Gestisci NFS con la CLI

ONTAP 9

NetApp
April 24, 2024

Sommario

Gestisci NFS con la CLI . . . 1
Panoramica di riferimento di NFS . . . 1
Comprendere l’accesso al file NAS . . . 1
Creare e gestire volumi di dati in spazi dei nomi NAS . . . 9
Configurare gli stili di sicurezza . . . 14
Impostare l’accesso al file utilizzando NFS . . . 19
Gestire l’accesso ai file con NFS . . . 56
Versioni e client NFS supportati . . . 108
Dipendenze di nomi di file e directory NFS e SMB . . . 111

Gestisci NFS con la CLI

Panoramica di riferimento di NFS

ONTAP include funzionalità di accesso ai file disponibili per il protocollo NFS. È possibile attivare un server NFS ed esportare volumi o qtree.

Eseguire questa procedura nei seguenti casi:

- Vuoi conoscere la gamma di funzionalità del protocollo NFS di ONTAP.
- Si desidera eseguire attività di configurazione e manutenzione meno comuni, non la configurazione NFS di base.
- Si desidera utilizzare l'interfaccia della riga di comando (CLI), non System Manager o uno strumento di scripting automatico.

Comprendere l'accesso al file NAS

Spazi dei nomi e punti di giunzione

Panoramica degli spazi dei nomi e dei punti di giunzione

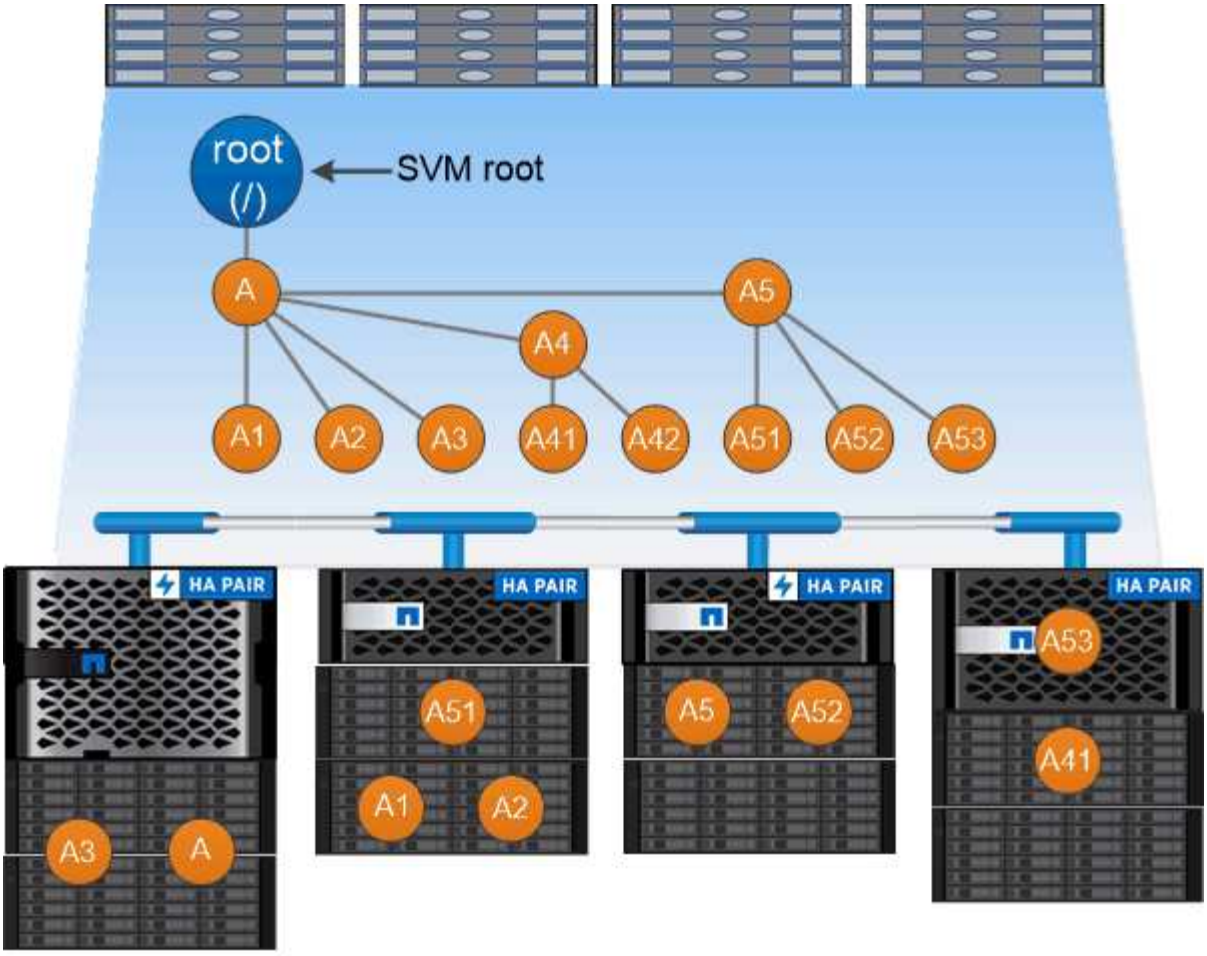
Un *namespace* NAS è un raggruppamento logico di volumi Uniti in *punti di giunzione* per creare una singola gerarchia di file system. Un client con autorizzazioni sufficienti può accedere ai file nello spazio dei nomi senza specificare la posizione dei file nello storage. I volumi Junctioned possono risiedere in qualsiasi punto del cluster.

Invece di montare ogni volume contenente un file di interesse, i client NAS montano un NFS *export* o accedono a una *share.* SMB. L'esportazione o la condivisione rappresenta l'intero namespace o una posizione intermedia all'interno dello spazio dei nomi. Il client accede solo ai volumi montati sotto il proprio access point.

È possibile aggiungere volumi allo spazio dei nomi in base alle esigenze. È possibile creare punti di giunzione direttamente sotto una giunzione di un volume padre o in una directory all'interno di un volume. Il percorso di una giunzione di volume per un volume denominato "vol3" potrebbe essere `/vol1/vol2/vol3`, o. `/vol1/dir2/vol3`, o persino `/dir1/dir2/vol3`. Il percorso è chiamato *percorso di giunzione.*

Ogni SVM dispone di uno spazio dei nomi univoco. Il volume root SVM è il punto di ingresso della gerarchia dello spazio dei nomi.

> Per garantire che i dati rimangano disponibili in caso di interruzione o failover di un nodo, è necessario creare una copia *mirror per la condivisione del carico* per il volume root SVM.



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

Esempio

Nell'esempio riportato di seguito viene creato un volume denominato "home4" situato su SVM vs1 con un percorso di giunzione `/eng/home`:

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

Quali sono le tipiche architetture dello spazio dei nomi NAS

Esistono diverse architetture dello spazio dei nomi NAS tipiche che è possibile utilizzare per creare lo spazio dei nomi SVM. È possibile scegliere l'architettura dello spazio dei nomi che soddisfa le esigenze di business e workflow.

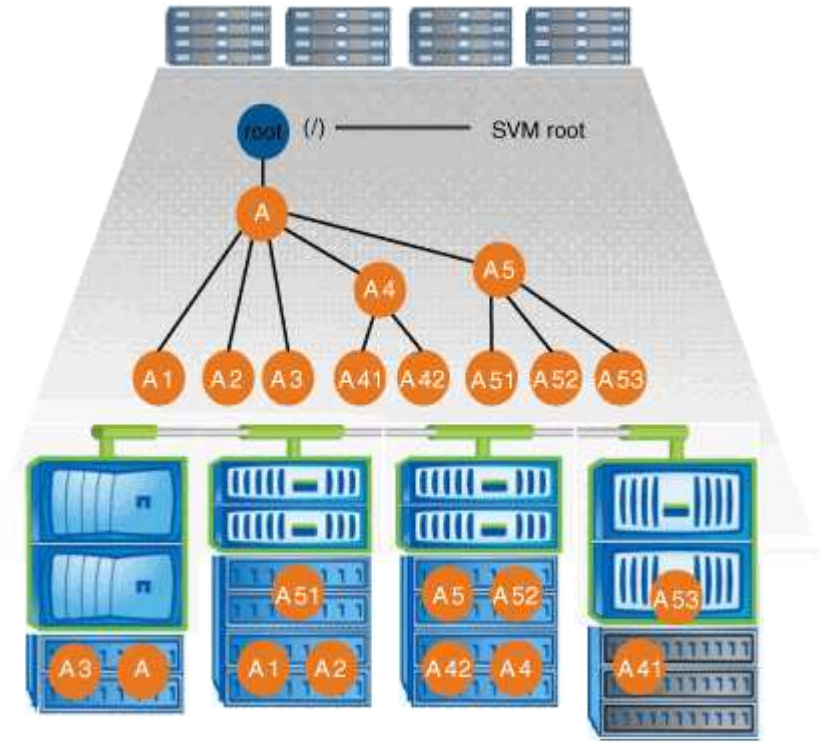
La parte superiore dello spazio dei nomi è sempre il volume root, rappresentato da una barra (/). L'architettura dello spazio dei nomi sotto la radice si suddivide in tre categorie di base:

- Un singolo albero ramificato, con una sola giunzione alla radice dello spazio dei nomi

- Più alberi ramificati, con più punti di giunzione alla radice dello spazio dei nomi
- Più volumi standalone, ciascuno con un punto di giunzione separato per la radice dello spazio dei nomi

Namespace con singolo albero ramificato

Un'architettura con un singolo albero ramificato ha un singolo punto di inserimento alla radice dello spazio dei nomi SVM. Il singolo punto di inserimento può essere un volume giuntato o una directory sotto la root. Tutti gli altri volumi vengono montati nei punti di giunzione sotto il singolo punto di inserimento (che può essere un volume o una directory).

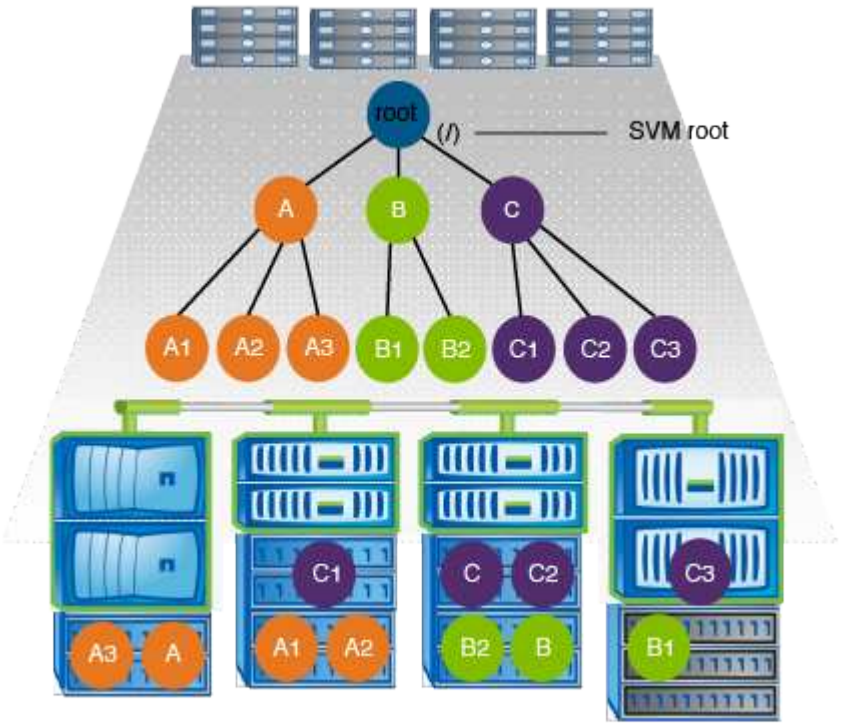


Ad esempio, una configurazione tipica di giunzione di volumi con l'architettura dello spazio dei nomi sopra descritta potrebbe essere simile alla seguente configurazione, in cui tutti i volumi sono congiunti sotto il singolo punto di inserimento, che è una directory denominata "data":

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

Namespace con più alberi ramificati

Un'architettura con più alberi ramificati ha più punti di inserimento alla radice dello spazio dei nomi SVM. I punti di inserimento possono essere volumi congiunti o directory sotto la radice. Tutti gli altri volumi vengono montati nei punti di giunzione sotto i punti di inserimento (che possono essere volumi o directory).



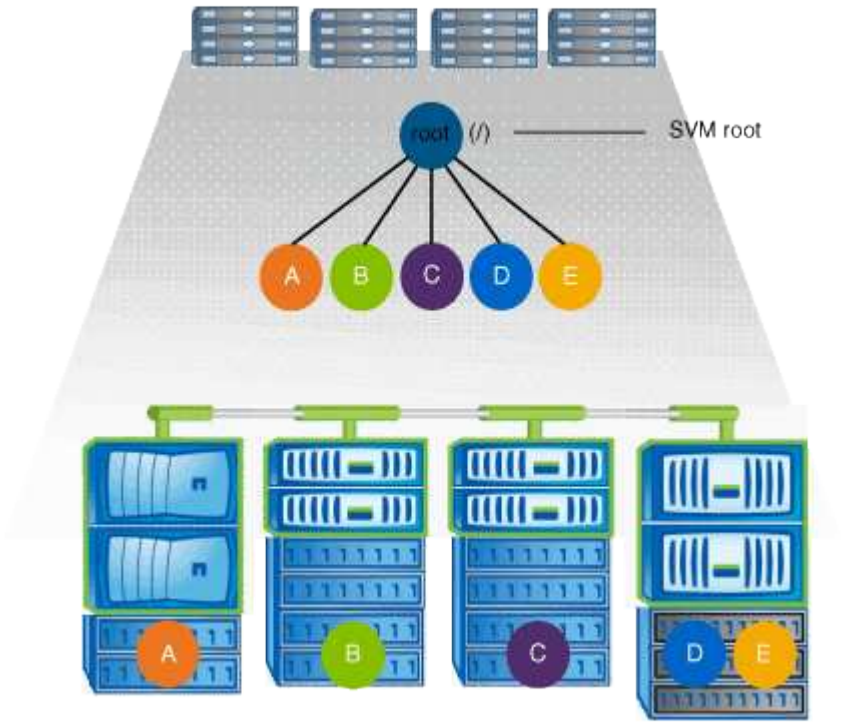
Ad esempio, una configurazione tipica di giunzione del volume con l'architettura dello spazio dei nomi di cui sopra potrebbe essere simile alla seguente configurazione, in cui sono presenti tre punti di inserimento nel volume root della SVM. Due punti di inserimento sono directory denominate "data" e "projects". Un punto di inserimento è un volume giuntato denominato "audit":

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

Namespace con più volumi standalone

In un'architettura con volumi standalone, ogni volume ha un punto di inserimento nella directory principale

dello spazio dei nomi SVM; tuttavia, il volume non è giuntato sotto un altro volume. Ogni volume ha un percorso univoco ed è posto direttamente sotto la root oppure è posto sotto una directory sotto la root.



Ad esempio, una configurazione tipica di giunzione del volume con l'architettura dello spazio dei nomi di cui sopra potrebbe essere simile alla seguente configurazione, in cui sono presenti cinque punti di inserimento nel volume root della SVM, con ciascun punto di inserimento che rappresenta un percorso per un volume.

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

Come ONTAP controlla l'accesso ai file

Panoramica delle modalità di controllo dell'accesso ai file da parte di ONTAP

ONTAP controlla l'accesso ai file in base alle restrizioni basate sull'autenticazione e sui file specificate dall'utente.

Quando un client si connette al sistema di storage per accedere ai file, ONTAP deve eseguire due operazioni:

- Autenticazione

ONTAP deve autenticare il client verificando l'identità con un'origine attendibile. Inoltre, il tipo di autenticazione del client è un metodo che può essere utilizzato per determinare se un client può accedere ai dati durante la configurazione dei criteri di esportazione (facoltativo per CIFS).

- Autorizzazione

  ONTAP deve autorizzare l'utente confrontando le credenziali dell'utente con le autorizzazioni configurate nel file o nella directory e determinando il tipo di accesso, se presente, da fornire.

Per gestire correttamente il controllo dell'accesso ai file, ONTAP deve comunicare con servizi esterni come server NIS, LDAP e Active Directory. La configurazione di un sistema storage per l'accesso ai file mediante CIFS o NFS richiede la configurazione dei servizi appropriati in base all'ambiente in uso in ONTAP.

Restrizioni basate sull'autenticazione

Con le restrizioni basate sull'autenticazione, è possibile specificare quali macchine client e quali utenti possono connettersi alla SVM (Storage Virtual Machine).

ONTAP supporta l'autenticazione Kerberos da server UNIX e Windows.

Restrizioni basate su file

ONTAP valuta tre livelli di sicurezza per determinare se un'entità è autorizzata a eseguire un'azione richiesta su file e directory che risiedono su una SVM. L'accesso è determinato dalle autorizzazioni effettive dopo la valutazione dei tre livelli di protezione.

Qualsiasi oggetto di storage può contenere fino a tre tipi di livelli di sicurezza:

- Sicurezza di esportazione (NFS) e condivisione (SMB)

  La sicurezza di esportazione e condivisione si applica all'accesso client a una data esportazione NFS o condivisione SMB. Gli utenti con privilegi amministrativi possono gestire la sicurezza a livello di esportazione e condivisione dai client SMB e NFS.

- Protezione di file e directory di Access Guard a livello di storage

  La sicurezza di Access Guard a livello di storage si applica all'accesso dei client SMB e NFS ai volumi SVM. Sono supportate solo le autorizzazioni di accesso NTFS. Affinché ONTAP esegua controlli di sicurezza sugli utenti UNIX per l'accesso ai dati sui volumi per i quali è stato applicato Storage-Level Access Guard, l'utente UNIX deve eseguire il mapping a un utente Windows sulla SVM proprietaria del volume.

  > Se si visualizzano le impostazioni di sicurezza su un file o una directory da un client NFS o SMB, la protezione Storage-Level Access Guard non viene visualizzata. La protezione di Storage-Level Access Guard non può essere revocata da un client, nemmeno da un amministratore di sistema (Windows o UNIX).

- Sicurezza nativa a livello di file in NTFS, UNIX e NFSv4

  La protezione nativa a livello di file esiste nel file o nella directory che rappresenta l'oggetto di storage. È possibile impostare la sicurezza a livello di file da un client. Le autorizzazioni dei file sono efficaci indipendentemente dal fatto che SMB o NFS vengano utilizzati per accedere ai dati.

Come ONTAP gestisce l'autenticazione del client NFS

Panoramica su come ONTAP gestisce l'autenticazione del client NFS

I client NFS devono essere autenticati correttamente prima di poter accedere ai dati sulla SVM. ONTAP autentica i client verificando le credenziali UNIX in base ai servizi di nomi configurati.

Quando un client NFS si connette a SVM, ONTAP ottiene le credenziali UNIX per l'utente controllando i diversi name service, a seconda della configurazione dei name service di SVM. ONTAP può controllare le credenziali per gli account UNIX locali, i domini NIS e i domini LDAP. Almeno uno di questi deve essere configurato in modo che ONTAP possa autenticare correttamente l'utente. È possibile specificare più servizi di nomi e l'ordine in cui ONTAP li cerca.

In un ambiente NFS puro con stili di sicurezza dei volumi UNIX, questa configurazione è sufficiente per autenticare e fornire l'accesso corretto ai file per un utente che si connette da un client NFS.

Se si utilizzano stili di protezione di volumi misti, NTFS o unificati, ONTAP deve ottenere un nome utente SMB per l'utente UNIX per l'autenticazione con un controller di dominio Windows. Ciò può avvenire mappando singoli utenti utilizzando account UNIX locali o domini LDAP oppure utilizzando un utente SMB predefinito. È possibile specificare quali servizi di nomi ONTAP esegue la ricerca in quale ordine o specificare un utente SMB predefinito.

Modalità di utilizzo dei servizi di nome da parte di ONTAP

ONTAP utilizza i name service per ottenere informazioni su utenti e client. ONTAP utilizza queste informazioni per autenticare gli utenti che accedono ai dati sul sistema di storage o ne amministrano l'amministrazione e per mappare le credenziali dell'utente in un ambiente misto.

Quando si configura il sistema di storage, è necessario specificare i servizi dei nomi che si desidera utilizzare per ottenere le credenziali utente per l'autenticazione di ONTAP. ONTAP supporta i seguenti servizi per i nomi:

- Utenti locali (file)
- NIS (External NIS Domain)
- Domini LDAP esterni (LDAP)

Si utilizza `vserver services name-service ns-switch` Famiglia di comandi per configurare le SVM con le origini per la ricerca delle informazioni di rete e l'ordine in cui eseguirne la ricerca. Questi comandi forniscono le funzionalità equivalenti di `/etc/nsswitch.conf` File su sistemi UNIX.

Quando un client NFS si connette a SVM, ONTAP verifica i servizi dei nomi specificati per ottenere le credenziali UNIX per l'utente. Se i name service sono configurati correttamente e ONTAP è in grado di ottenere le credenziali UNIX, ONTAP autentica correttamente l'utente.

In un ambiente con stili di sicurezza misti, ONTAP potrebbe dover mappare le credenziali dell'utente. Per consentire a ONTAP di mappare correttamente le credenziali dell'utente, è necessario configurare i name service in modo appropriato per l'ambiente in uso.

ONTAP utilizza inoltre i servizi di nome per autenticare gli account amministratore di SVM. È necessario tenere presente questo aspetto durante la configurazione o la modifica dello switch del name service per evitare di disattivare accidentalmente l'autenticazione per gli account amministratore SVM. Per ulteriori informazioni sugli

utenti di amministrazione di SVM, vedere "Autenticazione amministratore e RBAC".

In che modo ONTAP garantisce l'accesso ai file SMB dai client NFS

ONTAP utilizza la semantica di protezione del file system di Windows NT per determinare se un utente UNIX, su un client NFS, ha accesso a un file con autorizzazioni NTFS.

A tale scopo, ONTAP converte l'ID utente UNIX dell'utente in una credenziale SMB e utilizza la credenziale SMB per verificare che l'utente disponga dei diritti di accesso al file. Una credenziale SMB è costituita da un identificatore di protezione (SID) primario, di solito il nome utente Windows dell'utente, e da uno o più SID di gruppo che corrispondono ai gruppi Windows di cui l'utente è membro.

Il tempo impiegato da ONTAP per convertire l'UID UNIX in una credenziale SMB può essere compreso tra decine di millisecondi e centinaia di millisecondi, poiché il processo richiede il contatto con un controller di dominio. ONTAP esegue il mapping dell'UID alla credenziale SMB e inserisce il mapping in una cache delle credenziali per ridurre il tempo di verifica causato dalla conversione.

Come funziona la cache delle credenziali NFS

Quando un utente NFS richiede l'accesso alle esportazioni NFS sul sistema di storage, ONTAP deve recuperare le credenziali dell'utente dai name server esterni o dai file locali per autenticare l'utente. ONTAP memorizza quindi queste credenziali in una cache interna per riferimenti futuri. La comprensione del funzionamento delle cache delle credenziali NFS consente di gestire potenziali problemi di performance e accesso.

Senza la cache delle credenziali, ONTAP dovrebbe eseguire query sui servizi dei nomi ogni volta che un utente NFS ha richiesto l'accesso. In un sistema storage occupato a cui molti utenti accedono, questo può causare rapidamente gravi problemi di performance, causando ritardi indesiderati o addirittura negazioni dell'accesso al client NFS.

Con la cache delle credenziali, ONTAP recupera le credenziali dell'utente e le memorizza per un periodo di tempo prestabilito per un accesso rapido e semplice nel caso in cui il client NFS invii un'altra richiesta. Questo metodo offre i seguenti vantaggi:

- Semplifica il carico sul sistema storage gestendo meno richieste ai name server esterni (come NIS o LDAP).
- Semplifica il carico sui server dei nomi esterni inviando loro un numero inferiore di richieste.
- Accelera l'accesso degli utenti eliminando i tempi di attesa per ottenere le credenziali da origini esterne prima che l'utente possa essere autenticato.

ONTAP memorizza le credenziali positive e negative nella cache delle credenziali. Le credenziali positive significano che l'utente è stato autenticato e ha ottenuto l'accesso. Le credenziali negative significano che l'utente non è stato autenticato e l'accesso è stato negato.

Per impostazione predefinita, ONTAP memorizza le credenziali positive per 24 ore, ovvero, dopo l'autenticazione iniziale di un utente, ONTAP utilizza le credenziali memorizzate nella cache per tutte le richieste di accesso da parte di tale utente per 24 ore. Se l'utente richiede l'accesso dopo 24 ore, il ciclo ha inizio: ONTAP ignora le credenziali memorizzate nella cache e ottiene nuovamente le credenziali dall'origine del name service appropriata. Se le credenziali sono state modificate nel server dei nomi durante le 24 ore precedenti, ONTAP memorizza nella cache le credenziali aggiornate per l'utilizzo nelle 24 ore successive.

Per impostazione predefinita, ONTAP memorizza le credenziali negative per due ore, ovvero, dopo aver

inizialmente negato l'accesso a un utente, ONTAP continua a negare qualsiasi richiesta di accesso da parte di tale utente per due ore. Se l'utente richiede l'accesso dopo 2 ore, il ciclo ricomincia: ONTAP ottiene nuovamente le credenziali dall'origine del name service appropriata. Se le credenziali sono state modificate nel server dei nomi nelle due ore precedenti, ONTAP memorizza nella cache le credenziali aggiornate per l'utilizzo nelle due ore successive.

Creare e gestire volumi di dati in spazi dei nomi NAS

Creare volumi di dati con punti di giunzione specificati

È possibile specificare il punto di giunzione quando si crea un volume di dati. Il volume risultante viene montato automaticamente nel punto di giunzione ed è immediatamente disponibile per la configurazione dell'accesso NAS.

Prima di iniziare

- L'aggregato in cui si desidera creare il volume deve già esistere.
- A partire da ONTAP 9.13.1, puoi creare volumi con l'analisi della capacità e il monitoraggio delle attività abilitati. Per attivare il monitoraggio della capacità o dell'attività, eseguire il `volume create` comando con `-analytics-state` oppure `-activity-tracking-state` impostare su `on`.

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

> I seguenti caratteri non possono essere utilizzati nel percorso di giunzione: * N. " > < | ? .

+ inoltre, la lunghezza del percorso di giunzione non può superare i 255 caratteri.

Fasi

1. Creare il volume con un punto di giunzione:

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

   Il percorso di giunzione deve iniziare con root (/) e può contenere sia directory che volumi congiunti. Il percorso di giunzione non deve contenere il nome del volume. I percorsi di giunzione sono indipendenti dal nome del volume.

   Specificare uno stile di sicurezza del volume è facoltativo. Se non si specifica uno stile di protezione, ONTAP crea il volume con lo stesso stile di protezione applicato al volume root della macchina virtuale di storage (SVM). Tuttavia, lo stile di sicurezza del volume root potrebbe non corrispondere allo stile di sicurezza che si desidera applicare al volume di dati creato. Si consiglia di specificare lo stile di protezione quando si crea il volume per ridurre al minimo i problemi di accesso ai file difficili da risolvere.

   Il percorso di giunzione è privo di maiuscole e minuscole; `/ENG` è uguale a. `/eng`. Se si crea una condivisione CIFS, Windows considera il percorso di giunzione come se fosse sensibile alla distinzione tra maiuscole e minuscole. Ad esempio, se la giunzione è `/ENG`, Il percorso di una condivisione SMB deve iniziare con `/ENG`, non `/eng`.

   Per personalizzare un volume di dati, è possibile utilizzare molti parametri opzionali. Per ulteriori informazioni, consultare le pagine man del `volume create` comando.

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

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

Esempio

Nell'esempio riportato di seguito viene creato un volume denominato "home4" situato su SVM vs1 con un percorso di giunzione `/eng/home`:

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

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

Creare volumi di dati senza specificare punti di giunzione

È possibile creare un volume di dati senza specificare un punto di giunzione. Il volume risultante non viene montato automaticamente e non è disponibile per la configurazione per l'accesso NAS. È necessario montare il volume prima di poter configurare le condivisioni SMB o le esportazioni NFS per quel volume.

Prima di iniziare

- L'aggregato in cui si desidera creare il volume deve già esistere.
- A partire da ONTAP 9.13.1, puoi creare volumi con l'analisi della capacità e il monitoraggio delle attività abilitati. Per attivare il monitoraggio della capacità o dell'attività, eseguire il `volume create` comando con `-analytics-state` oppure `-activity-tracking-state` impostare su `on`.

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

Fasi

1. Creare il volume senza un punto di giunzione utilizzando il seguente comando:

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

   Specificare uno stile di sicurezza del volume è facoltativo. Se non si specifica uno stile di protezione, ONTAP crea il volume con lo stesso stile di protezione applicato al volume root della macchina virtuale di storage (SVM). Tuttavia, lo stile di sicurezza del volume root potrebbe non corrispondere allo stile di sicurezza che si desidera applicare al volume di dati. Si consiglia di specificare lo stile di protezione quando si crea il volume per ridurre al minimo i problemi di accesso ai file difficili da risolvere.

   Per personalizzare un volume di dati, è possibile utilizzare molti parametri opzionali. Per ulteriori

informazioni, consultare le pagine man del `volume create` comando.

2. Verificare che il volume sia stato creato senza un punto di giunzione:

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

Esempio

Nell'esempio seguente viene creato un volume denominato "sales" situato su SVM vs1 che non è montato in un punto di giunzione:

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

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

Montare o smontare i volumi esistenti nello spazio dei nomi NAS

È necessario montare un volume sullo spazio dei nomi NAS prima di poter configurare l'accesso del client NAS ai dati contenuti nei volumi SVM (Storage Virtual Machine). È possibile montare un volume su un punto di giunzione se non è attualmente montato. È anche possibile smontare i volumi.

A proposito di questa attività

Se si smonta e si porta un volume offline, tutti i dati all'interno del punto di giunzione, inclusi i dati nei volumi con punti di giunzione contenuti nello spazio dei nomi del volume non montato, sono inaccessibili ai client NAS.

> Per interrompere l'accesso del client NAS a un volume, non è sufficiente smontare semplicemente il volume. È necessario portare il volume offline o eseguire altre operazioni per assicurarsi che le cache degli handle dei file sul lato client siano invalidate. Per ulteriori informazioni, consultare il seguente articolo della Knowledge base:
>
> "I client NFSv3 hanno ancora accesso a un volume dopo essere stati rimossi dallo spazio dei nomi in ONTAP"

Quando si disinstalla e si disconnette un volume, i dati all'interno del volume non vengono persi. Inoltre, vengono mantenute le policy di esportazione dei volumi esistenti e le condivisioni SMB create sul volume o su directory e punti di giunzione all'interno del volume non montato. Se si rimonta il volume non montato, i client NAS possono accedere ai dati contenuti nel volume utilizzando le policy di esportazione e le condivisioni SMB esistenti.

Fasi

1. Eseguire l'azione desiderata:

Se si desidera…	Immettere i comandi…
Montare un volume	`volume mount -vserver` *`svm_name`* `-volume` *`volume_name`* `-junction-path` *`junction_path`*
Smontare un volume	`volume unmount -vserver` *`svm_name`* `-volume` *`volume_name`* `volume offline -vserver` *`svm_name`* `-volume` *`volume_name`*

2. Verificare che il volume si trovi nello stato di montaggio desiderato:

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

Esempi

Nell'esempio seguente viene montato un volume denominato "sques" situato su SVM "`VS1'" al punto di giunzione "`/sales»":

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

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

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

Il seguente esempio smonta e porta offline un volume chiamato "dati" situato su SVM "`VS1'":

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

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

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

Visualizzare le informazioni sul punto di giunzione e sul montaggio del volume

È possibile visualizzare informazioni sui volumi montati per le macchine virtuali di storage (SVM) e sui punti di giunzione in cui vengono montati i volumi. È inoltre possibile determinare quali volumi non sono montati su un punto di giunzione. È possibile utilizzare queste informazioni per comprendere e gestire lo spazio dei nomi SVM.

Fase

1. Eseguire l'azione desiderata:

Se si desidera visualizzare…	Immettere il comando…
Informazioni riepilogative sui volumi montati e non montati su SVM	`volume show -vserver` *`vserver_name`* `-junction`
Informazioni dettagliate sui volumi montati e non montati su SVM	`volume show -vserver` *`vserver_name`* `-volume` *`volume_name`* `-instance`
Informazioni specifiche sui volumi montati e non montati su SVM	a. Se necessario, è possibile visualizzare campi validi per `-fields` utilizzando il seguente comando: `volume show -fields ?` b. Visualizzare le informazioni desiderate utilizzando `-fields` parametro: `volume show -vserver` *`vserver_name`* `-fields` *`fieldname`*`,…`

Esempi

Nell'esempio seguente viene visualizzato un riepilogo dei volumi montati e non montati su SVM vs1:

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

Nell'esempio seguente vengono visualizzate informazioni sui campi specificati per i volumi che si trovano su SVM vs2:

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

Configurare gli stili di sicurezza

In che modo gli stili di sicurezza influiscono sull'accesso ai dati

Quali sono gli stili di sicurezza e i loro effetti

Esistono quattro diversi stili di sicurezza: UNIX, NTFS, misto e unificato. Ogni stile di sicurezza ha un effetto diverso sul modo in cui vengono gestite le autorizzazioni per i dati.

È necessario comprendere i diversi effetti per assicurarsi di selezionare lo stile di sicurezza appropriato per i propri scopi.

È importante comprendere che gli stili di sicurezza non determinano quali tipi di client possono o non possono accedere ai dati. Gli stili di sicurezza determinano solo il tipo di autorizzazioni utilizzate da ONTAP per controllare l'accesso ai dati e il tipo di client in grado di modificare tali autorizzazioni.

Ad esempio, se un volume utilizza lo stile di sicurezza UNIX, i client SMB possono comunque accedere ai dati (purché autenticino e autorizzino correttamente) a causa della natura multiprotocollo di ONTAP. Tuttavia, ONTAP utilizza autorizzazioni UNIX che solo i client UNIX possono modificare utilizzando strumenti nativi.

Stile di sicurezza	Client in grado di modificare le autorizzazioni	Autorizzazioni che i client possono utilizzare	Risultato di uno stile di sicurezza efficace	Client che possono accedere ai file
UNIX	NFS	Bit di modalità NFSv3	UNIX	NFS e SMB
		ACL NFSv4.x		
NTFS	PMI	ACL NTFS	NTFS	
Misto	NFS o SMB	Bit di modalità NFSv3	UNIX	
		NFSv4.ACL		
		ACL NTFS	NTFS	
Unificato (solo per volumi infiniti, in ONTAP 9.4 e versioni precedenti).	NFS o SMB	Bit di modalità NFSv3	UNIX	
		ACL NFSv4.1		
		ACL NTFS	NTFS	

I volumi FlexVol supportano UNIX, NTFS e stili di sicurezza misti. Quando lo stile di sicurezza è misto o unificato, le autorizzazioni effettive dipendono dal tipo di client che ha modificato le autorizzazioni per ultima, perché gli utenti impostano lo stile di sicurezza su base individuale. Se l'ultimo client che ha modificato le autorizzazioni era un client NFSv3, le autorizzazioni sono bit di modalità UNIX NFSv3. Se l'ultimo client era un client NFSv4, le autorizzazioni sono ACL NFSv4. Se l'ultimo client era un client SMB, le autorizzazioni sono ACL NTFS di Windows.

Lo stile di sicurezza unificato è disponibile solo con volumi infiniti, che non sono più supportati in ONTAP 9.5 e versioni successive. Per ulteriori informazioni, vedere Panoramica sulla gestione dei volumi FlexGroup.

A partire da ONTAP 9.2, la `show-effective-permissions` al `vserver security file-directory` Il comando consente di visualizzare le autorizzazioni effettive concesse a un utente Windows o UNIX sul percorso di file o cartella specificato. Inoltre, il parametro opzionale `-share-name` consente di visualizzare l'autorizzazione di condivisione effettiva.

ONTAP imposta inizialmente alcune autorizzazioni predefinite per i file. Per impostazione predefinita, lo stile di sicurezza effettivo su tutti i dati nei volumi UNIX, misti e di sicurezza unificata è UNIX e il tipo di permessi effettivo è UNIX mode bits (0755 se non diversamente specificato) fino a quando non viene configurato da un client come consentito dallo stile di sicurezza predefinito. Per impostazione predefinita, lo stile di sicurezza effettivo su tutti i dati nei volumi di sicurezza NTFS è NTFS e dispone di un ACL che consente il controllo completo di tutti.

Dove e quando impostare gli stili di sicurezza

Gli stili di sicurezza possono essere impostati su volumi FlexVol (sia root che volumi di dati) e qtree. Gli stili di sicurezza possono essere impostati manualmente al momento della creazione, ereditati automaticamente o modificati in un secondo momento.

Decidere quale stile di sicurezza utilizzare sulle SVM

Per aiutarti a decidere quale stile di sicurezza utilizzare su un volume, devi considerare due fattori. Il fattore principale è il tipo di amministratore che gestisce il file system. Il fattore secondario è il tipo di utente o servizio che accede ai dati sul volume.

Quando si configura lo stile di protezione su un volume, è necessario considerare le esigenze dell'ambiente per assicurarsi di selezionare lo stile di protezione migliore ed evitare problemi con la gestione delle autorizzazioni. Le seguenti considerazioni possono aiutarti a decidere:

Stile di sicurezza	Scegliere se…
UNIX	• Il file system è gestito da un amministratore UNIX. • La maggior parte degli utenti sono client NFS. • Un'applicazione che accede ai dati utilizza un utente UNIX come account del servizio.
NTFS	• Il file system è gestito da un amministratore di Windows. • La maggior parte degli utenti è costituita da client SMB. • Un'applicazione che accede ai dati utilizza un utente Windows come account del servizio.
Misto	• Il file system è gestito dagli amministratori UNIX e Windows e gli utenti sono costituiti da client NFS e SMB.

Come funziona l'ereditarietà dello stile di sicurezza

Se non si specifica lo stile di protezione durante la creazione di un nuovo volume FlexVol o di un qtree, questo eredita il proprio stile di protezione in modi diversi.

Gli stili di sicurezza vengono ereditati nel modo seguente:

- Un volume FlexVol eredita lo stile di sicurezza del volume root del volume SVM contenente.
- Un qtree eredita lo stile di protezione del volume FlexVol contenente.

- Un file o una directory eredita lo stile di protezione del volume o qtree FlexVol contenente.

In che modo ONTAP conserva le autorizzazioni UNIX

Quando i file in un volume FlexVol che dispongono attualmente di autorizzazioni UNIX vengono modificati e salvati dalle applicazioni Windows, ONTAP può conservare le autorizzazioni UNIX.

Quando le applicazioni sui client Windows modificano e salvano i file, leggono le proprietà di protezione del file, creano un nuovo file temporaneo, applicano tali proprietà al file temporaneo e assegnano al file temporaneo il nome del file originale.

Quando i client Windows eseguono una query per le proprietà di protezione, ricevono un ACL costruito che rappresenta esattamente le autorizzazioni UNIX. L'unico scopo di questo ACL costruito è quello di preservare le autorizzazioni UNIX del file, poiché i file vengono aggiornati dalle applicazioni Windows per garantire che i file risultanti abbiano le stesse autorizzazioni UNIX. ONTAP non imposta alcun ACL NTFS utilizzando l'ACL costruito.

Gestire le autorizzazioni UNIX utilizzando la scheda protezione di Windows

Se si desidera modificare le autorizzazioni UNIX di file o cartelle in volumi misti di sicurezza o qtree su SVM, è possibile utilizzare la scheda Security (protezione) sui client Windows. In alternativa, è possibile utilizzare applicazioni in grado di eseguire query e impostare gli ACL di Windows.

- Modifica delle autorizzazioni UNIX

  È possibile utilizzare la scheda protezione di Windows per visualizzare e modificare le autorizzazioni UNIX per un volume misto di sicurezza o qtree. Se si utilizza la scheda principale di Windows Security per modificare le autorizzazioni UNIX, è necessario rimuovere prima l'ACE esistente che si desidera modificare (in questo modo i bit di modalità vengono impostati su 0) prima di apportare le modifiche. In alternativa, è possibile utilizzare l'editor avanzato per modificare le autorizzazioni.

  Se vengono utilizzate le autorizzazioni di modalità, è possibile modificare direttamente le autorizzazioni di modalità per UID, GID e altri (tutti gli altri utenti con un account sul computer). Ad esempio, se l'UID visualizzato dispone delle autorizzazioni r-x, è possibile modificare le autorizzazioni UID in rwx.

- Modifica delle autorizzazioni UNIX in autorizzazioni NTFS

  È possibile utilizzare la scheda protezione di Windows per sostituire gli oggetti di protezione UNIX con oggetti di protezione di Windows su un volume misto di tipo sicurezza o qtree in cui i file e le cartelle hanno uno stile di protezione efficace UNIX.

  Prima di poter sostituire le voci di autorizzazione UNIX con gli oggetti utente e gruppo di Windows desiderati, è necessario rimuovere tutte le voci di autorizzazione UNIX elencate. È quindi possibile configurare gli ACL basati su NTFS sugli oggetti utente e Gruppo di Windows. Rimuovendo tutti gli oggetti di protezione UNIX e aggiungendo solo utenti e gruppi Windows a un file o a una cartella in un volume o qtree misto di sicurezza, è possibile modificare lo stile di protezione effettivo del file o della cartella da UNIX a NTFS.

  Quando si modificano le autorizzazioni di una cartella, il comportamento predefinito di Windows consiste nel propagare queste modifiche a tutte le sottocartelle e a tutti i file. Pertanto, se non si desidera propagare una modifica dello stile di protezione a tutte le cartelle figlio, le sottocartelle e i file, è necessario modificare

l'impostazione di propagazione desiderata.

Configurare gli stili di sicurezza sui volumi root SVM

È possibile configurare lo stile di protezione del volume root SVM (Storage Virtual Machine) per determinare il tipo di autorizzazioni utilizzate per i dati sul volume root di SVM.

Fasi

1. Utilizzare `vserver create` con il `-rootvolume-security-style` parametro per definire lo stile di sicurezza.

   Le opzioni possibili per lo stile di protezione del volume root sono: `unix`, `ntfs`, o. `mixed`.

2. Visualizzare e verificare la configurazione, incluso lo stile di sicurezza del volume root della SVM creata:

   ```
   vserver show -vserver vserver_name
   ```

Configurare gli stili di sicurezza sui volumi FlexVol

È possibile configurare lo stile di sicurezza del volume FlexVol per determinare il tipo di autorizzazioni utilizzate per i dati sui volumi FlexVol della macchina virtuale di storage (SVM).

Fasi

1. Eseguire una delle seguenti operazioni:

Se il volume FlexVol…	Utilizzare il comando…
Non esiste ancora	`volume create` e includono `-security-style` parametro per specificare lo stile di sicurezza.
Esiste già	`volume modify` e includono `-security-style` parametro per specificare lo stile di sicurezza.

   Le opzioni possibili per lo stile di protezione del volume FlexVol sono `unix`, `ntfs`, o. `mixed`.

   Se non si specifica uno stile di protezione durante la creazione di un volume FlexVol, il volume eredita lo stile di protezione del volume root.

   Per ulteriori informazioni su `volume create` oppure `volume modify` comandi, vedere "Gestione dello storage logico".

2. Per visualizzare la configurazione, incluso lo stile di protezione del volume FlexVol creato, immettere il seguente comando:

   ```
   volume show -volume volume_name -instance
   ```

Configurare gli stili di sicurezza sui qtree

Lo stile di protezione del volume qtree viene configurato per determinare il tipo di autorizzazioni utilizzate per i dati su qtree.

Fasi

1. Eseguire una delle seguenti operazioni:

Se il qtree…	Utilizzare il comando…
Non esiste ancora	`volume qtree create` e includono `-security-style` parametro per specificare lo stile di sicurezza.
Esiste già	`volume qtree modify` e includono `-security-style` parametro per specificare lo stile di sicurezza.

   Le opzioni possibili per lo stile di sicurezza qtree sono: `unix`, `ntfs`, o. `mixed`.

   Se non si specifica uno stile di protezione durante la creazione di un qtree, lo stile di protezione predefinito è `mixed`.

   Per ulteriori informazioni su `volume qtree create` oppure `volume qtree modify` comandi, vedere "Gestione dello storage logico".

2. Per visualizzare la configurazione, incluso lo stile di sicurezza del qtree creato, immettere il seguente comando: `volume qtree show -qtree` *`qtree_name`* `-instance`

Impostare l'accesso al file utilizzando NFS

Impostare l'accesso al file utilizzando la panoramica NFS

È necessario completare una serie di passaggi per consentire ai client di accedere ai file sulle macchine virtuali di storage (SVM) utilizzando NFS. A seconda della configurazione corrente dell'ambiente, sono disponibili alcuni passaggi aggiuntivi opzionali.

Per consentire ai client di accedere ai file su SVM utilizzando NFS, è necessario completare le seguenti operazioni:

1. Abilitare il protocollo NFS su SVM.

   È necessario configurare SVM per consentire l'accesso ai dati dai client tramite NFS.

2. Creare un server NFS su SVM.

   Un server NFS è un'entità logica su SVM che consente a SVM di fornire file su NFS. È necessario creare il server NFS e specificare le versioni del protocollo NFS che si desidera consentire.

3. Configurare i criteri di esportazione su SVM.

   È necessario configurare i criteri di esportazione per rendere disponibili volumi e qtree ai client.

4. Configurare il server NFS con la sicurezza appropriata e altre impostazioni a seconda della rete e dell'ambiente di storage.

   Questo passaggio può includere la configurazione di Kerberos, LDAP, NIS, mappature dei nomi e utenti locali.

Accesso sicuro a NFS tramite policy di esportazione

In che modo le policy di esportazione controllano l'accesso dei client ai volumi o ai qtree

I criteri di esportazione contengono una o più *regole di esportazione* che elaborano ogni richiesta di accesso client. Il risultato del processo determina se al client viene negato o concesso l'accesso e quale livello di accesso. Affinché i client possano accedere ai dati, è necessario che sulla macchina virtuale di storage (SVM) sia presente un criterio di esportazione con regole di esportazione.

Per configurare l'accesso del client al volume o al qtree, è necessario associare esattamente un criterio di esportazione a ciascun volume o qtree. La SVM può contenere più policy di esportazione. Ciò consente di eseguire le seguenti operazioni per le SVM con più volumi o qtree:

- Assegnare criteri di esportazione diversi a ciascun volume o qtree di SVM per il controllo degli accessi dei singoli client a ciascun volume o qtree di SVM.
- Assegnare la stessa policy di esportazione a più volumi o qtree di SVM per un controllo identico dell'accesso client senza dover creare una nuova policy di esportazione per ciascun volume o qtree.

Se un client effettua una richiesta di accesso non consentita dalla policy di esportazione applicabile, la richiesta non riesce e viene visualizzato un messaggio di autorizzazione negata. Se un client non corrisponde a nessuna regola nella policy di esportazione, l'accesso viene negato. Se un criterio di esportazione è vuoto, tutti gli accessi vengono implicitamente negati.

È possibile modificare dinamicamente un criterio di esportazione su un sistema che esegue ONTAP.

Policy di esportazione predefinita per le SVM

Ogni SVM dispone di un criterio di esportazione predefinito che non contiene regole. Prima che i client possano accedere ai dati su SVM, deve esistere un criterio di esportazione con regole. Ogni volume FlexVol contenuto nella SVM deve essere associato a una policy di esportazione.

Quando si crea una SVM, il sistema storage crea automaticamente una policy di esportazione predefinita chiamata `default` Per il volume root di SVM. È necessario creare una o più regole per il criterio di esportazione predefinito prima che i client possano accedere ai dati sulla SVM. In alternativa, è possibile creare una policy di esportazione personalizzata con regole. È possibile modificare e rinominare il criterio di esportazione predefinito, ma non è possibile eliminare il criterio di esportazione predefinito.

Quando si crea un volume FlexVol nella sua SVM contenente, il sistema di storage crea il volume e lo associa alla policy di esportazione predefinita per il volume root della SVM. Per impostazione predefinita, ogni volume creato in SVM è associato al criterio di esportazione predefinito per il volume root. È possibile utilizzare il criterio di esportazione predefinito per tutti i volumi contenuti in SVM oppure creare un criterio di esportazione univoco per ciascun volume. È possibile associare più volumi alla stessa policy di esportazione.

Come funzionano le regole di esportazione

Le regole di esportazione sono gli elementi funzionali di una policy di esportazione. Le regole di esportazione consentono di associare le richieste di accesso client a un volume a parametri specifici configurati per determinare come gestire le richieste di accesso client.

Un criterio di esportazione deve contenere almeno una regola di esportazione per consentire l'accesso ai client. Se un criterio di esportazione contiene più di una regola, le regole vengono elaborate nell'ordine in cui appaiono nel criterio di esportazione. L'ordine delle regole è determinato dal numero di indice delle regole. Se una regola corrisponde a un client, vengono utilizzate le autorizzazioni di tale regola e non vengono elaborate ulteriori regole. Se nessuna regola corrisponde, al client viene negato l'accesso.

È possibile configurare le regole di esportazione per determinare le autorizzazioni di accesso del client utilizzando i seguenti criteri:

- Il protocollo di accesso al file utilizzato dal client che invia la richiesta, ad esempio NFSv4 o SMB.
- Identificatore del client, ad esempio nome host o indirizzo IP.

  La dimensione massima di `-clientmatch` il campo è composto da 4096 caratteri.

- Il tipo di protezione utilizzato dal client per autenticare, ad esempio Kerberos v5, NTLM o AUTH_SYS.

Se una regola specifica più criteri, il client deve corrispondere a tutti i criteri affinché la regola venga applicata.

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

Esempio

Il criterio di esportazione contiene una regola di esportazione con i seguenti parametri:

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

La richiesta di accesso client viene inviata utilizzando il protocollo NFSv3 e il client ha l'indirizzo IP 10.1.17.37.

Anche se il protocollo di accesso client corrisponde, l'indirizzo IP del client si trova in una subnet diversa da quella specificata nella regola di esportazione. Pertanto, la corrispondenza dei client non riesce e questa regola non si applica a questo client.

Esempio

Il criterio di esportazione contiene una regola di esportazione con i seguenti parametri:

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

La richiesta di accesso client viene inviata utilizzando il protocollo NFSv4 e il client ha l'indirizzo IP 10.1.16.54.

Il protocollo di accesso client corrisponde e l'indirizzo IP del client si trova nella subnet specificata. Pertanto, la corrispondenza dei client viene eseguita correttamente e questa regola si applica a questo client. Il client ottiene l'accesso in lettura/scrittura indipendentemente dal tipo di protezione.

Esempio

Il criterio di esportazione contiene una regola di esportazione con i seguenti parametri:

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

Il client n. 1 ha l'indirizzo IP 10.1.16.207, invia una richiesta di accesso utilizzando il protocollo NFSv3 e viene autenticato con Kerberos v5.

Il client n. 2 ha l'indirizzo IP 10.1.16.211, invia una richiesta di accesso utilizzando il protocollo NFSv3 e viene autenticato con AUTH_SYS.

Il protocollo di accesso client e l'indirizzo IP corrispondono per entrambi i client. Il parametro di sola lettura consente l'accesso in sola lettura a tutti i client, indipendentemente dal tipo di protezione con cui sono stati autenticati. Pertanto, entrambi i client ottengono l'accesso in sola lettura. Tuttavia, solo il client n. 1 ottiene l'accesso in lettura/scrittura perché per l'autenticazione è stato utilizzato il tipo di protezione approvato Kerberos v5. Il client n. 2 non ottiene l'accesso in lettura/scrittura.

Gestire i client con un tipo di protezione non elencato

Quando un client si presenta con un tipo di protezione non elencato in un parametro di accesso di una regola di esportazione, è possibile scegliere di negare l'accesso al client o di associarlo all'ID utente anonimo utilizzando invece l'opzione `none` nel parametro access.

Un client potrebbe presentarsi con un tipo di protezione non elencato in un parametro di accesso perché autenticato con un tipo di protezione diverso o non autenticato affatto (tipo di protezione AUTH_NONE). Per impostazione predefinita, al client viene automaticamente negato l'accesso a tale livello. Tuttavia, è possibile aggiungere l'opzione `none` al parametro di accesso. Di conseguenza, i client con uno stile di sicurezza non elencato vengono mappati all'ID utente anonimo. Il `-anon` Il parametro determina l'ID utente assegnato a tali client. L'ID utente specificato per `-anon` il parametro deve essere un utente valido configurato con le autorizzazioni che si ritiene appropriate per l'utente anonimo.

Valori validi per `-anon` intervallo di parametri da `0` a. `65535`.

ID utente assegnato a. `-anon`	Gestione risultante delle richieste di accesso del client
`0 - 65533`	La richiesta di accesso client viene mappata all'ID utente anonimo e ottiene l'accesso in base alle autorizzazioni configurate per l'utente.
`65534`	La richiesta di accesso client viene mappata all'utente nessuno e ottiene l'accesso in base alle autorizzazioni configurate per l'utente. Questa è l'impostazione predefinita.
`65535`	La richiesta di accesso da qualsiasi client viene negata quando viene mappata a questo ID e il client si presenta con il tipo di sicurezza AUTH_NONE. La richiesta di accesso dai client con ID utente 0 viene negata quando viene mappata a questo ID e il client si presenta con qualsiasi altro tipo di sicurezza.

Quando si utilizza l'opzione `none`, è importante ricordare che il parametro di sola lettura viene elaborato per primo. Per configurare le regole di esportazione per i client con tipi di protezione non elencati, prendere in considerazione le seguenti linee guida:

Include la funzione di sola lettura `none`	La lettura/scrittura include `none`	Accesso risultante per i client con tipi di sicurezza non elencati
No	No	Negato
No	Sì	Negato perché viene elaborata per prima la sola lettura
Sì	No	Sola lettura come anonimo
Sì	Sì	Lettura/scrittura anonima

Esempio

Il criterio di esportazione contiene una regola di esportazione con i seguenti parametri:

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

Il client n. 1 ha l'indirizzo IP 10.1.16.207, invia una richiesta di accesso utilizzando il protocollo NFSv3 e viene autenticato con Kerberos v5.

Il client n. 2 ha l'indirizzo IP 10.1.16.211, invia una richiesta di accesso utilizzando il protocollo NFSv3 e viene

autenticato con AUTH_SYS.

Il client n. 3 ha l'indirizzo IP 10.1.16.234, invia una richiesta di accesso utilizzando il protocollo NFSv3 e non ha eseguito l'autenticazione (ovvero il tipo di protezione AUTH_NONE).

Il protocollo di accesso client e l'indirizzo IP corrispondono per tutti e tre i client. Il parametro di sola lettura consente l'accesso in sola lettura ai client con il proprio ID utente autenticato con AUTH_SYS. Il parametro di sola lettura consente l'accesso in sola lettura come utente anonimo con ID utente 70 ai client autenticati utilizzando qualsiasi altro tipo di protezione. Il parametro Read-write consente l'accesso in lettura/scrittura a qualsiasi tipo di protezione, ma in questo caso si applica solo ai client già filtrati dalla regola di sola lettura.

Pertanto, i client 1 e 3 ottengono l'accesso in lettura/scrittura solo come utente anonimo con ID utente 70. Il client n. 2 ottiene l'accesso in lettura/scrittura con il proprio ID utente.

Esempio

Il criterio di esportazione contiene una regola di esportazione con i seguenti parametri:

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

Il client n. 1 ha l'indirizzo IP 10.1.16.207, invia una richiesta di accesso utilizzando il protocollo NFSv3 e viene autenticato con Kerberos v5.

Il client n. 2 ha l'indirizzo IP 10.1.16.211, invia una richiesta di accesso utilizzando il protocollo NFSv3 e viene autenticato con AUTH_SYS.

Il client n. 3 ha l'indirizzo IP 10.1.16.234, invia una richiesta di accesso utilizzando il protocollo NFSv3 e non ha eseguito l'autenticazione (ovvero il tipo di protezione AUTH_NONE).

Il protocollo di accesso client e l'indirizzo IP corrispondono per tutti e tre i client. Il parametro di sola lettura consente l'accesso in sola lettura ai client con il proprio ID utente autenticato con AUTH_SYS. Il parametro di sola lettura consente l'accesso in sola lettura come utente anonimo con ID utente 70 ai client autenticati utilizzando qualsiasi altro tipo di protezione. Il parametro Read-write consente l'accesso in lettura/scrittura solo come utente anonimo.

Pertanto, il client n. 1 e il client n. 3 ottengono l'accesso in lettura/scrittura solo come utente anonimo con ID utente 70. Il client n. 2 ottiene l'accesso in sola lettura con il proprio ID utente, ma viene negato l'accesso in lettura/scrittura.

In che modo i tipi di sicurezza determinano i livelli di accesso del client

Il tipo di protezione autenticato dal client gioca un ruolo speciale nelle regole di esportazione. È necessario comprendere in che modo il tipo di protezione determina i livelli di accesso che il client ottiene a un volume o qtree.

I tre livelli di accesso possibili sono i seguenti:

1. Sola lettura

2. Lettura/scrittura
3. Superuser (per client con ID utente 0)

Poiché il livello di accesso in base al tipo di protezione viene valutato in questo ordine, è necessario osservare le seguenti regole quando si costruiscono i parametri del livello di accesso nelle regole di esportazione:

Per ottenere un livello di accesso da parte di un client…	**Questi parametri di accesso devono corrispondere al tipo di sicurezza del client…**
Utente normale di sola lettura	Sola lettura (`-rorule`)
Lettura/scrittura utente normale	Sola lettura (`-rorule`) e read-write (`-rwrule`)
Superuser di sola lettura	Sola lettura (`-rorule`) e. `-superuser`
Lettura/scrittura superutente	Sola lettura (`-rorule`) e read-write (`-rwrule`) e. `-superuser`

Di seguito sono riportati i tipi di protezione validi per ciascuno di questi tre parametri di accesso:

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

  Questo tipo di protezione non è valido per l'utilizzo con `-superuser` parametro.

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

Quando si abbina un tipo di sicurezza di un client a ciascuno dei tre parametri di accesso, si possono ottenere tre risultati:

Se il tipo di protezione del client…	**Quindi il client…**
Corrisponde a quello specificato nel parametro di accesso.	Ottiene l'accesso per quel livello con il proprio ID utente.
Non corrisponde a quello specificato, ma il parametro di accesso include l'opzione `none`.	Ottiene l'accesso per quel livello, ma come utente anonimo con l'ID utente specificato da `-anon` parametro.

Se il tipo di protezione del client…	Quindi il client…
Non corrisponde a quello specificato e il parametro di accesso non include l'opzione `none`.	Non ottiene alcun accesso per quel livello.questo non si applica a. `-superuser` parametro perché include sempre `none` anche se non specificato.

Esempio

Il criterio di esportazione contiene una regola di esportazione con i seguenti parametri:

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

Il client n. 1 ha l'indirizzo IP 10.1.16.207, ha l'ID utente 0, invia una richiesta di accesso utilizzando il protocollo NFSv3 e viene autenticato con Kerberos v5.

Il client n. 2 ha l'indirizzo IP 10.1.16.211, ha l'ID utente 0, invia una richiesta di accesso utilizzando il protocollo NFSv3 e viene autenticato con AUTH_SYS.

Il client n. 3 ha l'indirizzo IP 10.1.16.234, ha l'ID utente 0, invia una richiesta di accesso utilizzando il protocollo NFSv3 e non ha eseguito l'autenticazione (AUTH_NONE).

Il protocollo di accesso client e l'indirizzo IP corrispondono a tutti e tre i client. Il parametro di sola lettura consente l'accesso in sola lettura a tutti i client, indipendentemente dal tipo di protezione. Il parametro Read-write consente l'accesso in lettura/scrittura ai client con il proprio ID utente autenticato con AUTH_SYS o Kerberos v5. Il parametro superuser consente l'accesso del superutente ai client con ID utente 0 autenticati con Kerberos v5.

Pertanto, il client n. 1 ottiene l'accesso di lettura/scrittura superutente perché corrisponde a tutti e tre i parametri di accesso. Il client n. 2 ottiene l'accesso in lettura/scrittura ma non l'accesso al superutente. Il client n. 3 ottiene l'accesso in sola lettura, ma non l'accesso al superutente.

Gestire le richieste di accesso dei superutenti

Quando si configurano i criteri di esportazione, è necessario considerare ciò che si desidera che accada se il sistema storage riceve una richiesta di accesso client con ID utente 0, vale a dire come superutente, e impostare le regole di esportazione di conseguenza.

Nel mondo UNIX, un utente con ID utente 0 è noto come superutente, in genere chiamato root, che ha diritti di accesso illimitati su un sistema. L'utilizzo dei privilegi dei superutenti può essere pericoloso per diversi motivi, tra cui la violazione della sicurezza del sistema e dei dati.

Per impostazione predefinita, ONTAP esegue il mapping dei client che presentano l'ID utente 0 all'utente anonimo. Tuttavia, è possibile specificare `- superuser` Parametro nelle regole di esportazione per determinare come gestire i client che presentano ID utente 0 a seconda del tipo di protezione. Di seguito sono riportate le opzioni valide per `-superuser` parametro:

- `any`
- `none`

  Questa è l'impostazione predefinita se non si specifica `-superuser` parametro.

- `krb5`
- `ntlm`
- `sys`

Esistono due modi diversi per gestire i client che presentano un ID utente 0, a seconda di `-superuser` configurazione dei parametri:

Se il `-superuser` parametro e tipo di sicurezza del client…	Quindi il client…
Corrispondenza	Ottiene l'accesso al superutente con ID utente 0.
Non corrispondono	Ottiene l'accesso come utente anonimo con l'ID utente specificato da `-anon` e le relative autorizzazioni assegnate. Ciò indipendentemente dal fatto che il parametro di sola lettura o di lettura/scrittura specifichi l'opzione `none`.

Se un client presenta l'ID utente 0 per accedere a un volume con lo stile di protezione NTFS e a. `-superuser` il parametro è impostato su `none`, ONTAP utilizza la mappatura dei nomi per l'utente anonimo per ottenere le credenziali corrette.

Esempio

Il criterio di esportazione contiene una regola di esportazione con i seguenti parametri:

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

Il client n. 1 ha l'indirizzo IP 10.1.16.207, ha l'ID utente 746, invia una richiesta di accesso utilizzando il protocollo NFSv3 e viene autenticato con Kerberos v5.

Il client n. 2 ha l'indirizzo IP 10.1.16.211, ha l'ID utente 0, invia una richiesta di accesso utilizzando il protocollo NFSv3 e viene autenticato con AUTH_SYS.

Il protocollo di accesso client e l'indirizzo IP corrispondono per entrambi i client. Il parametro di sola lettura consente l'accesso in sola lettura a tutti i client, indipendentemente dal tipo di protezione con cui sono stati autenticati. Tuttavia, solo il client n. 1 ottiene l'accesso in lettura/scrittura perché per l'autenticazione è stato utilizzato il tipo di protezione approvato Kerberos v5.

Il client n. 2 non ottiene l'accesso superutente. Invece, viene mappato ad anonimo perché `-superuser`

parametro non specificato. Ciò significa che il valore predefinito è `none` E mappa automaticamente l'ID utente 0 in anonimo. Il client n. 2 ottiene anche solo l'accesso in sola lettura perché il tipo di protezione non corrisponde al parametro di lettura/scrittura.

Esempio

Il criterio di esportazione contiene una regola di esportazione con i seguenti parametri:

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

Il client n. 1 ha l'indirizzo IP 10.1.16.207, ha l'ID utente 0, invia una richiesta di accesso utilizzando il protocollo NFSv3 e viene autenticato con Kerberos v5.

Il client n. 2 ha l'indirizzo IP 10.1.16.211, ha l'ID utente 0, invia una richiesta di accesso utilizzando il protocollo NFSv3 e viene autenticato con AUTH_SYS.

Il protocollo di accesso client e l'indirizzo IP corrispondono per entrambi i client. Il parametro di sola lettura consente l'accesso in sola lettura a tutti i client, indipendentemente dal tipo di protezione con cui sono stati autenticati. Tuttavia, solo il client n. 1 ottiene l'accesso in lettura/scrittura perché per l'autenticazione è stato utilizzato il tipo di protezione approvato Kerberos v5. Il client n. 2 non ottiene l'accesso in lettura/scrittura.

La regola di esportazione consente l'accesso al superutente per i client con ID utente 0. Il client n. 1 ottiene l'accesso al superutente perché corrisponde all'ID utente e al tipo di sicurezza per la modalità di sola lettura e. `-superuser` parametri. Il client n. 2 non ottiene l'accesso in lettura/scrittura o superutente perché il suo tipo di protezione non corrisponde al parametro di lettura/scrittura o a. `-superuser` parametro. Invece, il client n. 2 viene mappato all'utente anonimo, che in questo caso ha l'ID utente 0.

Modalità di utilizzo delle cache delle policy di esportazione da parte di ONTAP

Per migliorare le performance del sistema, ONTAP utilizza cache locali per memorizzare informazioni come nomi host e netgroup. Ciò consente a ONTAP di elaborare le regole delle policy di esportazione più rapidamente rispetto al recupero delle informazioni da fonti esterne. La comprensione delle cache e delle relative funzioni può aiutare a risolvere i problemi di accesso dei client.

I criteri di esportazione vengono configurati per controllare l'accesso dei client alle esportazioni NFS. Ogni policy di esportazione contiene regole e ogni regola contiene parametri che consentono di associare la regola ai client che richiedono l'accesso. Alcuni di questi parametri richiedono che ONTAP contatti un'origine esterna, ad esempio server DNS o NIS, per risolvere oggetti come nomi di dominio, nomi host o netgroup.

Queste comunicazioni con le fonti esterne richiedono una piccola quantità di tempo. Per aumentare le performance, ONTAP riduce il tempo necessario per risolvere gli oggetti delle regole dei criteri di esportazione memorizzando le informazioni in locale su ciascun nodo in diverse cache.

Nome della cache	Tipo di informazioni memorizzate
Accesso	Mappature dei client ai criteri di esportazione corrispondenti
Nome	Mapping dei nomi utente UNIX agli ID utente UNIX corrispondenti
ID	Mapping degli ID utente UNIX agli ID utente UNIX corrispondenti e agli ID gruppo UNIX estesi
Host	Mapping dei nomi host agli indirizzi IP corrispondenti
Netgroup	Mapping dei netgroup agli indirizzi IP corrispondenti dei membri
Showmount	Elenco delle directory esportate dallo spazio dei nomi SVM

Se si modificano le informazioni sui server dei nomi esterni dell'ambiente dopo il recupero e l'archiviazione in locale da parte di ONTAP, le cache potrebbero ora contenere informazioni obsolete. Sebbene ONTAP aggiorni automaticamente le cache dopo determinati periodi di tempo, diverse cache hanno tempi di scadenza e refresh e algoritmi diversi.

Un'altra possibile ragione per cui le cache contengono informazioni obsolete è quando ONTAP tenta di aggiornare le informazioni memorizzate nella cache ma incontra un errore quando tenta di comunicare con i server dei nomi. In questo caso, ONTAP continua a utilizzare le informazioni attualmente memorizzate nelle cache locali per evitare interruzioni del client.

Di conseguenza, le richieste di accesso client che dovrebbero avere esito positivo potrebbero non riuscire e le richieste di accesso client che dovrebbero fallire potrebbero avere esito positivo. È possibile visualizzare e svuotare manualmente alcune cache delle policy di esportazione durante la risoluzione di tali problemi di accesso client.

Come funziona la cache di accesso

ONTAP utilizza una cache di accesso per memorizzare i risultati della valutazione delle regole dei criteri di esportazione per le operazioni di accesso client su un volume o qtree. Ciò comporta miglioramenti delle performance in quanto le informazioni possono essere recuperate molto più velocemente dalla cache di accesso rispetto al processo di valutazione delle regole dei criteri di esportazione ogni volta che un client invia una richiesta di i/O.

Ogni volta che un client NFS invia una richiesta di i/o per accedere ai dati su un volume o qtree, ONTAP deve valutare ogni richiesta di i/o per determinare se concedere o negare la richiesta di i/O. Questa valutazione implica il controllo di ogni regola dei criteri di esportazione dei criteri associati al volume o al qtree. Se il percorso al volume o al qtree comporta l'attraversamento di uno o più punti di giunzione, potrebbe essere necessario eseguire questa verifica per più policy di esportazione lungo il percorso.

Si noti che questa valutazione si verifica per ogni richiesta di i/o inviata da un client NFS, come lettura,

scrittura, elenco, copia e altre operazioni, non solo per le richieste di montaggio iniziali.

Dopo che ONTAP ha identificato le regole dei criteri di esportazione applicabili e ha deciso se consentire o negare la richiesta, ONTAP crea una voce nella cache di accesso per memorizzare queste informazioni.

Quando un client NFS invia una richiesta di i/o, ONTAP prende nota dell'indirizzo IP del client, dell'ID della SVM e della policy di esportazione associata al volume di destinazione o al qtree, quindi verifica prima la presenza di una voce corrispondente nella cache di accesso. Se nella cache di accesso esiste una voce corrispondente, ONTAP utilizza le informazioni memorizzate per consentire o negare la richiesta di i/O. Se non esiste una voce corrispondente, ONTAP passa attraverso il normale processo di valutazione di tutte le regole di policy applicabili, come spiegato in precedenza.

Le voci della cache di accesso non utilizzate attivamente non vengono aggiornate. In questo modo si riducono le comunicazioni inutili e dispendiose con i name serves esterni.

Il recupero delle informazioni dalla cache di accesso è molto più rapido rispetto all'intero processo di valutazione delle regole dei criteri di esportazione per ogni richiesta di i/O. Pertanto, l'utilizzo della cache di accesso migliora notevolmente le performance riducendo l'overhead dei controlli di accesso del client.

Come funzionano i parametri della cache di accesso

Diversi parametri controllano i periodi di refresh per le voci nella cache di accesso. La comprensione del funzionamento di questi parametri consente di modificarli per ottimizzare la cache di accesso e bilanciare le performance con la frequenza delle informazioni memorizzate.

La cache di accesso memorizza le voci costituite da una o più regole di esportazione applicabili ai client che tentano di accedere a volumi o qtree. Queste voci vengono memorizzate per un certo periodo di tempo prima dell'aggiornamento. Il tempo di refresh è determinato dai parametri della cache di accesso e dipende dal tipo di voce della cache di accesso.

È possibile specificare i parametri della cache di accesso per le singole SVM. In questo modo, i parametri possono variare in base ai requisiti di accesso SVM. Le voci della cache di accesso che non vengono utilizzate attivamente non vengono aggiornate, il che riduce le comunicazioni inutili e dispendiose con i server di nomi esterni.

Tipo di voce della cache di accesso	Descrizione	Periodo di refresh in secondi
Voci positive	Voci della cache di accesso che non hanno portato ad un DOS (Access Denial) per i client.	Minimo: 300 Massimo: 86,400 Predefinito: 3,600
Voci negative	Voci della cache di accesso che hanno portato ad un DOS (Access Denial) per i client.	Minimo: 60 Massimo: 86,400 Predefinito: 3,600

Esempio

Un client NFS tenta di accedere a un volume su un cluster. ONTAP associa il client a una regola dei criteri di

esportazione e determina che il client ottiene l'accesso in base alla configurazione della regola dei criteri di esportazione. ONTAP memorizza la regola dei criteri di esportazione nella cache di accesso come voce positiva. Per impostazione predefinita, ONTAP mantiene la voce positiva nella cache di accesso per un'ora (3,600 secondi), quindi aggiorna automaticamente la voce per mantenere aggiornate le informazioni.

Per evitare che la cache di accesso si riempia inutilmente, è disponibile un parametro aggiuntivo per cancellare le voci della cache di accesso esistenti che non sono state utilizzate per un certo periodo di tempo per decidere l'accesso del client. Questo `-harvest-timeout` il parametro ha un intervallo consentito compreso tra 60 e 2,592,000 secondi e un'impostazione predefinita di 86,400 secondi.

Rimuovere un criterio di esportazione da un qtree

Se si decide di non assegnare più un criterio di esportazione specifico a un qtree, è possibile rimuovere il criterio di esportazione modificando il qtree in modo da ereditare il criterio di esportazione del volume contenente. Per eseguire questa operazione, utilizzare `volume qtree modify` con il `-export-policy` e una stringa di nome vuota ("").

Fasi

1. Per rimuovere un criterio di esportazione da un qtree, immettere il seguente comando:

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

2. Verificare che il qtree sia stato modificato di conseguenza:

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

Convalidare gli ID qtree per le operazioni del file qtree

ONTAP può eseguire un'ulteriore convalida facoltativa degli ID qtree. Questa convalida garantisce che le richieste di operazione del file client utilizzino un ID qtree valido e che i client possano spostare solo i file all'interno dello stesso qtree. È possibile attivare o disattivare questa convalida modificando il `-validate-qtree-export` parametro. Questo parametro è attivato per impostazione predefinita.

A proposito di questa attività

Questo parametro è valido solo se è stata assegnata una policy di esportazione direttamente a uno o più qtree sulla macchina virtuale di storage (SVM).

Fasi

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

   ```
   set -privilege advanced
   ```

2. Eseguire una delle seguenti operazioni:

Se si desidera che la convalida dell'ID qtree sia…	Immettere il seguente comando…
Attivato	`vserver nfs modify -vserver vserver_name -validate-qtree-export enabled`
Disattivato	`vserver nfs modify -vserver vserver_name -validate-qtree-export disabled`

3. Tornare al livello di privilegio admin:

   ```
   set -privilege admin
   ```

Restrizioni dei criteri di esportazione e giunzioni nidificate per i volumi FlexVol

Se sono stati configurati criteri di esportazione per impostare un criterio meno restrittivo su una giunzione nidificata ma un criterio più restrittivo su una giunzione di livello superiore, l'accesso alla giunzione di livello inferiore potrebbe non riuscire.

È necessario garantire che le giunzioni di livello superiore abbiano policy di esportazione meno restrittive rispetto alle giunzioni di livello inferiore.

Utilizzo di Kerberos con NFS per una maggiore sicurezza

Supporto ONTAP per Kerberos

Kerberos offre un'autenticazione sicura e sicura per le applicazioni client/server. L'autenticazione consente di verificare le identità di utenti e processi di un server. Nell'ambiente ONTAP, Kerberos fornisce l'autenticazione tra le macchine virtuali di storage (SVM) e i client NFS.

In ONTAP 9, sono supportate le seguenti funzionalità Kerberos:

- Autenticazione Kerberos 5 con controllo dell'integrità (krb5i)

  Krb5i utilizza checksum per verificare l'integrità di ogni messaggio NFS trasferito tra client e server. Ciò è utile sia per motivi di sicurezza (ad esempio, per garantire che i dati non siano stati manomessi) che per motivi di integrità dei dati (ad esempio, per prevenire la corruzione dei dati quando si utilizza NFS su reti non affidabili).

- Autenticazione Kerberos 5 con controllo della privacy (krb5p)

  Krb5p utilizza checksum per crittografare tutto il traffico tra il client e il server. Questo è più sicuro e comporta un carico maggiore.

- Crittografia AES a 128 e 256 bit

  Advanced Encryption Standard (AES) è un algoritmo di crittografia per la protezione dei dati elettronici. ONTAP supporta AES con chiavi a 128 bit (AES-128) e AES con chiavi a 256 bit (AES-256) per Kerberos

per una maggiore protezione.

- Configurazioni di area di autenticazione Kerberos a livello di SVM

  Gli amministratori di SVM possono ora creare configurazioni di area di autenticazione Kerberos a livello di SVM. Ciò significa che gli amministratori di SVM non devono più affidarsi all'amministratore del cluster per la configurazione dell'area di autenticazione Kerberos e possono creare singole configurazioni dell'area di autenticazione Kerberos in un ambiente multi-tenancy.

Requisiti per la configurazione di Kerberos con NFS

Prima di configurare Kerberos con NFS sul sistema, è necessario verificare che alcuni elementi dell'ambiente di rete e di storage siano configurati correttamente.

> La procedura per configurare l'ambiente dipende dalla versione e dal tipo di sistema operativo client, controller di dominio, Kerberos, DNS e così via. che stai utilizzando. La documentazione di tutte queste variabili non rientra nell'ambito di questo documento. Per ulteriori informazioni, consultare la documentazione relativa a ciascun componente.
>
> Per un esempio dettagliato di come configurare ONTAP e Kerberos 5 con NFSv3 e NFSv4 in un ambiente che utilizza Active Directory di Windows Server 2008 R2 e host Linux, consultare il report tecnico 4073.

È necessario configurare prima i seguenti elementi:

Requisiti dell'ambiente di rete

- Kerberos

  È necessario disporre di una configurazione Kerberos funzionante con un centro di distribuzione delle chiavi (KDC), ad esempio Kerberos basato su Windows Active Directory o MIT Kerberos.

  I server NFS devono utilizzare `nfs` come componente principale del computer.

- Servizio di directory

  È necessario utilizzare un servizio directory sicuro nell'ambiente, ad esempio Active Directory o OpenLDAP, configurato per l'utilizzo di LDAP su SSL/TLS.

- NTP

  È necessario disporre di un server dell'orario di lavoro che esegue NTP. Ciò è necessario per evitare errori di autenticazione Kerberos dovuti a un disallineamento temporale.

- DNS (Domain Name Resolution)

  Ciascun client UNIX e ciascun LIF SVM devono disporre di un record di servizio (SRV) appropriato registrato con il KDC nelle zone di ricerca in avanti e indietro. Tutti i partecipanti devono essere risolutibili correttamente tramite DNS.

- Account utente

  Ogni client deve disporre di un account utente nell'area Kerberos. I server NFS devono utilizzare "nfs" come componente principale del computer.

Requisiti del client NFS

- NFS

  Ciascun client deve essere configurato correttamente per comunicare in rete utilizzando NFSv3 o NFSv4.

  I client devono supportare RFC1964 e RFC2203.

- Kerberos

  Ciascun client deve essere configurato correttamente per utilizzare l'autenticazione Kerberos, inclusi i seguenti dettagli:

  - La crittografia per la comunicazione TGS è attivata.

    AES-256 per la massima sicurezza.

  - Il tipo di crittografia più sicuro per la comunicazione TGT è attivato.
  - Il dominio e l'area di autenticazione Kerberos sono configurati correttamente.
  - Il GSS è attivato.

    Quando si utilizzano le credenziali del computer:

  - Non eseguire `gssd` con `-n` parametro.
  - Non eseguire `kinit` come utente root.

- Ogni client deve utilizzare la versione più recente e aggiornata del sistema operativo.

  In questo modo si ottiene la migliore compatibilità e affidabilità per la crittografia AES con Kerberos.

- DNS

  Ciascun client deve essere configurato correttamente per utilizzare il DNS per la corretta risoluzione dei nomi.

- NTP

  Ciascun client deve essere sincronizzato con il server NTP.

- Informazioni su host e dominio

  Di ogni client `/etc/hosts` e. `/etc/resolv.conf` I file devono contenere rispettivamente il nome host e le informazioni DNS corretti.

- File keytab

  Ogni client deve avere un file keytab dal KDC. L'area di autenticazione deve essere in lettere maiuscole. Il tipo di crittografia deve essere AES-256 per garantire la massima sicurezza.

- Opzionale: Per ottenere le migliori performance, i client traggono vantaggio dalla presenza di almeno due interfacce di rete: Una per la comunicazione con la rete locale e una per la comunicazione con la rete di storage.

Requisiti di sistema per lo storage

- Licenza NFS

  Il sistema storage deve avere una licenza NFS valida installata.

- Licenza CIFS

  La licenza CIFS è opzionale. È necessario solo per il controllo delle credenziali Windows quando si utilizza la mappatura dei nomi multiprotocollo. Non è richiesto in un ambiente UNIX-only rigoroso.

- SVM

  È necessario configurare almeno una SVM sul sistema.

- DNS su SVM

  È necessario aver configurato il DNS su ogni SVM.

- Server NFS

  È necessario aver configurato NFS su SVM.

- Crittografia AES

  Per una maggiore sicurezza, è necessario configurare il server NFS in modo che consenta solo la crittografia AES-256 per Kerberos.

- Server SMB

  Se si utilizza un ambiente multiprotocollo, è necessario aver configurato SMB su SVM. Il server SMB è necessario per la mappatura dei nomi multiprotocollo.

- Volumi

  È necessario disporre di un volume root e di almeno un volume di dati configurati per l'utilizzo da parte di SVM.

- Volume root

  Il volume root di SVM deve avere la seguente configurazione:

Nome	Impostazione
Stile di sicurezza	UNIX
UID	Root o ID 0
GID	Root o ID 0
Autorizzazioni UNIX	777

  A differenza del volume root, i volumi di dati possono avere uno stile di sicurezza.

- Gruppi UNIX

  La SVM deve avere i seguenti gruppi UNIX configurati:

Nome del gruppo	ID gruppo
daemon	1
root	0
pcuser	65534 (creato automaticamente da ONTAP quando si crea la SVM)

- Utenti UNIX

  La SVM deve avere i seguenti utenti UNIX configurati:

Nome utente	ID utente	ID gruppo primario	Commento
nfs	500	0	Necessario per la fase DI INIT GSS Il primo componente dell'SPN dell'utente client NFS viene utilizzato come utente.
pcuser	65534	65534	Necessario per l'utilizzo multiprotocollo NFS e CIFS Creato e aggiunto automaticamente al gruppo pcuser da ONTAP quando si crea la SVM.
root	0	0	Necessario per il montaggio

  L'utente nfs non è richiesto se esiste una mappatura dei nomi Kerberos-UNIX per l'SPN dell'utente client NFS.

- Policy e regole di esportazione

  È necessario aver configurato i criteri di esportazione con le regole di esportazione necessarie per i volumi root e dati e qtree. Se si accede a tutti i volumi della SVM tramite Kerberos, è possibile impostare le opzioni della regola di esportazione `-rorule`, `-rwrule`, e. `-superuser` per il volume root a. `krb5` , `krb5i`, o. `krb5p`.

- Mappatura dei nomi Kerberos-UNIX

Se si desidera che l'utente identificato dall'utente client NFS SPN disponga delle autorizzazioni root, è necessario creare una mappatura dei nomi nella directory root.

Informazioni correlate

"Report tecnico di NetApp 4073: Autenticazione unificata sicura"

"Tool di matrice di interoperabilità NetApp"

"Amministrazione del sistema"

"Gestione dello storage logico"

Specificare il dominio ID utente per NFSv4

Per specificare il dominio ID utente, è possibile impostare `-v4-id-domain` opzione.

A proposito di questa attività

Per impostazione predefinita, ONTAP utilizza il dominio NIS per il mapping dell'ID utente NFSv4, se impostato. Se non viene impostato un dominio NIS, viene utilizzato il dominio DNS. Potrebbe essere necessario impostare il dominio ID utente se, ad esempio, si dispone di più domini ID utente. Il nome di dominio deve corrispondere alla configurazione del dominio sul controller di dominio. Non è richiesto per NFSv3.

Fase

1. Immettere il seguente comando:

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

Configurare i name service

Funzionamento della configurazione dello switch ONTAP name service

ONTAP memorizza le informazioni di configurazione del name service in una tabella equivalente a `/etc/nsswitch.conf` File su sistemi UNIX. È necessario comprendere la funzione della tabella e il modo in cui ONTAP la utilizza in modo da poterla configurare in modo appropriato per l'ambiente in uso.

La tabella ONTAP name service switch determina le origini del servizio di nomi che ONTAP consulta per recuperare le informazioni relative a un determinato tipo di informazioni sul servizio di nomi. ONTAP gestisce una tabella di switch del name service separata per ogni SVM.

Tipi di database

La tabella memorizza un elenco di name service separato per ciascuno dei seguenti tipi di database:

Tipo di database	Definisce le origini del servizio nome per…	Le origini valide sono…
host	Conversione dei nomi host in indirizzi IP	file, dns

Tipo di database	Definisce le origini del servizio nome per…	Le origini valide sono…
gruppo	Ricerca di informazioni sul gruppo di utenti	file, nis, ldap
password	Ricerca delle informazioni dell'utente	file, nis, ldap
netgroup	Ricerca di informazioni sul netgroup	file, nis, ldap
mappa dei nomi	Mappatura dei nomi utente	file, ldap

Tipi di origine

Le origini specificano quale nome di origine del servizio utilizzare per recuperare le informazioni appropriate.

Specifica tipo di origine…	Per cercare informazioni in…	Gestito dalle famiglie di comandi…

file	File di origine locali	`vserver services name-service unix-user` `vserver services name-service unix-group`
		
		`vserver services name-service netgroup`
		
		`vserver services name-service dns hosts`

nis	Server NIS esterni come specificato nella configurazione del dominio NIS di SVM	`vserver services name-service nis-domain`
ldap	Server LDAP esterni come specificato nella configurazione del client LDAP di SVM	`vserver services name-service ldap`
dns	Server DNS esterni come specificato nella configurazione DNS di SVM	`vserver services name-service dns`

Anche se si prevede di utilizzare NIS o LDAP per l'accesso ai dati e l'autenticazione dell'amministrazione SVM, è comunque necessario includere `files` E configurare gli utenti locali come fallback nel caso in cui l'autenticazione NIS o LDAP non riesca.

Protocolli utilizzati per accedere a fonti esterne

Per accedere ai server per le origini esterne, ONTAP utilizza i seguenti protocolli:

Origine esterna del name service	Protocollo utilizzato per l'accesso
NIS	UDP
DNS	UDP
LDAP	TCP

Esempio

Nell'esempio seguente viene visualizzata la configurazione dello switch name service per SVM svm_1:

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

Per cercare gli indirizzi IP degli host, ONTAP consulta innanzitutto i file di origine locali. Se la query non restituisce alcun risultato, i server DNS vengono controllati in seguito.

Per cercare informazioni su utenti o gruppi, ONTAP consulta solo i file di origine locali. Se la query non restituisce alcun risultato, la ricerca non riesce.

Per cercare informazioni sui netgroup, ONTAP consulta prima i server NIS esterni. Se la query non restituisce alcun risultato, viene selezionato il file netgroup locale.

Non sono presenti voci di name service per la mappatura dei nomi nella tabella per SVM svm_1. Pertanto, ONTAP consulta solo i file di origine locali per impostazione predefinita.

Informazioni correlate

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

Utilizzare LDAP

Panoramica LDAP

Un server LDAP (Lightweight Directory Access Protocol) consente di gestire centralmente le informazioni dell'utente. Se si memorizza il database utente su un server LDAP nell'ambiente in uso, è possibile configurare il sistema di storage in modo che cerchi le informazioni utente nel database LDAP esistente.

- Prima di configurare LDAP per ONTAP, verificare che l'implementazione del sito soddisfi le Best practice per la configurazione del server e del client LDAP. In particolare, devono essere soddisfatte le seguenti condizioni:
  - Il nome di dominio del server LDAP deve corrispondere alla voce del client LDAP.
  - I tipi di hash della password utente LDAP supportati dal server LDAP devono includere quelli supportati da ONTAP:
    - CRYPT (tutti i tipi) e SHA-1 (SHA, SSHA).
    - A partire da ONTAP 9.8, hash SHA-2 (SHA-256, SSH-384, SHA-512, SSHA-256, Sono supportati anche SSHA-384 e SSHA-512).
  - Se il server LDAP richiede misure di protezione della sessione, è necessario configurarle nel client LDAP.

    Sono disponibili le seguenti opzioni di sicurezza della sessione:

    - Firma LDAP (verifica dell'integrità dei dati) e firma e sigillatura LDAP (verifica e crittografia dell'integrità dei dati)
    - AVVIARE TLS
    - LDAPS (LDAP su TLS o SSL)
  - Per abilitare le query LDAP firmate e sealed, è necessario configurare i seguenti servizi:
    - I server LDAP devono supportare il meccanismo GSSAPI (Kerberos) SASL.
    - I server LDAP devono disporre di record DNS A/AAAA e di record PTR impostati sul server DNS.
    - I server Kerberos devono avere record SRV presenti sul server DNS.
  - Per abilitare L'AVVIO di TLS o LDAPS, tenere in considerazione i seguenti punti.
    - L'utilizzo di Start TLS anziché LDAPS è una Best practice di NetApp.
    - Se si utilizza LDAPS, il server LDAP deve essere abilitato per TLS o per SSL in ONTAP 9.5 e versioni successive. SSL non è supportato in ONTAP 9.0-9.4.
    - Nel dominio deve essere già configurato un server dei certificati.
  - Per abilitare la funzione LDAP referral chasing (in ONTAP 9.5 e versioni successive), devono essere soddisfatte le seguenti condizioni:
    - Entrambi i domini devono essere configurati con una delle seguenti relazioni di trust:
      - Bidirezionale
      - Unidirezionale, in cui il primario si affida al dominio di riferimento
      - Genitore-figlio
    - Il DNS deve essere configurato in modo da risolvere tutti i nomi dei server indicati.
    - Le password di dominio devono essere le stesse per autenticare quando `--bind-as-cifs-server` impostare su true.

Le seguenti configurazioni non sono supportate con la funzione LDAP referral chasing.

- Per tutte le versioni di ONTAP:
- Client LDAP su una SVM amministrativa
- Per ONTAP 9.8 e versioni precedenti (sono supportati nella versione 9.9.1 e successive):
- Firma e sigillatura LDAP (il `-session-security` opzionale)
- Connessioni TLS crittografate (il `-use-start-tls` opzionale)
- Comunicazioni tramite la porta LDAPS 636 (la `-use-ldaps-for-ad-ldap` opzionale)

- A partire da ONTAP 9.11.1, è possibile utilizzare "LDAP fast bind per l'autenticazione nsswitch."
- È necessario inserire uno schema LDAP durante la configurazione del client LDAP su SVM.

  Nella maggior parte dei casi, uno degli schemi ONTAP predefiniti sarà appropriato. Tuttavia, se lo schema LDAP nel proprio ambiente differisce da questi, è necessario creare un nuovo schema client LDAP per ONTAP prima di creare il client LDAP. Rivolgersi all'amministratore LDAP per informazioni sui requisiti dell'ambiente in uso.

- L'utilizzo di LDAP per la risoluzione dei nomi host non è supportato.

Per ulteriori informazioni, vedere "Report tecnico di NetApp 4835: Come configurare LDAP in ONTAP".

Concetti relativi alla firma e al sealing LDAP

A partire da ONTAP 9, è possibile configurare la firma e il sealing per abilitare la sicurezza della sessione LDAP sulle query a un server Active Directory (ad). È necessario configurare le impostazioni di sicurezza del server NFS sulla macchina virtuale di storage (SVM) in modo che corrispondano a quelle del server LDAP.

La firma conferma l'integrità dei dati del payload LDAP utilizzando la tecnologia a chiave segreta. Il sealing crittografa i dati del payload LDAP per evitare la trasmissione di informazioni sensibili in testo non crittografato. Un'opzione *LDAP Security Level* indica se il traffico LDAP deve essere firmato, firmato e sigillato o no. L'impostazione predefinita è `none`. test

La firma LDAP e il sealing sul traffico SMB sono attivati sulla SVM con `-session-security-for-ad-ldap` al `vserver cifs security modify` comando.

Concetti LDAPS

È necessario comprendere alcuni termini e concetti relativi al modo in cui ONTAP protegge le comunicazioni LDAP. ONTAP può utilizzare TLS O LDAPS DI AVVIO per impostare sessioni autenticate tra server LDAP integrati in Active Directory o server LDAP basati su UNIX.

Terminologia

È necessario comprendere alcuni termini relativi all'utilizzo di LDAPS da parte di ONTAP per proteggere le comunicazioni LDAP.

- **LDAP**

  (Lightweight Directory Access Protocol) protocollo per l'accesso e la gestione delle directory di informazioni. LDAP viene utilizzato come directory di informazioni per la memorizzazione di oggetti come utenti, gruppi e netgroup. LDAP fornisce inoltre servizi di directory che gestiscono questi oggetti e soddisfano le richieste LDAP dai client LDAP.

- **SSL**

  (Secure Sockets Layer) protocollo sviluppato per l'invio sicuro di informazioni su Internet. SSL è supportato da ONTAP 9 e versioni successive, ma è stato deprecato a favore di TLS.

- **TLS**

  (Transport Layer Security) un protocollo di tracciamento degli standard IETF basato sulle specifiche SSL precedenti. È il successore di SSL. TLS è supportato da ONTAP 9,5 e versioni successive.

- **LDAPS (LDAP su SSL o TLS)**

  Protocollo che utilizza TLS o SSL per proteggere le comunicazioni tra client LDAP e server LDAP. I termini *LDAP su SSL* e *LDAP su TLS* vengono talvolta utilizzati in modo intercambiabile. LDAPS è supportato da ONTAP 9,5 e versioni successive.

  - In ONTAP 9.5-9.8, LDAPS può essere attivato solo sulla porta 636. A tale scopo, utilizzare `-use-ldaps-for-ad-ldap` con il `vserver cifs security modify` comando.
  - A partire da ONTAP 9.9.1, LDAPS può essere attivato su qualsiasi porta, anche se la porta 636 rimane quella predefinita. A tale scopo, impostare `-ldaps-enabled` parametro a. `true` e specificare il desiderato `-port` parametro. Per ulteriori informazioni, consultare `vserver services name-service ldap client create` pagina man

  L'utilizzo di Start TLS anziché LDAPS è una Best practice di NetApp.

- **Avvia TLS**

  (Noto anche come *start_tls*, *STARTTLS* e *STARTTLS*) un meccanismo per fornire comunicazioni sicure utilizzando i protocolli TLS.

  ONTAP utilizza STARTTLS per proteggere la comunicazione LDAP e la porta LDAP predefinita (389) per comunicare con il server LDAP. Il server LDAP deve essere configurato in modo da consentire le connessioni sulla porta LDAP 389; in caso contrario, le connessioni LDAP TLS dalla SVM al server LDAP non funzionano.

Utilizzo di LDAPS da parte di ONTAP

ONTAP supporta l'autenticazione del server TLS, che consente al client LDAP SVM di confermare l'identità del server LDAP durante l'operazione di binding. I client LDAP abilitati per TLS possono utilizzare tecniche standard di crittografia a chiave pubblica per verificare che il certificato e l'ID pubblico di un server siano validi e siano stati emessi da un'autorità di certificazione (CA) elencata nell'elenco delle CA attendibili del client.

LDAP supporta STARTTLS per crittografare le comunicazioni utilizzando TLS. STARTTLS inizia come connessione non crittografata sulla porta LDAP standard (389) e la connessione viene quindi aggiornata a TLS.

ONTAP supporta:

- LDAPS per il traffico SMB tra i server LDAP integrati in Active Directory e SVM
- LDAPS per il traffico LDAP per la mappatura dei nomi e altre informazioni UNIX

  I server LDAP integrati in Active Directory o i server LDAP basati su UNIX possono essere utilizzati per memorizzare informazioni per la mappatura dei nomi LDAP e altre informazioni UNIX, come utenti, gruppi e netgroup.

- Certificati della CA principale autofirmati

  Quando si utilizza un LDAP integrato in Active-Directory, il certificato root autofirmato viene generato quando il servizio certificati di Windows Server viene installato nel dominio. Quando si utilizza un server LDAP basato su UNIX per la mappatura dei nomi LDAP, il certificato root autofirmato viene generato e salvato utilizzando i mezzi appropriati per l'applicazione LDAP.

Per impostazione predefinita, LDAPS è disattivato.

Attiva il supporto LDAP RFC2307bis

Se si desidera utilizzare LDAP e si desidera utilizzare le appartenenze a gruppi nidificati, è possibile configurare ONTAP per abilitare il supporto di LDAP RFC2307bis.

Di cosa hai bisogno

È necessario aver creato una copia di uno degli schemi client LDAP predefiniti che si desidera utilizzare.

A proposito di questa attività

Negli schemi client LDAP, gli oggetti di gruppo utilizzano l'attributo memberUid. Questo attributo può contenere più valori ed elenca i nomi degli utenti che appartengono a quel gruppo. Negli schemi client LDAP abilitati per RFC2307bis, gli oggetti di gruppo utilizzano l'attributo uniqueMember. Questo attributo può contenere il nome distinto completo (DN) di un altro oggetto nella directory LDAP. In questo modo è possibile utilizzare gruppi nidificati poiché i gruppi possono avere altri gruppi come membri.

L'utente non deve essere membro di più di 256 gruppi, inclusi i gruppi nidificati. ONTAP ignora tutti i gruppi che superano il limite di 256 gruppi.

Per impostazione predefinita, il supporto RFC2307bis è disattivato.

> Il supporto RFC2307bis viene attivato automaticamente in ONTAP quando viene creato un client LDAP con lo schema MS-ad-BIS.

Per ulteriori informazioni, vedere "Report tecnico di NetApp 4835: Come configurare LDAP in ONTAP".

Fasi

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

   ```
   set -privilege advanced
   ```

2. Modificare lo schema del client LDAP RFC2307 copiato per abilitare il supporto RFC2307bis:

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

3. Modificare lo schema in modo che corrisponda alla classe di oggetti supportata nel server LDAP:

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

4. Modificare lo schema in modo che corrisponda al nome dell'attributo supportato nel server LDAP:

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

5. Tornare al livello di privilegio admin:

```
set -privilege admin
```

Opzioni di configurazione per le ricerche nelle directory LDAP

È possibile ottimizzare le ricerche nelle directory LDAP, incluse le informazioni relative a utenti, gruppi e netgroup, configurando il client LDAP di ONTAP per la connessione ai server LDAP nel modo più appropriato per il proprio ambiente. È necessario capire quando sono sufficienti i valori di ricerca predefiniti di base e ambito LDAP e quali parametri specificare quando i valori personalizzati sono più appropriati.

Le opzioni di ricerca del client LDAP per le informazioni relative a utenti, gruppi e netgroup possono aiutare a evitare query LDAP non riuscite e, di conseguenza, l'accesso del client ai sistemi di storage non riuscito. Inoltre, contribuiscono a garantire che le ricerche siano il più efficienti possibile per evitare problemi di performance del client.

Valori di base e di ricerca dell'ambito predefiniti

La base LDAP è il DN di base predefinito utilizzato dal client LDAP per eseguire query LDAP. Tutte le ricerche, incluse quelle relative a utenti, gruppi e netgroup, vengono eseguite utilizzando il DN di base. Questa opzione è appropriata quando la directory LDAP è relativamente piccola e tutte le voci pertinenti si trovano nello stesso DN.

Se non si specifica un DN di base personalizzato, il valore predefinito è `root`. Ciò significa che ogni query esegue la ricerca nell'intera directory. Sebbene questo massimizzi le possibilità di successo della query LDAP, può essere inefficiente e causare una riduzione significativa delle prestazioni con directory LDAP di grandi dimensioni.

L'ambito di base LDAP è l'ambito di ricerca predefinito utilizzato dal client LDAP per eseguire query LDAP. Tutte le ricerche, incluse quelle relative a utenti, gruppi e netgroup, vengono eseguite utilizzando l'ambito di base. Determina se la query LDAP ricerca solo la voce denominata, le voci di un livello al di sotto del DN o l'intera sottostruttura al di sotto del DN.

Se non si specifica un ambito di base personalizzato, il valore predefinito è `subtree`. Ciò significa che ogni query esegue la ricerca nell'intero sottostruttura sotto il DN. Sebbene questo massimizzi le possibilità di successo della query LDAP, può essere inefficiente e causare una riduzione significativa delle prestazioni con directory LDAP di grandi dimensioni.

Valori di ricerca di base e ambito personalizzati

In alternativa, è possibile specificare valori di base e di ambito separati per le ricerche di utenti, gruppi e netgroup. La limitazione della base di ricerca e dell'ambito delle query in questo modo può migliorare significativamente le prestazioni, poiché limita la ricerca a una sottosezione più piccola della directory LDAP.

Se si specificano valori di base e ambito personalizzati, questi sovrascrivono la base di ricerca predefinita generale e l'ambito per le ricerche di utenti, gruppi e netgroup. I parametri per specificare i valori di base e ambito personalizzati sono disponibili a livello di privilegio avanzato.

Parametro client LDAP…	Specifica custom…
`-base-dn`	DN di base per tutte le ricerche LDAP è possibile inserire più valori, se necessario (ad esempio, se la funzione LDAP referral chasing è attivata in ONTAP 9.5 e versioni successive).
`-base-scope`	Ambito di base per tutte le ricerche LDAP
`-user-dn`	DNS di base per tutte le ricerche degli utenti LDAP questo parametro si applica anche alle ricerche di mappatura dei nomi utente.
`-user-scope`	Ambito di base per tutte le ricerche degli utenti LDAP questo parametro si applica anche alle ricerche di associazione dei nomi utente.
`-group-dn`	DNS di base per tutte le ricerche di gruppi LDAP
`-group-scope`	Ambito di base per tutte le ricerche di gruppi LDAP
`-netgroup-dn`	DNS di base per tutte le ricerche dei netgroup LDAP
`-netgroup-scope`	Ambito di base per tutte le ricerche dei netgroup LDAP

Più valori DN di base personalizzati

Se la struttura della directory LDAP è più complessa, potrebbe essere necessario specificare più DNS di base per cercare determinate informazioni in più parti della directory LDAP. È possibile specificare più DNS per i parametri DN dell'utente, del gruppo e del netgroup separandoli con un punto e virgola (;) e racchiudendo l'intero elenco di ricerca DN con virgolette doppie ("). Se un DN contiene un punto e virgola, è necessario aggiungere un carattere di escape () immediatamente prima del punto e virgola nel DN.

Si noti che l'ambito si applica all'intero elenco di DNS specificato per il parametro corrispondente. Ad esempio, se si specifica un elenco di tre diversi DNS utente e sottostruttura per l'ambito utente, l'utente LDAP ricerca nell'intera sottostruttura ciascuno dei tre DNS specificati.

A partire da ONTAP 9.5, è anche possibile specificare LDAP *referral chasing*, che consente al client LDAP di indirizzare le richieste di ricerca ad altri server ONTAP se il server LDAP primario non restituisce una risposta di riferimento LDAP. Il client utilizza i dati di riferimento per recuperare l'oggetto di destinazione dal server descritto nei dati di riferimento. Per cercare oggetti presenti nei server LDAP indicati, è possibile aggiungere la base-dn degli oggetti indicati alla base-dn come parte della configurazione del client LDAP. Tuttavia, gli oggetti referrati vengono ricercati solo quando è attivata la funzione di referral chasing (ricerca riferimenti), utilizzando il `-referral-enabled true` Durante la creazione o la modifica del client LDAP.

Migliorare le performance delle ricerche di directory LDAP netgroup-by-host

Se l'ambiente LDAP è configurato per consentire ricerche netgroup-by-host, è possibile

configurare ONTAP in modo che ne tragga vantaggio ed eseguire ricerche netgroup-by-host. In questo modo è possibile accelerare notevolmente le ricerche dei netgroup e ridurre i possibili problemi di accesso al client NFS dovuti alla latenza durante le ricerche dei netgroup.

Di cosa hai bisogno

La directory LDAP deve contenere un `netgroup.byhost` mappa.

I server DNS devono contenere record di ricerca sia in avanti (A) che in retromarcia (PTR) per i client NFS.

Quando si specificano gli indirizzi IPv6 nei netgroup, è sempre necessario accorciare e comprimere ciascun indirizzo come specificato in RFC 5952.

A proposito di questa attività

I server NIS memorizzano le informazioni del netgroup in tre mappe distinte denominate `netgroup`, `netgroup.byuser`, e. `netgroup.byhost`. Lo scopo di `netgroup.byuser` e. `netgroup.byhost` maps consente di velocizzare le ricerche di netgroup. ONTAP può eseguire ricerche netgroup-by-host sui server NIS per migliorare i tempi di risposta del montaggio.

Per impostazione predefinita, le directory LDAP non dispongono di tale opzione `netgroup.byhost` mappare come i server NIS. Tuttavia, con l'aiuto di strumenti di terze parti, è possibile importare un NIS `netgroup.byhost` eseguire la mappatura nelle directory LDAP per consentire ricerche rapide netgroup-by-host. Se l'ambiente LDAP è stato configurato per consentire ricerche netgroup-by-host, è possibile configurare il client LDAP ONTAP con `netgroup.byhost` nome mappa, DN e ambito di ricerca per ricerche più rapide tra netgroup e host.

La ricezione più rapida dei risultati per le ricerche netgroup-by-host consente a ONTAP di elaborare più rapidamente le regole di esportazione quando i client NFS richiedono l'accesso alle esportazioni. In questo modo si riduce la possibilità di ritardi di accesso dovuti a problemi di latenza della ricerca nel netgroup.

Fasi

1. Ottenere l'esatto nome completo del NIS `netgroup.byhost` mappatura importata nella directory LDAP.

   Il DN della mappa può variare a seconda dello strumento di terze parti utilizzato per l'importazione. Per ottenere prestazioni ottimali, specificare il DN esatto della mappa.

2. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
3. Abilitare le ricerche netgroup-by-host nella configurazione client LDAP della macchina virtuale di storage (SVM): `vserver services name-service ldap client modify -vserver vserver_name -client-config config_name -is-netgroup-byhost-enabled true -netgroup-byhost -dn netgroup-by-host_map_distinguished_name -netgroup-byhost-scope netgroup-by-host_search_scope`

   `-is-netgroup-byhost-enabled` {`true` `false`} Attiva o disattiva la ricerca netgroup-by-host delle directory LDAP. L'impostazione predefinita è `false`.

   `-netgroup-byhost-dn` `netgroup-by-host_map_distinguished_name` specifica il nome distinto di `netgroup.byhost` mappare la directory LDAP. Sovrascrive il DN di base per le ricerche netgroup-by-host. Se non si specifica questo parametro, ONTAP utilizza invece il DN di base.

   `-netgroup-byhost-scope` {`base`|`onelevel` `subtree`} specifica l'ambito di ricerca per le ricerche netgroup-by-host. Se non si specifica questo parametro, l'impostazione predefinita è `subtree`.

Se la configurazione del client LDAP non esiste ancora, è possibile attivare le ricerche netgroup-by-host specificando questi parametri quando si crea una nuova configurazione del client LDAP utilizzando `vserver services name-service ldap client create` comando.

> A partire da ONTAP 9.2, il campo `-ldap-servers` sostituisce il campo `-servers`. Questo nuovo campo può includere un nome host o un indirizzo IP per il server LDAP.

4. Tornare al livello di privilegio admin: `set -privilege admin`

Esempio

Il seguente comando modifica la configurazione del client LDAP esistente denominata “ldap_corp” per abilitare le ricerche netgroup-by-host utilizzando `netgroup.byhost` mappa denominata “nisMapName="netgroup.byhost",DC=corp,DC=example,DC=com” e l’ambito di ricerca predefinito `subtree`:

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

Al termine

Il `netgroup.byhost` e. `netgroup` le mappe nella directory devono essere sempre sincronizzate per evitare problemi di accesso al client.

Informazioni correlate

"IETF RFC 5952: Una raccomandazione per la rappresentazione del testo dell’indirizzo IPv6"

Utilizza il binding rapido LDAP per l’autenticazione nsswitch

A partire da ONTAP 9.11.1, è possibile sfruttare la funzionalità LDAP *fast bind* (nota anche come *Concurrent BIND*) per richieste di autenticazione client più semplici e veloci. Per utilizzare questa funzionalità, il server LDAP deve supportare la funzionalità di associazione rapida.

A proposito di questa attività

Senza il binding rapido, ONTAP utilizza il binding semplice LDAP per autenticare gli utenti amministratori con il server LDAP. Con questo metodo di autenticazione, ONTAP invia un nome utente o di gruppo al server LDAP, riceve la password hash memorizzata e confronta il codice hash del server con il codice hash generato localmente dalla password utente. Se sono identici, ONTAP concede l’autorizzazione di accesso.

Grazie alla funzionalità di associazione rapida, ONTAP invia solo le credenziali utente (nome utente e password) al server LDAP tramite una connessione sicura. Il server LDAP convalida quindi queste credenziali e richiede a ONTAP di concedere le autorizzazioni di accesso.

Uno dei vantaggi di fast bind è che non è necessario che ONTAP supporti ogni nuovo algoritmo di hashing supportato dai server LDAP, perché l’hashing delle password viene eseguito dal server LDAP.

"Scopri come utilizzare fast bind."

È possibile utilizzare le configurazioni client LDAP esistenti per l’associazione rapida LDAP. Tuttavia, si consiglia vivamente di configurare il client LDAP per TLS o LDAPS; in caso contrario, la password viene inviata via cavo in testo normale.

Per abilitare il binding rapido LDAP in un ambiente ONTAP, è necessario soddisfare i seguenti requisiti:

- Gli utenti admin di ONTAP devono essere configurati su un server LDAP che supporti il fast bind.
- ONTAP SVM deve essere configurato per LDAP nel database name Services switch (nsswitch).
- Gli account di gruppo e utente amministratore di ONTAP devono essere configurati per l'autenticazione nsswitch utilizzando il collegamento rapido.

Fasi

1. Verificare con l'amministratore LDAP che il collegamento rapido LDAP sia supportato sul server LDAP.
2. Assicurarsi che le credenziali dell'utente amministratore di ONTAP siano configurate sul server LDAP.
3. Verificare che l'amministratore o l'SVM dei dati sia configurato correttamente per il binding rapido LDAP.

   a. Per confermare che il server fast bind LDAP è elencato nella configurazione del client LDAP, immettere:

   ```
   vserver services name-service ldap client show
   ```

   "Informazioni sulla configurazione del client LDAP."

   b. Per confermare `ldap` è una delle sorgenti configurate per nsswitch `passwd` database, inserire:

   ```
   vserver services name-service ns-switch show
   ```

   "Scopri di più sulla configurazione di nsswitch."

4. Assicurarsi che gli utenti admin stiano autenticando con nsswitch e che l'autenticazione LDAP fast bind sia attivata nei propri account.

   - Per gli utenti esistenti, immettere `security login modify` e verificare le seguenti impostazioni dei parametri:

   ```
   -authentication-method nsswitch
   ```

   ```
   -is-ldap-fastbind true
   ```

   - Per i nuovi utenti admin, vedere "Abilitare l'accesso all'account LDAP o NIS."

Visualizzare le statistiche LDAP

A partire da ONTAP 9.2, è possibile visualizzare le statistiche LDAP per le macchine virtuali di storage (SVM) su un sistema storage per monitorare le performance e diagnosticare i problemi.

Di cosa hai bisogno

- È necessario aver configurato un client LDAP su SVM.
- Gli oggetti LDAP da cui è possibile visualizzare i dati devono essere stati identificati.

Fase

1. Visualizzare i dati delle performance per gli oggetti del contatore:

   ```
   statistics show
   ```

Esempi

Nell'esempio riportato di seguito vengono illustrati i dati relativi alle prestazioni per l'oggetto `secd_external_service_op`:

```
cluster::*> statistics show -vserver vserverName -object
secd_external_service_op -instance "vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1"

Object: secd_external_service_op
Instance: vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1
Start-time: 4/13/2016 22:15:38
End-time: 4/13/2016 22:15:38
Scope: vserverName
Counter                             Value
-------------------------------- --------------------------------
instance_name                       vserverName:LDAP (NIS & Name
                                    Mapping):GetUserInfoFromName:
                                    1.1.1.1
last_modified_time                  1460610787
node_name                           nodeName
num_not_found_responses             1
num_request_failures                1
num_requests_sent                   1
num_responses_received              1
num_successful_responses            0
num_timeouts                        0
operation                           GetUserInfoFromName
process_name                        secd
request_latency                     52131us
```

Configurare le mappature dei nomi

Panoramica sulla configurazione delle mappature dei nomi

ONTAP utilizza la mappatura dei nomi per mappare le identità SMB alle identità UNIX, le identità Kerberos alle identità UNIX e le identità UNIX alle identità SMB. Queste informazioni sono necessarie per ottenere le credenziali dell'utente e fornire l'accesso corretto ai file, indipendentemente dal fatto che si stia connettendo da un client NFS o SMB.

Esistono due eccezioni per le quali non è necessario utilizzare la mappatura dei nomi:

- Si configura un ambiente UNIX puro e non si prevede di utilizzare l'accesso SMB o lo stile di sicurezza NTFS sui volumi.
- Viene configurato l'utente predefinito da utilizzare.

In questo scenario, la mappatura dei nomi non è necessaria perché, invece di mappare ogni singola credenziale client, tutte le credenziali client vengono mappate allo stesso utente predefinito.

Si noti che è possibile utilizzare la mappatura dei nomi solo per gli utenti, non per i gruppi.

Tuttavia, è possibile mappare un gruppo di singoli utenti a un utente specifico. Ad esempio, è possibile mappare tutti gli utenti ad che iniziano o terminano con la parola SALES a un utente UNIX specifico e all'UID dell'utente.

Come funziona la mappatura dei nomi

Quando ONTAP deve mappare le credenziali per un utente, controlla innanzitutto il database di mappatura dei nomi locali e il server LDAP per verificare la presenza di una mappatura esistente. Se controlla uno o entrambi e in quale ordine viene determinato dalla configurazione del servizio di nomi della SVM.

- Per la mappatura da Windows a UNIX

  Se non viene trovata alcuna mappatura, ONTAP verifica se il nome utente Windows minuscolo è un nome utente valido nel dominio UNIX. Se non funziona, utilizza l'utente UNIX predefinito, a condizione che sia configurato. Se l'utente UNIX predefinito non è configurato e ONTAP non può ottenere un mapping in questo modo, il mapping non riesce e viene restituito un errore.

- Per la mappatura da UNIX a Windows

  Se non viene trovata alcuna mappatura, ONTAP tenta di trovare un account Windows che corrisponda al nome UNIX nel dominio SMB. Se non funziona, utilizza l'utente SMB predefinito, a condizione che sia configurato. Se l'utente SMB predefinito non è configurato e ONTAP non può ottenere un mapping in questo modo, il mapping non riesce e viene restituito un errore.

Per impostazione predefinita, gli account del computer vengono mappati all'utente UNIX predefinito specificato. Se non viene specificato alcun utente UNIX predefinito, il mapping degli account del computer non riesce.

- A partire da ONTAP 9.5, è possibile mappare gli account dei computer a utenti diversi da quelli predefiniti.
- In ONTAP 9.4 e versioni precedenti, non è possibile mappare gli account dei computer ad altri utenti.

  Anche se vengono definite le mappature dei nomi per gli account macchina, le mappature vengono ignorate.

Multidominio ricerca le mappature dei nomi utente da UNIX a Windows

ONTAP supporta le ricerche su più domini durante la mappatura degli utenti UNIX agli utenti Windows. In tutti i domini attendibili rilevati vengono ricercate le corrispondenze del modello di sostituzione fino a quando non viene restituito un risultato corrispondente. In alternativa, è possibile configurare un elenco di domini attendibili preferiti, che viene utilizzato al posto dell'elenco di domini attendibili rilevati e che viene ricercato in ordine fino a quando non viene restituito un risultato corrispondente.

Il modo in cui i trust di dominio influiscono sulle ricerche di mappatura dei nomi utente da UNIX a Windows

Per comprendere il funzionamento della mappatura dei nomi utente multidominio, è necessario comprendere il funzionamento dei trust di dominio con ONTAP. Le relazioni di trust di Active Directory con il dominio principale del server SMB possono essere un trust bidirezionale o uno dei due tipi di trust unidirezionali, un trust in entrata o un trust in uscita. Il dominio principale è il dominio a cui appartiene il server SMB sulla SVM.

- *Fiducia bidirezionale*

  Con trust bidirezionali, entrambi i domini si fidano l'uno dell'altro. Se il dominio principale del server SMB ha un trust bidirezionale con un altro dominio, il dominio principale può autenticare e autorizzare un utente appartenente al dominio attendibile e viceversa.

  Le ricerche di associazione dei nomi utente da UNIX a Windows possono essere eseguite solo su domini con trust bidirezionali tra il dominio principale e l'altro dominio.

- *Fiducia in uscita*

  Con un trust in uscita, il dominio principale considera attendibile l'altro dominio. In questo caso, il dominio principale può autenticare e autorizzare un utente appartenente al dominio trusted in uscita.

  Un dominio con un trust in uscita con il dominio principale viene *not* ricercato quando si eseguono ricerche di mappatura da utente UNIX a nome utente Windows.

- *Fiducia in entrata*

  Con un trust inbound, l'altro dominio considera attendibile il dominio principale del server SMB. In questo caso, il dominio principale non può autenticare o autorizzare un utente appartenente al dominio trusted in entrata.

  Un dominio con un trust in entrata con il dominio principale viene *not* ricercato quando si eseguono ricerche di associazione tra utenti UNIX e nomi utente Windows.

Modalità di utilizzo dei caratteri jolly (*) per configurare le ricerche su più domini per la mappatura dei nomi

Le ricerche di mappatura dei nomi multidominio sono facilitate dall'utilizzo di caratteri jolly nella sezione dominio del nome utente di Windows. Nella tabella seguente viene illustrato come utilizzare i caratteri jolly nella parte di dominio di una voce di mappatura dei nomi per abilitare le ricerche su più domini:

Schema	Sostituzione	Risultato
root	amministratore di *\\	L'utente UNIX "root" viene mappato all'utente "Administrator". Tutti i domini attendibili vengono ricercati in ordine fino a quando non viene trovato il primo utente corrispondente "Administrator".

Schema	Sostituzione	Risultato
*	**	Gli utenti UNIX validi vengono mappati ai corrispondenti utenti Windows. Tutti i domini attendibili vengono ricercati in ordine fino a quando non viene trovato il primo utente corrispondente a tale nome. Il modello {asterisco}\\{asterisco} è valido solo per la mappatura dei nomi da UNIX a Windows, non viceversa.

Come vengono eseguite le ricerche di nomi multidominio

È possibile scegliere uno dei due metodi per determinare l'elenco di domini attendibili utilizzati per la ricerca di nomi di più domini:

- Utilizzare l'elenco di attendibilità bidirezionale rilevato automaticamente compilato da ONTAP
- Utilizzare l'elenco di domini attendibili preferito compilato

Se un utente UNIX viene mappato a un utente Windows con un carattere jolly utilizzato per la sezione di dominio del nome utente, l'utente Windows viene ricercato in tutti i domini attendibili nel modo seguente:

- Se viene configurato un elenco di domini attendibili preferito, l'utente Windows mappato viene ricercato solo in questo elenco di ricerca, in ordine.
- Se un elenco preferito di domini attendibili non è configurato, l'utente Windows viene ricercato in tutti i domini attendibili bidirezionali del dominio principale.
- Se non esistono domini trusted bidirezionalmente per il dominio principale, l'utente viene ricercato nel dominio principale.

Se un utente UNIX viene mappato a un utente Windows senza una sezione di dominio nel nome utente, l'utente Windows viene ricercato nel dominio principale.

Regole di conversione del mapping dei nomi

Un sistema ONTAP mantiene una serie di regole di conversione per ogni SVM. Ogni regola è composta da due parti: Un *pattern* e un *replacement*. Le conversioni iniziano all'inizio dell'elenco appropriato ed eseguono una sostituzione in base alla prima regola di corrispondenza. Il modello è un'espressione regolare in stile UNIX. La sostituzione è una stringa contenente sequenze di escape che rappresentano sottoespressioni del modello, come in UNIX `sed` programma.

Creare una mappatura dei nomi

È possibile utilizzare `vserver name-mapping create` per creare una mappatura dei

nomi. Si utilizzano le mappature dei nomi per consentire agli utenti Windows di accedere ai volumi di sicurezza UNIX e viceversa.

A proposito di questa attività

Per ogni SVM, ONTAP supporta fino a 12,500 mappature di nomi per ciascuna direzione.

Fase

1. Creazione di una mappatura dei nomi:

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

   > Il `-pattern` e. `-replacement` le dichiarazioni possono essere formulate come espressioni regolari. È inoltre possibile utilizzare `-replacement` per negare esplicitamente un mapping all'utente utilizzando la stringa di sostituzione nulla `" "` (il carattere dello spazio). Vedere `vserver name-mapping create` pagina man per i dettagli.

   Quando vengono create mappature da Windows a UNIX, tutti i client SMB che hanno connessioni aperte al sistema ONTAP al momento della creazione delle nuove mappature devono disconnettersi e riconnessi per visualizzare le nuove mappature.

Esempi

Il seguente comando crea un mapping dei nomi sulla SVM denominata vs1. Il mapping è un mapping da UNIX a Windows nella posizione 1 nell'elenco delle priorità. Il mapping associa l'utente UNIX Johnd all'utente Windows ENG/JohnDoe.

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

Il seguente comando crea un'altra mappatura dei nomi sulla SVM denominata vs1. Il mapping è un mapping da Windows a UNIX nella posizione 1 nell'elenco delle priorità. Qui il modello e la sostituzione includono espressioni regolari. Il mapping associa ogni utente CIFS nel dominio ENG agli utenti nel dominio LDAP associato alla SVM.

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

Il seguente comando crea un'altra mappatura dei nomi sulla SVM denominata vs1. Qui il modello include "``" come elemento nel nome utente di Windows che deve essere escapato. La mappatura mappa l'utente Windows ENG all'utente UNIX john_Ops.

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

Configurare l'utente predefinito

È possibile configurare un utente predefinito da utilizzare se tutti gli altri tentativi di mappatura non riescono per un utente o se non si desidera mappare singoli utenti tra UNIX e Windows. In alternativa, se si desidera che l'autenticazione degli utenti non mappati non venga eseguita correttamente, non è necessario configurare un utente predefinito.

A proposito di questa attività

Per l'autenticazione CIFS, se non si desidera associare ciascun utente Windows a un singolo utente UNIX, è possibile specificare un utente UNIX predefinito.

Per l'autenticazione NFS, se non si desidera associare ciascun utente UNIX a un singolo utente Windows, è possibile specificare un utente Windows predefinito.

Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera…	Immettere il seguente comando…
Configurare l'utente UNIX predefinito	`vserver cifs options modify -default-unix-user user_name`
Configurare l'utente Windows predefinito	`vserver nfs modify -default-win-user user_name`

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.

Abilitare l'accesso per i client NFS di Windows

ONTAP supporta l'accesso ai file dai client NFSv3 di Windows. Ciò significa che i client che eseguono sistemi operativi Windows con supporto NFSv3 possono accedere ai file delle esportazioni NFSv3 nel cluster. Per utilizzare correttamente questa funzionalità, è necessario configurare correttamente la macchina virtuale di storage (SVM) ed essere consapevoli di determinati requisiti e limitazioni.

A proposito di questa attività

Per impostazione predefinita, il supporto del client Windows NFSv3 è disattivato.

Prima di iniziare

NFSv3 deve essere attivato su SVM.

Fasi

1. Abilitare il supporto del client Windows NFSv3:

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

2. Su tutti gli SVM che supportano i client Windows NFSv3, disattivare `-enable-ejukebox` e. `-v3 -connection-drop` parametri:

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

   I client Windows NFSv3 possono ora montare le esportazioni sul sistema storage.

3. Assicurarsi che ogni client Windows NFSv3 utilizzi i supporti rigidi specificando `-o mtype=hard` opzione.

   Questo è necessario per garantire montaggi affidabili.

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

Abilitare la visualizzazione delle esportazioni NFS sui client NFS

I client NFS possono utilizzare `showmount -e` Per visualizzare un elenco delle esportazioni disponibili da un server NFS ONTAP. In questo modo, gli utenti possono identificare il file system che desiderano montare.

A partire da ONTAP 9.2, ONTAP consente ai client NFS di visualizzare l'elenco di esportazione per impostazione predefinita. Nelle versioni precedenti, il `showmount` opzione di `vserver nfs modify` il comando deve essere attivato in modo esplicito. Per visualizzare l'elenco di esportazione, è necessario attivare NFSv3 su SVM.

Esempio

Il seguente comando mostra la funzione showmount sulla SVM denominata vs1:

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

Il seguente comando eseguito su un client NFS visualizza l'elenco delle esportazioni su un server NFS con l'indirizzo IP 10.63.21.9:

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

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

Se la versione di ONTAP è…	Il valore predefinito di pNFS è…
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`
Visualizza informazioni sui limiti dei gruppi UNIX locali	`vserver services unix-group max-limit show`

Se si desidera…	Utilizzare il comando…
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.

Problema	Azione correttiva
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.
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.
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`

Se si desidera eseguire il lavaggio…	Immettere il comando…
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`
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`
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
```

Versioni e client NFS supportati

Panoramica delle versioni e dei client NFS supportati

Prima di poter utilizzare NFS nella rete, è necessario conoscere le versioni e i client NFS supportati da ONTAP.

Questa tabella indica quando le versioni principali e minori dei protocolli NFS sono supportate per impostazione predefinita in ONTAP. Il supporto predefinito non indica che si tratta della prima versione di ONTAP che supporta tale protocollo NFS.

Versione	Attivato per impostazione predefinita
NFSv3	Sì
NFSv4.0	Sì, a partire da ONTAP 9.9.1
NFSv4.1	Sì, a partire da ONTAP 9.9.1
NFSv4.2	Sì, a partire da ONTAP 9.9.1
PNFS	No

Per informazioni aggiornate sui client NFS supportati da ONTAP, consulta la matrice di interoperabilità.

"Tool di matrice di interoperabilità NetApp"

Funzionalità NFSv4.0 supportata da ONTAP

ONTAP supporta tutte le funzionalità obbligatorie di NFSv4.0, ad eccezione dei meccanismi di sicurezza SPKM3 e LIPKEY.

Sono supportate le seguenti funzionalità DI NFSV4:

- **COMPOSTO**

  Consente a un client di richiedere più operazioni di file in una singola richiesta RPC (Remote procedure Call).

- **Delega del file**

Consente al server di delegare il controllo del file ad alcuni tipi di client per l'accesso in lettura e scrittura.

- **Pseudo-fs**

  Utilizzato dai server NFSv4 per determinare i punti di montaggio sul sistema storage. NFSv4 non contiene alcun protocollo di montaggio.

- **Blocco**

  Basato sul leasing. Non esistono protocolli NLM (Network Lock Manager) o NSM (Network Status Monitor) separati in NFSv4.

Per ulteriori informazioni sul protocollo NFSv4.0, vedere RFC 3530.

Limitazioni del supporto ONTAP per NFSv4

È necessario conoscere diverse limitazioni del supporto ONTAP per NFSv4.

- La funzione di delega non è supportata da ogni tipo di client.
- In ONTAP 9.4 e versioni precedenti, i nomi con caratteri non ASCII su volumi diversi da UTF8 vengono rifiutati dal sistema di storage.

  In ONTAP 9.5 e versioni successive, i volumi creati con l'impostazione del linguaggio utf8mb4 e montati utilizzando NFS v4 non sono più soggetti a questa restrizione.

- Tutti gli handle di file sono persistenti; il server non fornisce handle di file volatili.
- Migrazione e replica non sono supportate.
- I client NFSv4 non sono supportati con mirror di sola lettura per la condivisione del carico.

  ONTAP indirizza i client NFSv4 all'origine del mirror di condivisione del carico per l'accesso diretto in lettura e scrittura.

- Gli attributi denominati non sono supportati.
- Sono supportati tutti gli attributi consigliati, ad eccezione di:
  - `archive`
  - `hidden`
  - `homogeneous`
  - `mimetype`
  - `quota_avail_hard`
  - `quota_avail_soft`
  - `quota_used`
  - `system`
  - `time_backup`

> Anche se non supporta `quota*` ONTAP supporta le quote utente e di gruppo tramite il protocollo RQUOTA Side Band.

Supporto ONTAP per NFSv4.1

A partire da ONTAP 9.8, la funzionalità nconnect è disponibile per impostazione predefinita quando NFSv4.1 è attivato.

Le implementazioni dei client NFS precedenti utilizzano solo una singola connessione TCP con un mount. In ONTAP, una singola connessione TCP può diventare un collo di bottiglia con un aumento degli IOPS. Tuttavia, un client abilitato a nconnect può avere più connessioni TCP (fino a 16) associate a un singolo montaggio NFS. Un client NFS di questo tipo moltiplica le operazioni di file su più connessioni TCP in modo round-robin e ottiene così un throughput più elevato dalla larghezza di banda di rete disponibile. NConnect è consigliato solo per i supporti NFSv3 e NFSv4.1.

Consultare la documentazione del client NFS per verificare se nconnect è supportato nella versione del client.

NFSv4.1 è attivato per impostazione predefinita in ONTAP 9.9.1 e versioni successive. Nelle versioni precedenti, è possibile attivarlo specificando `-v4.1` e impostarlo su `enabled` Quando si crea un server NFS sulla macchina virtuale di storage (SVM).

ONTAP non supporta le deleghe a livello di file e directory NFSv4.1.

Supporto ONTAP per NFSv4.2

A partire da ONTAP 9,8, ONTAP supporta il protocollo NFSv4,2 per consentire l'accesso a client abilitati per NFSv4,2.

NFSv4,2 è attivato per impostazione predefinita in ONTAP 9.9.1 e versioni successive. In ONTAP 9,8, è necessario attivare manualmente v4,2 specificando il `-v4.1` e impostarlo su `enabled` Quando si crea un server NFS sulla macchina virtuale di storage (SVM). L'abilitazione di NFSv4.1 consente inoltre ai client di utilizzare le funzionalità di NFSv4.1 mentre sono montati come v4.2.

Le successive versioni di ONTAP ampliano il supporto per NFSv4,2 funzioni opzionali.

A partire da…	NFSv4,2 caratteristiche opzionali includono …
ONTAP 9.12.1	• Attributi estesi NFS • File sparse • Prenotazioni di spazio
ONTAP 9.9.1	Obbligatorio Access Control (MAC) con etichetta NFS

Etichette di sicurezza NFS v4,2

A partire da ONTAP 9.9.1, è possibile attivare le etichette di sicurezza NFS. Sono disattivati per impostazione predefinita.

Con le etichette di sicurezza NFS v4.2, i server NFS ONTAP sono compatibili con il controllo di accesso obbligatorio (MAC), memorizzando e recuperando gli attributi sec_label inviati dai client.

Per ulteriori informazioni, vedere "RFC 7240".

A partire da ONTAP 9.12.1, le etichette di sicurezza NFS v4.2 sono supportate per le operazioni di dump NDMP. Se vengono rilevate etichette di sicurezza su file o directory nelle release precedenti, il dump non

riesce.

Fasi

1. Impostare i privilegi su Advanced (avanzato):

```
set -privilege advanced
```

2. Abilitare le etichette di sicurezza:

```
vserver nfs modify -vserver _svm_name_ -v4.2-seclabel enabled
```

Attributi estesi NFS

A partire da ONTAP 9.12.1, gli attributi estesi NFS (xattrs) sono attivati per impostazione predefinita.

Gli attributi estesi sono attributi NFS standard definiti da "RFC 8276" E abilitato nei moderni client NFS. Possono essere utilizzate per collegare metadati definiti dall'utente a oggetti del file system e sono interessanti per implementazioni di sicurezza avanzate.

Gli attributi estesi NFS non sono attualmente supportati per le operazioni di dump NDMP. Se vengono rilevati attributi estesi su file o directory, il dump procede ma non esegue il backup degli attributi estesi su tali file o directory.

Se è necessario disattivare gli attributi estesi, utilizzare `vserver nfs modify -v4.2-xattrs disabled` comando.

Supporto ONTAP per NFS parallelo

ONTAP supporta NFS paralleli (pNFS). Il protocollo pNFS offre miglioramenti delle performance offrendo ai client l'accesso diretto ai dati di un set di file distribuiti su più nodi di un cluster. Aiuta i clienti a individuare il percorso ottimale per un volume.

Utilizzo di supporti rigidi

Durante la risoluzione dei problemi di montaggio, assicurarsi di utilizzare il tipo di montaggio corretto. NFS supporta due tipi di montaggio: Supporti morbidi e hard mount. Per motivi di affidabilità, utilizzare solo supporti rigidi.

Non si consiglia di utilizzare supporti soft, soprattutto quando è possibile che si verificano frequenti timeout NFS. Le condizioni di gara possono verificarsi in seguito a questi timeout, che possono portare alla corruzione dei dati.

Dipendenze di nomi di file e directory NFS e SMB

Panoramica delle dipendenze di nomi di file e directory NFS e SMB

Le convenzioni di denominazione di file e directory dipendono dai` sistemi operativi dei

client di rete e dai protocolli di condivisione file, oltre alle impostazioni della lingua del cluster e dei client ONTAP.

Il sistema operativo e i protocolli di condivisione file determinano quanto segue:

- Caratteri che possono essere utilizzati da un nome file
- Distinzione tra maiuscole e minuscole per un nome file

ONTAP supporta caratteri multi-byte nei nomi di file, directory e qtree, a seconda della versione di ONTAP.

Caratteri che possono essere utilizzati da un nome di file o di directory

Se si accede a un file o a una directory da client con sistemi operativi diversi, utilizzare caratteri validi in entrambi i sistemi operativi.

Ad esempio, se si utilizza UNIX per creare un file o una directory, non utilizzare i due punti (:) nel nome perché i due punti non sono consentiti nei nomi di file o directory MS-DOS. Poiché le restrizioni sui caratteri validi variano da un sistema operativo all'altro, consultare la documentazione del sistema operativo client per ulteriori informazioni sui caratteri non consentiti.

Distinzione tra maiuscole e minuscole dei nomi di file e directory in un ambiente multiprotocollo

I nomi di file e directory sono sensibili al maiuscolo/minuscolo per i client NFS e non al maiuscolo/minuscolo ma conservano il maiuscolo/minuscolo per i client SMB. È necessario comprendere le implicazioni di un ambiente multiprotocollo e le azioni da intraprendere quando si specifica il percorso durante la creazione di condivisioni SMB e quando si accede ai dati all'interno delle condivisioni.

Se un client SMB crea una directory denominata `testdir`, Sia i client SMB che NFS visualizzano il nome del file come `testdir`. Tuttavia, se un utente SMB tenta in seguito di creare un nome di directory `TESTDIR`, Il nome non è consentito perché, per il client SMB, tale nome esiste attualmente. Se un utente NFS successivamente crea una directory denominata `TESTDIR`I client , NFS e SMB visualizzano il nome della directory in modo diverso, come segue:

- Sui client NFS, ad esempio, vengono visualizzati entrambi i nomi di directory così come sono stati creati `testdir` e. `TESTDIR`, perché i nomi delle directory sono sensibili al maiuscolo/minuscolo.
- I client SMB utilizzano i nomi 8.3 per distinguere le due directory. Una directory ha il nome del file di base. Alle directory aggiuntive viene assegnato un nome file 8.3.
  - Sui client SMB, viene visualizzato `testdir` e. `TESTDI~1`.
  - ONTAP crea il `TESTDI~1` nome della directory per differenziare le due directory.

    In questo caso, è necessario utilizzare il nome 8.3 quando si specifica un percorso di condivisione durante la creazione o la modifica di una condivisione su una macchina virtuale di storage (SVM).

Analogamente per i file, se viene creato un client SMB `test.txt`, Sia i client SMB che NFS visualizzano il nome del file come `text.txt`. Tuttavia, se un utente SMB tenta di creare in un secondo momento `Test.txt`, Il nome non è consentito perché, per il client SMB, tale nome esiste attualmente. Se un utente NFS successivamente crea un file denominato `Test.txt`I client , NFS e SMB visualizzano il nome del file in modo

diverso, come segue:

- Sui client NFS, vengono visualizzati entrambi i nomi dei file così come sono stati creati, `test.txt` e. `Test.txt`, perché i nomi dei file sono sensibili al maiuscolo/minuscolo.
- I client SMB utilizzano i nomi 8.3 per distinguere i due file. Un file ha il nome del file di base. Ai file aggiuntivi viene assegnato un nome file 8.3.
  - Sui client SMB, viene visualizzato `test.txt` e. `TEST~1.TXT`.
  - ONTAP crea il `TEST~1.TXT` nome del file per differenziare i due file.

> Se è stata creata una mappatura dei caratteri utilizzando i comandi di mappatura dei caratteri CIFS di Vserver, una ricerca di Windows che normalmente non fa distinzione tra maiuscole e minuscole può diventare sensibile al maiuscolo/minuscolo. Ciò significa che le ricerche dei nomi file distinguono tra maiuscole e minuscole solo se la mappatura dei caratteri è stata creata e il nome del file sta utilizzando la mappatura dei caratteri.

Come ONTAP crea i nomi di file e directory

ONTAP crea e mantiene due nomi per i file o le directory in qualsiasi directory che ha accesso da un client SMB: Il nome lungo originale e un nome in formato 8.3.

Per i nomi di file o directory che superano il nome di otto caratteri o il limite di estensione di tre caratteri (per i file), ONTAP genera un nome in formato 8.3 come segue:

- Il nome del file o della directory originale viene troncato a sei caratteri, se il nome supera i sei caratteri.
- Aggiunge una tilde (~) e un numero, da uno a cinque, ai nomi di file o directory che non sono più univoci dopo essere stati troncati.

  Se esaurisce i numeri perché ci sono più di cinque nomi simili, crea un nome unico che non ha alcuna relazione con il nome originale.

- Nel caso dei file, l'estensione del nome del file viene troncata a tre caratteri.

Ad esempio, se un client NFS crea un file denominato `specifications.html`, Il nome del file di formato 8.3 creato da ONTAP è `specif~1.htm`. Se questo nome esiste già, ONTAP utilizza un numero diverso alla fine del nome del file. Ad esempio, se un client NFS crea un altro file denominato `specifications_new.html`, il formato 8.3 di `specifications_new.html` è `specif~2.htm`.

Come ONTAP gestisce i nomi di file, directory e qtree multi-byte

A partire da ONTAP 9.5, il supporto per i nomi codificati UTF-8 a 4 byte consente la creazione e la visualizzazione di nomi di file, directory e albero che includono caratteri aggiuntivi Unicode al di fuori del piano multilingua di base (BMP). Nelle versioni precedenti, questi caratteri supplementari non erano visualizzati correttamente negli ambienti multiprotocollo.

Per abilitare il supporto per i nomi codificati UTF-8 a 4 byte, è disponibile un nuovo codice lingua *utf8mb4* per `vserver` e. `volume` famiglie di comandi.

- È necessario creare un nuovo volume in uno dei seguenti modi:

- Impostazione del volume `-language` opzione esplicitamente:

  ```
  volume create -language utf8mb4 {…}
  ```

- Ereditare il volume `-language` Opzione da una SVM creata con o modificata per l'opzione:

  ```
  vserver [create|modify] -language utf8mb4 {…}``volume create {…}
  ```

- Se si utilizza ONTAP 9.6 e versioni precedenti, non è possibile modificare i volumi esistenti per il supporto di utf8mb4; è necessario creare un nuovo volume utf8mb4-ready e quindi migrare i dati utilizzando strumenti di copia basati su client.

  Se si utilizza ONTAP 9.7P1 o versione successiva, è possibile modificare i volumi esistenti per utf8mb4 con una richiesta di supporto. Per ulteriori informazioni, vedere "È possibile modificare la lingua del volume dopo la creazione in ONTAP?".

  È possibile aggiornare le SVM per il supporto di utf8mb4, ma i volumi esistenti conservano i codici lingua originali.

  > I nomi LUN con caratteri UTF-8 a 4 byte non sono attualmente supportati.

- I dati dei caratteri Unicode sono generalmente rappresentati nelle applicazioni di file system Windows che utilizzano il formato di trasformazione Unicode a 16 bit (UTF-16) e nei file system NFS che utilizzano il formato di trasformazione Unicode a 8 bit (UTF-8).

  Nelle release precedenti a ONTAP 9.5, i nomi, inclusi i caratteri supplementari UTF-16 creati dai client Windows, venivano visualizzati correttamente su altri client Windows ma non sono stati tradotti correttamente in UTF-8 per i client NFS. Analogamente, i nomi con caratteri supplementari UTF-8 creati dai client NFS non sono stati tradotti correttamente in UTF-16 per i client Windows.

- Quando si creano nomi di file su sistemi con ONTAP 9.4 o versioni precedenti che contengono caratteri supplementari validi o non validi, ONTAP rifiuta il nome del file e restituisce un errore di nome del file non valido.

  Per evitare questo problema, utilizzare solo caratteri BMP nei nomi dei file ed evitare di utilizzare caratteri supplementari oppure eseguire l'aggiornamento a ONTAP 9.5 o versioni successive.

I caratteri Unicode sono consentiti nei nomi qtree.

- È possibile utilizzare il `volume qtree` Command Family o System Manager per impostare o modificare i nomi di qtree.
- I nomi qtree possono includere caratteri multi-byte in formato Unicode, ad esempio caratteri giapponesi e cinesi.
- Nelle versioni precedenti a ONTAP 9.5, erano supportati solo i caratteri BMP (ovvero quelli che potevano essere rappresentati in 3 byte).

> Nelle release precedenti a ONTAP 9.5, il percorso di giunzione del volume padre del qtree può contenere nomi di qtree e directory con caratteri Unicode. Il `volume show` Il comando visualizza correttamente questi nomi quando il volume d'origine dispone di un'impostazione della lingua UTF-8. Tuttavia, se la lingua del volume padre non è una delle impostazioni della lingua UTF-8, alcune parti del percorso di giunzione vengono visualizzate utilizzando un nome alternativo NFS numerico.

- Nella versione 9.5 e successive, i caratteri a 4 byte sono supportati nei nomi qtree, a condizione che il qtree si trovi in un volume abilitato per utf8mb4.

Configurare la mappatura dei caratteri per la conversione dei nomi file SMB sui volumi

I client NFS possono creare nomi di file che contengono caratteri non validi per i client SMB e alcune applicazioni Windows. È possibile configurare la mappatura dei caratteri per la conversione dei nomi file sui volumi per consentire ai client SMB di accedere ai file con nomi NFS che altrimenti non sarebbero validi.

A proposito di questa attività

Quando i client SMB accedono ai file creati dai client NFS, ONTAP esamina il nome del file. Se il nome non è un nome file SMB valido (ad esempio, se ha un carattere ":" incorporato), ONTAP restituisce il nome file 8.3 che viene mantenuto per ciascun file. Tuttavia, questo causa problemi per le applicazioni che codificano informazioni importanti in nomi di file lunghi.

Pertanto, se si condivide un file tra client su sistemi operativi diversi, è necessario utilizzare caratteri nei nomi dei file validi in entrambi i sistemi operativi.

Tuttavia, se si dispone di client NFS che creano nomi file contenenti caratteri non validi per i client SMB, è possibile definire una mappa che converte i caratteri NFS non validi in caratteri Unicode accettati sia da SMB che da alcune applicazioni Windows. Ad esempio, questa funzionalità supporta le applicazioni CATIA MCAD e Mathematica e altre applicazioni che richiedono questo requisito.

È possibile configurare la mappatura dei caratteri volume per volume.

Quando si configura la mappatura dei caratteri su un volume, è necessario tenere presente quanto segue:

- La mappatura dei caratteri non viene applicata tra i punti di giunzione.

  È necessario configurare esplicitamente la mappatura dei caratteri per ciascun volume di giunzione.

- È necessario assicurarsi che i caratteri Unicode utilizzati per rappresentare caratteri non validi o non validi siano caratteri che normalmente non vengono visualizzati nei nomi dei file; in caso contrario, si verificano mappature indesiderate.

  Ad esempio, se si tenta di mappare i due punti (:) a un trattino (-) ma il trattino (-) è stato utilizzato correttamente nel nome del file, un client Windows che tenta di accedere a un file denominato "a-b" avrebbe la sua richiesta mappata al nome NFS "a:b" (non il risultato desiderato).

- Dopo aver applicato la mappatura dei caratteri, se la mappatura contiene ancora un carattere Windows non valido, ONTAP torna ai nomi file di Windows 8.3.
- Nelle notifiche FPolicy, nei registri di controllo NAS e nei messaggi di traccia di sicurezza, vengono visualizzati i nomi dei file mappati.

- Quando viene creata una relazione SnapMirror di tipo DP, la mappatura dei caratteri del volume di origine non viene replicata sul volume DP di destinazione.
- Distinzione tra maiuscole e minuscole: Poiché i nomi Windows mappati diventano nomi NFS, la ricerca dei nomi segue la semantica NFS. Ciò include il fatto che le ricerche NFS sono sensibili al maiuscolo/minuscolo. Ciò significa che le applicazioni che accedono alle condivisioni mappate non devono fare affidamento sul comportamento di Windows senza distinzione tra maiuscole e minuscole. Tuttavia, il nome 8.3 è disponibile, senza distinzione tra maiuscole e minuscole.
- Mappature parziali o non valide: Dopo aver mappato un nome da restituire ai client che eseguono l'enumerazione della directory ("dir"), il nome Unicode risultante viene controllato per la validità di Windows. Se il nome contiene ancora caratteri non validi o se non è valido per Windows (ad esempio, termina con "." o vuoto) viene restituito il nome 8.3 invece del nome non valido.

Fase

1. Configurare la mappatura dei caratteri:

   ```
   vserver cifs character-mapping create -vserver vserver_name -volume
   volume_name -mapping mapping_text, ...
   ```

   Il mapping è costituito da un elenco di coppie di caratteri origine-destinazione separate da ":". I caratteri sono caratteri Unicode immessi utilizzando cifre esadecimali. Ad esempio: 3C:E03C.

   Il primo valore di ciascuno `mapping_text` La coppia separata dai due punti è il valore esadecimale del carattere NFS che si desidera convertire, mentre il secondo valore è il valore Unicode utilizzato da SMB. Le coppie di mappatura devono essere univoche (deve esistere una mappatura uno a uno).

   - Mappatura di origine

     La tabella seguente mostra il set di caratteri Unicode consentito per il mapping di origine:

Carattere Unicode	Carattere stampato	Descrizione
0x01-0x19	Non applicabile	Caratteri di controllo non stampabili
0x5C	.	Barra rovesciata
0x3A	:	Due punti
0x2A	*	Asterisco
0x3F	?	Punto interrogativo
0x22	"	Virgoletta
0x3C	<	Inferiore a.
0x3E	>	Maggiore di
0x7C		

Linea verticale	0xB1	±

- Mappatura di destinazione

  È possibile specificare i caratteri di destinazione nella “Private Use Area” di Unicode nel seguente intervallo: U+E0000…U+F8FF.

Esempio

Il seguente comando crea un mapping di caratteri per un volume denominato “data” su storage virtual machine (SVM) vs1:

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show

Vserver         Volume Name  Character Mapping
--------------  -----------  -----------------------------------------
vs1             data         3c:e17c, 3e:f17d, 2a:f745
```

Comandi per la gestione delle mappature dei caratteri per la conversione dei nomi file SMB

È possibile gestire la mappatura dei caratteri creando, modificando, visualizzando o eliminando le mappature dei caratteri dei file utilizzate per la conversione dei nomi dei file SMB sui volumi FlexVol.

Se si desidera…	Utilizzare questo comando…
Creare nuove mappature dei caratteri del file	`vserver cifs character-mapping create`
Visualizza le informazioni sulle mappature dei caratteri del file	`vserver cifs character-mapping show`
Modificare le mappature dei caratteri del file esistente	`vserver cifs character-mapping modify`
Eliminare le mappature dei caratteri del file	`vserver cifs character-mapping delete`

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