Impostare l'accesso ai file utilizzando SMB

ONTAP 9

NetApp
April 24, 2024

Sommario

Impostare l’accesso ai file utilizzando SMB

Configurare gli stili di sicurezza

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

Quali sono gli stili di sicurezza e i loro effetti

Esistono quattro diversi stili di sicurezza: UNIX, NTFS, misto e unificato. Ogni stile di sicurezza ha un effetto diverso sul modo in cui vengono gestite le autorizzazioni per i dati. È necessario comprendere i diversi effetti per assicurarsi di selezionare lo stile di sicurezza appropriato per i propri scopi.

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

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

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

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

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

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

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

Dove e quando impostare gli stili di sicurezza

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

Decidere quale stile di sicurezza utilizzare sulle SVM

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

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

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

Come funziona l'ereditarietà dello stile di sicurezza

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

Gli stili di sicurezza vengono ereditati nel modo seguente:

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

In che modo ONTAP conserva le autorizzazioni UNIX

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

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

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

Gestire le autorizzazioni UNIX utilizzando la scheda protezione di Windows

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

- Modifica delle autorizzazioni UNIX

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

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

- Modifica delle autorizzazioni UNIX in autorizzazioni NTFS

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

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

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

Configurare gli stili di sicurezza sui volumi root SVM

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

Fasi

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

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

2. Visualizzare e verificare la configurazione, incluso lo stile di sicurezza del volume root della SVM creata: `vserver show -vserver` *`vserver_name`*

Configurare gli stili di sicurezza sui volumi FlexVol

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

Fasi

1. Eseguire una delle seguenti operazioni:

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

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

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

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

storage logico".

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

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

Configurare gli stili di sicurezza sui qtree

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

Fasi

1. Eseguire una delle seguenti operazioni:

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

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

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

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

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

Creare e gestire volumi di dati in spazi dei nomi NAS

Panoramica sulla creazione e gestione dei volumi di dati negli spazi dei nomi NAS

Per gestire l'accesso ai file in un ambiente NAS, è necessario gestire i volumi di dati e i punti di giunzione sulla macchina virtuale di storage (SVM). Ciò include la pianificazione dell'architettura dello spazio dei nomi, la creazione di volumi con o senza punti di giunzione, il montaggio o lo smontaggio di volumi e la visualizzazione di informazioni sui volumi di dati e sugli spazi dei nomi dei server NFS o CIFS.

Creare volumi di dati con punti di giunzione specificati

È possibile specificare il punto di giunzione quando si crea un volume di dati. Il volume

risultante viene montato automaticamente nel punto di giunzione ed è immediatamente disponibile per la configurazione dell'accesso NAS.

Prima di iniziare

L'aggregato in cui si desidera creare il volume deve già esistere.

> I seguenti caratteri non possono essere utilizzati nel percorso di giunzione: * N. " > < | ? .
>
> Inoltre, la lunghezza del percorso di giunzione non può superare i 255 caratteri.

Fasi

1. Creare il volume con un punto di giunzione: `volume create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed} -junction-path` *`junction_path`*

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

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

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

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

2. Verificare che il volume sia stato creato con il punto di giunzione desiderato: `volume show -vserver` *`vserver_name`* `-volume` *`volume_name`* `-junction`

Esempio

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

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

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

Creare volumi di dati senza specificare punti di giunzione

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

Prima di iniziare

L'aggregato in cui si desidera creare il volume deve già esistere.

Fasi

1. Creare il volume senza un punto di giunzione utilizzando il seguente comando: `volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed}`

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

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

2. Verificare che il volume sia stato creato senza un punto di giunzione: `volume show -vserver vserver_name -volume volume_name -junction`

Esempio

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

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

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

Montare o smontare i volumi esistenti nello spazio dei nomi NAS

È necessario montare un volume sullo spazio dei nomi NAS prima di poter configurare l'accesso del client NAS ai dati contenuti nei volumi SVM (Storage Virtual Machine). È

possibile montare un volume su un punto di giunzione se non è attualmente montato. È anche possibile smontare i volumi.

A proposito di questa attività

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

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

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

Fasi

1. Eseguire l'azione desiderata:

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

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

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

Esempi

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

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

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

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

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

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

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

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

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

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

Fasi

1. Eseguire l'azione desiderata:

Se si desidera visualizzare…	Immettere il comando…
Informazioni riepilogative sui volumi montati e non montati su SVM	`volume show -vserver vserver_name -junction`
Informazioni dettagliate sui volumi montati e non montati su SVM	`volume show -vserver vserver_name -volume volume_name -instance`

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

Esempi

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

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

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

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

Configurare le mappature dei nomi

Panoramica sulla configurazione delle mappature dei nomi

ONTAP utilizza la mappatura dei nomi per mappare le identità CIFS alle identità UNIX, le identità Kerberos alle identità UNIX e le identità UNIX alle identità CIFS. 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 CIFS.

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 CIFS o lo stile di sicurezza NTFS sui volumi.
- Viene configurato l'utente predefinito da utilizzare.

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

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

Tuttavia, è possibile mappare un gruppo di singoli utenti a un utente specifico. Ad esempio, è possibile

mappare tutti gli utenti ad che iniziano o terminano con la parola SALES a un utente UNIX specifico e all'UID dell'utente.

Come funziona la mappatura dei nomi

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

- Per la mappatura da Windows a UNIX

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

- Per la mappatura da UNIX a Windows

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

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

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

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

Multidominio ricerca le mappature dei nomi utente da UNIX a Windows

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

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

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

- *Fiducia bidirezionale*

  Con trust bidirezionali, entrambi i domini si fidano l'uno dell'altro. Se il dominio principale del server CIFS 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 CIFS. 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	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 è valido solo per la mappatura dei nomi da UNIX a Windows, non viceversa.

Come vengono eseguite le ricerche di nomi multidominio

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

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

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

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

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

Regole di conversione del mapping dei nomi

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

Creare una mappatura dei nomi

È possibile utilizzare `vserver name-mapping create` per creare una mappatura dei nomi. Si utilizzano le mappature dei nomi per consentire agli utenti Windows di accedere

ai volumi di sicurezza UNIX e viceversa.

A proposito di questa attività

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

Fase

1. Creazione di una mappatura dei nomi: `vserver name-mapping create -vserver` *`vserver_name`* `-direction {krb-unix|win-unix|unix-win} -position` *`integer`* `-pattern text -replacement` *`text`*

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

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

Esempi

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

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

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

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

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

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

Configurare l'utente predefinito

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

A proposito di questa attività

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

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

Fasi

1. Eseguire una delle seguenti operazioni:

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

Comandi per la gestione delle mappature dei nomi

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

Se si desidera…	Utilizzare questo comando…
Creare una mappatura dei nomi	`vserver name-mapping create`
Inserire una mappatura dei nomi in una posizione specifica	`vserver name-mapping insert`
Visualizza mappature dei nomi	`vserver name-mapping show`
Scambiare la posizione di due mappature dei nomi Lo swap non è consentito 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`

Se si desidera…	Utilizzare questo comando…
Eliminare una mappatura dei nomi	`vserver name-mapping delete`
Convalidare la corretta mappatura dei nomi	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

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

Configurare le ricerche di mappatura dei nomi di più domini

Attivare o disattivare le ricerche di mappatura dei nomi multidominio

Con le ricerche di mappatura dei nomi di più domini, è possibile utilizzare un carattere jolly (**) nella parte di dominio di un nome Windows quando si configura l'associazione di utenti UNIX con nomi utente Windows. L'utilizzo di un wild card (**) nella parte di dominio del nome consente a ONTAP di cercare tutti i domini con un trust bidirezionale con il dominio che contiene l'account del computer del server CIFS.

A proposito di questa attività

In alternativa alla ricerca di tutti i domini con attendenza bidirezionale, è possibile configurare un elenco di domini attendibili preferiti. Quando viene configurato un elenco di domini trusted preferiti, ONTAP utilizza l'elenco di domini trusted preferito invece dei domini trusted bidirezionalmente rilevati per eseguire ricerche di mappatura dei nomi a più domini.

- Per impostazione predefinita, le ricerche di mappatura dei nomi multidominio sono attivate.
- Questa opzione è disponibile al livello di privilegio avanzato.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
2. Eseguire una delle seguenti operazioni:

Se si desidera che le ricerche di mappatura dei nomi di più domini siano…	Immettere il comando…
Attivato	`vserver cifs options modify -vserver` *`vserver_name`* `-is-trusted-domain-enum -search-enabled true`
Disattivato	`vserver cifs options modify -vserver` *`vserver_name`* `-is-trusted-domain-enum -search-enabled false`

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

Informazioni correlate

Opzioni server SMB disponibili

Reimpostare e riscoprire i domini attendibili

È possibile forzare la riscoperta di tutti i domini attendibili. Ciò può risultare utile quando i server di dominio attendibili non rispondono in modo appropriato o le relazioni di trust sono cambiate. Vengono rilevati solo i domini con un trust bidirezionale con il dominio principale, ovvero il dominio contenente l'account del computer del server CIFS.

Fase

1. Reimpostare e riscoprire i domini attendibili utilizzando `vserver cifs domain trusts rediscover` comando.

   ```
   vserver cifs domain trusts rediscover -vserver vs1
   ```

Informazioni correlate

Visualizzazione delle informazioni sui domini attendibili rilevati

Visualizza informazioni sui domini attendibili rilevati

È possibile visualizzare informazioni sui domini attendibili rilevati per il dominio principale del server CIFS, ovvero il dominio contenente l'account del computer del server CIFS. Ciò può essere utile quando si desidera sapere quali domini attendibili vengono rilevati e come vengono ordinati all'interno dell'elenco di domini attendibili rilevati.

A proposito di questa attività

Vengono rilevati solo i domini con trust bidirezionali con il dominio principale. Poiché il domain controller (DC) del dominio principale restituisce l'elenco dei domini attendibili in un ordine determinato dal controller di dominio, non è possibile prevedere l'ordine dei domini all'interno dell'elenco. Visualizzando l'elenco dei domini attendibili, è possibile determinare l'ordine di ricerca per le ricerche di mappatura dei nomi multidominio.

Le informazioni di dominio attendibile visualizzate sono raggruppate per nodo e SVM (Storage Virtual Machine).

Fase

1. Visualizzare le informazioni sui domini attendibili rilevati utilizzando `vserver cifs domain trusts show` comando.

   ```
   vserver cifs domain trusts show -vserver vs1
   ```

```
   Node: node1
Vserver: vs1

Home Domain            Trusted Domain
---------------------  -----------------------------------
EXAMPLE.COM            CIFS1.EXAMPLE.COM,
                       CIFS2.EXAMPLE.COM
                       EXAMPLE.COM

   Node: node2
Vserver: vs1

Home Domain            Trusted Domain
---------------------  -----------------------------------
EXAMPLE.COM            CIFS1.EXAMPLE.COM,
                       CIFS2.EXAMPLE.COM
                       EXAMPLE.COM
```

Informazioni correlate

Reimpostazione e riscoperta di domini attendibili

Aggiungere, rimuovere o sostituire i domini attendibili negli elenchi di domini attendibili preferiti

È possibile aggiungere o rimuovere domini attendibili dall'elenco dei domini attendibili preferiti per il server SMB oppure modificare l'elenco corrente. Se si configura un elenco di domini trusted preferito, questo elenco viene utilizzato al posto dei domini trusted bidirezionali rilevati durante le ricerche di mappatura dei nomi di più domini.

A proposito di questa attività

- Se si aggiungono domini attendibili a un elenco esistente, il nuovo elenco viene Unito all'elenco esistente con le nuove voci alla fine I domini attendibili vengono ricercati nell'ordine in cui vengono visualizzati nell'elenco dei domini attendibili.
- Se si rimuovono domini attendibili dall'elenco esistente e non si specifica un elenco, l'intero elenco di domini attendibili per la macchina virtuale di storage (SVM) specificata viene rimosso.
- Se si modifica l'elenco esistente di domini attendibili, il nuovo elenco sovrascrive quello esistente.

> Nell'elenco Preferred trusted domain (dominio trusted preferito), inserire solo domini trusted bidirezionalmente attendibili. Anche se è possibile inserire domini trust in uscita o in entrata nell'elenco dei domini preferiti, questi non vengono utilizzati durante le ricerche di mappatura dei nomi di più domini. ONTAP ignora la voce relativa al dominio unidirezionale e passa al successivo dominio attendibile bidirezionale nell'elenco.

Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera eseguire le seguenti operazioni con l'elenco dei domini attendibili preferiti…	Utilizzare il comando…
Aggiungere domini attendibili all'elenco	`vserver cifs domain name-mapping-search add -vserver _vserver_name_ -trusted-domains FQDN, ...`
Rimuovere i domini attendibili dall'elenco	`vserver cifs domain name-mapping-search remove -vserver _vserver_name_ [-trusted-domains FQDN, ...]`
Modificare l'elenco esistente	`vserver cifs domain name-mapping-search modify -vserver _vserver_name_ -trusted-domains FQDN, ...`

Esempi

Il seguente comando aggiunge due domini attendibili (cifs1.example.com e cifs2.example.com) all'elenco di domini attendibili preferito utilizzato da SVM vs1:

```
cluster1::> vserver cifs domain name-mapping-search add -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

Il seguente comando rimuove due domini attendibili dall'elenco utilizzato da SVM vs1:

```
cluster1::> vserver cifs domain name-mapping-search remove -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

Il seguente comando modifica l'elenco di domini attendibili utilizzato da SVM vs1. Il nuovo elenco sostituisce quello originale:

```
cluster1::> vserver cifs domain name-mapping-search modify -vserver vs1
-trusted-domains cifs3.example.com
```

Informazioni correlate

Visualizzazione delle informazioni sull'elenco di domini attendibili preferiti

Visualizzare le informazioni relative all'elenco di domini attendibili preferiti

È possibile visualizzare le informazioni sui domini attendibili presenti nell'elenco dei domini attendibili preferiti e l'ordine in cui vengono ricercati se sono attivate le ricerche di mappatura dei nomi multidominio. È possibile configurare un elenco di domini attendibili preferito in alternativa all'elenco di domini attendibili rilevati automaticamente.

Fasi

1. Eseguire una delle seguenti operazioni:

Se si desidera visualizzare informazioni su…	Utilizzare il comando…
Tutti i domini trusted preferiti nel cluster raggruppati per SVM (Storage Virtual Machine)	`vserver cifs domain name-mapping-search show`
Tutti i domini trusted preferiti per una SVM specificata	`vserver cifs domain name-mapping-search show -vserver` *`vserver_name`*

Il seguente comando visualizza informazioni su tutti i domini attendibili preferiti nel cluster:

```
cluster1::> vserver cifs domain name-mapping-search show
Vserver         Trusted Domains
--------------  ----------------------------------
vs1             CIFS1.EXAMPLE.COM
```

Informazioni correlate

Aggiunta, rimozione o sostituzione di domini attendibili in elenchi di domini attendibili preferiti

Creare e configurare le condivisioni SMB

Panoramica sulla creazione e la configurazione delle condivisioni SMB

Prima che utenti e applicazioni possano accedere ai dati sul server CIFS tramite SMB, è necessario creare e configurare le condivisioni SMB, che è un access point denominato in un volume. È possibile personalizzare le condivisioni specificando i parametri di condivisione e le proprietà di condivisione. È possibile modificare una condivisione esistente in qualsiasi momento.

Quando si crea una condivisione SMB, ONTAP crea un ACL predefinito per la condivisione con autorizzazioni di controllo completo per tutti.

Le condivisioni SMB sono legate al server CIFS sulla macchina virtuale di storage (SVM). Le condivisioni SMB vengono eliminate se la SVM viene eliminata o se il server CIFS a cui è associata viene cancellato dalla SVM. Se si ricrea il server CIFS su SVM, è necessario ricreare le condivisioni SMB.

Informazioni correlate

Gestire l'accesso ai file utilizzando SMB

"Configurazione SMB per Microsoft Hyper-V e SQL Server"

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

Quali sono le condivisioni amministrative predefinite

Quando si crea un server CIFS sulla macchina virtuale di storage (SVM), vengono create

automaticamente le condivisioni amministrative predefinite. È necessario comprendere quali sono le condivisioni predefinite e come vengono utilizzate.

Quando si crea il server CIFS, ONTAP crea le seguenti condivisioni amministrative predefinite:

> A partire da ONTAP 9.8, la condivisione in dollari di amministrazione non viene più creata per impostazione predefinita.

- ipc
- admin (solo ONTAP 9.7 e versioni precedenti)
- €

Poiché le condivisioni che terminano con il carattere € sono condivisioni nascoste, le condivisioni amministrative predefinite non sono visibili da risorse del computer, ma è possibile visualizzarle utilizzando le cartelle condivise.

Come vengono utilizzate le condivisioni predefinite ipc e admin

Le condivisioni ipc e admin vengono utilizzate da ONTAP e non possono essere utilizzate dagli amministratori Windows per accedere ai dati che risiedono sulla SVM.

- condivisione ipc

  La condivisione ipc è una risorsa che condivide le named pipe che sono essenziali per la comunicazione tra i programmi. La condivisione ipc viene utilizzata durante l'amministrazione remota di un computer e durante la visualizzazione delle risorse condivise di un computer. Non è possibile modificare le impostazioni di condivisione, le proprietà di condivisione o gli ACL della condivisione ipc. Inoltre, non è possibile rinominare o eliminare la condivisione ipc.

- Quota amministrativa (solo ONTAP 9.7 e versioni precedenti)

  > A partire da ONTAP 9.8, la condivisione in dollari di amministrazione non viene più creata per impostazione predefinita.

  La condivisione admin viene utilizzata durante l'amministrazione remota di SVM. Il percorso di questa risorsa è sempre il percorso verso la radice SVM. Non è possibile modificare le impostazioni di condivisione, le proprietà di condivisione o gli ACL per la condivisione admin. Inoltre, non è possibile rinominare o eliminare la condivisione admin.

Modalità di utilizzo della condivisione predefinita

La condivisione è una condivisione amministrativa che il cluster o l'amministratore SVM può utilizzare per accedere e gestire il volume root SVM.

Di seguito sono riportate le caratteristiche della quota:

- Il percorso per questa condivisione è sempre il percorso del volume root SVM e non può essere modificato.
- L'ACL predefinito per la condivisione è Amministratore/controllo completo.

  Questo utente è il BUILTIN/amministratore. Per impostazione predefinita, il BUILTIN/amministratore può eseguire il mapping alla condivisione e visualizzare, creare, modificare o eliminare file e cartelle nella

directory principale mappata. Prestare attenzione durante la gestione di file e cartelle in questa directory.

- È possibile modificare l'ACL della condivisione.
- È possibile modificare le impostazioni di condivisione e le proprietà di condivisione.
- Non è possibile eliminare la condivisione.
- L'amministratore di SVM può accedere al resto dello spazio dei nomi SVM dalla condivisione mappata incrociando le giunzioni dello spazio dei nomi.
- È possibile accedere alla condivisione utilizzando Microsoft Management Console.

Informazioni correlate

Configurazione delle autorizzazioni avanzate per i file NTFS mediante la scheda protezione di Windows

Requisiti di naming delle condivisioni SMB

Quando si creano condivisioni SMB sul server SMB, è necessario tenere presenti i requisiti di denominazione delle condivisioni ONTAP.

Le convenzioni di denominazione delle condivisioni per ONTAP sono le stesse di Windows e includono i seguenti requisiti:

- Il nome di ciascuna condivisione deve essere univoco per il server SMB.
- I nomi delle condivisioni non rilevano la distinzione tra maiuscole e minuscole.
- La lunghezza massima del nome di condivisione è di 80 caratteri.
- I nomi di condivisione Unicode sono supportati.
- I nomi delle condivisioni che terminano con il carattere € sono condivisioni nascoste.
- Per ONTAP 9.7 e versioni precedenti, le condivisioni amministrative admin, ipc e c vengono create automaticamente su ogni server CIFS e sono nomi di condivisione riservati. A partire da ONTAP 9.8, la condivisione admin non viene più creata automaticamente.
- Non è possibile utilizzare il nome di condivisione ONTAP_ADMIN quando si crea una condivisione.
- Sono supportati i nomi di condivisione contenenti spazi:
  - Non è possibile utilizzare uno spazio come primo carattere o come ultimo carattere di un nome di condivisione.
  - È necessario racchiudere i nomi delle condivisioni contenenti uno spazio tra virgolette.

> Le virgolette singole sono considerate parte del nome della condivisione e non possono essere utilizzate al posto delle virgolette.

- I seguenti caratteri speciali sono supportati quando si assegnano le condivisioni SMB:

  ! @ % E ' _ - . ~ ( ) { }

- I seguenti caratteri speciali non sono supportati quando si assegnano nomi SMB share:
  - " / " ; | < > , ? * =

Requisiti di distinzione tra maiuscole e minuscole per la creazione di condivisioni in un ambiente multiprotocollo

Se si creano condivisioni in una SVM in cui viene utilizzato lo schema di denominazione 8.3 per distinguere tra nomi di directory in cui esistono solo differenze di maiuscole e minuscole tra i nomi, è necessario utilizzare il nome 8.3 nel percorso di condivisione per garantire che il client si connetta al percorso di directory desiderato.

Nell'esempio seguente, due directory denominate "testdir" e "TESTDIR" sono state create su un client Linux. Il percorso di giunzione del volume contenente le directory è `/home`. Il primo output proviene da un client Linux e il secondo da un client SMB.

```
 ls -l
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:23 testdir
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:24 TESTDIR
```

```
dir

 Directory of Z:\

04/17/2015  11:23 AM    <DIR>          testdir
04/17/2015  11:24 AM    <DIR>          TESTDI~1
```

Quando si crea una condivisione nella seconda directory, è necessario utilizzare il nome 8.3 nel percorso di condivisione. In questo esempio, il percorso di condivisione per la prima directory è `/home/testdir` il percorso di condivisione per la seconda directory è `/home/TESTDI~1`.

Utilizzare le proprietà di condivisione SMB

Utilizza la panoramica delle proprietà di condivisione SMB

È possibile personalizzare le proprietà delle condivisioni SMB.

Le proprietà di condivisione disponibili sono le seguenti:

Condividere le proprietà	Descrizione
`oplocks`	Questa proprietà specifica che la condivisione utilizza blocchi opportunistici, noti anche come caching lato client.
`browsable`	Questa proprietà consente ai client Windows di esplorare la condivisione.
`showsnapshot`	Questa proprietà specifica che le copie Snapshot possono essere visualizzate e attraversate dai client.

Condividere le proprietà	Descrizione
`changenotify`	Questa proprietà specifica che la condivisione supporta le richieste di notifica delle modifiche. Per le condivisioni su una SVM, si tratta di una proprietà iniziale predefinita.
`attributecache`	Questa proprietà abilita il caching degli attributi del file nella condivisione SMB per fornire un accesso più rapido agli attributi. L'impostazione predefinita prevede la disattivazione del caching degli attributi. Questa proprietà deve essere attivata solo se ci sono client che si connettono alle condivisioni su SMB 1.0. Questa proprietà di condivisione non è applicabile se i client si connettono alle condivisioni tramite SMB 2.x o SMB 3.0.
`continuously-available`	Questa proprietà consente ai client SMB che lo supportano di aprire i file in modo persistente. I file aperti in questo modo sono protetti da eventi di interruzione, come failover e giveback.
`branchcache`	Questa proprietà specifica che la condivisione consente ai client di richiedere gli hash BranchCache sui file all'interno di questa condivisione. Questa opzione è utile solo se si specifica "per-share" come modalità operativa nella configurazione CIFS BranchCache.
`access-based-enumeration`	Questa proprietà specifica che l'opzione *Access Based Enumeration* (ABE) è attivata per questa condivisione. Le cartelle condivise con filtro ABE sono visibili a un utente in base ai diritti di accesso del singolo utente, impedendo la visualizzazione di cartelle o altre risorse condivise a cui l'utente non dispone dei diritti di accesso.
`namespace-caching`	Questa proprietà specifica che i client SMB che si connettono a questa condivisione possono memorizzare nella cache i risultati dell'enumerazione delle directory restituiti dai server CIFS, in modo da ottenere performance migliori. Per impostazione predefinita, i client SMB 1 non memorizzano nella cache i risultati dell'enumerazione delle directory. Poiché i client SMB 2 e SMB 3 memorizzano nella cache i risultati dell'enumerazione delle directory per impostazione predefinita, la specifica di questa proprietà di condivisione offre vantaggi in termini di prestazioni solo per le connessioni client SMB 1.

Condividere le proprietà	Descrizione
`encrypt-data`	Questa proprietà specifica che la crittografia SMB deve essere utilizzata quando si accede a questa condivisione. I client SMB che non supportano la crittografia durante l'accesso ai dati SMB non potranno accedere a questa condivisione.

Aggiungere o rimuovere le proprietà di condivisione su una condivisione SMB esistente

È possibile personalizzare una condivisione SMB esistente aggiungendo o rimuovendo le proprietà della condivisione. Questo può essere utile se si desidera modificare la configurazione della condivisione per soddisfare i requisiti in continuo cambiamento nell'ambiente.

Prima di iniziare

La condivisione di cui si desidera modificare le proprietà deve esistere.

A proposito di questa attività

Linee guida per l'aggiunta di proprietà di condivisione:

- È possibile aggiungere una o più proprietà di condivisione utilizzando un elenco delimitato da virgole.
- Tutte le proprietà di condivisione precedentemente specificate rimangono attive.

  Le nuove proprietà aggiunte vengono aggiunte all'elenco esistente di proprietà di condivisione.

- Se si specifica un nuovo valore per le proprietà di condivisione già applicate alla condivisione, il nuovo valore specificato sostituisce il valore originale.
- Non è possibile rimuovere le proprietà di condivisione utilizzando `vserver cifs share properties add` comando.

  È possibile utilizzare `vserver cifs share properties remove` comando per rimuovere le proprietà di condivisione.

Linee guida per la rimozione delle proprietà di condivisione:

- È possibile rimuovere una o più proprietà di condivisione utilizzando un elenco delimitato da virgole.
- Tutte le proprietà di condivisione precedentemente specificate ma non rimosse rimangono attive.

Fasi

1. Immettere il comando appropriato:

Se si desidera…	Immettere il comando…
Aggiungere proprietà di condivisione	`vserver cifs share properties add -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...`

Se si desidera…	Immettere il comando…
Rimuovere le proprietà di condivisione	`vserver cifs share properties remove -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...`

2. Verificare le impostazioni della proprietà di condivisione: `vserver cifs share show -vserver vserver_name -share-name share_name`

Esempi

Il seguente comando aggiunge `showsnapshot` Condividere la proprietà con una condivisione denominata "share1" su SVM vs1:

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties showsnapshot

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share   Path      Properties   Comment    ACL
---------  ------  --------  ----------   --------   -----------
vs1        share1  /share1   oplocks      -          Everyone / Full
Control
                             browsable
                             changenotify
                             showsnapshot
```

Il seguente comando rimuove `browsable` Condividere la proprietà da una condivisione denominata "share2" su SVM vs1:

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share2 -share-properties browsable

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share   Path      Properties   Comment    ACL
---------  ------  --------  ----------   --------   -----------
vs1        share2  /share2   oplocks      -          Everyone / Full
Control
                             changenotify
```

Informazioni correlate

Comandi per la gestione delle condivisioni SMB

Ottimizza l'accesso degli utenti SMB con l'impostazione di force-group share

Quando si crea una condivisione dalla riga di comando di ONTAP ai dati con protezione effettiva UNIX, è possibile specificare che tutti i file creati dagli utenti SMB in tale condivisione appartengano allo stesso gruppo, noto come *force-group*, che deve essere un gruppo predefinito nel database dei gruppi UNIX. L'utilizzo di un gruppo di forze semplifica l'accesso ai file da parte degli utenti SMB appartenenti a diversi gruppi.

Specificare un gruppo di forze è significativo solo se la condivisione si trova in un qtree UNIX o misto. Non è necessario impostare un gruppo di forza per le condivisioni in un volume o qtree NTFS, in quanto l'accesso ai file in queste condivisioni è determinato dalle autorizzazioni di Windows, non dai GID UNIX.

Se è stato specificato un gruppo di forze per una condivisione, si verifica quanto segue:

- Gli utenti SMB nel gruppo di forza che accedono a questa condivisione vengono temporaneamente modificati in GID del gruppo di forze.

  Questo GID consente loro di accedere ai file in questa condivisione che non sono normalmente accessibili con il GID o UID primario.

- Tutti i file in questa condivisione creati dagli utenti SMB appartengono allo stesso gruppo di forze, indipendentemente dal GID primario del proprietario del file.

Quando gli utenti SMB tentano di accedere a un file creato da NFS, i GID primari degli utenti SMB determinano i diritti di accesso.

Il force-group non influisce sul modo in cui gli utenti NFS accedono ai file in questa condivisione. Un file creato da NFS acquisisce il GID dal proprietario del file. La determinazione delle autorizzazioni di accesso si basa sull'UID e sul GID primario dell'utente NFS che sta tentando di accedere al file.

L'utilizzo di un gruppo di forze semplifica l'accesso ai file da parte degli utenti SMB appartenenti a diversi gruppi. Ad esempio, se si desidera creare una condivisione per memorizzare le pagine Web dell'azienda e concedere l'accesso in scrittura agli utenti dei reparti Engineering e Marketing, è possibile creare una condivisione e assegnare l'accesso in scrittura a un gruppo di forze denominato "webgroup1". A causa del gruppo di forza, tutti i file creati dagli utenti SMB in questa condivisione sono di proprietà del gruppo "webgroup1". Inoltre, agli utenti viene assegnato automaticamente il GID del gruppo "webgroup1" quando accedono alla condivisione. Di conseguenza, tutti gli utenti possono scrivere su questa condivisione senza dover gestire i diritti di accesso degli utenti nei reparti Engineering e Marketing.

Informazioni correlate

Creazione di una condivisione SMB con l'impostazione force-group share

Creare una condivisione SMB con l'impostazione di force-group share

È possibile creare una condivisione SMB con l'impostazione force-group share se si desidera che gli utenti SMB che accedono ai dati su volumi o qtree con sicurezza dei file UNIX siano considerati da ONTAP come appartenenti allo stesso gruppo UNIX.

Fase

1. Creare la condivisione SMB: `vserver cifs share create -vserver vserver_name -share -name share_name -path path -force-group-for-create UNIX_group_name`

Se il percorso UNC (`\\servername\sharename\filepath`) della condivisione contiene più di 256 caratteri (escluso il " iniziale`\\`" Nel percorso UNC), la scheda **Security** nella casella Proprietà di Windows non è disponibile. Si tratta di un problema del client Windows piuttosto che di un problema ONTAP. Per evitare questo problema, non creare condivisioni con percorsi UNC con più di 256 caratteri.

Se si desidera rimuovere il gruppo di forza dopo la creazione della condivisione, è possibile modificare la condivisione in qualsiasi momento e specificare una stringa vuota ("") come valore per `-force-group -for-create` parametro. Se si rimuove il gruppo di forza modificando la condivisione, tutte le connessioni esistenti a questa condivisione continueranno a avere il gruppo di forza precedentemente impostato come GID primario.

Esempio

Il seguente comando crea una condivisione “webpages” accessibile sul Web in `/corp/companyinfo` Directory in cui tutti i file creati dagli utenti SMB sono assegnati al gruppo webgroup1:

```
vserver cifs share create -vserver vs1 -share-name webpages -path
/corp/companyinfo -force-group-for-create webgroup1
```

Informazioni correlate

Ottimizza l’accesso degli utenti SMB con l’impostazione di force-group share

Visualizzare le informazioni sulle condivisioni SMB utilizzando MMC

È possibile visualizzare informazioni sulle condivisioni SMB sulla SVM ed eseguire alcune attività di gestione utilizzando Microsoft Management Console (MMC). Prima di poter visualizzare le condivisioni, è necessario collegare MMC a SVM.

A proposito di questa attività

È possibile eseguire le seguenti attività sulle condivisioni contenute in SVM utilizzando MMC:

- Visualizza condivisioni
- Visualizzare le sessioni attive
- Visualizzare i file aperti
- Enumerare l’elenco di sessioni, file e connessioni ad albero nel sistema
- Chiudere i file aperti nel sistema
- Chiudere le sessioni aperte
- Creare/gestire le condivisioni

> Le viste visualizzate dalle funzionalità precedenti sono specifiche del nodo e non del cluster. Pertanto, quando si utilizza MMC per connettersi al nome host del server SMB (cioè, cifs01.domain.local), si viene indirizzati, in base alla configurazione del DNS, a una singola LIF all’interno del cluster.

Le seguenti funzioni non sono supportate in MMC per ONTAP:

- Creazione di nuovi utenti/gruppi locali
- Gestione/visualizzazione di utenti/gruppi locali esistenti
- Visualizzazione di eventi o log delle performance

- Storage
- Servizi e applicazioni

Nei casi in cui l'operazione non è supportata, potrebbe verificarsi un'operazione `remote procedure call failed` errori.

"Domande frequenti: Utilizzo di Windows MMC con ONTAP"

Fasi

1. Per aprire la MMC Gestione computer su qualsiasi server Windows, nel pannello di controllo, selezionare **Strumenti di amministrazione** > **Gestione computer**.
2. Selezionare **azione** > **connessione a un altro computer**.

   Viene visualizzata la finestra di dialogo Select computer (Seleziona computer).

3. Digitare il nome del sistema di storage o fare clic su **Browse** (Sfoglia) per individuare il sistema di storage.
4. Fare clic su **OK**.

   MMC si connette a SVM.

5. Nel riquadro di navigazione, fare clic su **Shared Folders** > **Shares**.

   Nel riquadro di visualizzazione di destra viene visualizzato un elenco di condivisioni su SVM.

6. Per visualizzare le proprietà di una condivisione, fare doppio clic sulla condivisione per aprire la finestra di dialogo **Proprietà**.
7. Se non è possibile connettersi al sistema di storage utilizzando MMC, è possibile aggiungere l'utente al gruppo BUILTIN/Administrators o al gruppo BUILTIN/Power Users utilizzando uno dei seguenti comandi sul sistema di storage:

   ```
   cifs users-and-groups local-groups add-members -vserver <vserver_name>
   -group-name BUILTIN\Administrators -member-names <domainuser>

   cifs users-and-groups local-groups add-members -vserver <vserver_name>
   -group-name "BUILTIN\Power Users" -member-names <domainuser>
   ```

Comandi per la gestione delle condivisioni SMB

Si utilizza `vserver cifs share` e. `vserver cifs share properties` Comandi per gestire le condivisioni SMB.

Se si desidera…	Utilizzare questo comando…
Creare una condivisione SMB	`vserver cifs share create`
Visualizzare le condivisioni SMB	`vserver cifs share show`

Se si desidera…	Utilizzare questo comando…
Modificare una condivisione SMB	`vserver cifs share modify`
Eliminare una condivisione SMB	`vserver cifs share delete`
Aggiungere le proprietà di condivisione a una condivisione esistente	`vserver cifs share properties add`
Rimuovere le proprietà di condivisione da una condivisione esistente	`vserver cifs share properties remove`
Visualizza le informazioni sulle proprietà di condivisione	`vserver cifs share properties show`

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

Accesso sicuro ai file utilizzando gli ACL di condivisione SMB

Linee guida per la gestione degli ACL a livello di condivisione SMB

È possibile modificare gli ACL a livello di condivisione per offrire agli utenti più o meno diritti di accesso alla condivisione. È possibile configurare ACL a livello di condivisione utilizzando utenti e gruppi Windows o utenti e gruppi UNIX.

Dopo aver creato una condivisione, per impostazione predefinita, l'ACL a livello di condivisione fornisce l'accesso in lettura al gruppo standard denominato Everyone. L'accesso in lettura nell'ACL significa che tutti gli utenti del dominio e tutti i domini attendibili hanno accesso in sola lettura alla condivisione.

È possibile modificare un ACL a livello di condivisione utilizzando la console di gestione Microsoft su un client Windows o la riga di comando di ONTAP.

Quando si utilizza MMC, si applicano le seguenti linee guida:

- I nomi utente e gruppo specificati devono essere nomi Windows.
- È possibile specificare solo le autorizzazioni di Windows.

Quando si utilizza la riga di comando ONTAP, si applicano le seguenti linee guida:

- I nomi utente e gruppo specificati possono essere nomi Windows o UNIX.

  Se durante la creazione o la modifica degli ACL non viene specificato un tipo di utente e gruppo, il tipo predefinito è utenti e gruppi Windows.

- È possibile specificare solo le autorizzazioni di Windows.

Creare elenchi di controllo degli accessi di condivisione SMB

La configurazione delle autorizzazioni di condivisione mediante la creazione di elenchi di controllo degli accessi (ACL) per le condivisioni SMB consente di controllare il livello di accesso a una condivisione per utenti e gruppi.

A proposito di questa attività

È possibile configurare gli ACL a livello di condivisione utilizzando nomi di utenti o gruppi Windows locali o di dominio o nomi di utenti o gruppi UNIX.

Prima di creare un nuovo ACL, è necessario eliminare l'ACL di condivisione predefinito `Everyone / Full Control`, che comporta un rischio per la sicurezza.

In modalità workgroup, il nome di dominio locale è il nome del server SMB.

Fasi

1. Eliminare l'ACL della condivisione predefinita:`vserver cifs share access control delete -vserver *vserver_name* -share *share_name* -user-or-group everyone`
2. Configurare il nuovo ACL:

Se si desidera configurare gli ACL utilizzando un…	Immettere il comando…
Utente Windows	`vserver cifs share access-control create -vserver` *`vserver_name`* `-share` *`share_name`* `-user-group-type windows -user-or-group` *`Windows_domain_name\user_name`* `-permission` *`access_right`*
Gruppo di Windows	`vserver cifs share access-control create -vserver` *`vserver_name`* `-share` *`share_name`* `-user-group-type windows -user-or-group` *`Windows_domain_name\group_name`* `-permission` *`access_right`*
Utente UNIX	`vserver cifs share access-control create -vserver` *`vserver_name`* `-share` *`share_name`* `-user-group-type` *`unix-user`* `-user-or-group` *`UNIX_user_name`* `-permission access_right`
Gruppo UNIX	`vserver cifs share access-control create -vserver` *`vserver_name`* `-share` *`share_name`* `-user-group-type` *`unix-group`* `-user-or-group` *`UNIX_group_name`* `-permission access_right`

3. Verificare che l'ACL applicato alla condivisione sia corretto utilizzando `vserver cifs share access-control show` comando.

Esempio

Il seguente comando fornisce `Change` Permessi al gruppo Windows "Sales Team" per la condivisione "sales" su "`vs1.example.com` "SVM:

```
cluster1::> vserver cifs share access-control create -vserver
vs1.example.com -share sales -user-or-group "DOMAIN\Sales Team"
-permission Change

cluster1::> vserver cifs share access-control show -vserver
vs1.example.com
                Share       User/Group              User/Group  Access
Vserver         Name        Name                    Type
Permission
---------------- ----------- --------------------    ---------
-----------
vs1.example.com  c$          BUILTIN\Administrators  windows
Full_Control
vs1.example.com  sales       DOMAIN\Sales Team     windows     Change
```

Il seguente comando fornisce `Read` Autorizzazione al gruppo UNIX "engineering" per la condivisione "eng" su "`vs2.example.com` "SVM:

```
cluster1::> vserver cifs share access-control create -vserver
vs2.example.com -share eng -user-group-type unix-group -user-or-group
engineering -permission Read

cluster1::> vserver cifs share access-control show -vserver
vs2.example.com
                Share       User/Group               User/Group  Access
Vserver         Name        Name                     Type
Permission
---------------- ----------- -------------------      -----------
-----------
vs2.example.com  c$          BUILTIN\Administrators   windows
Full_Control
vs2.example.com  eng         engineering              unix-group  Read
```

I seguenti comandi impartire `Change` Autorizzazione al gruppo Windows locale denominato "Tiger Team" e. `Full_Control` Autorizzazione all'utente Windows locale "Sue Chang" per la condivisione "datavol5" su "`vs1` "SVM:

```
cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vserver cifs share access-control show -vserver vs1
               Share       User/Group                  User/Group  Access
Vserver        Name        Name                        Type
Permission
-------------- ----------- --------------------------- -----------
-----------
vs1            c$          BUILTIN\Administrators      windows
Full_Control
vs1            datavol5    Tiger Team         windows     Change
vs1            datavol5    Sue Chang          windows     Full_Control
```

Comandi per la gestione degli elenchi di controllo degli accessi di condivisione SMB

È necessario conoscere i comandi per la gestione degli ACL (Access Control List) SMB, che includono la creazione, la visualizzazione, la modifica e l'eliminazione di tali elenchi.

Se si desidera…	Utilizzare questo comando…
Creare un nuovo ACL	`vserver cifs share access-control create`
Visualizza ACL	`vserver cifs share access-control show`
Modificare un ACL	`vserver cifs share access-control modify`
Eliminare un ACL	`vserver cifs share access-control delete`

Proteggere l'accesso ai file utilizzando i permessi

Configurare le autorizzazioni avanzate per i file NTFS utilizzando la scheda protezione di Windows

È possibile configurare le autorizzazioni standard per i file NTFS su file e cartelle

utilizzando la scheda **Windows Security** nella finestra Proprietà di Windows.

Prima di iniziare

L'amministratore che esegue questa attività deve disporre di autorizzazioni NTFS sufficienti per modificare le autorizzazioni sugli oggetti selezionati.

A proposito di questa attività

La configurazione delle autorizzazioni dei file NTFS viene eseguita su un host Windows aggiungendo voci agli elenchi di controllo degli accessi discrezionali (DACL) NTFS associati a un descrittore di protezione NTFS. Il descrittore di protezione viene quindi applicato ai file e alle directory NTFS. Queste attività vengono gestite automaticamente dalla GUI di Windows.

Fasi

1. Dal menu **Strumenti** di Esplora risorse, selezionare **Connetti unità di rete**.
2. Completare la finestra di dialogo **Map Network Drive** (Connetti unità di rete):

   a. Selezionare una lettera **Drive**.

   b. Nella casella **Folder**, digitare il nome del server CIFS contenente la condivisione contenente i dati a cui si desidera applicare le autorizzazioni e il nome della condivisione.

      Se il nome del server CIFS è "CIFS_SERVER" e la condivisione è denominata "share1", digitare `\\CIFS_SERVER\share1`.

      > È possibile specificare l'indirizzo IP dell'interfaccia dati per il server CIFS invece del nome del server CIFS.

   c. Fare clic su **fine**.

   Il disco selezionato viene montato e pronto con la finestra Esplora risorse che visualizza i file e le cartelle contenuti nella condivisione.

3. Selezionare il file o la directory per cui si desidera impostare le autorizzazioni per il file NTFS.
4. Fare clic con il pulsante destro del mouse sul file o sulla directory, quindi selezionare **Proprietà**.
5. Selezionare la scheda **sicurezza**.

   La scheda **Security** visualizza l'elenco di utenti e gruppi per i quali è impostata l'autorizzazione NTFS. La casella **Permissions for** (autorizzazioni per) visualizza un elenco delle autorizzazioni Allow e Nega in vigore per ogni utente o gruppo selezionato.

6. Fare clic su **Avanzate**.

   La finestra Proprietà di Windows visualizza informazioni sulle autorizzazioni file esistenti assegnate a utenti e gruppi.

7. Fare clic su **Modifica permessi**.

   Viene visualizzata la finestra Permissions (autorizzazioni).

8. Eseguire le azioni desiderate:

Se si desidera…	Effettuare le seguenti operazioni…
Impostare autorizzazioni NTFS avanzate per un nuovo utente o gruppo	a. Fare clic su **Aggiungi**. b. Nella casella **inserire il nome dell'oggetto da selezionare**, digitare il nome dell'utente o del gruppo che si desidera aggiungere. c. Fare clic su **OK**.
Modificare le autorizzazioni NTFS avanzate da un utente o da un gruppo	a. Nella casella **Permissions entries:**, selezionare l'utente o il gruppo di cui si desidera modificare le autorizzazioni avanzate. b. Fare clic su **Edit** (Modifica).
Rimuovere le autorizzazioni NTFS avanzate per un utente o un gruppo	a. Nella casella **Permissions entries:**, selezionare l'utente o il gruppo che si desidera rimuovere. b. Fare clic su **Rimuovi**. c. Passare alla fase 13.

Se si aggiungono autorizzazioni NTFS avanzate a un nuovo utente o gruppo o si modificano le autorizzazioni avanzate NTFS per un utente o un gruppo esistente, viene visualizzata la finestra immissione autorizzazioni per <Object>.

9. Nella casella **Apply to** (Applica a), selezionare la modalità di applicazione della voce di autorizzazione del file NTFS.

   Se si impostano le autorizzazioni per un file NTFS su un singolo file, la casella **Apply to** (Applica a) non è attiva. L'impostazione predefinita di **Apply to** (Applica a) è **solo questo oggetto**.

10. Nella casella **Permissions** (autorizzazioni), selezionare le caselle **Allow** (Consenti) o **Nega** per le autorizzazioni avanzate che si desidera impostare su questo oggetto.

    - Per consentire l'accesso specificato, selezionare la casella **allow**.
    - Per non consentire l'accesso specificato, selezionare la casella **Nega**. È possibile impostare le autorizzazioni per i seguenti diritti avanzati:
    - **Controllo completo**

      Se si sceglie questo diritto avanzato, tutti gli altri diritti avanzati vengono scelti automaticamente (diritti Allow o Nega).

    - **Cartella Traverse / file di esecuzione**
    - **Elenca cartella / leggi dati**
    - **Attributi di lettura**
    - **Leggi attributi estesi**
    - **Creare file / scrivere dati**
    - **Crea cartelle/Aggiungi dati**
    - **Attributi di scrittura**

- **Scrivi attributi estesi**
- **Elimina sottocartelle e file**
- **Elimina**
- **Permessi di lettura**
- **Modifica delle autorizzazioni**
- **Assumere la proprietà**

> Se una delle caselle di autorizzazione avanzate non è selezionabile, le autorizzazioni vengono ereditate dall'oggetto padre.

11. Se si desidera che le sottocartelle e i file di questo oggetto ereditino queste autorizzazioni, selezionare la casella **Applica queste autorizzazioni solo agli oggetti e/o ai contenitori all'interno di questo contenitore**.
12. Fare clic su **OK**.
13. Dopo aver aggiunto, rimosso o modificato le autorizzazioni NTFS, specificare l'impostazione di ereditarietà per questo oggetto:
    - Selezionare la casella **include ereditable permissions from this object's parent**.

      Questa è l'impostazione predefinita.
    - Selezionare la casella **Sostituisci tutte le autorizzazioni dell'oggetto figlio con le autorizzazioni ereditabili da questo oggetto**.

      Questa impostazione non è presente nella casella permessi se si impostano i permessi del file NTFS su un singolo file.

      > Fare attenzione quando si seleziona questa impostazione. Questa impostazione rimuove tutte le autorizzazioni esistenti su tutti gli oggetti figlio e le sostituisce con le impostazioni di autorizzazione dell'oggetto. È possibile rimuovere inavvertitamente le autorizzazioni che non si desidera rimuovere. È particolarmente importante quando si impostano le autorizzazioni in un volume misto di sicurezza o in un qtree. Se gli oggetti figlio dispongono di uno stile di protezione UNIX effettivo, la propagazione delle autorizzazioni NTFS a tali oggetti figlio comporta la modifica di tali oggetti da stile di protezione UNIX a stile di protezione NTFS da parte di ONTAP e la sostituzione di tutte le autorizzazioni UNIX per tali oggetti figlio con autorizzazioni NTFS.
    - Selezionare entrambe le caselle.
    - Selezionare nessuna delle due caselle.
14. Fare clic su **OK** per chiudere la casella **Permissions**.
15. Fare clic su **OK** per chiudere la casella **Impostazioni di protezione avanzate per <Object>**.

    Per ulteriori informazioni su come impostare le autorizzazioni NTFS avanzate, consultare la documentazione di Windows.

Informazioni correlate

Configurare e applicare la protezione dei file su file e cartelle NTFS utilizzando l'interfaccia CLI

Visualizzazione delle informazioni sulla sicurezza dei file sui volumi NTFS di tipo Security

Visualizzazione di informazioni sulla sicurezza dei file su volumi misti di tipo sicurezza

Visualizzazione delle informazioni sulla sicurezza dei file sui volumi UNIX di tipo Security

Configurare le autorizzazioni per i file NTFS utilizzando l'interfaccia utente di ONTAP

È possibile configurare le autorizzazioni dei file NTFS su file e directory utilizzando l'interfaccia utente di ONTAP. Ciò consente di configurare le autorizzazioni per i file NTFS senza la necessità di connettersi ai dati utilizzando una condivisione SMB su un client Windows.

È possibile configurare le autorizzazioni dei file NTFS aggiungendo voci agli elenchi di controllo degli accessi discrezionali (DACL) NTFS associati a un descrittore di protezione NTFS. Il descrittore di protezione viene quindi applicato ai file e alle directory NTFS.

È possibile configurare le autorizzazioni dei file NTFS solo dalla riga di comando. Non è possibile configurare gli ACL NFSv4 utilizzando l'interfaccia CLI.

Fasi

1. Creare un descrittore di protezione NTFS.

   ```
   vserver security file-directory ntfs create -vserver svm_name -ntfs-sd
   ntfs_security_descriptor_name -owner owner_name -group primary_group_name
   -control-flags-raw raw_control_flags
   ```

2. Aggiungere DACL al descrittore di protezione NTFS.

   ```
   vserver security file-directory ntfs dacl add -vserver svm_name -ntfs-sd
   ntfs_security_descriptor_name -access-type {deny|allow} -account account_name
   -rights {no-access|full-control|modify|read-and-execute|read|write} -apply-to
   {this-folder|sub-folders|files}
   ```

3. Creare una policy di sicurezza per file/directory.

   ```
   vserver security file-directory policy create -vserver svm_name -policy-name
   policy_name
   ```

In che modo le autorizzazioni dei file UNIX forniscono il controllo degli accessi quando si accede ai file tramite SMB

Un volume FlexVol può avere uno dei tre tipi di protezione: NTFS, UNIX o misto. È possibile accedere ai dati tramite SMB indipendentemente dallo stile di sicurezza; tuttavia, sono necessarie autorizzazioni appropriate per i file UNIX per accedere ai dati con una protezione efficace UNIX.

Quando si accede ai dati tramite SMB, vengono utilizzati diversi controlli di accesso per determinare se un utente è autorizzato a eseguire un'azione richiesta:

- Permessi di esportazione

La configurazione delle autorizzazioni di esportazione per l'accesso SMB è facoltativa.

- Autorizzazioni di condivisione
- Permessi del file

  I seguenti tipi di permessi di file potrebbero essere applicati ai dati sui quali l'utente desidera eseguire un'azione:

  - NTFS
  - ACL NFSv4 UNIX
  - Bit di modalità UNIX

Per i dati con ACL NFSv4 o bit di modalità UNIX impostati, vengono utilizzate autorizzazioni di stile UNIX per determinare i diritti di accesso ai dati. L'amministratore di SVM deve impostare l'autorizzazione file appropriata per garantire che gli utenti dispongano dei diritti per eseguire l'azione desiderata.

> I dati in un volume misto di sicurezza potrebbero avere uno stile di sicurezza efficace NTFS o UNIX. Se i dati hanno uno stile di sicurezza UNIX effettivo, le autorizzazioni NFSv4 o i bit di modalità UNIX vengono utilizzati per determinare i diritti di accesso ai dati.

Accesso sicuro ai file utilizzando il controllo dinamico degli accessi (DAC)

Proteggere l'accesso ai file utilizzando la panoramica del controllo dinamico dell'accesso (DAC)

È possibile proteggere l'accesso utilizzando il controllo dinamico degli accessi e creando policy di accesso centrali in Active Directory e applicandole a file e cartelle su SVM tramite oggetti Criteri di gruppo applicati (GPO). È possibile configurare il controllo in modo che utilizzi gli eventi di staging dei criteri di accesso centrale per visualizzare gli effetti delle modifiche ai criteri di accesso centrale prima di applicarli.

Aggiunte alle credenziali CIFS

Prima di Dynamic Access Control, una credenziale CIFS includeva l'identità di un'entità di protezione (l'utente) e l'appartenenza al gruppo Windows. Con Dynamic Access Control, alla credenziale vengono aggiunti altri tre tipi di informazioni: Identità del dispositivo, attestazioni del dispositivo e attestazioni dell'utente:

- Identità del dispositivo

  L'analogo delle informazioni di identità dell'utente, ad eccezione dell'identità e dell'appartenenza al gruppo del dispositivo da cui l'utente effettua l'accesso.

- Dichiarazioni dei dispositivi

  Asserzioni su un'entità di sicurezza del dispositivo. Ad esempio, un'attestazione del dispositivo potrebbe essere che è un membro di una specifica unità organizzativa.

- Richieste dell'utente

  Asserzioni su un'identità di sicurezza dell'utente. Ad esempio, un utente può affermare che il proprio

account ad è membro di una specifica unità organizzativa.

Policy di accesso centrale

I criteri di accesso centrale per i file consentono alle organizzazioni di implementare e gestire centralmente policy di autorizzazione che includono espressioni condizionali utilizzando gruppi di utenti, attestazioni utente, attestazioni dispositivo e proprietà delle risorse.

Ad esempio, per accedere ai dati ad alto impatto sul business, un utente deve essere un dipendente a tempo pieno e avere accesso ai dati solo da un dispositivo gestito. I criteri di accesso centrale sono definiti in Active Directory e distribuiti ai file server tramite il meccanismo GPO.

Staging dei criteri di accesso centralizzato con auditing avanzato

Le policy di accesso centrale possono essere “staged”, nel qual caso vengono valutate in modo “what-if” durante i controlli di accesso ai file. I risultati di ciò che sarebbe accaduto se la policy fosse stata applicata e in che modo differisce da ciò che è attualmente configurato vengono registrati come evento di audit. In questo modo, gli amministratori possono utilizzare i registri degli eventi di audit per studiare l’impatto di una modifica dei criteri di accesso prima di mettere effettivamente in pratica i criteri. Dopo aver valutato l’impatto di una modifica della policy di accesso, la policy può essere implementata tramite GPO nelle SVM desiderate.

Informazioni correlate

GPO supportati

Applicazione di oggetti Criteri di gruppo ai server CIFS

Attivazione o disattivazione del supporto GPO su un server CIFS

Visualizzazione delle informazioni sulle configurazioni dell’oggetto Criteri di gruppo

Visualizzazione di informazioni sui criteri di accesso centrale

Visualizzazione delle informazioni sulle regole dei criteri di accesso centrale

Configurazione delle policy di accesso centrale per proteggere i dati sui server CIFS

Visualizzazione di informazioni sulla sicurezza del controllo dinamico degli accessi

"Controllo SMB e NFS e tracciamento della sicurezza"

Funzionalità Dynamic Access Control supportata

Se si desidera utilizzare il controllo dinamico degli accessi (DAC) sul server CIFS, è necessario comprendere in che modo ONTAP supporta la funzionalità di controllo dinamico degli accessi negli ambienti Active Directory.

Supportato per Dynamic Access Control

ONTAP supporta le seguenti funzionalità quando il controllo dinamico degli accessi è attivato sul server CIFS:

Funzionalità	Commenti
Attestazioni nel file system	Le affermazioni sono semplici coppie di nomi e valori che indicano una certa verità su un utente. Le credenziali utente contengono informazioni sulle attestazioni e i descrittori di protezione sui file possono eseguire controlli di accesso che includono controlli delle attestazioni. In questo modo, gli amministratori possono avere un maggiore controllo sugli utenti che possono accedere ai file.
Espressioni condizionali per i controlli di accesso al file	Quando si modificano i parametri di protezione di un file, gli utenti possono aggiungere espressioni condizionali arbitrariamente complesse al descrittore di protezione del file. L'espressione condizionale può includere controlli per le attestazioni.
Controllo centralizzato dell'accesso ai file tramite policy di accesso centrali	I criteri di accesso centrale sono un tipo di ACL memorizzato in Active Directory che può essere contrassegnato in un file. L'accesso al file viene concesso solo se i controlli di accesso del descrittore di protezione su disco e del criterio di accesso centrale con tag consentono l'accesso. In questo modo, gli amministratori possono controllare l'accesso ai file da una posizione centrale (ad) senza dover modificare il descrittore di protezione su disco.
Staging dei criteri di accesso centrale	Aggiunge la possibilità di provare le modifiche di sicurezza senza influire sull'accesso effettivo ai file, "eseguendo `staging`" una modifica alle policy di accesso centrale e osservando l'effetto della modifica in un report di audit.
Supporto per la visualizzazione di informazioni sulla sicurezza dei criteri di accesso centrale mediante l'interfaccia utente di ONTAP	Estende `vserver security file-directory show` per visualizzare le informazioni sui criteri di accesso centrale applicati.
Analisi della sicurezza che include policy di accesso centralizzate	Estende `vserver security trace` famiglia di comandi per visualizzare i risultati che includono informazioni sui criteri di accesso centrale applicati.

Non supportato per Dynamic Access Control

ONTAP non supporta le seguenti funzionalità quando il controllo dinamico degli accessi è attivato sul server CIFS:

Funzionalità	Commenti
Classificazione automatica degli oggetti del file system NTFS	Si tratta di un'estensione dell'infrastruttura di classificazione dei file di Windows non supportata in ONTAP.
Auditing avanzato diverso dalla gestione temporanea dei criteri di accesso centrale	Solo lo staging dei criteri di accesso centrale è supportato per il controllo avanzato.

Considerazioni sull'utilizzo del controllo dinamico degli accessi e delle policy di accesso centrale con i server CIFS

È necessario tenere presente alcune considerazioni quando si utilizza il controllo dinamico dell'accesso (DAC) e i criteri di accesso centrale per proteggere file e cartelle sui server CIFS.

L'accesso NFS può essere negato all'utente root se la regola dei criteri si applica all'utente di dominio/amministratore

In alcuni casi, l'accesso NFS a root potrebbe essere negato quando la sicurezza del criterio di accesso centrale viene applicata ai dati a cui l'utente root sta tentando di accedere. Il problema si verifica quando il criterio di accesso centrale contiene una regola che viene applicata al dominio/amministratore e l'account root viene mappato all'account di dominio/amministratore.

Invece di applicare una regola all'utente di dominio/amministratore, è necessario applicarla a un gruppo con privilegi amministrativi, ad esempio il gruppo dominio/amministratori. In questo modo, è possibile mappare root all'account di dominio/amministratore senza che root sia interessato da questo problema.

Il gruppo BUILTIN/Administrators del server CIFS ha accesso alle risorse quando il criterio di accesso centrale applicato non viene trovato in Active Directory

È possibile che alle risorse contenute nel server CIFS siano applicati criteri di accesso centrale, ma quando il server CIFS utilizza il SID del criterio di accesso centrale per tentare di recuperare informazioni da Active Directory, il SID non corrisponde ai SID dei criteri di accesso centrale esistenti in Active Directory. In questi casi, il server CIFS applica il criterio di ripristino locale predefinito per tale risorsa.

Il criterio di ripristino locale predefinito consente al gruppo BUILTIN/Administrators del server CIFS di accedere a tale risorsa.

Attiva o disattiva la panoramica del controllo dinamico degli accessi

L'opzione che consente di utilizzare il controllo dinamico dell'accesso (DAC) per proteggere gli oggetti sul server CIFS è disattivata per impostazione predefinita. Attivare l'opzione se si desidera utilizzare Dynamic Access Control sul server CIFS. Se in seguito si decide di non utilizzare il controllo dinamico degli accessi per proteggere gli oggetti memorizzati nel server CIFS, è possibile disattivare l'opzione.

A proposito di questa attività

Una volta attivato il controllo dinamico degli accessi, il file system può contenere ACL con voci correlate al controllo dinamico degli accessi. Se Dynamic Access Control è disattivato, le voci correnti di Dynamic Access Control verranno ignorate e non saranno consentite le nuove.

Questa opzione è disponibile solo al livello di privilegio avanzato.

Fase

1. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
2. Eseguire una delle seguenti operazioni:

Se si desidera che Dynamic Access Control sia…	Immettere il comando…
Attivato	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled true`
Disattivato	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled false`

3. Tornare al livello di privilegi di amministratore: `set -privilege admin`

Informazioni correlate

Configurazione delle policy di accesso centrale per proteggere i dati sui server CIFS

Gestire gli ACL che contengono le ACE di controllo dinamico degli accessi quando il controllo dinamico degli accessi è disattivato

Se si dispone di risorse con ACL applicati con ACE di controllo dinamico degli accessi e si disattiva il controllo dinamico degli accessi sulla macchina virtuale di storage (SVM), è necessario rimuovere le ACE di controllo dinamico degli accessi prima di poter gestire le ACE di controllo degli accessi non dinamico su tale risorsa.

A proposito di questa attività

Una volta disattivato il controllo dinamico degli accessi, non è possibile rimuovere le ACE di controllo degli accessi non dinamiche esistenti o aggiungere nuove ACE di controllo degli accessi non dinamiche fino a quando non sono state rimosse le ACE di controllo degli accessi dinamici esistenti.

È possibile utilizzare lo strumento utilizzato normalmente per gestire gli ACL per eseguire questi passaggi.

Fasi

1. Determinare quali ACE di controllo dinamico degli accessi vengono applicati alla risorsa.
2. Rimuovere le ACE di controllo dinamico degli accessi dalla risorsa.
3. Aggiungere o rimuovere ACE di controllo degli accessi non dinamici come desiderato dalla risorsa.

Configurare le policy di accesso centrale per proteggere i dati sui server CIFS

Per proteggere l'accesso ai dati sul server CIFS mediante criteri di accesso centrali, è necessario eseguire diversi passaggi, tra cui l'attivazione del controllo dinamico dell'accesso (DAC) sul server CIFS, la configurazione dei criteri di accesso centrale in Active Directory, l'applicazione dei criteri di accesso centrale ai container Active Directory con GPO, E abilitazione degli oggetti Criteri di gruppo sul server CIFS.

Prima di iniziare

- Active Directory deve essere configurato per utilizzare criteri di accesso centrali.
- È necessario disporre di un accesso sufficiente sui domain controller di Active Directory per creare criteri di accesso centrali e per creare e applicare gli oggetti Criteri di gruppo ai container che contengono i server CIFS.
- Per eseguire i comandi necessari, è necessario disporre di un accesso amministrativo sufficiente sulla macchina virtuale di storage (SVM).

A proposito di questa attività

I criteri di accesso centrale vengono definiti e applicati agli oggetti Criteri di gruppo (GPO) in Active Directory. Per istruzioni sulla configurazione dei criteri di accesso centrale e degli oggetti Criteri di gruppo, consultare la Microsoft TechNet Library.

"Microsoft TechNet Library"

Fasi

1. Attivare Dynamic Access Control (controllo dinamico degli accessi) su SVM se non è già attivato utilizzando `vserver cifs options modify` comando.

   ```
   vserver cifs options modify -vserver vs1 -is-dac-enabled true
   ```

2. Abilitare gli oggetti Criteri di gruppo (GPO) sul server CIFS se non sono già abilitati mediante `vserver cifs group-policy modify` comando.

   ```
   vserver cifs group-policy modify -vserver vs1 -status enabled
   ```

3. Creare regole di accesso centrali e policy di accesso centrali in Active Directory.
4. Creare un oggetto Criteri di gruppo (GPO) per implementare i criteri di accesso centrale in Active Directory.
5. Applicare l'oggetto Criteri di gruppo al container in cui si trova l'account del computer del server CIFS.
6. Aggiornare manualmente gli oggetti Criteri di gruppo applicati al server CIFS utilizzando `vserver cifs group-policy update` comando.

   ```
   vserver cifs group-policy update -vserver vs1
   ```

7. Verificare che il criterio di accesso centrale dell'oggetto Criteri di gruppo sia applicato alle risorse sul server CIFS utilizzando `vserver cifs group-policy show-applied` comando.

   L'esempio seguente mostra che il criterio di dominio predefinito dispone di due criteri di accesso centrali applicati al server CIFS:

   ```
   vserver cifs group-policy show-applied
   ```

   ```
   Vserver: vs1
   ----------------------------
       GPO Name: Default Domain Policy
          Level: Domain
         Status: enabled
     Advanced Audit Settings:
         Object Access:
             Central Access Policy Staging: failure
   ```

```
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2

  GPO Name: Resultant Set of Policy
     Level: RSOP
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
```

```
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
2 entries were displayed.
```

Informazioni correlate

Visualizzazione delle informazioni sulle configurazioni dell'oggetto Criteri di gruppo

Visualizzazione di informazioni sui criteri di accesso centrale

Visualizzazione delle informazioni sulle regole dei criteri di accesso centrale

Attivazione o disattivazione del controllo dinamico degli accessi

Visualizza informazioni sulla sicurezza del controllo dinamico degli accessi

È possibile visualizzare informazioni sulla sicurezza del controllo dinamico degli accessi (DAC) sui volumi NTFS e sui dati con protezione effettiva NTFS su volumi misti di tipo sicurezza. Ciò include informazioni su ACE condizionali, ACE di risorse e ACE di policy di

accesso centrale. È possibile utilizzare i risultati per convalidare la configurazione di sicurezza o per risolvere i problemi di accesso ai file.

A proposito di questa attività

Specificare il nome della macchina virtuale di storage (SVM) e il percorso dei dati di cui si desidera visualizzare le informazioni di sicurezza relative al file o alla cartella. È possibile visualizzare l'output in forma di riepilogo o come elenco dettagliato.

Fase

1. Visualizzare le impostazioni di sicurezza di file e directory con il livello di dettaglio desiderato:

Se si desidera visualizzare le informazioni…	Immettere il seguente comando…
In forma riassuntiva	`vserver security file-directory show -vserver vserver_name -path path`
Con dettagli più dettagliati	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`
Dove viene visualizzato l'output con SID di gruppo e utente	`vserver security file-directory show -vserver vserver_name -path path -lookup-names false`
Informazioni sulla sicurezza di file e directory per file e directory in cui la bit mask esadecimale viene convertita in formato testuale	`vserver security file-directory show -vserver vserver_name -path path -textual-mask true`

Esempi

Nell'esempio riportato di seguito vengono visualizzate le informazioni di sicurezza del controllo dinamico degli accessi relative al percorso `/vol1` In SVM vs1:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /vol1
                           Vserver: vs1
                         File Path: /vol1
                  File Inode Number: 112
                     Security Style: mixed
                    Effective Style: ntfs
                     DOS Attributes: 10
             DOS Attributes in Text: ----D---
             Expanded Dos Attribute: -
                       Unix User Id: 0
                      Unix Group Id: 1
                     Unix Mode Bits: 777
             Unix Mode Bits in Text: rwxrwxrwx
                               ACLs: NTFS Security Descriptor
                                     Control:0xbf14
                                     Owner:CIFS1\Administrator
                                     Group:CIFS1\Domain Admins
                                     SACL - ACEs
                                        ALL-Everyone-0xf01ff-OI|CI|SA|FA
                                        RESOURCE ATTRIBUTE-Everyone-0x0

("Department_MS",TS,0x10020,"Finance")
                                        POLICY ID-All resources - No Write-
0x0-OI|CI
                                     DACL - ACEs
                                        ALLOW-CIFS1\Administrator-0x1f01ff-
OI|CI
                                        ALLOW-Everyone-0x1f01ff-OI|CI
                                        ALLOW CALLBACK-DAC\user1-0x1200a9-
OI|CI

((@User.department==@Resource.Department_MS&&@Resource.Impact_MS>1000)&&@D
evice.department==@Resource.Department_MS)
```

Informazioni correlate

Visualizzazione delle informazioni sulle configurazioni dell'oggetto Criteri di gruppo

Visualizzazione di informazioni sui criteri di accesso centrale

Visualizzazione delle informazioni sulle regole dei criteri di accesso centrale

Considerazioni sul revert per il controllo dinamico degli accessi

È necessario essere consapevoli di cosa accade quando si torna a una versione di ONTAP che non supporta il controllo dinamico degli accessi (DAC) e di cosa si deve fare prima e dopo il ripristino.

Se si desidera ripristinare il cluster a una versione di ONTAP che non supporta il controllo dinamico degli accessi e che il controllo dinamico degli accessi sia attivato su una o più macchine virtuali dello storage (SVM), prima di eseguire il ripristino è necessario eseguire le seguenti operazioni:

- È necessario disattivare il controllo dinamico degli accessi su tutte le SVM che lo hanno attivato nel cluster.
- È necessario modificare le configurazioni di controllo del cluster che contengono `cap-staging` tipo di evento per utilizzare solo `file-op` tipo di evento.

È necessario comprendere e agire in base ad alcune importanti considerazioni di revert per file e cartelle con le ACE di controllo dinamico degli accessi:

- Se il cluster viene invertito, le ACE di controllo dinamico degli accessi esistenti non vengono rimosse; tuttavia, verranno ignorate nei controlli di accesso ai file.
- Poiché le ACE di controllo dinamico degli accessi vengono ignorate dopo la revisione, l'accesso ai file cambia nei file con le ACE di controllo dinamico degli accessi.

  Ciò potrebbe consentire agli utenti di accedere a file che in precedenza non potevano o che non potevano accedere a file che in precedenza potevano.

- Per ripristinare il livello di protezione precedente, è necessario applicare ACE di controllo degli accessi non dinamici ai file interessati.

  Questa operazione può essere eseguita prima del ripristino o immediatamente dopo il completamento della revisione.

> Poiché le ACE di controllo dinamico degli accessi vengono ignorate dopo la reversione, non è necessario rimuoverle quando si applicano ACE di controllo degli accessi non dinamici ai file interessati. Tuttavia, se lo si desidera, è possibile rimuoverli manualmente.

Dove trovare ulteriori informazioni sulla configurazione e l'utilizzo del controllo dinamico degli accessi e delle policy di accesso centrali

Sono disponibili risorse aggiuntive per la configurazione e l'utilizzo di Dynamic Access Control e policy di accesso centrali.

Nella Microsoft TechNet Library sono disponibili informazioni su come configurare il controllo dinamico degli accessi e i criteri di accesso centrale in Active Directory.

"Microsoft TechNet: Panoramica dello scenario di controllo dinamico degli accessi"

"Microsoft TechNet: Scenario dei criteri di accesso centrale"

I seguenti riferimenti consentono di configurare il server SMB in modo che utilizzi e supporti il controllo dinamico degli accessi e le policy di accesso centrale:

- **Utilizzo di GPO sul server SMB**

  Applicazione di oggetti Criteri di gruppo ai server SMB

- **Configurazione del controllo NAS sul server SMB**

  "Controllo SMB e NFS e tracciamento della sicurezza"

Accesso sicuro alle PMI tramite policy di esportazione

Come vengono utilizzate le policy di esportazione con l'accesso SMB

Se i criteri di esportazione per l'accesso SMB sono attivati sul server SMB, i criteri di esportazione vengono utilizzati per controllare l'accesso ai volumi SVM da parte dei client SMB. Per accedere ai dati, è possibile creare un criterio di esportazione che consenta l'accesso SMB e associare il criterio ai volumi contenenti condivisioni SMB.

Una policy di esportazione prevede l'applicazione di una o più regole che specificano i client ai quali è consentito l'accesso ai dati e i protocolli di autenticazione supportati per l'accesso in sola lettura e in lettura/scrittura. È possibile configurare i criteri di esportazione per consentire l'accesso tramite SMB a tutti i client, a una subnet di client o a un client specifico e per consentire l'autenticazione utilizzando l'autenticazione Kerberos, l'autenticazione NTLM o l'autenticazione Kerberos e NTLM quando si determina l'accesso di sola lettura e lettura/scrittura ai dati.

Dopo aver elaborato tutte le regole di esportazione applicate ai criteri di esportazione, ONTAP può determinare se al client viene concesso l'accesso e quale livello di accesso viene concesso. Le regole di esportazione si applicano ai computer client, non agli utenti e ai gruppi Windows. Le regole di esportazione non sostituiscono l'autenticazione e l'autorizzazione basate su utenti e gruppi di Windows. Le regole di esportazione offrono un altro livello di sicurezza degli accessi oltre alle autorizzazioni di condivisione e accesso ai file.

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

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

Ogni SVM dispone di almeno una policy di esportazione chiamata "default", che non contiene regole. Non è possibile eliminare questo criterio di esportazione, ma è possibile rinominarlo o modificarlo. Per impostazione predefinita, ciascun volume della SVM è associato al criterio di esportazione predefinito. Se i criteri di esportazione per l'accesso SMB sono disattivati sulla SVM, la policy di esportazione "default" non ha alcun effetto sull'accesso SMB.

È possibile configurare le regole che forniscono l'accesso agli host NFS e SMB e associare tale regola a un criterio di esportazione, che può quindi essere associato al volume che contiene i dati a cui devono accedere gli host NFS e SMB. In alternativa, se esistono volumi in cui solo i client SMB richiedono l'accesso, è possibile configurare un criterio di esportazione con regole che consentono l'accesso solo utilizzando il protocollo SMB e che utilizzano solo Kerberos o NTLM (o entrambi) per l'autenticazione in sola lettura e in scrittura. Il criterio di esportazione viene quindi associato ai volumi in cui si desidera solo l'accesso SMB.

Se i criteri di esportazione per SMB sono attivati e 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 del volume, l'accesso viene negato. Se un criterio di esportazione è vuoto, tutti gli accessi vengono implicitamente negati. Ciò è vero anche se le autorizzazioni di condivisione e file consentirebbero altrimenti l'accesso. Ciò significa che è necessario configurare la policy di esportazione in modo da consentire in modo minimo quanto segue sui volumi contenenti condivisioni SMB:

- Consentire l'accesso a tutti i client o al sottoinsieme appropriato di client

- Consentire l'accesso tramite SMB
- Consentire l'accesso di sola lettura e scrittura appropriato utilizzando l'autenticazione Kerberos o NTLM (o entrambe)

Scopri di più "configurazione e gestione delle 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.

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.

Esempi di regole dei criteri di esportazione che limitano o consentono l'accesso tramite SMB

Gli esempi mostrano come creare regole di policy di esportazione che limitano o consentono l'accesso tramite SMB su una SVM con criteri di esportazione per l'accesso SMB abilitati.

I criteri di esportazione per l'accesso SMB sono disattivati per impostazione predefinita. È necessario configurare le regole dei criteri di esportazione che limitano o consentono l'accesso su SMB solo se sono state attivate le policy di esportazione per l'accesso SMB.

Regola di esportazione solo per l'accesso SMB

Il seguente comando crea una regola di esportazione sulla SVM denominata "vs1" con la seguente configurazione:

- Nome policy: Cifs1
- Numero indice: 1
- Client match (corrispondenza client): Corrisponde solo ai client sulla rete 192.168.1.0/24
- Protocol (protocollo): Consente solo l'accesso SMB

- Accesso di sola lettura: Ai client che utilizzano l'autenticazione NTLM o Kerberos
- Accesso in lettura/scrittura: Ai client che utilizzano l'autenticazione Kerberos

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifs1 -ruleindex 1 -protocol cifs -clientmatch 192.168.1.0/255.255.255.0
-rorule krb5,ntlm -rwrule krb5
```

Regola di esportazione per accesso SMB e NFS

Il seguente comando crea una regola di esportazione sulla SVM denominata"` vs1`" con la seguente configurazione:

- Nome policy: Cifsnfs1
- Numero indice: 2
- Client match (corrispondenza client): Corrisponde a tutti i client
- Protocollo: Accesso SMB e NFS
- Accesso in sola lettura: A tutti i client
- Accesso in lettura/scrittura: Ai client che utilizzano Kerberos (NFS e SMB) o autenticazione NTLM (SMB)
- Mapping per ID utente UNIX 0 (zero): Mappato all'ID utente 65534 (che in genere viene mappato al nome utente nessuno)
- Accesso SUID e sgid: Consente

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifsnfs1 -ruleindex 2 -protocol cifs,nfs -clientmatch 0.0.0.0/0 -rorule any
-rwrule krb5,ntlm -anon 65534 -allow-suid true
```

Regola di esportazione per l'accesso SMB utilizzando solo NTLM

Il seguente comando crea una regola di esportazione sulla SVM denominata "vs1" con la seguente configurazione:

- Nome policy: Ntlm1
- Numero indice: 1
- Client match (corrispondenza client): Corrisponde a tutti i client
- Protocol (protocollo): Consente solo l'accesso SMB
- Accesso di sola lettura: Solo ai client che utilizzano NTLM
- Accesso di lettura/scrittura: Solo ai client che utilizzano NTLM

> Se si configura l'opzione di sola lettura o l'opzione di lettura/scrittura per l'accesso solo NTLM, è necessario utilizzare le voci basate sull'indirizzo IP nell'opzione di corrispondenza del client. In caso contrario, ricevi `access denied` errori. Questo perché ONTAP utilizza i nomi principali del servizio Kerberos (SPN) quando si utilizza un nome host per verificare i diritti di accesso del client. L'autenticazione NTLM non supporta i nomi SPN.

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
ntlm1 -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule ntlm
-rwrule ntlm
```

Attiva o disattiva i criteri di esportazione per l'accesso SMB

È possibile attivare o disattivare le policy di esportazione per l'accesso SMB sulle macchine virtuali di storage (SVM). L'utilizzo di policy di esportazione per controllare l'accesso SMB alle risorse è facoltativo.

Prima di iniziare

Di seguito sono riportati i requisiti per l'attivazione delle policy di esportazione per SMB:

- Il client deve disporre di un record "PTR" nel DNS prima di creare le regole di esportazione per tale client.
- Se la SVM fornisce l'accesso ai client NFS e se il nome host che si desidera utilizzare per l'accesso NFS è diverso dal nome del server CIFS, è necessario disporre di un set aggiuntivo di record "A" e "PTR" per i nomi host.

A proposito di questa attività

Quando si imposta un nuovo server CIFS su SVM, l'utilizzo dei criteri di esportazione per l'accesso SMB viene disattivato per impostazione predefinita. È possibile attivare i criteri di esportazione per l'accesso SMB se si desidera controllare l'accesso in base al protocollo di autenticazione o agli indirizzi IP o ai nomi host dei client. È possibile attivare o disattivare i criteri di esportazione per l'accesso SMB in qualsiasi momento.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
2. Attivare o disattivare i criteri di esportazione:
   - Abilitare i criteri di esportazione: `vserver cifs options modify -vserver` *`vserver_name`* `-is-exportpolicy-enabled true`
   - Disattiva policy di esportazione: `vserver cifs options modify -vserver` *`vserver_name`* `-is-exportpolicy-enabled false`
3. Tornare al livello di privilegio admin: `set -privilege admin`

Esempio

L'esempio seguente consente l'utilizzo di policy di esportazione per controllare l'accesso del client SMB alle risorse su SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-exportpolicy
-enabled true

cluster1::*> set -privilege admin
```

Proteggere l'accesso ai file utilizzando Storage-Level Access Guard

Proteggere l'accesso ai file utilizzando Storage-Level Access Guard

Oltre a proteggere l'accesso utilizzando la sicurezza nativa a livello di file e di esportazione e condivisione, è possibile configurare la protezione dell'accesso a livello di storage, un terzo livello di sicurezza applicato da ONTAP a livello di volume. Storage-Level Access Guard si applica all'accesso da tutti i protocolli NAS all'oggetto di storage a cui è applicato.

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

Comportamento di Access Guard a livello di storage

- Storage-Level Access Guard si applica a tutti i file o a tutte le directory di un oggetto di storage.

  Poiché tutti i file o le directory di un volume sono soggetti alle impostazioni di Storage-Level Access Guard, non è richiesta l'ereditarietà attraverso la propagazione.

- È possibile configurare Storage-Level Access Guard in modo che si applichi solo ai file, solo alle directory o sia ai file che alle directory all'interno di un volume.
  - Sicurezza di file e directory

    Si applica a ogni directory e file all'interno dell'oggetto di storage. Questa è l'impostazione predefinita.

  - Sicurezza del file

    Si applica a tutti i file all'interno dell'oggetto di storage. L'applicazione di questa protezione non influisce sull'accesso o sul controllo delle directory.

  - Sicurezza della directory

    Si applica a ogni directory all'interno dell'oggetto di storage. L'applicazione di questa protezione non influisce sull'accesso o sul controllo dei file.

- Storage-Level Access Guard viene utilizzato per limitare le autorizzazioni.

  Non assegnerà mai autorizzazioni di accesso aggiuntive.

- Se si visualizzano le impostazioni di sicurezza su un file o una directory da un client NFS o SMB, la protezione Storage-Level Access Guard non viene visualizzata.

  Viene applicato a livello di oggetto di storage e memorizzato nei metadati utilizzati per determinare le autorizzazioni effettive.

- La sicurezza a livello di storage non può essere revocata da un client, nemmeno da un amministratore di sistema (Windows o UNIX).

  È progettato per essere modificato solo dagli amministratori dello storage.

- È possibile applicare Storage-Level Access Guard a volumi con NTFS o stile di sicurezza misto.
- È possibile applicare Storage-Level Access Guard ai volumi con lo stile di sicurezza UNIX, purché la SVM contenente il volume abbia configurato un server CIFS.
- Quando i volumi sono montati sotto un percorso di giunzione del volume e se Storage-Level Access Guard è presente su tale percorso, non verrà propagata ai volumi montati sotto di esso.
- Il descrittore di sicurezza Storage-Level Access Guard viene replicato con la replica dei dati SnapMirror e con la replica SVM.
- Esiste una dispensazione speciale per i virus scanner.

  A questi server è consentito un accesso eccezionale per lo screening di file e directory, anche se Storage-Level Access Guard nega l'accesso all'oggetto.

- Le notifiche FPolicy non vengono inviate se l'accesso viene negato a causa di Storage-Level Access Guard.

Ordine dei controlli di accesso

L'accesso a un file o a una directory è determinato dall'effetto combinato delle autorizzazioni di esportazione o condivisione, delle autorizzazioni Storage-Level Access Guard impostate sui volumi e delle autorizzazioni native dei file applicate a file e/o directory. Tutti i livelli di sicurezza vengono valutati per determinare le autorizzazioni effettive di un file o di una directory. I controlli di accesso di sicurezza vengono eseguiti nel seguente ordine:

1. Permessi di condivisione SMB o NFS a livello di esportazione
2. Access Guard a livello di storage
3. ACL (Access Control List) file/cartelle NTFS, ACL NFSv4 o bit di modalità UNIX

Casi di utilizzo di Storage-Level Access Guard

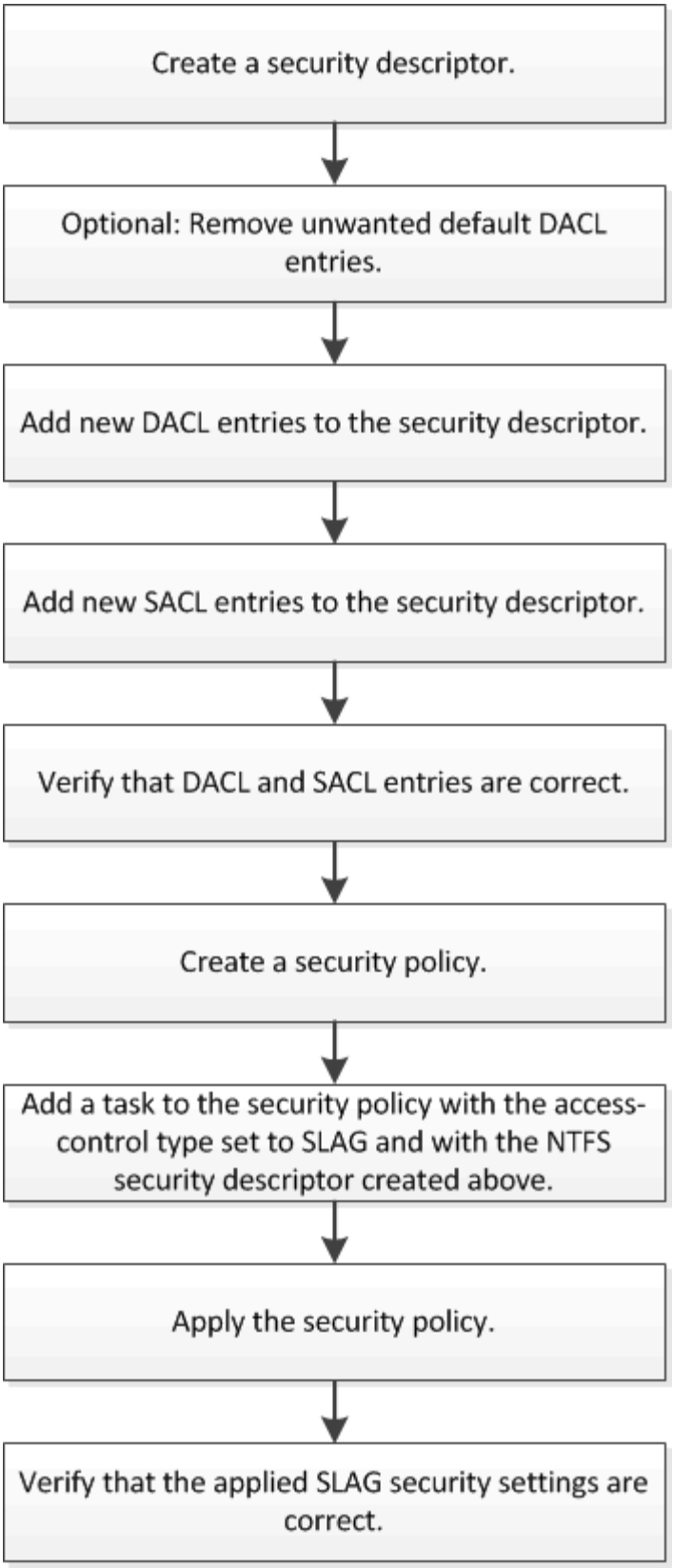
Storage-Level Access Guard offre una sicurezza aggiuntiva a livello di storage, che non è visibile dal lato client; pertanto, non può essere revocata da nessuno degli utenti o degli amministratori dai propri desktop. Esistono alcuni casi di utilizzo in cui la capacità di controllare l'accesso a livello di storage è vantaggiosa.

I casi di utilizzo tipici di questa funzionalità includono i seguenti scenari:

- Protezione della proprietà intellettuale attraverso il controllo e il controllo dell'accesso di tutti gli utenti` a livello di storage
- Storage per le società di servizi finanziari, inclusi gruppi bancari e commerciali
- Servizi governativi con storage di file separato per singoli reparti
- Le università proteggono tutti i file degli studenti

Workflow per configurare Storage-Level Access Guard

Il flusso di lavoro per la configurazione di Storage-Level Access Guard (SLAG) utilizza gli stessi comandi CLI di ONTAP utilizzati per configurare le autorizzazioni dei file NTFS e i criteri di controllo. Invece di configurare l'accesso a file e directory su una destinazione designata, è possibile configurare LO SLAG sul volume SVM (Storage Virtual Machine) designato.



Informazioni correlate

Configurazione di Storage-Level Access Guard

Configurare Storage-Level Access Guard

Per configurare Storage-Level Access Guard su un volume o su un qtree, è necessario seguire una serie di passaggi. Storage-Level Access Guard offre un livello di sicurezza degli accessi impostato a livello di storage. Fornisce una sicurezza che si applica a tutti gli accessi da tutti i protocolli NAS all'oggetto di storage a cui è stato applicato.

Fasi

1. Creare un descrittore di protezione utilizzando `vserver security file-directory ntfs create` comando.

   `vserver security file-directory ntfs create -vserver vs1 -ntfs-sd sd1` `vserver security file-directory ntfs show -vserver vs1`

   ```
   Vserver: vs1

      NTFS Security    Owner Name
      Descriptor Name
      ------------     --------------
      sd1              -
   ```

   Viene creato un descrittore di protezione con le seguenti quattro voci di controllo di accesso DACL predefinite:

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       BUILTIN\Administrators
                        allow    full-control   this-folder, sub-folders,
   files
       BUILTIN\Users    allow    full-control   this-folder, sub-folders,
   files
       CREATOR OWNER    allow    full-control   this-folder, sub-folders,
   files
       NT AUTHORITY\SYSTEM
                        allow    full-control   this-folder, sub-folders,
   files
   ```

   Se non si desidera utilizzare le voci predefinite durante la configurazione di Storage-Level Access Guard, è possibile rimuoverle prima di creare e aggiungere le proprie ACE al descrittore di protezione.

2. Rimuovere dal descrittore di protezione una delle ACL DACL predefinite che non si desidera configurare con la protezione Storage-Level Access Guard:

a. Rimuovere eventuali ACL DACL indesiderati utilizzando `vserver security file-directory ntfs dacl remove` comando.

   In questo esempio, tre ACL DACL predefiniti vengono rimossi dal descrittore di protezione: BUILTIN/Administrators, BUILTIN/Users e CREATOR OWNER.

   ```
   vserver security file-directory ntfs dacl remove -vserver vs1 -ntfs-sd sd1
   -access-type allow -account builtin\users vserver security file-directory
   ntfs dacl remove -vserver vs1 -ntfs-sd sd1 -access-type allow -account
   builtin\administrators vserver security file-directory ntfs dacl remove
   -vserver vs1 -ntfs-sd sd1 -access-type allow -account "creator owner"
   ```

b. Verificare che le ACL DACL che non si desidera utilizzare per la protezione Storage-Level Access Guard siano rimosse dal descrittore di protezione utilizzando `vserver security file-directory ntfs dacl show` comando.

   In questo esempio, l'output del comando verifica che tre ACL DACL predefinite siano state rimosse dal descrittore di protezione, lasciando solo la voce ACE DACL predefinita di sistema/AUTORITÀ NT:

   ```
   vserver security file-directory ntfs dacl show -vserver vs1
   ```

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    NT AUTHORITY\SYSTEM
                     allow    full-control   this-folder, sub-folders,
files
```

3. Aggiungere una o più voci DACL a un descrittore di protezione utilizzando `vserver security file-directory ntfs dacl add` comando.

   In questo esempio, due ACL DACL vengono aggiunti al descrittore di protezione:

   ```
   vserver security file-directory ntfs dacl add -vserver vs1 -ntfs-sd sd1
   -access-type allow -account example\engineering -rights full-control -apply-to
   this-folder,sub-folders,files vserver security file-directory ntfs dacl add
   -vserver vs1 -ntfs-sd sd1 -access-type allow -account "example\Domain Users"
   -rights read -apply-to this-folder,sub-folders,files
   ```

4. Aggiungere una o più voci SACL a un descrittore di protezione utilizzando `vserver security file-directory ntfs sacl add` comando.

   In questo esempio, due ACL SACL vengono aggiunti al descrittore di protezione:

   ```
   vserver security file-directory ntfs sacl add -vserver vs1 -ntfs-sd sd1
   -access-type failure -account "example\Domain Users" -rights read -apply-to
   this-folder,sub-folders,files vserver security file-directory ntfs sacl add
   ```

```
-vserver vs1 -ntfs-sd sd1 -access-type success -account example\engineering
-rights full-control -apply-to this-folder,sub-folders,files
```

5. Verificare che le ACL DACL e SACL siano configurate correttamente utilizzando `vserver security file-directory ntfs dacl show` e. `vserver security file-directory ntfs sacl show` comandi, rispettivamente.

   In questo esempio, il comando seguente visualizza informazioni sulle voci DACL per il descrittore di protezione “sd1”:

   ```
   vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
   ```

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       EXAMPLE\Domain Users
                        allow    read           this-folder, sub-folders,
   files
       EXAMPLE\engineering
                        allow    full-control   this-folder, sub-folders,
   files
       NT AUTHORITY\SYSTEM
                        allow    full-control   this-folder, sub-folders,
   files
   ```

   In questo esempio, il comando seguente visualizza informazioni sulle voci SACL per il descrittore di protezione “sd1”:

   ```
   vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
   ```

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       EXAMPLE\Domain Users
                        failure  read           this-folder, sub-folders,
   files
       EXAMPLE\engineering
                        success  full-control   this-folder, sub-folders,
   files
   ```

6. Creare un criterio di protezione utilizzando `vserver security file-directory policy create` comando.

   Nell'esempio seguente viene creata una policy denominata "policy1":

   ```
   vserver security file-directory policy create -vserver vs1 -policy-name
   policy1
   ```

7. Verificare che il criterio sia configurato correttamente utilizzando `vserver security file-directory policy show` comando.

   ```
   vserver security file-directory policy show
   ```

   ```
   Vserver          Policy Name
   ------------     --------------
   vs1              policy1
   ```

8. Aggiungere un'attività con un descrittore di protezione associato al criterio di protezione utilizzando `vserver security file-directory policy task add` con il `-access-control` parametro impostato su `slag`.

   Anche se un criterio può contenere più di un'attività Storage-Level Access Guard, non è possibile configurare un criterio in modo che contenga sia le attività file-directory che Storage-Level Access Guard. Un criterio deve contenere tutte le attività Storage-Level Access Guard o tutte le attività di file-directory.

   In questo esempio, viene aggiunto un task alla policy denominata "policy1", assegnata al descrittore di sicurezza "sd1". Viene assegnato a. `/datavol1` percorso con il tipo di controllo dell'accesso impostato su "slag".

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name
   policy1 -path /datavol1 -access-control slag -security-type ntfs -ntfs-mode
   propagate -ntfs-sd sd1
   ```

9. Verificare che l'attività sia configurata correttamente utilizzando `vserver security file-directory policy task show` comando.

   ```
   vserver security file-directory policy task show -vserver vs1 -policy-name
   policy1
   ```

```
 Vserver: vs1
  Policy: policy1

   Index  File/Folder  Access           Security  NTFS       NTFS
Security
          Path         Control          Type      Mode       Descriptor
Name
   -----  -----------  ---------------  --------  ----------
---------------
   1      /datavol1    slag             ntfs      propagate  sd1
```

10. Applicare il criterio di protezione Storage-Level Access Guard utilizzando `vserver security file-directory apply` comando.

    ```
    vserver security file-directory apply -vserver vs1 -policy-name policy1
    ```

    Il processo di applicazione della policy di sicurezza è pianificato.

11. Verificare che le impostazioni di protezione di Storage-Level Access Guard applicate siano corrette utilizzando `vserver security file-directory show` comando.

    In questo esempio, l'output del comando indica che la protezione Storage-Level Access Guard è stata applicata al volume NTFS `/datavol1`. Anche se il DACL predefinito che consente il controllo completo a tutti rimane, la protezione di Storage-Level Access Guard limita (e controlla) l'accesso ai gruppi definiti nelle impostazioni di Storage-Level Access Guard.

    ```
    vserver security file-directory show -vserver vs1 -path /datavol1
    ```

```
                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Informazioni correlate

Gestione della sicurezza dei file NTFS, delle policy di audit NTFS e di Storage-Level Access Guard su SVM mediante CLI

Workflow per configurare Storage-Level Access Guard

Visualizzazione di informazioni su Storage-Level Access Guard

Rimozione di Storage-Level Access Guard

Matrice DI SCORIE efficace

È possibile configurare LO SLAG su un volume, un qtree o entrambi. La matrice DELLE SCORIE definisce su quale volume o qtree è la configurazione DELLE SCORIE applicabile in diversi scenari elencati nella tabella.

	SCORIA di volume in un AFS	SCORIE di volume in una copia Snapshot	SCORIE del qtree in un AFS	SCORIE del qtree in una copia Snapshot
Accesso al volume in un file system di accesso (AFS)	SÌ	NO	N/A.	N/A.
Accesso al volume in una copia Snapshot	SÌ	NO	N/A.	N/A.
Accesso al qtree in un AFS (quando LA SCORIA è presente nel qtree)	NO	NO	SÌ	NO
Accesso al qtree in un AFS (quando LA SCORIA non è presente in qtree)	SÌ	NO	NO	NO
Accesso al qtree nella copia Snapshot (quando LA SCORIA è presente nel qtree AFS)	NO	NO	SÌ	NO
Accesso al qtree nella copia Snapshot (quando LA SCORIA non è presente nel qtree AFS)	SÌ	NO	NO	NO

Visualizza informazioni su Storage-Level Access Guard

Storage-Level Access Guard è un terzo livello di sicurezza applicato a un volume o qtree. Le impostazioni di Storage-Level Access Guard non possono essere visualizzate utilizzando la finestra Proprietà di Windows. È necessario utilizzare l'interfaccia utente di ONTAP per visualizzare informazioni sulla protezione di Access Guard a livello di storage, che è possibile utilizzare per convalidare la configurazione o risolvere i problemi

di accesso ai file.

A proposito di questa attività

Specificare il nome della macchina virtuale di storage (SVM) e il percorso del volume o del qtree di cui si desidera visualizzare le informazioni di protezione Storage-Level Access Guard. È possibile visualizzare l'output in forma di riepilogo o come elenco dettagliato.

Fase

1. Visualizzare le impostazioni di sicurezza di Storage-Level Access Guard con il livello di dettaglio desiderato:

Se si desidera visualizzare le informazioni…	Immettere il seguente comando…
In forma riassuntiva	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
Con dettagli più dettagliati	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

Esempi

Nell'esempio riportato di seguito vengono visualizzate le informazioni di protezione di Storage-Level Access Guard per il volume di sicurezza NTFS con il percorso `/datavol1` In SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Nell'esempio seguente vengono visualizzate le informazioni di Storage-Level Access Guard relative al volume misto di sicurezza nel percorso `/datavol5` In SVM vs1. Il livello superiore di questo volume offre una protezione efficace per UNIX. Il volume dispone della protezione di Storage-Level Access Guard.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5
                Vserver: vs1
              File Path: /datavol5
      File Inode Number: 3374
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
                   ACLs: Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Rimuovere Storage-Level Access Guard

È possibile rimuovere Storage-Level Access Guard su un volume o qtree se non si desidera più impostare la sicurezza dell'accesso a livello di storage. La rimozione di Storage-Level Access Guard non modifica o rimuove la normale protezione di file e directory NTFS.

Fasi

1. Verificare che nel volume o nel qtree sia configurato Storage-Level Access Guard utilizzando `vserver security file-directory show` comando.

   ```
   vserver security file-directory show -vserver vs1 -path /datavol2
   ```

```
                Vserver: vs1
              File Path: /datavol2
      File Inode Number: 99
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xbf14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI

                         Storage-Level Access Guard security
                         DACL (Applies to Directories):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         DACL (Applies to Files):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

2. Rimuovere Storage-Level Access Guard utilizzando `vserver security file-directory remove-slag` comando.

   ```
   vserver security file-directory remove-slag -vserver vs1 -path /datavol2
   ```

3. Verificare che Storage-Level Access Guard sia stato rimosso dal volume o dal qtree utilizzando `vserver security file-directory show` comando.

   ```
   vserver security file-directory show -vserver vs1 -path /datavol2
   ```

```
                Vserver: vs1
              File Path: /datavol2
      File Inode Number: 99
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xbf14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI
```