RFC 5531. È possibile aumentare il numero massimo fino a 1,024 se si dispone di utenti che fanno parte di un numero di gruppi superiore a quello predefinito.

A proposito di questa attività

Se un utente dispone di un numero di ID di gruppo superiore a quello predefinito nelle proprie credenziali, gli ID di gruppo rimanenti vengono troncati e l'utente potrebbe ricevere errori quando tenta di accedere ai file dal sistema di storage. Impostare il numero massimo di gruppi, per SVM, su un numero che rappresenta il numero

massimo di gruppi nell'ambiente.

La seguente tabella mostra i due parametri di `vserver nfs modify` Comando che determina il numero massimo di ID di gruppo in tre configurazioni di esempio:

Parametri	Impostazioni	Limite ID gruppo risultante

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`32`
	
	`disabled`
	
	Queste sono le impostazioni predefinite.
		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

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

   ```
   set -privilege advanced
   ```

2. Eseguire l'azione desiderata:

Se si desidera impostare il numero massimo di gruppi ausiliari consentiti…	Immettere il comando…
Solo per RPCSEC_GSS e lasciare AUTH_SYS impostato sul valore predefinito 16	`vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups disabled`
Per RPCSEC_GSS e AUTH_SYS	`vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups enabled`

3. Verificare `-extended-groups-limit` Valutare e verificare se AUTH_SYS utilizza gruppi estesi: `vserver nfs show -vserver vserver_name -fields auth-sys-extended-groups,extended-groups-limit`
4. Tornare al livello di privilegio admin:

   ```
   set -privilege admin
   ```

Esempio

Nell'esempio riportato di seguito vengono abiliti i gruppi estesi per l'autenticazione AUTH_SYS e viene impostato il numero massimo di gruppi estesi su 512 per l'autenticazione AUTH_SYS e RPCSEC_GSS. Queste modifiche vengono apportate solo ai client che accedono alla SVM denominata 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
```

Controllare l'accesso dell'utente root ai dati di sicurezza NTFS

È possibile configurare ONTAP per consentire ai client NFS di accedere ai dati di sicurezza NTFS e ai client NTFS per accedere ai dati di sicurezza NFS. Quando si utilizza lo stile di sicurezza NTFS su un archivio dati NFS, è necessario decidere come trattare l'accesso da parte dell'utente root e configurare di conseguenza la macchina virtuale di storage (SVM).

A proposito di questa attività

Quando un utente root accede ai dati di sicurezza NTFS, sono disponibili due opzioni:

- Mappare l'utente root a un utente Windows come qualsiasi altro utente NFS e gestire l'accesso in base agli ACL NTFS.
- Ignorare gli ACL NTFS e fornire l'accesso completo all'utente root.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

   ```
   set -privilege advanced
   ```

2. Eseguire l'azione desiderata:

Se si desidera che l'utente root…	Immettere il comando…

Essere mappato a un utente Windows	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root disabled`
Ignorare il controllo dell'ACL NT	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root enabled`

Per impostazione predefinita, questo parametro è disattivato.

Se questo parametro è attivato ma non esiste alcuna mappatura dei nomi per l'utente root, ONTAP utilizza una credenziale di amministratore SMB predefinita per il controllo.

3. Tornare al livello di privilegio admin:

   ```
   set -privilege admin
   ```