Accesso sicuro a NFS tramite policy di esportazione

ONTAP 9

NetApp
April 24, 2024

Sommario

Accesso sicuro a NFS tramite policy di esportazione . . . 1
In che modo le policy di esportazione controllano l'accesso dei client ai volumi o ai qtree . . . 1
Policy di esportazione predefinita per le SVM . . . 1
Come funzionano le regole di esportazione . . . 2
Gestire i client con un tipo di protezione non elencato . . . 3
In che modo i tipi di sicurezza determinano i livelli di accesso del client . . . 5
Gestire le richieste di accesso dei superutenti . . . 7
Modalità di utilizzo delle cache delle policy di esportazione da parte di ONTAP . . . 9
Come funziona la cache di accesso . . . 10
Come funzionano i parametri della cache di accesso . . . 11
Rimuovere un criterio di esportazione da un qtree . . . 12
Convalidare gli ID qtree per le operazioni del file qtree . . . 12
Restrizioni dei criteri di esportazione e giunzioni nidificate per i volumi FlexVol . . . 13

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.