Impostare l'accesso al file utilizzando NFS

ONTAP 9

NetApp
February 13, 2026

Sommario

Impostare l’accesso al file utilizzando NFS

Scopri come impostare l’accesso ai file NFS sulle SVM ONTAP

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

Come le policy di esportazione controllano l’accesso client ai volumi NFS o qtree ONTAP

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.

Criteri di esportazione predefiniti per SVM NFS ONTAP

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 NFS di ONTAP

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 l'accesso ONTAP SVM per i client NFS con tipi di sicurezza non elencati

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

Esempi

L'esempio seguente mostra una politica di esportazione con un `-rwrule any` parametro:

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.

L'esempio seguente mostra una politica di esportazione con un `-rwrule none` parametro:

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.

Come i tipi di sicurezza ONTAP determinano i livelli di accesso del client NFS

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.
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.

Scopri come gestire le richieste di accesso del superutente ONTAP NFS

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.

Informazioni sulle cache dei criteri di esportazione NFS 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.

Informazioni sulle cache di accesso NFS ONTAP

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.

Informazioni sui parametri della cache di accesso NFS ONTAP

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 le policy di esportazione dai qtree NFS di ONTAP

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
```

Convalida gli ID qtree NFS ONTAP per le operazioni sui 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 della politica di esportazione e giunzioni nidificate per i volumi ONTAP NFS 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 NFS 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 ONTAP 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 dell'ID utente ONTAP 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

Ulteriori informazioni sulla configurazione dello switch ONTAP NFS 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
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

Informazioni su LDAP per SVM NFS ONTAP

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 9.4 - 9.0.
- 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 "Utilizzare LDAP fast bind per l'autenticazione nsswitch per ONTAP NFS SVM."
- 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".

Informazioni sulla firma e la sigillatura LDAP per le SVM NFS ONTAP

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.

Scopri di più su LDAPS per ONTAP NFS SVM

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 9.8-9.5, LDAPS può essere abilitato solo sulla porta 636. Per farlo, utilizzare il `-use-ldaps-for-ad-ldap` parametro 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 il `-ldaps-enabled` parametro su `true` e specificare il parametro desiderato `-port`. Ulteriori informazioni su `vserver services name-service ldap client create` nella "Riferimento al comando ONTAP".

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.

Abilita il supporto LDAP RFC2307bis per SVM ONTAP NFS

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.

Prima di iniziare

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 ONTAP NFS 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 ricerca dei referral LDAP è abilitata in ONTAP 9.5 e versioni successive).
`-base-scope`	Ambito di base per tutte le ricerche LDAP.
`-user-dn`	DN di base per tutte le ricerche utente LDAP. Questo parametro si applica anche alle ricerche di mappatura dei nomi utente.
`-user-scope`	Ambito di base per tutte le ricerche utente LDAP. Questo parametro si applica anche alle ricerche basate sulla mappatura dei nomi utente.
`-group-dn`	DN di base per tutte le ricerche di gruppi LDAP.

`-group-scope`	Ambito di base per tutte le ricerche nei gruppi LDAP.
`-netgroup-dn`	DN di base per tutte le ricerche nei netgroup LDAP.
`-netgroup-scope`	Ambito di base per tutte le ricerche nei 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.

Filtri di ricerca LDAP personalizzati

È possibile utilizzare il parametro di opzione di configurazione LDAP per creare un filtro di ricerca personalizzato. Il `-group-membership-filter` parametro specifica il filtro di ricerca da utilizzare quando si cerca l'appartenenza al gruppo da un server LDAP.

Un esempio di filtri validi è:

```
(cn=*99), (cn=1*), (|(cn=*22)(cn=*33))
```

Ulteriori informazioni su "Come configurare LDAP in ONTAP".

Migliorare le prestazioni delle ricerche netgroup-by-host delle directory LDAP per gli SVM NFS ONTAP

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.

Prima di iniziare

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.

   > IL `-ldap-servers` il campo sostituisce il `-servers` campo. Puoi usare il `-ldap -servers` campo per specificare 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"

Utilizzare il fast bind LDAP per l’autenticazione nsswitch per le SVM ONTAP NFS

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."

Prima di iniziare

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.
- Il numero UID e il numero GID dell'amministratore devono essere compilati e interrogabili affinché il fast bind abbia successo.

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`

   Ulteriori informazioni su `security login modify` nella "Riferimento al comando ONTAP".

   ◦ Per i nuovi utenti amministratori, vedere "Attiva l'accesso all'account LDAP o NIS ONTAP".

Visualizza le statistiche LDAP per gli SVM NFS ONTAP

È possibile visualizzare le statistiche LDAP per le macchine virtuali di archiviazione (SVM) su un sistema di archiviazione per monitorare le prestazioni e diagnosticare i problemi.

Prima di iniziare

- 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 seguente vengono visualizzate le statistiche per l'esempio denominato **smpl_1** per i contatori: avg_processor_busy e cpu_busy

```
cluster1::*> statistics start -object system -counter
avg_processor_busy|cpu_busy -sample-id smpl_1
Statistics collection is being started for Sample-id: smpl_1

cluster1::*> statistics stop -sample-id smpl_1
Statistics collection is being stopped for Sample-id: smpl_1

cluster1::*> statistics show -sample-id smpl_1
Object: system
Instance: cluster
Start-time: 8/2/2012 18:27:53
End-time: 8/2/2012 18:27:56
Cluster: cluster1
   Counter                                                     Value
   -------------------------------- --------------------------------
   avg_processor_busy                                             6%
   cpu_busy
```

Informazioni correlate

- "le statistiche mostrano"
- "inizio delle statistiche"
- "le statistiche si fermano"

Configurare le mappature dei nomi

Informazioni sulla configurazione del mapping dei nomi per le SVM NAS ONTAP

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.

Informazioni sulle mappature dei nomi per le SVM NAS ONTAP

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.

Ricerche multidominio per mappature di nomi utente da UNIX a Windows su SVM NAS ONTAP

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 per SVM NAS ONTAP

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 mappature dei nomi per le SVM NAS ONTAP

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
```

> Le `-pattern` istruzioni e `-replacement` possono essere formulate come espressioni regolari. È inoltre possibile utilizzare l' `-replacement`istruzione per negare esplicitamente un mapping all'utente utilizzando la stringa di sostituzione null `"" (il carattere di spazio). Ulteriori informazioni su `vserver name-mapping create` nella "Riferimento al comando ONTAP".

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 per gli SVM NAS ONTAP

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 ONTAP per la gestione delle mappature dei nomi NFS

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`

Ulteriori informazioni su `vserver name-mapping` nella "Riferimento al comando ONTAP".

Abilitare l'accesso per i client NFS Windows per ONTAP SVM

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:\
```

Abilita la visualizzazione delle esportazioni sui client NFS per le SVM ONTAP

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.

ONTAP consente ai client NFS di visualizzare l'elenco delle esportazioni per impostazione predefinita. Nelle versioni precedenti, l' `showmount`opzione del `vserver nfs modify` comando deve essere attivata esplicitamente. 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)
```

Informazioni sul copyright

Informazioni sul marchio commerciale